A matematikai analízis alapjai

(A matematikai analízis logikai, halmazelméleti, algebrai és topológiai alapjai, Bevezetés a matematikai struktúrák elméletébe)

Kristóf János

Tartalomjegyzék

NÉV SZERINTI HIVATKOZÁSOK

LOG A matematikai analízis logikai alapjai (0. kötet, I. rész)
ENS A matematikai analízis halmazelméleti alapjai (0. kötet, II. rész)
ALG A matematikai analízis algebrai alapjai (0. kötet, III. rész)
TOP A matematikai analízis topológiai alapjai (0. kötet, IV. rész)
STR Bevezetés a matematikai struktúrák elméletébe (0. kötet, V. rész)
REA Valós és komplex számok/Elemi függvényanalízis (1. kötet, I./II. rész)
ESP Függvényterek és függvényalgebrák (1. kötet, III. rész)
MET Metrikus terek (1. kötet, IV. rész)
LIN Folytonos lineáris és multilineáris operátorok (2. kötet, I. rész)
DIF Differenciálelmélet (2. kötet, II. rész)
MES Additív halmazfüggvények és mértékek (2. kötet, III. rész)
INT Integrálelmélet (2. kötet, IV. rész)
GEO A geometriai integrálelmélet alapjai (2. kötet, V. rész)
HOL Holomorf függvények (3. kötet, I. rész)
FUN A funkcionálanalízis elemei (3. kötet, II. rész)
GEA Az analitikus geometria elemei (3. kötet, III. rész)
EVT Topologikus vektorterek (4. kötet, I. rész)
CON Kompakt konvex halmazok (4. kötet, II. rész)
ALN Normált algebrák (4. kötet, III. rész)
ORT Ortohálók (4. kötet, IV. rész)
AHA Absztrakt harmonikus analízis (5. kötet, I. rész)
RAD A topologikus integrálelmélet elemei (5. kötet, II. rész)
VAR Differenciálható sokaságok (6. kötet, I. rész)
VEC Vektormezők és kovariáns deriválások (6. kötet, II. rész)
TEN Tenzormezők (6. kötet, III. rész)
RIE Pszeudo-Riemann sokaságok (6. kötet, IV. rész)
INV Integrálás differenciálható sokaságokon (6. kötet, V. rész)
LIE Lie-csoportok és Lie-algebrák (7. kötet, I. rész)
REP Lie-csoportok ábrázolásai (7. kötet, II. rész)

I. rész

A matematikai analízis logikai alapjai

Előszó

Ennek a résznek az a célja, hogy az érdeklődő olvasót a lehető legrövidebb úton, de kellő alapossággal megismertesse a matematikai logikának azzal a bevezető fejezetével, amely szilárd logikai alapokat ad a halmazelmélet számára. Később nyilvánvalóvá válik, hogy a matematikai analízis felépíthető a halmazelméletre, ezért az analízis nem éppen triviális fogalmainak és állításainak bizonyossága a számára alapként szolgáló halmazelmélet gondolati szilárdságán múlik. Ezért fontos a halmazelméletet megalapozó matematikai logika ismerete.

A *matematikai logika*, mint a matematikában alkalmazott helyes gondolkodási szabályokat, valamint a matematikai objektumok gondolati előállításának módszereit vizsgáló elméleti tudomány, több ezer éves múltra tekint vissza. Ebből következik, hogy a matematikai logikában az idők folyamán rendkívüli mennyiségű gondolat halmozódott fel, ezért nem könnyű eligazodni ebben a hatalmas gondolat-tömegben. Ráadásul a matematikai logikának nagyon határozott filozófiai, pontosabban ismeretelméleti vonatkozásai vannak, ezért a kezdők számára komoly nehézséget jelenthet megkülönböztetni egymástól az ideológiai tartalmat hordozó (filozofikus) állításokat a matematikában hasznosítható (metamatematikai) állításoktól. Ez a fejezet azok számára lehet értékes, akik az életüket nem a matematikai logika vizsgálatának akarják szentelni, viszont igényük van arra, hogy a matematikát a lehető legmélyebben megértsék.

Azoknak, akik a tudományos színvonalú analízis tanulmányozását most kezdik, bizonyára tetszene az a kijelentés, hogy a tanulmány által tartalmazott anyag megértéséhez semmiféle előzetes matematikai ismeretre nincs szükség. Azonban az emberi felfogóképesség és gondolkodás sajátosságaiból következik, hogy ez nem így van. A kezdők számára azt javaslom, hogy először olvassák el az analízis elemeinek első fejezetét, amely az analízis *halmazelméleti* alapjaival foglalkozik, és az abban található, nem kellően indokoltnak tűnő állítások magyarázata céljából forduljanak ehhez a tanulmányhoz. Ebből a szempontból nincs szükség az ítéletkalkulussal foglalkozó 1. fejezet, valamint a predikátumkalkulus és a halmazelmélet ellentmondásmentességét vizsgáló 3. fejezet és **4.2.** pont anyagának ismeretére. De nélkülözhetetlen a **2.** fejezetben és a **4.1.** pontban foglaltak ismerete.

Ugyanolyan félrevezető volna elhallgatni a matematikai logika filozófiai problémáinak létezését, mint túlhangsúlyozni azokat. Azonban ezek részletes vizsgálata egészen más irányba vezetne, mint ami a tanulmány voltaképpeni célja. A bevezetésben és a befejezésben kizárólag azokat a filozófiai kérdéseket érintjük, amelyek megválaszolása nélkülözhetetlennek látszik a matematikai analízis logikai alapjainak megértéséhez.

Bevezetés

A matematikai logika tárgya

Minden *elmélet* két jól megkülönböztethető részből áll. Az egyik egy *nyelv*, amelyen megfogalmazhatók az elmélet *kijelentései* és az elmélet által vizsgált *gondolati objektumok*. Ez a nyelv általában egy kifejezésekben eléggé gazdag természetes nyelv. A másik egy *igazság-fogalom*, vagyis olyan szabály, amelynek segítségével az elmélet nyelvének kijelentései közül kiválaszthatók az *igaz* kijelentések. Minden elmélet alapfeladata a saját nem triviális gondolati objektumainak előállítása abból a célból, hogy azok tulajdonságaira és egymással való kapcsolataira vonatkozóan nem triviális, igaz kijelentéseket fogalmazzon meg.

A *matematikai elméletek* annyiban speciális elméletek, hogy az általuk vizsgált gondolati objektumok *matematikai természetűek*. A matematikai természetű gondolati objektumok rendkívüli sokfélesége miatt aligha lehet ezeket egységesen értelmezni. Valójában egyáltalán nem tudunk olyan szigorú definíciót adni, amely az összes eddig kidolgozott matematikai elméletben előforduló matematikai objektum általános meghatározását adná. Szerencsére a matematikában erre nincs is szükség. Létezik ugyanis egy elmélet, a matematikai logika, amely előállítja és vizsgálat alá veti azokat az elméleteket, amelyek gondolati objektumai "matematikai természetűeknek" tekinthetők.

A szűkebb értelemben vett *matematikai logika* annyiban különleges elmélet, hogy az általa vizsgált gondolati objektumok csakis a matematikai elméletek. Ebben az értelemben a matematikai logika alapvető feladata a saját gondolati ojektumainak, vagyis a matematikai elméletek fogalmának pontos meghatározása, valamint a matematikai elméletek tulajdonságainak és ezek kapcsolatainak vizsgálata. Ezzel foglalkozunk részletesen a **2.** fejezetben. Tágabb értelemben a matematikai logika a matematikában alkalmazott helyes gondolkodási szabályokat, valamint a matematikai objektumok gondolati konstrukcióinak módszereit vizsgáló elméleti tudomány. A matematika alapjainak kidolgozása céljából ez a tágabb felfogás feleslegesen általános, ezért a továbbiakban a matematikai logika szűkebb értelmezéséhez tartjuk magunkat.

Egyáltalán nem idegen az emberi szemlélettől az a felfogás, hogy a matematikai logika a matematikai *elméletek elmélete*. Amikor idegen nyelvet tanulunk, akkor általában az anyanyelvünk nyelvtanának alkalmazásával vizsgáljuk az adott idegen nyelv tanát. Ilyenkor azt mondjuk, hogy az adott idegen nyelv a *tárgy-* vagy *objektum-nyelv*, és az ezt vizsgáló nyelv a *metanyelv*. Sőt, az anyanyelvet is meg tudjuk tanulni önmagának egy korlátozott alakja ismeretében. Tehát még azt is természetesnek kell tekintenünk, hogy egy elmélet képes olyan elméletet létrehozni és vizsgálni, amelynek az eredeti elmélet része. Másként fogalmazva: egy természetes nyelv korlátozott formája metanyelve lehet a teljes nyelvnek.

Szemantikus pardoxonok

A természetes nyelveken kifejtett gondolati rendszerekben általában a kijelentésekhez automatikusan hozzárendelünk két magától értetődő tulajdonságot: az *értelmességet* és az *igazságértéket.* Az alábbiakban két példa segítségével illusztrálni fogjuk azt, hogy ha ezt a két tulajdonságot csak az intuitív szinten tekintjük, akkor logikai ellentmondásra jutunk.

Mint minden elmélet, egy matematikai elmélet előállítása is megköveteli valamilyen nyelv alkalmazását az általa vizsgált gondolati objektumok és az ezekre vonatkozó kijelentések konstrukciója céljából. A huszadik század elejéig minden matematikai elméletet valamilyen természetes nyelven fejtettek ki, betartva az adott természetes nyelv (korántsem mindig egyértelmű) szabályait. Korábban fel sem vetődött az, hogy a természetes nyelvek gazdagsága és rugalmassága logikai ellentmondásra vezethet még olyan egyszerű és konkrét elmélet esetében is, mint a természetes számok elmélete.

Logikai ellentmondáson (másnéven: *antinómián*, *paradoxonon*) azt a tényállást értjük, amikor egy elmélet valamely kijelentése a tagadásával együtt igaznak bizonyul az adott elméletben. Logikai ellentmondást nem tűrhetünk meg olyan gondolati rendszerben, amely rendelkezik azzal a tulajdonsággal, hogy ha csak egyetlen állítás is igaz benne a tagadásával együtt, akkor *minden* benne megfogalmazható állítás igaz is és hamis is. Világos, hogy egy ilyen gondolati rendszer teljesen értéktelen volna.

Szemantikus paradoxonnak nevezünk minden olyan logikai ellentmondást, amelynek az oka valamilyen fogalom *értelmezésével* kapcsolatos. Most bemutatjuk azt a két legegyszerűbben megfogalmazható és legkönnyebben megérthető szemantikus paradoxont, amelyek kiküszöbölésére tett szellemi erőfeszítések döntő befolyást gyakoroltak a matematika jelenlegi formájának kialakulására.

Egyszerűsítve *Jules Richard* egy korábbi gondolatmenetét, *G. G. Berry* és *Bertrand Russel* 1906-ban megfogalmazták a természetes számok elméletének egyik tanulságos paradoxonát, amelyet ma *Richard-paradoxonnak* nevezünk. Ennek lényege egy olyan természetes szám természetes nyelven történő értelmezése, amely logikai ellentmondásra vezet.

Nevezzük *karakternek* a latin ábécé (esetleg ékezetes) betűit, az írásjeleket és a szóközjelet. Világos, hogy véges sok karakter van. Képezzük az ezernél kevesebb karaktert tartalmazó szövegek összességét. Véges sok ilyen van, és ezek zöme magyar nyelven értelmetlen. Azonban a magyar nyelven értelmes, ezernél kevesebb karaktert tartalmazó szövegek között sok olyan is van, amely egyértelműen meghatároz egy természetes számot. Például leírhatjuk egy természetes szám nevét: "száztizenkilenc"; nem kérdéses, hogy melyik az a természetes szám, amelyet ez a szöveg értelmez. Bonyolultabb példaként írjuk le a következő szöveget: "A legkisebb összetett szám, amely harminccal osztva huszonkilencet ad maradékul."; világos, hogy ez a szöveg ugyanazt a természetes számot határozza meg, mint az előbbi. Jelölje H az ilyen módon értelmezhető természetes számok halmazát. Tehát az n természetes szám akkor és csak akkor eleme H-nak, ha létezik olyan ezernél kevesebb karaktert tartalmazó szöveg, amely magyar nyelven egyértelműen meghatározza n-et. Az előzőek szerint ez nem üres, véges halmaz, így létezik legnagyobb eleme. Tekintsük most a következő szöveget: "Az ezernél kevesebb karaktert tartalmazó szöveggel magyar nyelven értelmezhető legnagyobb természetes számnál eggyel nagyobb természetes szám.". Ez a szöveg ezernél kevesebb karaktert tartalmaz és magyar nyelven egyértelműen meghatároz egy természetes számot, amely tehát – H definíciója szerint – *eleme H-nak.* Ugyanakkor az is világos, hogy ez a természetes szám *nem eleme H-nak*, hiszen – a szám értelmezése szerint – a H halmaz legnagyobb eleménél is nagyobb. Ezt a logikai ellentmondást nevezzük *Richard-paradoxonnak.*

A Richard-paradoxont a H halmaz értelmezésében rejlő *bizonytalanság* okozza. Könnyen belátható, hogy teljesen szubjektív megítélés kérdése lehet az, hogy egy (ezernél kevesebb karaktert tartalmazó) szöveg (magyar nyelven) meghatároz-e egy természetes számot vagy sem? Ez a bizonytalanság mindaddig megmarad, amíg nem adjuk meg pontosan a természetes nyelveken kifejezhető kijelentések *értelmességének* fogalmát. Ha a természetes nyelveken megfogalmazható matematikai állításaink többféleképpen értelmezhetők, akkor rájuk - az értelmezéstől függően - bármit bizonyítani lehet. Ez intuitíve teljesen nyilvánvaló volt a huszadik század előtt tevékenykedő matematikusok számára is, ezért ösztönösen helyesen elkerülték a Richard-paradoxonhoz vezető "definíciók" alkalmazását. Tehát nem arról van szó, hogy az előző korokban kidolgozott matematika a huszadik század elejére elavulttá vált volna. Mindössze arról van szó, hogy a tudatalatti szintjéről a tudatosság szintjére emeljük ezt a *szemantikus problémát*, és olyan matematika létrehozására törekszünk, amelyben tudatosan kiküszöbölhető az értelmesség fogalmában rejlő bizonytalanság. A következő pontban részletesebben körvonalazzuk annak ideológiáját, hogy miként hajtható ez végre a *formalista* nézőpont alapján. Az **1.** és **2.** fejezetben tárgyszerűen bemutatjuk azoknak a matematikai nyelveknek a felépítését, amelyekben a Richard-paradoxonhoz vezető állítás és az ahhoz hasonlók meg sem fogalmazhatók.

A Richard-paradoxont nyelvi természetű értelmezési (szemantikus) probléma okozza. Azonban kiderül, hogy az intuitív (vagyis magától értetődőnek tekintett) *igazság-fogalommal* kapcsolatban is súlyos problémák vannak. Ennek illusztrációjaként bemutatunk egy régóta ismert, tisztán logikai természetű paradoxont.

A "hazug paradoxona" már az ókori görögök előtt ismert volt. Tekintsük a következő állítást: "Ez a kijelentés nem igaz."; az a kérdés, hogy igaz-e ez a kijelentés vagy sem? Ha igaz volna, akkor – a kijelentés tartalma alapján – nem igaz. Ez lehetetlen, így arra következtetünk, hogy ez a kijelentés *nem igaz*. Ez azt jelenti, hogy nem igaz az, hogy a szóban forgó kijelentés nem igaz, ezért az illető kijelentés igaz. Tehát az adott kijelentésről megmutattuk, hogy igaz *és* nem igaz, így logikai ellentmondásra jutottunk.

A "hazug paradoxonát" egy olyan kijelentés természetes nyelven történő megfogalmazhatósága okozta, amely a saját logikai értékéről, vagyis igazságáról állít valamit. Másként fogalmazva: a természetes nyelveken kifejtett logika (az ún. *naiv logika*) intuitív igazság-fogalma lehetővé teszi ilyen kijelentés előállítását. A logikai ellentmondás eltűnne akkor, ha a "nem igaz az, hogy nem igaz" kijelentés *nem* ugyanazt jelentené, hogy "igaz", vagyis a kettős negáció jól ismert klasszikus szabálya nem volna érvényes. A *Brower* által kezdeményezett *intuicionista logikában* valóban érvényes az, hogy ha $\mathbf{A}$ egy kijelentést jelöl, akkor $\mathbf{A}$-ból következik $\neg\neg\mathbf{A}$ (vagyis "nem nem $\mathbf{A}$"), de a $\neg\neg\mathbf{A}$ kijelentésből nem feltétlenül következik az $\mathbf{A}$ kijelentés. Azonban ilyen radikális logikai módosítás nélkül is megszűnne a paradoxon akkor, ha biztosan állíthatnánk, hogy az ellentmondáshoz vezető kijelentés *értelmetlen*, hiszen ebben az esetben nincs olyan (értelmes) állítás, amelynek a logikai értékét vizsgálni lehetne.

Láthatóan a "hazug paradoxonának" kiküszöbölése valamivel nehezebb a Richard-paradoxonénál, mert összekeveredik benne egy nyelvi probléma (ti. a logikai ellentmondáshoz vezető állítás értelmességének problémája), és egy logikai probléma (ti. az igazság-fogalom tulajdonságainak problémája). A paradoxon kiküszöbölésének *formalista* nézőpontja szerint pontos *definíciót kell adni* a kijelentések értelmességének fogalmára, továbbá a kijelentések igazságának fogalmát szintén pontosan *értelmezni kell* olymódon, hogy sem a Richard-paradoxonra vezető bizonytalan kijelentések, sem a saját logikai értékükről nyilatkozó kijelentések ne legyenek értelmesnek tekinthetők.

Ezen a ponton összefonódik a *formalista* és a *konvencionalista* logikai nézőpont. Ha elfogadjuk a formalista ideológiát, akkor a kijelentések igazságának fogalmát *értelmeznünk* *kell*, és a definíció után azok a kijelentések lesznek igazak, amelyek az önkényesen választott definíció szerint igaznak bizonyulnak. Így az igazság fogalma a képzeletünk szabad játékává válik; ugyanaz az állítás igaz lesz egy bizonyos igazság-fogalom szerint, míg hamis lehet, ha más igazság-fogalmat választunk; tehát a kijelentések igazság-tartalma végül is *megállapodáson* (*konvención*) múlik. Ha a matematika építményét formalista-konvencionalista alapra húzzuk fel, akkor nehezen magyarázható meg az, hogy miként alkalmazható a matematika bizonyos természeti jelenségkörök leírására? Hiszen a természeti jelenségkörökkel kapcsolatos állítások igazság-tartalma semmiképpen nem függhet egy olyan megállapodástól, amelyet az emberi gondolkodás önkényesen előír a saját maga számára. Ez nagyon lényeges ismeretelméleti kérdés, amelynek érdemi vizsgálata mindaddig lehetetlen, amíg nem látunk egyetlen olyan konkrét matematikai elméletet sem, amely ilyen formalista-konvencionalista alapon készült.

Formális matematikai nyelvek és a formalizáció

A Richard-paradoxon megmutatta, hogy a természetes nyelvek gazdagsága lehetővé teszi olyan *matematikai objektum* értelmezését, amely szemantikus paradoxonra vezet. A logikai ellentmondáshoz vezető objektum létezése egy olyan természetes nyelven megfogalmazható kijelentés létezésén múlik, amelyben szerepel a kijelentések értelmességének fogalma. Ezért a logikai ellentmondások elkerülése céljából a matematikai kijelentések *értelmességének* az intuitív szintnél pontosabb meghatározására van szükség.

Értelmesnek tekinthető-e az a definíció, amely a Richard-paradoxonra vezet? A természetes (magyar) nyelvi szabályok tekintetében kétségkívül értelmesnek tűnik, mégsem szabad megengednünk. Ezek szerint szükség volna valamilyen szabályra, amelynek alkalmazásával eldönthetnénk, hogy bizonyos (nyelvi szempontból) értelmes kijelentések alkalmazhatók matematikai objektumok értelmezéséhez, mások meg nem. A természetes nyelvek elemi analízise megmutatja az e célból követendő utat.

A természetes nyelvekben egy kijelentés értelmességének szükséges feltétele az, hogy meghatározott *szerkezetű* (*szintaxisú*) legyen. Például a magyar nyelvtan szerint a legegyszerűbb értelmes kijelentő (tő)mondatban léteznie kell egy *alanynak* (amelyről a mondat állítmánya állít valamit) és egy *állítmánynak* (amely az alanyra állít valamit). Bonyolultabb kijelentő mondatok az egyszerűbbekből logikai műveletekkel ("nem ...", "... vagy ...", "... és ...", "ha ..., akkor ...", "... akkor és csak akkor, ha ...") állíthatók elő. A meghatározott *szerkezet* vagy *forma* nem elégséges a természetes nyelvek mondatainak értelmességéhez, de feltétlenül szükséges. Tekintsük most a magyar nyelv minden tőmondatát egyetlen egységnek (*atomnak*), amelynek az értelmességétől eltekintünk. Ezután könnyen és pontosan megadható az a jól ismert szabály-rendszer, amelynek alkalmazásával az elemi logikai műveletek segítségével a tőmondatok összetett mondatokká fűzhetők össze. Az így előálló mondatok, legalábbis szerkezeti, vagyis *formai* szempontból *értelmesek* (vagy inkább *szabályosak*), legfeljebb rendkívül furcsa *tartalmat* hordoznak, amennyiben a bennük szereplő tőmondatokat felbontjuk alanyra és állítmányra, és értelmezzük azokat. De *meg is állapodhatunk* abban, hogy mely tőmondatok értelmesek; ezután ezek készletéből kiindulva az elemi logikai műveletek alkalmazásával *az adott konvenció szerint formailag értelmes* kijelentéseket nyerünk.

Az *ítéletkalkulus* formális nyelvének előállításakor a fenti sémát követjük; erről lesz szó az 1.1. pontban. Tehát először rögzítjük szimbólumoknak egy összességét, amelynek elemei az értelmes tőmondatoknak felelnek meg, és amelyeket *elemi ítéleteknek* nevezünk. Ezután megadunk egy olyan konstrukciós szabályt, amelynek alkalmazásával az elemi ítéletekből a logikai műveletek alkalmazásával bonyolult *ítéletek* képezhetők. Ez a szabály abban az értelemben *finit* (azaz *véges*), hogy a formális nyelv bármely kifejezéséről véges sok lépésben eldönthető, hogy a kifejezés ítélet-e az adott konstrukciós szabály szerint? Egy természetes nyelv (egy részének) *formalizálása* azt jelenti, hogy hozzárendelünk egy formális nyelvet úgy, hogy a természetes nyelv (adott részének) minden kijelentése azonosíthatóvá válik a formális nyelv valamely ítéletével. Egy adott kijelentés *formalizáltjának* nevezzük azt az ítéletet, amely azonosul az adott kijelentéssel.

Világos, hogy az ítéletkalkulus formális nyelve csak a természetes nyelvek lényegesen leegyszerűsített alakjának formalizálására alkalmas. Mégis érdemes foglalkozni vele, mert a legtisztábban és legérthetőbben ez mutatja a formális nyelvek sajátosságait.

Nyilvánvaló, hogy a tartalmas matematikai elméletek nyelvén nemcsak kijelentéseket tudunk megfogalmazni, hanem kifejezhetők vele azok az *objektumok* is, amelyekről a kijelentések állítanak valamit. Az ítéletkalkulus formális nyelvén csak az ítéletek, vagyis a formalizált kijelentések fejezhetők ki, ezért szükség van a formális nyelvek általánosítására. A 2.1. pontban megadjuk azoknak a *formális matematikai nyelveknek* egy lehetséges értelmezését, amelyek lényegében a teljes nem formális matematikai nyelv formalizálására alkalmasak.

Tehát a formális matematikai nyelvekben kétféle értelmes kifejezést tudunk értelmezni: az *objektumokat* és a kijelentéseket formalizáló *formulákat.* Egy formális nyelvi kifejezés *értelmessége* egyszerűen és objektívan ellenőrizhető szabállyal van megadva; nem szükséges hozzá semmiféle intuitív értelmesség-fogalom. Ezáltal a Richard-paradoxonhoz hasonló szemantikus paradoxonok a formális matematikai nyelvekre alapozott elméletekben nem jelenhetnek meg.

Egy természetes (vagy intuitív) matematikai nyelv *formalizálása* itt azt jelenti, hogy meghatározunk egy formális matematikai nyelvet úgy, hogy a természetes nyelv állításai formulákkal, míg a természetes nyelven kifejezett objektumok a formális matematikai nyelv objektumaival azonosulnak. A formalizálást *tökéletesnek* mondjuk akkor, ha a formális matematikai nyelv formulái (illetve objektumai) a természetes matematikai nyelv kijelentéseivel (illetve objektumaival) kölcsönösen egyértelmű kapcsolatba kerülnek a formalizálás során.

Egyetlen előzetes megjegyzést fűzünk a formális matematikai nyelveket tárgyaló 4. pont anyagához. Ez az objektumok és formulák fogalmának lényegi összefonódásával kapcsolatos.

A természetes nyelvek mondatainak elemi szemantikus elemzése rávilágít arra, hogy az állítások megfogalmazásához szükség van azokra az objektumokra, amelyekre az állítások állítmányai kifejeznek valamit; továbbá, az állítások alanyaiként szolgáló objektumokat állítások segítségével tudjuk értelmezni. A természetes matematikai nyelvekben ugyanez a helyzet. Például a halmazelméletben a *halmazokat* (tehát a halmazelmélet objektumait) általában úgy értelmezzük, mint adott tulajdonságú halmazok halmazát, és a "tulajdonságok" pontos meghatározásához állításokra van szükségünk. Ezzel a problémával részletesen foglalkozunk a 4.1. pontban, ahol megmutatjuk, hogy a halmazelmélet formális nyelvén miként lehet ilyen módon (az ún. $\{\cdot|\cdot\}$-) objektumokat képezni. Mindez azt jelenti, hogy a matematikai állítások és matematikai objektumok fogalmát *nem lehet egymástól függetlenül megadni.* Ezt a tényt tükröznie kell(ene) minden olyan formális matematikai nyelvnek, amelytől elvárjuk, hogy a természetes matematikai nyelvek formalizációiként szolgáljanak. A 2.1. pontban értelmezett formális matematikai nyelvek ilyenek; *ezért* olyan bonyolult bennük az objektumok és formulák értelmezése.

Megjegyezzük még, hogy másféle formális matematikai nyelvek is léteznek, sőt a matematikai logikai szakirodalom előnyben részesíti az ún. *elsőrendű nyelveket*, amelyek jelentősen különböznek a 2.1. pontban értelmezett formális matematikai nyelvektől. Ennek okáról csak 2.1. pont anyagának ismeretében lehet beszélni, ezért erre a kérdésre később térünk vissza.

A nem formális matematikai nyelveket *naiv* matematikai nyelveknek szokták nevezni. Itt a "naiv" jelzőnek kizárólag megkülönböztető jelentése van; semmiféle pejoratív tartalom nem fűződik hozzá. Ugyanígy, a "formális" jelző egy matematikai nyelvvel kapcsolatban nem a "tartalmatlan" jelző szinonimája, hanem csak az illető matematikai nyelv felépítésének sajátosságára utal.

Axiomatikus matematikai elméletek és az igazság fogalma

Ha a matematikát formális nyelvi alapokra helyezzük, akkor a kijelentések értelmességével kapcsolatos szemantikus paradoxonok eltűnnek, azonban a kijelentések intuitív igazság-fogalmához kötődők még megmaradnak. A "hazug paradoxona" megmutatta, hogy a természetes nyelvek gazdagsága lehetővé teszi olyan kijelentés megfogalmazását, amely a saját igazságáról állít valamit, ezáltal logikai ellentmondásra vezet. Ezért a logikai ellentmondás elkerülése céljából a *matematikai igazság-fogalom* intuitív szintnél pontosabb meghatározására van szükség.

Ennek felismerése világosan látható Euklidész "Elemek" című művében, amely az első dokumentuma az axiomatikus igazság-fogalom bevezetésének és szisztematikus alkalmazásának. Az axiomatikus igazság-fogalom lényege a következő: először kijelöljük az elmélet nyelvének bizonyos kijelentéseit, amelyeket *megállapodás szerint igaznak* tekintünk (ezeket a kijelentéseket nevezzük *axiómáknak* vagy *alapigazságoknak*), majd rögzítünk egy szabály-rendszert, amelynek alkalmazásával az axiómákból új kijelentések állíthatók elő (ezek a *levezetési szabályok*); ezután egy kijelentést *igaznak* (vagy *tételnek*) nevezünk, ha az adott axiómákból az adott levezetési szabályok alkalmazásával előállítható.

A formális matematikai nyelvekre alapozott matematikában is a fentieknek megfelelően értelmezzük az axiomatikus igazság-fogalmat; így nyerjük az *axiomatikus formális matematikai elméleteket*, amelyeket a 2.3. pontban részletezünk. Nyilvánvalóan vannak bizonyos természetes feltételek, amelyeket az axiómák összességének (az *axiómarendszernek*) és a levezetési szabályoknak ki kell elégíteniük. E feltételek közül a legfontosabbak az *egyértelműség* és a *finitség*. Az egyértelműség feltétele azt jelenti, hogy az axiómák és a levezetési szabályok definíciójának olyannak kell lennie, hogy minden állításról (vagyis formális nyelvben: *ítéletről* vagy *formuláról*) egyértelműen el lehessen dönteni azt, hogy axióma- vagy tétel-e? Hiszen ha már annak *értelmezése* is kétséges, hogy egy kijelentés axióma vagy tétel, akkor az egész logikai rendszer igazság-fogalma bizonytalan. Másfelől azt is elvárjuk, hogy minden állításról *véges sok* lépésben (vagyis *finit* módszerrel) eldönthető legyen az a kérdés, hogy igaz-e; ez a feltétel szigorú előírás a levezetési szabályokra vonatkozóan.

Az 1.2. pontban bemutatjuk a legegyszerűbb axiomatikus formális elméletet; az *axiomatikus ítéletkalkulust.* Ezzel kapcsolatban megjegyezzük, hogy az ítéletkalkulus esetében nincs feltétlenül szükség az axiomatikus igazság-fogalomra, mert létezik egy alternatív módszer, az ún. *értékelések módszere*, amely ugyanazokra a tételekre vezet, mint az axiomatikus igazság-fogalom; ez a *Kalmár-féle teljességi tétel* tartalma. Mégis érdemes foglalkozni az ítéletkalkulus axiomatikus elméletével is, mert ez mutatja a legtisztábban és legérthetőbben az axiomatikus formális elméletek sajátosságait, ugyanakkor könnyen igazolni tudjuk az ellentmondásmentességét is.

A legegyszerűbb axiomatikus formális matematikai elméletek a *predikátumkalkulusok*; ezek voltaképpen azok a "matematikai" elméletek, amelyek csak a formális nyelvük tekintetében matematikai jellegűek, ugyanakkor az axióma-rendszerük csak a *logikai igazságok* meghatározására alkalmas. Kiderül, hogy minden axiomatikus formális matematikai elmélet egy predikátumkalkulus *bővítésének* tekinthető, ezért nagyon fontos annak ismerete, hogy legalább a predikátumkalkulusok ellentmondásmentesek-e? Az értékelések módszerének alkalmazásával a **3.** fejezetben bebizonyítjuk a predikátumkalkulusok ellentmondásmentességét.

Az axiomatikus formális matematikai elméletekre három lényegesen nemtriviális példát mutatunk be; a *halmazelméletet*, az *aritmetikát* és a *síkgeometriát*. A két utóbbi kizárólag illusztrációként szolgál, de fontos tudni azt, hogy az aritmetikának elvi jelentőségű alkalmazásai vannak a matematikai logikában. Megjegyezzük, hogy itt az euklidészi síkgeometria egy erősen korlátozott formáját mutatjuk be; ennek nagymértékű általánosításai is megadhatók, ha az a célunk, hogy a *logikai geometriát* felépítsük. Természetesen itt egyáltalán nem ez a célunk, hanem az analízis logikai alapjait akarjuk tisztázni. Ebből a szempontból alapvető jelentőségű a halmazelmélet, ezért ennek logikai alapjait részletes vizsgálat alá vetjük a **4.** fejezetben. A halmazelmélet fontosságának (nem éppen magától értetődő) okáról bővebben szólunk még a befejezésben.

Figyeljük meg, hogy az axiomatikus igazság-fogalom elfogadása a matematikai gondolkodásunk konvencionalista nézőpontjának újabb megerősítését jelenti! Az első megállapodásra a kijelentések értelmességének maghatározására volt szükségünk; így jutottunk el a formális matematikai nyelvekhez. Most viszont látható, hogy az axiomatikus igazság-fogalom is (kétféle) megállapodáson múlik; egyfelől teljesen önkényesen adhatjuk meg az axiómákat, másfelől a levezetési szabályok (vagy *bizonyítások*) kijelölése is konvención alapul. Világos, hogy ez az igazság-fogalom gyökeresen különbözik a természettudományos elméletek (például az *elméleti fizika*) igazság-fogalmától.

A matematikai logika belső ellentmondásai

Mint minden elmélet, a szűkebb értelemben vett matematikai logika is megköveteli egy nyelv alkalmazását a saját vizsgálati objektumai (a matematikai elméletek) és az azokra vonatkozó értelmes kijelentések előállítása céljából. Továbbá, mint minden gondolati rendszernek, a matematikai logikának is van egy igazság-fogalma, amelynek alapján a saját kijelentéseit minősíteni tudja azok igazság-tartalma szerint. Most tisztázzuk, hogy itt milyen nyelvről és miféle igazság-fogalomról van szó.

Az eddigiek alapján világos, hogy a matematikai logika által vizsgált objektumok az axiomatikus formális matematikai elméletek. A matematikai logika nyelve minden esetben valamilyen *természetes nyelv*, és az igazság-fogalma az *empirikus igazság-fogalom*. Az empirikus igazság-fogalom a magától értetődő (intuitív) igazság-fogalomnak az a lényegesen korlátozott speciális esete, amelynek megkülönböztető ismérve (differenciális specifikuma) a közvetlen, gyakorlati ellenőrizhetőség. Például, amikor a matematikai logikában valaminek a *létezését* állítjuk, akkor ennek bizonyításához *véges sok lépésben elő kell állítani* azt az objektumot, amelynek a létezéséről beszélünk. Továbbá, kizárólag olyan egyszerű eljárásokat alkalmazhatunk a matematikai logika gondolati objektumainak konstrukciójában és az azokra vonatkozó kijelentések bizonyításában, amelyek mindenki számára könnyen megérthetők és elfogadhatók.

Ezen a helyen jelenik meg a matematikai logika *alapvető belső ellentmondása.* Az axiomatikus formális matematikai elméletek fogalmára éppen az az igény vezetett, hogy mentesítsük a matematikát azoktól a szemantikus paradoxonoktól, amelyek éppen a természetes matematikai nyelv és az intuitív igazság-fogalom alkalmazása miatt lépnek fel. Ugyanakkor az axiomatikus formális matematikai elméletek előállítására és vizsgálatára hivatott matematikai logika természetes nyelvet és (korlátozottan) intuitív igazság-fogalmat használ. Hogyan lehetünk akkor bizonyosak az axiomatikus formális matematikai elméletekre vonatkozó matematikai logikai eredmények értelmességében és helyességében? Ez a matematikai logika *alapvető belső ellentmondása.*

Bizonyára érezhető, hogy ez nagyon mély ismeretelméleti probléma, amelynek megválaszolása egy nem matematikai tudomány, a filozófia dolga. Utólagosan, az elméleti tapasztalatok ismeretében (*a posteriori*) állíthatjuk, hogy e valóban létező belső ellentmondás semmiféle gyakorlati nehézséget nem okoz; sem a matematikai logika fogalmainak és módszereinek, sem az axiomatikus formális matematikai elméletek lényegének megértésében. Ennek ugyanaz az oka, amiért minden szellemileg ép újszülött képes megtanulni a saját anyanyelvét, annak ellenére, hogy születésekor semmiféle nyelvet nem ismer. Ehhez először kialakít magának egy primitív intuitív képet az anyanyelvéről (ez felel meg a matematikai logikának), majd annak alapján egészen gazdag elméletet (vagyis nyelvtant) dolgozhat ki rá (ez felel meg az axiomatikus formális matematikai elméleteknek). A matematika logika alapvető belső ellentmondásának kevésbé szemléletes, részletes vizsgálatára ez a tanulmány nem vállalkozhat.

A matematikai logikával első ízben találkozók számára komolyabb elvi nehézséget okozhat egy másik belső ellentmondás. A matematikai logika egyik alapfeladata magának a (formális és axiomatikus) *matematikának* az előállítása. Ugyanakkor a matematikai logika a saját állításainak bizonyítására *alkalmaz* bizonyos *matematikai módszereket.* Részletesebben; a matematikai logika felhasznál *halmazelméleti* fogalmakat (halmazok, véges halmazok, halmaz eleme, elem n-esek, relációk, függvények), továbbá *aritmetikai* fogalmakat (természetes számok, szukcesszor, rendezés, teljes indukció, rekurzív definíció); holott éppen a matematikai logika feladata volna a halmazelmélet és az aritmetika konstrukciója. Nyilvánvaló, hogy itt is egy belső ellentmondásról van szó. Az ellentmondás feloldásához hasonló utat követhetünk, mint az imént. A részletesebb magyarázatért az ide vonatkozó filozófiai szakirodalomra utalunk ([17]).

Irodalomjegyzék

[1] D. Hilbert - P. Bernays, **Grundlagen der Mathematik.** I-II, Springer-Verlag, Berlin-Heidelberg-New York, 1968-1970.

[2] N. Bourbaki, **Éleménts de mathématique. Théorie des ensembles.** Hermann, Paris, 1966.

[3] E. Mendelson, **Introduction to Mathematical Logic**, D. van Nostrand Co., Inc., Princeton, New Yersey, Toronto-New York-London, 1971.

[4] H. Rasiowa - R. Sikorski, **The Mathematics of Metamathematics**, Panstwowe Wydawnictwo Naukowe, Warsawa, 1963.

[5] S. C. Kleene, **Mathematical Logic**, John Wiley & Sons, Inc., New York-London-Sidney, 1967.

[6] J. R. Shoenfield, **Mathematical Logic**, Addison-Wesley Pub. Co., 1967.

[7] K. Kuratowski-A. Mostowski, **Set Theory**, North-Holland Pub. Co., Amsterdam-Warsaw, 1967.

[8] J. Barwise (editor), **Handbook of Mathematical Logic**, North-Holland Pub. Co., Amsterdam-New York-Oxford, 1977.

[9] P. J. Cohen, **Set Theory and the Continuum Hypothesis**, W.A.Benjamin, Inc., New York-Amsterdam, 1966.

[10] A. Mostowski, **Constructible sets with Applications**, North-Holland Pub. Co., 1969.

[11] T. Jeh, **Lectures in set theory with particular emphasis on the method of forcing**, Lecture notes in Mathematic, 1971.

[12] H. P. Barendregt, **The Lambda Calculus** (**Its Syntax and Semantics**), North Holland Pub. Co., 1981.

[13] I. Bucur-A. Deleanu, **Introduction to the Theory of Categories and Functors**, J.Wiley & Sons, Inc., London-New York-Sidney, 1968.

[14] P. T. Johnstone, **Topos Theory**, Academic Press, London-New York-San Francisco, 1977.

[15] R. Goldblatt, **TOPOI, The categorial analysis of logic**, North-Holland Pub. Co., Amsterdam-New York-Oxford, 1979.

[16] П. С. Новиков, **Элементы математической логики**, Наука, Москва, 1973.

[17] Ruzsa I.-Urbán J., **A matematika néhány filozófiai problémájáról. Matematikai logika.** Tankönyvkiadó, Budapest, 1966.

1. fejezet

Axiomatikus ítéletkalkulus

1.1. Az ítéletkalkulus formális nyelve

Az *ítéletkalkulus formális nyelvének* értelmezése három lépésben történik. Először értelmezzük a nyelv *szimbólum-rendszerét*, majd a nyelv *kifejezéseit*, végül megadunk egy szabályt, amelynek alkalmazásával a nyelv kifejezései közül kiválaszthatóak az értelmes kifejezések: az *ítéletek*.

A továbbiakban az ítéletkalkulusnak csakis *formális* nyelvéről lesz szó, ezért általában a "formális" jelzőt elhagyjuk.

Az ítéletkalkulus nyelvének szimbólum-rendszere két részből áll: az *elemi ítéletek*, valamint a *logikai operátorok* összességéből.

1.1.1. Definíció. (**Az ítéletkalkulus nyelvének szimbólumai.**) *Az ítéletkalkulus nyelvének szimbólumai a következők:*

- **Elemi ítéletek***: a latin ábécé nagybetűi, azzal a megállapodással, hogy minden elemi ítélet vesszővel ellátva szintén elemi ítélet.*
- **Logikai operátorok***: a* $\neg$ (**negáció**) *és a* $\vee$ (**diszjunkció**) *szimbólum.*

Például az $E, Q, Q', P, P', P'', P'''$ szimbólumok elemi ítéletek. Az elemi ítéletek definíciójában azért írjuk elő, hogy minden vesszővel ellátott elemi ítélet szintén elemi ítélet legyen, hogy biztosítsuk korlátlan mennyiségű elemi ítélet létezését. Ha csak a latin ábécé nagybetűit tekintenénk elemi ítéleteknek, akkor elvileg előfordulhatna olyan bonyolult matematikai kijelentés, amely azért nem volna formalizálható, mert a rendelkezésre álló elemi ítéletek nem elegendőek a kijelentés formalizálására.

A *zárójelek* és a *szóköz-jel* nem tartoznak hozzá az ítéletkalkulus szimbólum-készletéhez, azonban bizonyos kifejezések *jelöléséhez* célszerű a zárójelek alkalmazása, továbbá bonyolult kifejezések *tagolására* felhasználhatjuk a szóköz-jelet.

1.1.2. Definíció. (**Az ítéletkalkulus nyelvének kifejezései.**) *Az ítéletkalkulus* **kifejezésének** *nevezünk minden olyan karakterláncot, amelynek karakterei az ítéletkalkulus nyelvének szimbólumai, tehát elemi ítéletek vagy logikai operátorok.*

Megállapodunk abban, hogy kifejezésen mindenütt *nem üres* karakterláncot értünk. Világos, hogy az ítéletkalkulus minden elemi ítélete és minden szimbóluma kifejezés.

Az ítéletkalkulus két kifejezését akkor mondjuk *azonosnak*, ha karakterről-karakterre megegyeznek; a nem azonos kifejezéseket *különbözőeknek* nevezzük. Két kifejezés azonosságának a tényét úgy fejezzük ki, hogy leírjuk a két kifejezést, és közéjük tesszük az $\equiv$ (*azonosság*) vagy az $\stackrel{\mathrm{gr}}{=}$ (*grafikus egyenlőség*) jelét.

Megállapodunk abban, hogy az ítéletkalkulus tetszőleges kifejezésének *jelölésére* vastagon írt, esetleg vesszőkkel ellátott latin nagybetűket használunk. Tehát $\mathbf{A}$ tetszőleges kifejezést jelöl, ami egyáltalán nem szükségképpen azonos a A betűvel, ami elemi ítélet az ítéletkalkulus nyelvében.

Nagy különbség van egy *kifejezés*, valamint a *kifejezés jelölése* között. Az ítéletkalkulus kifejezéseinek előállításához csak az ítéletkalkulus szimbólumait alkalmazhatjuk, ugyanakkor egy kifejezés jelölése céljából bármely olyan szimbólum használható, amelyből egyértelműen rekonstruálható az a kifejezés, amelynek a jelöléséről van szó. Például a zárójeleket gyakran használjuk a kifejezések jelölésekor, holott azok nem szimbólumai az ítéletkalkulusnak. Azonban a gördülékenyebb fogalmazás kedvéért néha elmosódik a különbség a kifejezés és annak jelölése között. A továbbiakban sokszor mondjuk azt, hogy "$\mathbf{A}$ az ítéletkalkulusnak kifejezése", holott valójában úgy kellene fogalmazni, hogy "$\mathbf{A}$ *jelöli* az ítéletkalkulusnak egy kifejezését".

Nem szorul külön magyarázatra az a kijelentés, hogy "$\mathbf{P}$ szimbólum *szerepel* az $\mathbf{A}$ kifejezésben". Nyilvánvaló, hogy a $\mathbf{P}$ szimbólum és az $\mathbf{A}$ kifejezés karaktereinek összehasonlításával dönthető el e kijelentés helyessége. Az is világos, hogy egy $\mathbf{P}$ szimbólum az $\mathbf{A}$ kifejezésben több *karakterpozícióban* is szerepelhet; minden ilyen szereplést a $\mathbf{P}$ szimbólum *előfordulásának* nevezünk az $\mathbf{A}$ kifejezésben.

Az ítéletkalkulus kifejezéseiből leggyakrabban úgy állítunk elő újabb kifejezéseket, hogy azokat egymás mellé illesztjük (*konkatenáció*); ha $\mathbf{A}$ és $\mathbf{B}$ kifejezések, akkor az ezek konkatenálásával nyert kifejezést $\mathbf{AB}$ jelöli. Ha $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ kifejezések, akkor nyilvánvalóan $\mathbf{A}(\mathbf{BC}) \equiv (\mathbf{AB})\mathbf{C}$; ezt a kifejezést $\mathbf{ABC}$-vel jelöljük.

1.1.3. Definíció. (**Az ítéletek fogalma.**) **Ítélet-konstrukciónak** *nevezzük az ítéletkalkulus kifejezéseinek bármely olyan* $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ *n-esét, amelyre minden* $1 \le k \le n$ *esetén a következő feltételek valamelyike teljesül:*

a) $\mathbf{A}_k$ *elemi ítélet;*

b) *létezik olyan* $1 \le j < k$ *szám, hogy* $\mathbf{A}_k \equiv \neg\mathbf{A}_j$*;*

c) *léteznek olyan* $1 \le i, j < k$ *számok, hogy* $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$*.*

Az ítéletkalkulus $\mathbf{A}$ *kifejezését* **ítéletnek** *nevezzük, ha létezik olyan* $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ *ítélet-konstrukció, hogy* $\mathbf{A} \equiv \mathbf{A}_n$*.*

A definícióból látható, hogy az ítéletek olyan kifejezések, amelyek elemi ítéletek vagy a $\neg$ és $\vee$ szimbólumok valamelyikével kezdődnek. Az is nyilvánvaló, hogy ha $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ ítélet-konstrukció, akkor minden $1 \le k \le n$ esetén $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k)$ szintén ítélet-konstrukció, ezért $\mathbf{A}_k$ ítélet, vagyis ítélet-konstrukció minden tagja ítélet.

Példa. Megmutatjuk, hogy a $\vee\neg Q \vee \neg PQ$ kifejezés ítélet. Ehhez tekintsük a

$$\Big(P,\ Q,\ \neg P,\ \vee\neg PQ,\ \neg Q,\ \vee\neg Q \vee \neg PQ\Big)$$

kifejezés-hatost. Könnyen ellenőrizhető, hogy ez ítélet-konstrukció, és az utolsó tagja azonos a vizsgált kifejezéssel, tehát $\vee\neg Q \vee \neg PQ$ ítélet.

A $\vee$ logikai operátorral kapcsolatban gyakran alkalmazzuk az *infix jelölési konvenciót*, ami azt jelenti, hogy ha $\mathbf{A}$ és $\mathbf{B}$ kifejezések az ítéletkalkulus nyelvében, akkor a $\vee\mathbf{AB}$

kifejezést a $\mathbf{A} \vee \mathbf{B}$ szimbólummal *jelöljük*. Természetesen az infix jelölés alkalmazásakor elkerülhetetlen a zárójelek helyes használata. Például a $\vee\neg Q\vee\neg PQ$ ítélet infix jelöléssel így néz ki: $(\neg Q)\vee((\neg P)\vee Q)$. Vegyük észre, hogy ha $\mathbf{A}$ és $\mathbf{B}$ kifejezések, akkor az $\mathbf{A}\vee\mathbf{B}$ szimbólum egyértelműen jelöli a $\vee\mathbf{AB}$ kifejezést, ugyanakkor a $\vee\mathbf{AB}$ kifejezés általában *nem egyértelműen* jelölhető az infix jelölési konvenció alkalmazásával. Ha például $\mathbf{A}'$ és $\mathbf{B}'$ olyan kifejezések, hogy $\vee\mathbf{AB} \equiv \vee\mathbf{A}'\mathbf{B}'$, akkor világos, hogy az $\mathbf{A} \vee \mathbf{B}$ és $\mathbf{A}' \vee \mathbf{B}'$ infix kifejezések különbözőek lehetnek, de ugyanazt a kifejezést jelölik.

1.1.4. Definíció. *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *kifejezések az ítéletkalkulus nyelvében, akkor*

- $\mathbf{A} \Rightarrow \mathbf{B}$ *jelöli a* $\vee\neg\mathbf{AB}$ *kifejezést, vagyis* $\mathbf{A} \Rightarrow \mathbf{B} \equiv (\neg\mathbf{A}) \vee \mathbf{B}$*;*
- $\mathbf{A} \wedge \mathbf{B}$ *jelöli a* $\neg\vee\neg\mathbf{A}\neg\mathbf{B}$ *kifejezést, vagyis* $\mathbf{A} \wedge \mathbf{B} \equiv \neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$*;*
- $\mathbf{A}\Leftrightarrow\mathbf{B}$ *jelöli a* $\neg\vee\neg\vee\neg\mathbf{AB}\neg\vee\neg\mathbf{BA}$ *kifejezést, azaz* $\mathbf{A}\Leftrightarrow\mathbf{B} \equiv (\mathbf{A} \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow \mathbf{A})$*;*

A $\Rightarrow$ *(illetve* $\wedge$*, illetve* $\Leftrightarrow$*) szimbólumot* **implikációnak** *(illetve* **konjunkciónak***, illetve* **ekvivalenciának***) nevezzük. Az* $\wedge$ *szimbólum helyett az* & *szimbólum is használatos.*

1.1.5. Állítás. *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *ítéletek az ítéletkalkulus nyelvében, akkor a* $\neg\mathbf{A}$*,* $\mathbf{A} \vee \mathbf{B}$*,* $\mathbf{A} \Rightarrow \mathbf{B}$*,* $\mathbf{A} \wedge \mathbf{B}$ *és* $\mathbf{A}\Leftrightarrow\mathbf{B}$ *kifejezések szintén ítéletek.*

Bizonyítás. Legyenek $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ és $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m)$ olyan ítélet-konstrukciók, hogy $\mathbf{A} \equiv \mathbf{A}_n$ és $\mathbf{B} \equiv \mathbf{B}_m$. Nyilvánvaló, hogy

$$\Big(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \neg\mathbf{A}_n\Big),$$
$$\Big(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m, \vee\mathbf{A}_n\mathbf{B}_m\Big)$$

ítélet-konstrukciók, továbbá $\neg\mathbf{A} \equiv \neg\mathbf{A}_n$ és $\mathbf{A} \vee \mathbf{B} \equiv \mathbf{A}_n \vee \mathbf{B}_m$; ezért $\neg\mathbf{A}$ és $\mathbf{A} \vee \mathbf{B}$ ítéletek. Az implikáció, konjunkció és ekvivalencia értelmezése alapján ebből adódik, hogy a $\mathbf{A} \Rightarrow \mathbf{B}$, $\mathbf{A} \wedge \mathbf{B}$ és $\mathbf{A}\Leftrightarrow\mathbf{B}$ kifejezések szintén ítéletek. ■

A továbbiakban gyakran beszélünk az ítéletkalkulus kifejezéseinek *hosszáról*; ezen a kifejezésben szereplő karakterek számát értjük. Megállapodunk abban, hogy minden elemi ítélet hossza 1, függetlenül attól, hogy hány vessző szerepel benne.

1.1.6. Lemma. *Ha* $\mathbf{A}$ *ítélet és* $\mathbf{B}$ *kifejezés, akkor* **AB nem ítélet***.*

Bizonyítás. Az $\mathbf{A}$ ítélet hossza szerinti teljes indukcióval igazoljuk, hogy minden $\mathbf{B}$ kifejezésre $\mathbf{AB}$ nem ítélet. Tegyük fel, hogy $\mathbf{A}$ hossza 1, és legyen $\mathbf{B}$ tetszőleges kifejezés. Ekkor $\mathbf{A}$ elemi ítélet, és az $\mathbf{AB}$ kifejezés első karaktere nem logikai operátor, ezért $\mathbf{AB}$ csak úgy lehetne ítélet, ha elemi ítélet volna. Ez viszont lehetetlen, mert $\mathbf{AB}$ hossza 1-nél nagyobb, ugyanakkor elemi ítélet hossza 1. Ezért $\mathbf{AB}$ nem ítélet.

Legyen $\mathbf{A}$ hossza $n > 1$, és tegyük fel, hogy minden n-nél rövidebb $\mathbf{A}'$ ítéletre és minden $\mathbf{B}$ kifejezésre $\mathbf{A}'\mathbf{B}$ nem ítélet. A feltevés szerint $\mathbf{A}$ nem elemi ítélet, ezért két eset lehetséges:

1) Az $\mathbf{A}$ első karaktere a $\neg$ logikai operátor; ekkor van olyan $\mathbf{A}'$ ítélet, hogy $\mathbf{A} \equiv \neg\mathbf{A}'$. Tegyük fel, hogy $\mathbf{B}$ olyan kifejezés, amelyre $\mathbf{AB}$ ítélet. Ekkor $\neg\mathbf{A}'\mathbf{B}$ ítélet, tehát létezik olyan $\mathbf{C}$ ítélet, hogy $\neg\mathbf{A}'\mathbf{B} \equiv \neg\mathbf{C}$. Ebből az első $\neg$ karakter törlésével $\mathbf{A}'\mathbf{B} \equiv \mathbf{C}$ adódik, tehát $\mathbf{A}'\mathbf{B}$ ítélet, ami az indukciós hipotézis alapján lehetetlen, mert $\mathbf{A}'$ hossza kisebb n-nél. Ebből következik, hogy $\mathbf{AB}$ nem ítélet.

2) Az $\mathbf{A}$ első karaktere a $\vee$ logikai operátor; ekkor léteznek olyan $\mathbf{C}$ és $\mathbf{D}$ ítéletek, hogy

$\mathbf{A} \equiv \vee\mathbf{CD}$. Tegyük fel , hogy $\mathbf{B}$ olyan kifejezés, amelyre $\mathbf{AB}$ ítélet. Ekkor $\vee\mathbf{CDB}$ is ítélet, tehát léteznek olyan $\mathbf{C}'$ és $\mathbf{D}'$ ítéletek, amelyekre $\vee\mathbf{CDB} \equiv \vee\mathbf{C}'\mathbf{D}'$. Ebből az első $\vee$ karakter törlésével $\mathbf{CDB} \equiv \mathbf{C}'\mathbf{D}'$ adódik. Ha $\mathbf{C}$ hossza kisebb a $\mathbf{C}'$ hosszánál, akkor létezik olyan $\mathbf{B}'$ kifejezés, hogy $\mathbf{CB}' \equiv \mathbf{C}'$, így $\mathbf{CB}'$ ítélet, ami az indukciós hipotézis alapján lehetetlen, mert a $\mathbf{C}$ ítélet hossza kisebb, mint az $\mathbf{A}$ hossza. Ha $\mathbf{C}$ hossza nagyobb a $\mathbf{C}'$ hosszánál, akkor létezik olyan $\mathbf{B}''$ kifejezés, hogy $\mathbf{C} \equiv \mathbf{C}'\mathbf{B}''$, így $\mathbf{C}'\mathbf{B}''$ ítélet, ami az indukciós hipotézis alapján lehetetlen, mert a $\mathbf{C}'$ ítélet hossza kisebb, mint az $\mathbf{A}$ hossza. Ezért $\mathbf{C}$ és $\mathbf{C}'$ hossza egyenlő, tehát $\mathbf{CDB} \equiv \mathbf{C}'\mathbf{D}'$ miatt $\mathbf{DB} \equiv \mathbf{D}'$. Ez viszont azt jelenti, hogy $\mathbf{DB}$ ítélet, ami szintén ellentmond az indukciós hipotézisnek, mivel a $\mathbf{D}$ ítélet hossza kisebb az $\mathbf{A}$ hosszánál. Ebből adódik, hogy $\mathbf{AB}$ nem ítélet. ■

1.1.7. Állítás. (**Az antecedensek egyértelműsége.**) *Ha* $\mathbf{A}$ *olyan ítélet az ítéletkalkulus nyelvében, amelynek első karaktere a* $\neg$ *logikai operátor, akkor egyértelműen létezik olyan* $\mathbf{B}$ *ítélet, amelyre* $\mathbf{A} \equiv \neg\mathbf{B}$. *Ha* $\mathbf{A}$ *olyan ítélet az ítéletkalkulus nyelvében, amelynek első karaktere a* $\vee$ *logikai operátor, akkor egyértelműen léteznek olyan* $\mathbf{B}$ *és* $\mathbf{C}$ *ítéletek, amelyekre* $\mathbf{A} \equiv \vee\mathbf{BC}$.

Bizonyítás. (I) Ha $\mathbf{B}$ és $\mathbf{B}'$ olyan ítéletek, hogy $\mathbf{A} \equiv \neg\mathbf{B}$ és $\mathbf{A} \equiv \neg\mathbf{B}'$, akkor $\neg\mathbf{B} \equiv \neg\mathbf{B}'$, amiből az első $\neg$ szimbólum törlésével kapjuk, hogy $\mathbf{B} \equiv \mathbf{B}'$.

(II) Ha $\mathbf{B}$, $\mathbf{C}$, $\mathbf{B}'$ és $\mathbf{C}'$ olyan ítéletek, hogy $\mathbf{A} \equiv \vee\mathbf{BC}$ és $\mathbf{A} \equiv \vee\mathbf{B}'\mathbf{C}'$, akkor $\vee\mathbf{BC} \equiv \vee\mathbf{B}'\mathbf{C}'$. Ebből az első $\vee$ karakter törlésével kapjuk, hogy $\mathbf{BC} \equiv \mathbf{B}'\mathbf{C}'$. Ha $\mathbf{B}$ hossza kisebb volna $\mathbf{B}'$ hosszánál, akkor létezne olyan $\mathbf{D}$ kifejezés, hogy $\mathbf{BD} \equiv \mathbf{B}'$, tehát $\mathbf{BD}$ ítélet volna, ami az előző lemma szerint lehetetlen. Hasonlóan, ha $\mathbf{B}'$ hossza kisebb volna $\mathbf{B}$ hosszánál, akkor létezne olyan $\mathbf{D}'$ kifejezés, hogy $\mathbf{B}'\mathbf{D}' \equiv \mathbf{B}$, tehát $\mathbf{B}'\mathbf{D}'$ ítélet volna, ami az előző lemma szerint lehetetlen. Tehát $\mathbf{B}$ és $\mathbf{B}'$ hossza egyenlő, így $\mathbf{BC} \equiv \mathbf{B}'\mathbf{C}'$ miatt $\mathbf{B} \equiv \mathbf{B}'$ és $\mathbf{C} \equiv \mathbf{C}'$. ■

1.1.8. Definíció. *Ha* $\mathbf{A}$ *olyan ítélet az ítéletkalkulus nyelvében, amelynek első karaktere a* $\neg$ *logikai operátor, akkor az* $\mathbf{A}$ **antecedensének** *nevezzük azt a* $\mathbf{B}$ *ítéletet, amelyre* $\mathbf{A} \equiv \neg\mathbf{B}$ *teljesül. Ha* $\mathbf{A}$ *olyan ítélet az ítéletkalkulus nyelvében, amelynek első karaktere a* $\vee$ *logikai operátor, akkor az* $\mathbf{A}$ **antecedenseinek** *nevezzük azokat a* $\mathbf{B}$ *és* $\mathbf{C}$ *ítéleteket, amelyekre* $\mathbf{A} \equiv \vee\mathbf{BC}$ *teljesül.*

Vegyük észre, hogy az ítéletek antecedensének fogalmát az antecedensek egyértelműségi tétele nélkül nem lehetne bevezetni!

1.2. Az ítéletkalkulus axiómarendszere

Az előző pontban megadtuk az ítéletkalkulus kijelentéseket formalizáló kifejezéseinek, az ítéleteknek a fogalmát. Természetesen az ítéletkalkulusnak sok olyan kifejezése is létezik, amely nem ítélet; ezek a kifejezések *értelmetleneknek* tekinthetők. Azonban szó sincs arról, hogy az *értelmes kifejezések* (vagyis ítéletek) automatikusan *igazak* volnának. Természetesen az ítéletek igazságának érdemi vizsgálatához definíciót kell adni az igazság fogalmára.

Az ítéletkalkulusban az igazság-fogalom többféleképpen bevezethető; itt az *axiomatikus igazság-fogalomról* lesz szó. Ennek pontos meghatározásához először rögzítjük az ítéletkalkulus ítéleteinek egy összességét (*az axiómarendszert*), majd megadjuk azt a szabályt, amelynek alkalmazásával az *axiómákból* (vagyis az axiómarendszer elemeiből) előállíthatók a *tételek* (vagyis az "igaz" ítéletek).

1.2.1. Definíció. (**A Hilbert–Ackermann-féle axiómarendszer.**) *Azt mondjuk, hogy az ítéletkalkulus* **D** *ítélete* **axióma**, *ha léteznek olyan* **A**, **B** *vagy* **C** *ítéletek, hogy* **D** *azonos a következő ítéletek valamelyikével:*

$$(\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}$$
$$\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})$$
$$(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})$$
$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{B})).$$

Az ítéletkalkulus axiómáinak összességét **Hilbert–Ackermann-féle axiómarendszernek** *nevezzük.*

Figyeljük meg, hogy az ítéletkalkulus axiómáiban a $\neg$ logikai operátor nem közvetlenül, hanem csak a $\Rightarrow$ szimbólumon keresztül szerepel!

1.2.2. Definíció. (**A tételek fogalma az ítéletkalkulusban.**) *Legyen* **A** *ítélet és* Γ *az ítéletkalkulus ítéleteinek tetszőleges (esetleg üres) összessége. Azt mondjuk, hogy* **A** **levezethető** (*vagy* **bizonyítható**) Γ*-ból, ha létezik ítéleteknek olyan* $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ n*-ese, amelyre* $\mathbf{A} \equiv \mathbf{A}_n$ *és minden* $1 \le k \le n$ *számra a következő feltételek valamelyike teljesül:*

- $\mathbf{A}_k$ *axióma vagy eleme* Γ*-nak;*
- *léteznek olyan* $1 \le i, j < k$ *számok, hogy* $\mathbf{A}_j \equiv (\mathbf{A}_i \Rightarrow \mathbf{A}_k)$.

Minden ilyen tulajdonságú ítélet n*-est az* **A** *ítélet* Γ*-ból való* **bizonyításának** (*vagy* **levezetésének**) *nevezünk. Az ítéletkalkulus* **A** *ítéletét* **tételnek** (*vagy* **igaznak**) *nevezzük, ha* **A** *levezethető az üres ítélet-összességből. Az ítéletkalkulus* **A** *ítéletét* **cáfolhatónak** *nevezzük, ha a* $\neg\mathbf{A}$ *ítélet tétel.*

A tételek definíciójából nyilvánvalóan látható, hogy ha Γ ítéletek összessége, akkor az ítéletkalkulus minden axiómája, és az ítéletkalkulus minden tétele, valamint Γ minden eleme levezethető Γ-ból.

1.3. Az ítéletkalkulus bizonyítási módszerei

Most bemutatjuk az ítéletkalkulus néhány alapvetően fontos bizonyítási módszerét.

1.3.1. Tétel. (**A leválasztás szabálya: modus ponens.**) *Ha* **A** *és* **B** *ítéletek,* Γ *ítéletek összessége, továbbá az* **A** *és* $\mathbf{A} \Rightarrow \mathbf{B}$ *ítéletek levezethetők* Γ*-ból, akkor* **B** *is levezethető* Γ*-ból.*

Bizonyítás. Ha $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ az **A** ítélet és $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m)$ a $\mathbf{A} \Rightarrow \mathbf{B}$ ítélet levezetése Γ-ból, akkor nyilvánvaló, hogy

$$(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m, \mathbf{B})$$

a **B** ítélet levezetése Γ-ból, mert $\mathbf{B}_m \equiv (\mathbf{A}_n \Rightarrow \mathbf{B})$. ■

1.3.2. Tétel. (**Láncszabály: syllogismus.**) *Ha* **A**, **B** *és* **C** *ítéletek,* Γ *ítéletek összessége, továbbá* $\mathbf{A} \Rightarrow \mathbf{B}$ *és* $\mathbf{B} \Rightarrow \mathbf{C}$ *levezethetők* Γ*-ból, akkor* $\mathbf{A} \Rightarrow \mathbf{C}$ *is levezethető* Γ*-ból.*

Bizonyítás. Legyen $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ az $\mathbf{A} \Rightarrow \mathbf{B}$ és $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m)$ a $\mathbf{B} \Rightarrow \mathbf{C}$ ítélet levezetése Γ-ból. Ekkor

$$\Big(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m, (\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}))$$
$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}), \mathbf{A} \Rightarrow \mathbf{C}\Big)$$

az $\mathbf{A} \Rightarrow \mathbf{C}$ ítélet levezetése Γ-ból, ugyanis az implikáció értelmezése szerint

$$(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}))$$

azonos a $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\neg\mathbf{A} \vee \mathbf{B}) \Rightarrow (\neg\mathbf{A} \vee \mathbf{C}))$ ítélettel, ami axióma, és a feltételek alapján $\mathbf{B}_m \equiv (\mathbf{B} \Rightarrow \mathbf{C})$ és $\mathbf{A}_n \equiv (\mathbf{A} \Rightarrow \mathbf{B})$. ■

1.3.3. Állítás. (**A kizárt harmadik elve: tertium non datur.**) *Ha* $\mathbf{A}$ *ítélet, akkor* $(\neg\mathbf{A}) \vee \mathbf{A}$*, vagyis* $\mathbf{A} \Rightarrow \mathbf{A}$ *tétel.*

Bizonyítás. Az $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{A})$ és $(\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}$ ítéletek axiómák, tehát tételek, így a láncszabály alkalmazásával kapjuk, hogy $\mathbf{A} \Rightarrow \mathbf{A}$ tétel. ■

A láncszabály bizonyításából kiolvasható az, hogy miként lehet az $\mathbf{A} \Rightarrow \mathbf{C}$ ítélet levezetését előállítani akkor, ha ismerjük az $\mathbf{A} \Rightarrow \mathbf{B}$ és $\mathbf{B} \Rightarrow \mathbf{C}$ ítéletek levezetését. Például, ha $\mathbf{A}$ ítélet, akkor az

$$\Big(\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{A}), (\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}, ((\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}) \Rightarrow ((\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{A})),$$
$$(\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{A}), \mathbf{A} \Rightarrow \mathbf{A}\Big)$$

ítélet-ötös az $\mathbf{A} \Rightarrow \mathbf{A}$ ítélet levezetése.

1.3.4. Tétel. (**Az esetszétválasztás szabálya: alternatio.**) *Ha* $\mathbf{A}$*,* $\mathbf{B}$ *és* $\mathbf{C}$ *ítéletek,* Γ *ítéletek összessége, és az* $\mathbf{A} \vee \mathbf{B}$*,* $\mathbf{A} \Rightarrow \mathbf{C}$*,* $\mathbf{B} \Rightarrow \mathbf{C}$ *ítéletek levezethetők* Γ*-ból, akkor* $\mathbf{C}$ *levezethető* Γ*-ból.*

Bizonyítás. A $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee \mathbf{C}))$ ítélet axióma, és a feltevés szerint $\mathbf{B} \Rightarrow \mathbf{C}$ levezethető Γ-ból, ezért a leválasztás szabálya alapján $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee \mathbf{C})$ is levezethető Γ-ból. Az $(\mathbf{A} \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \mathbf{A})$ ítélet axióma, tehát a láncszabály szerint $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{C} \vee \mathbf{A})$ is levezethető Γ-ból. Ugyanakkor $\mathbf{A} \vee \mathbf{B}$ levezethető Γ-ból, tehát ismét a leválasztás szabálya alapján kapjuk, hogy $\mathbf{C} \vee \mathbf{A}$ levezethető Γ-ból. Az $(\mathbf{A} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{C}))$ ítélet axióma, és a feltevés szerint $\mathbf{A} \Rightarrow \mathbf{C}$ levezethető Γ-ból, ezért a leválasztás szabálya alapján $(\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{C})$ levezethető Γ-ból. A leválasztás szabálya alapján adódik, hogy $\mathbf{C} \vee \mathbf{C}$ levezethető Γ-ból. Végül, $(\mathbf{C} \vee \mathbf{C}) \Rightarrow \mathbf{C}$ axióma, tehát a leválasztás szabálya szerint $\mathbf{C}$ levezethető Γ-ból. ■

1.3.5. Állítás. (**Visszavezetés a lehetetlenre: reductio ad absurdum.**) *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *ítéletek,* Γ *ítéletek összessége, továbbá* $\mathbf{B} \Rightarrow \mathbf{A}$ *és* $(\neg\mathbf{B}) \Rightarrow \mathbf{A}$ *levezethetők* Γ*-ból, akkor* $\mathbf{A}$ *levezethető* Γ*-ból.*

Bizonyítás. A kizárt harmadik elve alapján a $(\neg\mathbf{B}) \vee \mathbf{B}$ ítélet tétel, ezért az esetszétválasztás szabálya szerint $\mathbf{A}$ levezethető Γ-ból. ■

1.3.6. Állítás. (**Igaz bármiből következik: verum sequitur ex quodlibet.**) *Ha* Γ *ítéletek összessége és az* $\mathbf{A}$ *ítélet levezethető* Γ*-ból, akkor minden* $\mathbf{B}$ *ítéletre* $\mathbf{B} \Rightarrow \mathbf{A}$ *levezethető* Γ*-ból.*

Bizonyítás. Az $\mathbf{A} \Rightarrow (\mathbf{A} \vee (\neg \mathbf{B}))$ ítélet axióma és $(\mathbf{A} \vee (\neg \mathbf{B})) \Rightarrow ((\neg \mathbf{B}) \vee \mathbf{A})$ is axióma. A láncszabály szerint $\mathbf{A} \Rightarrow ((\neg \mathbf{B}) \vee \mathbf{A})$, vagyis $\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})$ tétel, így levezethető Γ-ból. Ha $\mathbf{A}$ levezethető Γ-ból, akkor a leválasztás szabályát alkalmazva ebből következik, hogy $\mathbf{B} \Rightarrow \mathbf{A}$ levezethető Γ-ból. ■

1.3.7. Állítás. (**Hamisból bármi következik: ex falso sequitur quodlibet.**) *Ha Γ ítéletek összessége és a $\neg \mathbf{A}$ ítélet levezethető Γ-ból, akkor minden $\mathbf{B}$ ítéletre $\mathbf{A} \Rightarrow \mathbf{B}$ levezethető Γ-ból.*

Bizonyítás. A $\neg \mathbf{A} \Rightarrow ((\neg \mathbf{A}) \vee \mathbf{B})$ ítélet axióma, és a feltevés szerint $\neg \mathbf{A}$ levezethető Γ-ból, így a leválasztás szabálya szerint $(\neg \mathbf{A}) \vee \mathbf{B}$ is levezethető Γ-ból. Az implikáció definíciója szerint ez azt jelenti, hogy $\mathbf{A} \Rightarrow \mathbf{B}$ levezethető Γ-ból. ■

1.3.8. Állítás. (**A kettős tagadás szabálya.**) *Ha $\mathbf{A}$ ítélet, akkor az*

$$\mathbf{A} \Rightarrow (\neg\neg \mathbf{A}),$$
$$(\neg\neg \mathbf{A}) \Rightarrow \mathbf{A}$$

ítéletek az ítéletkalkulus tételei.

Bizonyítás. A kizárt harmadik elve alapján $(\neg\neg \mathbf{A}) \vee (\neg \mathbf{A})$ tétel. A

$$((\neg\neg \mathbf{A}) \vee (\neg \mathbf{A})) \Rightarrow ((\neg \mathbf{A}) \vee (\neg\neg \mathbf{A}))$$

ítélet axióma, tehát tétel, így a leválasztás szabálya szerint $(\neg \mathbf{A}) \vee (\neg\neg \mathbf{A})$ tétel. Az implikáció értelmezése alapján $((\neg \mathbf{A}) \vee (\neg\neg \mathbf{A})) \equiv (\mathbf{A} \Rightarrow (\neg\neg \mathbf{A}))$, tehát $\mathbf{A} \Rightarrow (\neg\neg \mathbf{A})$ tétel.

Ebből következik, hogy $(\neg \mathbf{A}) \Rightarrow (\neg\neg\neg \mathbf{A})$ tétel. Ugyanakkor

$$((\neg \mathbf{A}) \Rightarrow (\neg\neg\neg \mathbf{A})) \Rightarrow ((\mathbf{A} \vee (\neg \mathbf{A})) \Rightarrow (\mathbf{A} \vee (\neg\neg\neg \mathbf{A})))$$

axióma, ezért a leválasztás szabálya szerint $(\mathbf{A} \vee (\neg \mathbf{A})) \Rightarrow (\mathbf{A} \vee (\neg\neg\neg \mathbf{A}))$ tétel. A $((\neg \mathbf{A}) \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee (\neg \mathbf{A}))$ és a $(\mathbf{A} \vee (\neg\neg\neg \mathbf{A})) \Rightarrow ((\neg\neg\neg \mathbf{A}) \vee \mathbf{A})$ ítéletek axiómák, tehát kétszer alkalmazva a láncszabályt kapjuk, hogy $((\neg \mathbf{A}) \vee \mathbf{A}) \Rightarrow ((\neg\neg\neg \mathbf{A}) \vee \mathbf{A})$ tétel. A kizárt harmadik elve alapján $(\neg \mathbf{A}) \vee \mathbf{A}$ tétel, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\neg\neg\neg \mathbf{A}) \vee \mathbf{A}$ tétel. Ez az ítélet azonos a $(\neg\neg \mathbf{A}) \Rightarrow \mathbf{A}$ ítélettel. ■

1.3.9. Állítás. (**A kettős negáció elve.**) *Ha Γ ítéletek összessége, akkor az $\mathbf{A}$ ítélet pontosan akkor vezethető le Γ-ból, ha a $\neg\neg \mathbf{A}$ ítélet levezethető Γ-ból.*

Bizonyítás. A kettős negáció szabálya szerint $\mathbf{A} \Rightarrow (\neg\neg \mathbf{A})$ tétel az ítéletkalkulusban, így levezethető Γ-ból, tehát ha $\mathbf{A}$ levezethető Γ-ból, akkor a leválasztás szabálya szerint $\neg\neg \mathbf{A}$ is levezethető Γ-ból.

A kettős negáció szabálya szerint $(\neg\neg \mathbf{A}) \Rightarrow \mathbf{A}$ tétel az ítéletkalkulusban, így levezethető Γ-ból, tehát ha $\neg\neg \mathbf{A}$ levezethető Γ-ból, akkor a leválasztás szabálya szerint $\mathbf{A}$ is levezethető Γ-ból. ■

1.3.10. Állítás. (**A kontrapozíció szabálya: modus tollens.**) *Ha $\mathbf{A}$ és $\mathbf{B}$ ítéletek, akkor az*

$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg \mathbf{B}) \Rightarrow (\neg \mathbf{A})),$$
$$((\neg \mathbf{B}) \Rightarrow (\neg \mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$$

ítéletek tételek az ítéletkalkulusban.

Bizonyítás. A $(\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})) \Rightarrow (((\neg\mathbf{A}) \vee \mathbf{B}) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})))$ ítélet axióma és a kettős negáció szabálya szerint $\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})$ tétel, így a leválasztás szabályát, valamint az implikáció értelmezését alkalmazva kapjuk, hogy $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B}))$ tétel. Mivel a

$$((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})) \Rightarrow ((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A}))$$

ítélet axióma, így a láncszabály szerint $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A}))$ tétel. Az implikáció értelmezése alapján $((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A})) \equiv ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$, amiből azonnal kapjuk, hogy $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ tétel.

A kettős negáció szabálya szerint $(\neg\neg\mathbf{B}) \Rightarrow \mathbf{B}$ tétel, és $((\neg\neg\mathbf{B}) \Rightarrow \mathbf{B}) \Rightarrow (((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B})))$ axióma, tehát a leválasztás szabálya szerint $((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B})$ tétel. Továbbá, $((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B}))$ axióma, tehát a láncszabály szerint $((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B})$ tétel. Az implikáció értelmezése alapján ez azt jelenti, hogy $((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$ tétel. ■

1.3.11. Állítás. (**A kontrapozíció elve.**) *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *ítéletek, és* Γ *ítéletek összessége. Az* $\mathbf{A} \Rightarrow \mathbf{B}$ *ítélet pontosan akkor vezethető le* Γ*-ból, ha a* $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ *ítélet levezethető* Γ*-ból.*

Bizonyítás. A kontrapozíció szabálya szerint $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ tétel, így levezethető Γ-ból, tehát ha $\mathbf{A} \Rightarrow \mathbf{B}$ levezethető Γ-ból, akkor a leválasztás szabálya szerint $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ is levezethető Γ-ból.

A kontrapozíció szabálya szerint $((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$ tétel, így levezethető Γ-ból, tehát ha $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ levezethető Γ-ból, akkor a leválasztás szabálya szerint $\mathbf{A} \Rightarrow \mathbf{B}$ is levezethető Γ-ból. ■

1.3.12. Állítás. *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *ítéletek,* Γ *ítéletek összessége, továbbá* $\mathbf{A} \Rightarrow \mathbf{B}$ *levezethető* Γ*-ból, akkor* $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})$ *is levezethető* Γ*-ból.*

Bizonyítás. A hipotézis szerint az $\mathbf{A} \Rightarrow \mathbf{B}$ ítélet levezethető Γ-ból, ezért a kontrapozíció elve alapján $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ levezethető Γ-ból. A $((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow ((\mathbf{C} \vee (\neg\mathbf{B})) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{A})))$ ítélet axióma, tehát a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{C} \vee (\neg\mathbf{B})) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{A}))$ levezethető Γ-ból. Azonban $((\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{B}))$ axióma, így a láncszabály szerint $((\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{A}))$ levezethető Γ-ból. A $(\mathbf{C} \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{C})$ ítélet szintén axióma, tehát ismét a láncszabályt alkalmazva kapjuk, hogy $((\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{C})$ levezethető Γ-ból. Az implikáció értelmezése alapján ez azonos a $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})$ ítélettel. ■

Jelölés. Ha Γ ítéletek összessége és $\mathbf{A}$ ítélet, akkor $\Gamma[\mathbf{A}]$ jelöli azon ítéletek összességét, amelyek Γ-nak elemei, vagy azonosak $\mathbf{A}$-val.

1.3.13. Tétel. (**Dedukció-tétel.**) *Legyenek* $\mathbf{A}$, $\mathbf{B}$ *ítéletek és* Γ *ítéletek összessége. A* $\mathbf{B}$ *ítélet pontosan akkor vezethető le* $\Gamma[\mathbf{A}]$*-ból, ha az* $\mathbf{A} \Rightarrow \mathbf{B}$ *ítélet levezethető* Γ*-ból.*

Bizonyítás. (I) Legyen $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_n)$ a $\mathbf{B}$ ítélet levezetése $\Gamma[\mathbf{A}]$-ból. Megmutatjuk, hogy minden $1 \leq k \leq n$ számra $\mathbf{A} \Rightarrow \mathbf{B}_k$ levezethető Γ-ból, amiből adódik, hogy $\mathbf{A} \Rightarrow \mathbf{B}$ is levezethető Γ-ból, mivel $\mathbf{B} \equiv \mathbf{B}_n$.

A $\mathbf{B}_1$ ítélet axióma vagy eleme $\Gamma[\mathbf{A}]$-nak. Az első esetben $\mathbf{B}_1$ tétel, így $\mathbf{A} \Rightarrow \mathbf{B}_1$ is tétel (igaz bármiből következik), tehát $\mathbf{A} \Rightarrow \mathbf{B}_1$ levezethető Γ-ból. A második esetben $\mathbf{B}_1$ eleme Γ-nak vagy $\mathbf{B}_1 \equiv \mathbf{A}$. Ha $\mathbf{B}_1$ eleme Γ-nak, akkor $\mathbf{B}_1$ levezethető Γ-ból, tehát $\mathbf{A} \Rightarrow \mathbf{B}_1$ is levezethető Γ-ból (igaz bármiből következik). Ha $\mathbf{B}_1 \equiv \mathbf{A}$, akkor

$(\mathbf{A} \Rightarrow \mathbf{B}_1) \equiv (\mathbf{A} \Rightarrow \mathbf{A})$, és $\mathbf{A} \Rightarrow \mathbf{A}$ tétel (a kizárt harmadik elve), így $\mathbf{A} \Rightarrow \mathbf{B}_1$ levezethető Γ-ból.

Tegyük fel, hogy $1 \leq k \leq n$ olyan szám, hogy minden $1 \leq j < k$ számra $\mathbf{A} \Rightarrow \mathbf{B}_j$ levezethető Γ-ból; megmutatjuk, hogy ekkor $\mathbf{A} \Rightarrow \mathbf{B}_k$ is levezethető Γ-ból. Ha $\mathbf{B}_k$ axióma vagy eleme $\Gamma[\mathbf{A}]$-nak, akkor az előző érvelést megismételve $\mathbf{B}_1$ helyett $\mathbf{B}_k$-ra kapjuk, hogy $\mathbf{A} \Rightarrow \mathbf{B}_k$ levezethető Γ-ból. Ha $\mathbf{B}_k$ nem axióma és nem eleme $\Gamma[\mathbf{A}]$-nak, akkor legyenek $1 \leq i, j < k$ olyan számok, hogy $\mathbf{B}_j \equiv \mathbf{B}_i \Rightarrow \mathbf{B}_k$. A hipotézis szerint $\mathbf{A} \Rightarrow \mathbf{B}_i$ levezethető Γ-ból, így az előző állítás szerint $(\mathbf{B}_i \Rightarrow \mathbf{B}_k) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ is levezethető Γ-ból. Ugyancsak a hipotézis alapján $\mathbf{A} \Rightarrow (\mathbf{B}_i \Rightarrow \mathbf{B}_k)$ levezethető Γ-ból, így a láncszabály alkalmazásával kapjuk, hogy $\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ levezethető Γ-ból. A $(\neg\mathbf{A}) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B}_k)$ ítélet axióma, és ez azonos a $(\neg\mathbf{A}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ ítélettel, így $(\neg\mathbf{A}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ levezethető Γ-ból. Tehát az $\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ és $(\neg\mathbf{A}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ ítéletek levezethetőek Γ-ból, így a reductio ad absurdum elve alapján $\mathbf{A} \Rightarrow \mathbf{B}_k$ is levezethető Γ-ból.

Ebből következik, hogy az $\mathbf{A} \Rightarrow \mathbf{B}_n$ ítélet is levezethető Γ-ból, így $\mathbf{B}_n \equiv \mathbf{B}$ miatt $\mathbf{A} \Rightarrow \mathbf{B}$ levezethető Γ-ból.

(II) Ha $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ az $\mathbf{A} \Rightarrow \mathbf{B}$ ítélet levezetése Γ-ból, akkor nyilvánvaló, hogy $(\mathbf{A}_1, \cdots, \mathbf{A}_n, \mathbf{A}, \mathbf{B})$ a $\mathbf{B}$ ítélet levezetése $\Gamma[\mathbf{A}]$-ból. ■

1.3.14. Tétel. (Az indirekt bizonyítás elve.) *Legyen* $\mathbf{A}$ *ítélet és* Γ *ítéletek összessége. Ha létezik olyan* $\mathbf{B}$ *ítélet, hogy* $\mathbf{B}$ *és* $\neg\mathbf{B}$ *levezethetőek* $\Gamma[\neg\mathbf{A}]$*-ból, akkor* $\mathbf{A}$ *levezethető* Γ*-ból.*

Bizonyítás. Legyen $\mathbf{B}$ olyan ítélet, hogy $\mathbf{B}$ és $\neg\mathbf{B}$ levezethető $\Gamma[\neg\mathbf{A}]$-ból. A dedukciótételből következik, hogy ekkor $(\neg\mathbf{A}) \Rightarrow \mathbf{B}$ és $(\neg\mathbf{A}) \Rightarrow (\neg\mathbf{B})$ levezethetők Γ-ból. A kontrapozíció elvét kétszer alkalmazva ebből kapjuk, hogy $(\neg\mathbf{B}) \Rightarrow (\neg\neg\mathbf{A})$ és $(\neg\neg\mathbf{B}) \Rightarrow (\neg\neg\mathbf{A})$ levezethetők Γ-ból. Tehát a reductio ad absurdum alapján $\neg\neg\mathbf{A}$ levezethető Γ-ból. A kettős negáció elvét alkalmazva, ebből adódik, hogy $\mathbf{A}$ levezethető Γ-ból. ■

Az eddig bemutatott bizonyítási módszerek nagymértékben megkönnyítik annak eldöntését, hogy egy ítélet tétel-e vagy sem. A következő pontban látható lesz, hogy erre létezik egy teljesen elemi alternatív módszer is: az ítéletkalkulus *értékeléseinek* alkalmazása. Azonban ez a tény egyáltalán nem jelenti azt, hogy a fenti bizonyítási módszerek részletezése felesleges volt. A 2.4. pontban majd kiderül, hogy az ítéletkalkulusnál jóval bonyolultabb *matematikai elméletek* esetében szintén megfogalmazhatók és igazolhatók ugyanezek a bizonyítási eljárások, azonban a matematikai elméletek esetében az értékelések módszerével nyerhető bizonyítás-fogalom *nem egyenértékű* az eredetileg bevezetett bizonyítás fogalmával.

1.4. Az ítéletkalkulus ellentmondásmentessége

1.4.1. Definíció. *Azt mondjuk, hogy az ítéletkalkulus* **ellentmondásos***, ha létezik olyan* $\mathbf{A}$ *ítélet, hogy* $\mathbf{A}$ *és* $\neg\mathbf{A}$ *tételek. Az ítéletkalkulust* **ellentmondásmentesnek** *nevezzük, ha nem ellentmondásos.*

1.4.2. Állítás. *Ha az ítéletkalkulus ellentmondásos, akkor minden ítélet tétel.*

Bizonyítás. Legyen $\mathbf{B}$ olyan ítélet, hogy $\mathbf{B}$ és $\neg\mathbf{B}$ tételek. Legyen $\mathbf{A}$ tetszőleges ítélet. A $(\neg\mathbf{B}) \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})$ ítélet azonos a $(\neg\mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \vee \mathbf{A})$ ítélettel, ami axióma, tehát tétel. Kétszer alkalmazva a leválasztás szabályát kapjuk, hogy $\mathbf{A}$ tétel. ■

1.4.3. Definíció. (**Az ítéletkalkulus értékelései.**) *Az ítéletkalkulus* **értékelésének** *nevezünk minden olyan függvényt, amely az elemi ítéletek összességén értelmezett, és minden elemi ítélethez az* **i** *és* **h** *betűk közül pontosan az egyiket rendeli.*

Az ítéletkalkulusnak *létezik* értékelése, hiszen az a függvény, amely minden elemi ítélethez az **i** (vagy **h**) értéket rendeli nyilvánvalóan értékelés.

1.4.4. Definíció. (**Az értékelések kiterjesztése.**) *Ha* $\mathfrak{v}$ *az ítéletkalkulusnak értékelése, akkor minden* **A** *ítéletre az* **A***-ban szereplő logikai operátorok száma szerinti indukcióval értelmezzük a* $\overline{\mathfrak{v}}(\mathbf{A})$ *értéket a következőképpen:*

– *ha* **A***-ban nem szerepel logikai operátor, akkor* **A** *elemi ítélet; ekkor legyen* $\overline{\mathfrak{v}}(\mathbf{A})$ *az* **A***-hoz* $\mathfrak{v}$ *által rendelt érték;*

– *ha* **A** *első karaktere a* $\neg$ *logikai operátor, akkor egyértelműen létezik olyan* **B** *ítélet, hogy* $\mathbf{A} \equiv \neg\mathbf{B}$*; ekkor* **B***-ben kevesebb logikai operátor van, mint* **A***-ban, így* $\overline{\mathfrak{v}}(\mathbf{B})$ *már értelmezve van; ekkor legyen* $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{i}$*, ha* $\overline{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{h}$*, és* $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{h}$*, ha* $\overline{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{i}$*;*

– *ha* **A** *első karaktere a* $\vee$ *logikai operátor, akkor egyértelműen léteznek olyan* **B** *és* **C** *ítéletek, hogy* $\mathbf{A} \equiv \vee\mathbf{BC}$*; ekkor* **B***-ben és* **C***-ben kevesebb logikai operátor van, mint* **A***-ban, így* $\overline{\mathfrak{v}}(\mathbf{B})$ *és* $\overline{\mathfrak{v}}(\mathbf{C})$ *már értelmezve van; ekkor legyen* $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{h}$*, ha* $\overline{\mathfrak{v}}(\mathbf{B}) \equiv \overline{\mathfrak{v}}(\mathbf{C}) \equiv \mathbf{h}$*, egyébként legyen* $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{i}$.

Az így bevezetett $\overline{\mathfrak{v}}$ *függvényt, amely az ítéletek összességén értelmezett és minden ítélethez az* **i** *és* **h** *betűk közül pontosan az egyiket rendeli, a* $\mathfrak{v}$ *értékelés* **kiterjesztésének** *nevezzük.*

Figyeljük meg, hogy az ítéletek antecedenseinek egyértelműségi tétele *nélkül* nem lehetne bevezetni a $\overline{\mathfrak{v}}$ függvényt!

A következő *logikai táblázatok* megmutatják, hogy ha $\mathfrak{v}$ az ítéletkalkulusnak értékelése, akkor a $\overline{\mathfrak{v}}$ függvény értéke hogyan számítható ki a $\neg\mathbf{A}$, $\mathbf{A} \vee \mathbf{B}$, $\mathbf{A} \Rightarrow \mathbf{B}$, $\mathbf{A} \wedge \mathbf{B}$ és $\mathbf{A} \Leftrightarrow \mathbf{B}$ alakú ítéletek esetében, ha a $\overline{\mathfrak{v}}(\mathbf{A})$ és $\overline{\mathfrak{v}}(\mathbf{B})$ értékek ismertek. A két első táblázat a $\overline{\mathfrak{v}}$ függvény definícióját mutatja, a többi pedig ezek alapján egyszerű elemzéssel nyerhető. Természetesen hasonló logikai táblázatokkal tetszőlegesen bonyolult szerkezetű ítélet esetén is kiértékelhető a $\overline{\mathfrak{v}}$ függvény.

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\neg\mathbf{A})$
i	**h**
h	**i**

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{A} \vee \mathbf{B})$
i	**i**	**i**
i	**h**	**i**
h	**i**	**i**
h	**h**	**h**

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{B})$	$\overline{\mathfrak{v}}(\neg\mathbf{A}))$	$\overline{\mathfrak{v}}(\mathbf{A} \Rightarrow \mathbf{B})$
i	**i**	**h**	**i**
i	**h**	**h**	**h**
h	**i**	**i**	**i**
h	**h**	**i**	**i**

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{B})$	$\overline{\mathfrak{v}}(\neg\mathbf{A}))$	$\overline{\mathfrak{v}}(\neg\mathbf{B}))$	$\overline{\mathfrak{v}}((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$	$\overline{\mathfrak{v}}(\mathbf{A} \wedge \mathbf{B})$
i	**i**	**h**	**h**	**h**	**i**
i	**h**	**h**	**i**	**i**	**h**
h	**i**	**i**	**h**	**i**	**h**
h	**h**	**i**	**i**	**i**	**h**

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{A} \Rightarrow \mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{B} \Rightarrow \mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{A} \Leftrightarrow \mathbf{B})$
i	**i**	**i**	**i**	**i**
i	**h**	**h**	**i**	**h**
h	**i**	**i**	**h**	**h**
h	**h**	**i**	**i**	**i**

1.4.5. Definíció. *Az* $\mathbf{A}$ *ítéletet tautológiának nevezzük, ha az ítéletkalkulus minden* $\mathfrak{v}$ *értékelésére* $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{i}$.

Adott $\mathbf{A}$ ítélet esetén könnyű eldönteni azt, hogy $\mathbf{A}$ tautológia-e vagy sem. Ehhez elegendő tetszőleges $\mathfrak{v}$ értékelésre az $\mathbf{A}$-hoz tartozó logikai táblázatot elkészíteni, és ellenőrizni, hogy benne a $\overline{\mathfrak{v}}(\mathbf{A})$ alatt mindenütt az $\mathbf{i}$ érték áll-e? A következő tétel bizonyításában példákat látunk majd erre.

1.4.6. Tétel. *Az ítéletkalkulus minden tétele tautológia.*

Bizonyítás. (I) Először megmutatjuk, hogy az ítéletkalkulus minden axiómája tautológia. Ehhez elegendő rátekinteni a következő logikai táblázatokra, amelyekben $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ tetszőleges ítéleteket jelölnek, és $\mathfrak{v}$ az ítéletkalkulus tetszőleges értékelése.

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{A} \vee \mathbf{A})$	$\overline{\mathfrak{v}}((\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A})$
i	**i**	**i**
h	**h**	**i**

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{A} \vee \mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B}))$
i	**i**	**i**	**i**
i	**h**	**i**	**i**
h	**i**	**i**	**i**
h	**h**	**h**	**i**

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{A} \vee \mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{B} \vee \mathbf{A})$	$\overline{\mathfrak{v}}((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})$
i	**i**	**i**	**i**	**i**
i	**h**	**i**	**i**	**i**
h	**i**	**i**	**i**	**i**
h	**h**	**h**	**h**	**i**

$\overline{\mathfrak{v}}(\mathbf{A})$	$\overline{\mathfrak{v}}(\mathbf{B})$	$\overline{\mathfrak{v}}(\mathbf{C})$	$\overline{\mathfrak{v}}(\mathbf{A}{\Rightarrow}\mathbf{B})$	$\overline{\mathfrak{v}}((\mathbf{C}{\vee}\mathbf{A}){\Rightarrow}(\mathbf{C}{\vee}\mathbf{B}))$	$\overline{\mathfrak{v}}((\mathbf{A}{\Rightarrow}\mathbf{B}){\Rightarrow}((\mathbf{C}{\vee}\mathbf{A}){\Rightarrow}(\mathbf{C}{\vee}\mathbf{B})))$
i	**i**	**i**	**i**	**i**	**i**
i	**i**	**h**	**i**	**i**	**i**
i	**h**	**i**	**h**	**i**	**i**
i	**h**	**h**	**h**	**h**	**i**
h	**i**	**i**	**i**	**i**	**i**
h	**i**	**h**	**i**	**i**	**i**
h	**h**	**i**	**i**	**i**	**i**
h	**h**	**h**	**i**	**i**	**i**

(II) Ha $\mathbf{A}$ és $\mathbf{B}$ ítéletek, továbbá $\mathfrak{v}$ olyan értékelés, hogy $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{i}$ és $\overline{\mathfrak{v}}(\mathbf{A} \Rightarrow \mathbf{B}) \equiv \mathbf{i}$, akkor $\overline{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{i}$, hiszen ha $\overline{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{h}$ volna, akkor $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{i}$ miatt $\overline{\mathfrak{v}}(\mathbf{A} \Rightarrow \mathbf{B}) \equiv \mathbf{h}$ teljesülne; ehhez elég az értékelések kiterjesztésének és az implikáció definíciójára hivatkozni.

(III) Legyen $\mathbf{A}$ tétel és $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ az $\mathbf{A}$ bizonyítása. Megmutatjuk, hogy minden $1{\le}k{\le}n$ számra $\mathbf{A}_k$ tautológia, amiből kapjuk, hogy $\mathbf{A}_n$, azaz $\mathbf{A}$ is tautológia.

Az $\mathbf{A}_1$ ítélet axióma, ezért az (I) szerint tautológia. Legyen $1{\le}k{\le}n$ olyan szám, hogy minden $1{\le}j{<}k$ számra $\mathbf{A}_j$ tautológia; megmutatjuk, hogy ekkor $\mathbf{A}_k$ is tautológia.

Ha az $\mathbf{A}_k$ ítélet axióma, akkor az előző érvelést megismételve $\mathbf{A}_1$ helyett $\mathbf{A}_k$-ra kapjuk, hogy $\mathbf{A}_k$ tautológia. Ha az $\mathbf{A}_k$ ítélet nem axióma, akkor léteznek olyan $1{\le}i, j{<}k$ számok, amelyekre $\mathbf{A}_j \equiv (\mathbf{A}_i \Rightarrow \mathbf{A}_k)$. A hipotézis szerint $\mathbf{A}_i$ és $\mathbf{A}_j$ tautológiák, tehát ha $\mathfrak{v}$ értékelés, akkor $\overline{\mathfrak{v}}(\mathbf{A}_i) \equiv \mathbf{i}$ és $\overline{\mathfrak{v}}(\mathbf{A}_i \Rightarrow \mathbf{A}_k) \equiv \overline{\mathfrak{v}}(\mathbf{A}_j) \equiv \mathbf{i}$, így a (II) szerint $\overline{\mathfrak{v}}(\mathbf{A}_k) \equiv \mathbf{i}$. Ez azt jelent, hogy $\mathbf{A}_k$ tautológia. ■

1.4.7. Következmény. *Az ítéletkalkulus ellentmondásmentes.*

Bizonyítás. Van olyan $\mathbf{A}$ ítélet, amely tautológia, például bármelyik axióma ilyen. Ekkor az ítéletkalkulus bármely $\mathfrak{v}$ értékelésére $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{i}$, ezért $\overline{\mathfrak{v}}(\neg\mathbf{A}) \equiv \mathbf{h}$, tehát $\neg\mathbf{A}$ nem tautológia, így nem is tétel, tehát az ítéletkalkulus ellentmondásmentes. ■

Az előző állítás bizonyításában hallgatólagosan felhasználtuk azt a nyilvánvaló tényt, hogy az ítéletkalkulusnak *létezik* értékelése.

Az ítéletkalkulus témakörének utolsó tételeként megmutatjuk, hogy egy ítélet pontosan akkor tétel, ha tautológia. Ez nagyon értékes állítás, mert korábban láttuk, hogy egy ítéletről logikai táblázat segítségével nem nehéz eldönteni azt, hogy tautológia-e vagy sem; ugyanakkor egy ítélet bizonyíthatóságát levezetés előállításával megmutatni sokszor nem triviális feladat.

Jelölés. Ha $\mathfrak{v}$ az ítéletkalkulus értékelése, akkor minden $\mathbf{A}$ ítéletre az $\mathbf{A}^{\mathfrak{v}}$ ítéletet a következőképpen értelmezzük:

– ha $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{i}$, akkor $\mathbf{A}^{\mathfrak{v}} \equiv \mathbf{A}$;

– ha $\overline{\mathfrak{v}}(\mathbf{A}) \equiv \mathbf{h}$, akkor $\mathbf{A}^{\mathfrak{v}} \equiv \neg\mathbf{A}$.

Továbbá, ha Γ ítéletek összessége és $\mathfrak{v}$ az ítéletkalkulus értékelése, akkor $\Gamma^{\mathfrak{v}}$ jelöli az $\mathbf{A}^{\mathfrak{v}}$ alakú ítéletek összességét, ahol $\mathbf{A}$ eleme Γ-nak.

1.4.8. Állítás. *Legyen* $\mathbf{A}$ *ítélet és* Γ *ítéleteknek olyan összessége, amelynek minden* $\mathbf{A}$*-ban szereplő elemi ítélet eleme. Ha* $\mathfrak{v}$ *az ítéletkalkulus értékelése, akkor az* $\mathbf{A}^{\mathfrak{v}}$ *ítélet levezethető* $\Gamma^{\mathfrak{v}}$*-ből.*

Bizonyítás. Az $\mathbf{A}$ ítéletben szereplő logikai operátorok száma szerinti teljes indukcióval bizonyítunk.

Ha $\mathbf{A}$-ban nem szerepel logikai operátor, akkor $\mathbf{A}$ elemi ítélet, tehát $\mathbf{A}$ eleme Γ-nak. Ekkor $\mathbf{A}^{\mathfrak{v}}$ eleme $\Gamma^{\mathfrak{v}}$-nek, ezért triviális, hogy $\mathbf{A}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből.

Tegyük fel, hogy $\mathbf{A}$-ban szerepel logikai operátor, és az állítás igaz minden olyan ítéletre, amelyben kevesebb logikai operátor van, mint $\mathbf{A}$-ban. Ekkor két eset lehetséges.

(I) Létezik olyan $\mathbf{B}$ ítélet, hogy $\mathbf{A} \equiv \neg\mathbf{B}$. Ekkor $\mathbf{B}$-ben kevesebb logikai operátor van, mint $\mathbf{A}$-ban, és minden $\mathbf{B}$-ben szereplő elemi ítélet $\mathbf{A}$-ban is szerepel, tehát eleme Γ-nak. Ezért az indukciós hipotézisből következik, hogy $\mathbf{B}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből. A $\mathfrak{v}$ értékelésre $\bar{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{i}$ vagy $\bar{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{h}$ teljesül.

1) Ha $\bar{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{i}$, akkor $\bar{\mathfrak{v}}(\mathbf{A}) \equiv \bar{\mathfrak{v}}(\neg\mathbf{B}) \equiv \mathbf{h}$, tehát $\mathbf{B}^{\mathfrak{v}} \equiv \mathbf{B}$ és $\mathbf{A}^{\mathfrak{v}} \equiv \neg\mathbf{A} \equiv \neg\neg\mathbf{B}$. Az indukciós hipotézis szerint $\mathbf{B}$ levezethető $\Gamma^{\mathfrak{v}}$-ből, ugyanakkor a kettős negáció szabálya szerint $\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})$ tétel, így a leválasztás szabályát alkalmazva kapjuk, hogy $\neg\neg\mathbf{B}$ vagyis $\mathbf{A}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből.

2) Ha $\bar{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{h}$, akkor $\bar{\mathfrak{v}}(\mathbf{A}) \equiv \bar{\mathfrak{v}}(\neg\mathbf{B}) \equiv \mathbf{i}$, tehát $\mathbf{B}^{\mathfrak{v}} \equiv \neg\mathbf{B}$ és $\mathbf{A}^{\mathfrak{v}} \equiv \mathbf{A} \equiv \neg\mathbf{B}$. Az indukciós hipotézis szerint $\neg\mathbf{B}$ levezethető $\Gamma^{\mathfrak{v}}$-ből, ugyanakkor $\neg\mathbf{B}$ azonos $\mathbf{A}^{\mathfrak{v}}$-vel, tehát $\mathbf{A}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből.

(II) Léteznek olyan $\mathbf{B}$ és $\mathbf{C}$ ítéletek, hogy $\mathbf{A} \equiv \mathbf{B} \vee \mathbf{C}$. Ekkor $\mathbf{B}$-ben és $\mathbf{C}$-ben kevesebb logikai operátor szerepel, mint $\mathbf{A}$-ban, és minden $\mathbf{B}$-ben vagy $\mathbf{C}$-ben szereplő elemi ítélet $\mathbf{A}$-ban is szerepel, tehát eleme Γ-nak. Ezért az indukciós hipotézisből következik, hogy $\mathbf{B}^{\mathfrak{v}}$ és $\mathbf{C}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből. Most a $\mathfrak{v}$ értékelésre három eset lehetséges.

1) Ha $\bar{\mathfrak{v}}(\mathbf{B}) \equiv \mathbf{i}$, akkor $\bar{\mathfrak{v}}(\mathbf{A}) \equiv \bar{\mathfrak{v}}(\mathbf{B} \vee \mathbf{C}) \equiv \mathbf{i}$, tehát $\mathbf{B}^{\mathfrak{v}} \equiv \mathbf{B}$ és $\mathbf{A}^{\mathfrak{v}} \equiv \mathbf{A} \equiv \mathbf{B} \vee \mathbf{C}$. Az indukciós hipotézis szerint $\mathbf{B}$ levezethető $\Gamma^{\mathfrak{v}}$-ből, ugyanakkor $\mathbf{B} \Rightarrow (\mathbf{B} \vee \mathbf{C})$ axióma, így a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{B} \vee \mathbf{C}$ vagyis $\mathbf{A}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből.

2) Ha $\bar{\mathfrak{v}}(\mathbf{C}) \equiv \mathbf{i}$, akkor $\bar{\mathfrak{v}}(\mathbf{A}) \equiv \bar{\mathfrak{v}}(\mathbf{B} \vee \mathbf{C}) \equiv \mathbf{i}$, tehát $\mathbf{C}^{\mathfrak{v}} \equiv \mathbf{C}$ és $\mathbf{A}^{\mathfrak{v}} \equiv \mathbf{A} \equiv \mathbf{B} \vee \mathbf{C}$. Az indukciós hipotézis szerint $\mathbf{C}$ levezethető $\Gamma^{\mathfrak{v}}$-ből, ugyanakkor $\mathbf{C} \Rightarrow (\mathbf{C} \vee \mathbf{B})$ axióma, így a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{C} \vee \mathbf{B}$ levezethető $\Gamma^{\mathfrak{v}}$-ből. De $(\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{C})$ szintén axióma, ezért ismét a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{B} \vee \mathbf{C}$ vagyis $\mathbf{A}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből.

3) Ha $\bar{\mathfrak{v}}(\mathbf{B}) \equiv \bar{\mathfrak{v}}(\mathbf{C}) \equiv \mathbf{h}$, akkor $\bar{\mathfrak{v}}(\mathbf{A}) \equiv \bar{\mathfrak{v}}(\mathbf{B} \vee \mathbf{C}) \equiv \mathbf{h}$, tehát $\mathbf{B}^{\mathfrak{v}} \equiv \neg\mathbf{B}$, $\mathbf{C}^{\mathfrak{v}} \equiv \neg\mathbf{C}$, valamint $\mathbf{A}^{\mathfrak{v}} \equiv \neg\mathbf{A} \equiv \neg(\mathbf{B} \vee \mathbf{C})$. Az indukciós hipotézis szerint $\neg\mathbf{B}$ és $\neg\mathbf{C}$ levezethető $\Gamma^{\mathfrak{v}}$-ből. Az indirekt bizonyítás és az esetszétválasztás módszerének kombinálásával megmutatjuk, hogy ekkor $\mathbf{A}^{\mathfrak{v}}$, vagyis $\neg(\mathbf{B} \vee \mathbf{C})$ is levezethető $\Gamma^{\mathfrak{v}}$-ből. A kontrapozíció szabálya szerint $(\neg\neg(\mathbf{B} \vee \mathbf{C})) \Rightarrow (\mathbf{B} \vee \mathbf{C})$ tétel és $\neg\neg(\mathbf{B} \vee \mathbf{C})$ levezethető $\Gamma^{\mathfrak{v}}[\neg\neg(\mathbf{B} \vee \mathbf{C})]$-ből, ezért a leválasztás szabálya alapján $\mathbf{B} \vee \mathbf{C}$ levezethető $\Gamma^{\mathfrak{v}}[\neg\neg(\mathbf{B} \vee \mathbf{C})]$-ből. A $\neg\mathbf{B}$ és $\neg\mathbf{C}$ ítéletek szintén levezethetők $\Gamma^{\mathfrak{v}}[\neg\neg(\mathbf{B} \vee \mathbf{C})]$-ből. Legyen $\mathbf{D}$ tetszőlegesen rögzített ítélet. A $(\neg\mathbf{B}) \Rightarrow (\mathbf{B} \Rightarrow \mathbf{D})$ és $(\neg\mathbf{C}) \Rightarrow (\mathbf{C} \Rightarrow (\neg\mathbf{D}))$ ítéletek axiómák, tehát levezethetők $\Gamma^{\mathfrak{v}}[\neg\neg(\mathbf{B} \vee \mathbf{C})]$-ből. Kétszer alkalmazva a leválasztás szabályát kapjuk, hogy $\mathbf{B} \Rightarrow \mathbf{D}$ és $\mathbf{C} \Rightarrow (\neg\mathbf{D})$ levezethetők $\Gamma^{\mathfrak{v}}[\neg\neg(\mathbf{B} \vee \mathbf{C})]$-ből. De $\mathbf{B} \vee \mathbf{C}$ is levezethető $\Gamma^{\mathfrak{v}}[\neg\neg(\mathbf{B} \vee \mathbf{C})]$-ből, tehát az esetszétválasztás szabálya szerint a $\mathbf{D}$ és $\neg\mathbf{D}$ ítéletek levezethetők $\Gamma^{\mathfrak{v}}[\neg\neg(\mathbf{B} \vee \mathbf{C})]$-ből. Az indirekt bizonyítás elve alapján ebből következik, hogy a $\neg\neg(\mathbf{B} \vee \mathbf{C})$ ítélet levezethető $\Gamma^{\mathfrak{v}}$-ből. ■

1.4.9. Tétel. (**Kalmár-féle teljességi tétel.**) *Az ítéletkalkulus minden tautológiája tétel.*

Bizonyítás. Legyen $\mathbf{A}$ tautológia és jelölje Γ az $\mathbf{A}$-ban szereplő elemi ítéletek összességét. Legyen $\mathbf{A}_1$ a Γ-nak rögzített eleme és jelölje Γ_1 a Γ $\mathbf{A}_1$-től különböző elemeinek összességét. Világos, hogy Γ azonos $\Gamma_1[\mathbf{A}_1]$-gyel.

Legyen $\mathfrak{v}$ tetszőleges értékelés. Az előző állítás szerint $\mathbf{A}^{\mathfrak{v}}$ levezethető $\Gamma^{\mathfrak{v}}$-ből, ugyanakkor $\mathbf{A}^{\mathfrak{v}} \equiv \mathbf{A}$, mert $\mathbf{A}$ tautológia, továbbá $\Gamma^{\mathfrak{v}}$ azonos ${\Gamma_1}^{\mathfrak{v}}[{\mathbf{A}_1}^{\mathfrak{v}}]$-vel. A dedukció-tétel alapján ${\mathbf{A}_1}^{\mathfrak{v}} \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből.

Jelölje $\mathfrak{v}_1$ azt az értékelést, amely minden $\mathbf{A}_1$-től különböző elemi ítélethez ugyanazt az értéket rendeli, mint $\mathfrak{v}$, de $\mathfrak{v}_1(\mathbf{A}_1) \equiv \mathbf{i}$, ha $\mathfrak{v}(\mathbf{A}_1) \equiv \mathbf{h}$, és $\mathfrak{v}_1(\mathbf{A}_1) \equiv \mathbf{h}$, ha $\mathfrak{v}(\mathbf{A}_1) \equiv \mathbf{i}$. A definíció alapján világos, hogy ${\Gamma_1}^{\mathfrak{v}_1}$ azonos ${\Gamma_1}^{\mathfrak{v}}$-vel. Most két eset lehetséges.

1) $\mathfrak{v}(\mathbf{A}_1) \equiv \mathbf{i}$. Ekkor $\mathbf{A}_1 \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből, mert ${\mathbf{A}_1}^{\mathfrak{v}} \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből és ${\mathbf{A}_1}^{\mathfrak{v}} \equiv \mathbf{A}_1$. Továbbá, $(\neg\mathbf{A}_1) \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből, mert ${\mathbf{A}_1}^{\mathfrak{v}_1} \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}_1}$-ből, ${\mathbf{A}_1}^{\mathfrak{v}_1} \equiv \neg\mathbf{A}_1$ (hiszen $\mathfrak{v}_1(\mathbf{A}_1) \equiv \mathbf{h}$) és ${\Gamma_1}^{\mathfrak{v}_1}$ azonos ${\Gamma_1}^{\mathfrak{v}}$-vel.

2) $\mathfrak{v}(\mathbf{A}_1) \equiv \mathbf{h}$. Ekkor $(\neg\mathbf{A}_1) \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből, mert ${\mathbf{A}_1}^{\mathfrak{v}} \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből és ${\mathbf{A}_1}^{\mathfrak{v}} \equiv \neg\mathbf{A}_1$. Továbbá, $\mathbf{A}_1 \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből, mert ${\mathbf{A}_1}^{\mathfrak{v}_1} \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}_1}$-ből, ${\mathbf{A}_1}^{\mathfrak{v}_1} \equiv \mathbf{A}_1$ (hiszen $\mathfrak{v}_1(\mathbf{A}_1) \equiv \mathbf{i}$) és ${\Gamma_1}^{\mathfrak{v}_1}$ azonos ${\Gamma_1}^{\mathfrak{v}}$-vel.

Tehát azt kaptuk, hogy az ítéletkalkulus tetszőleges $\mathfrak{v}$ értékelésére $\mathbf{A}_1 \Rightarrow \mathbf{A}$ *és* $(\neg\mathbf{A}_1) \Rightarrow \mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből, így a *reductio ad absurdum* elve alapján $\mathbf{A}$ levezethető ${\Gamma_1}^{\mathfrak{v}}$-ből.

Ha Γ_1 üres, akkor ezzel megmutattuk, hogy $\mathbf{A}$ tétel. Ha Γ_1 nem üres, akkor rögzítjük Γ_1-nek egy $\mathbf{A}_2$ elemét, és Γ_2-vel jelöljük a Γ_1 $\mathbf{A}_2$-től különböző elemeinek összességét. Ezután tetszőleges $\mathfrak{v}$ értékelésre megismételve az előző érvelést Γ_1 helyett Γ_2-t és $\mathbf{A}_1$ helyett $\mathbf{A}_2$-t véve kapjuk, hogy $\mathbf{A}$ levezethető ${\Gamma_2}^{\mathfrak{v}}$-ből. Ha Γ-nak n darab eleme van, akkor ez az eljárás legfeljebb n-szer ismételhető, tehát szükségképpen oda jutunk, hogy $\mathbf{A}$ levezethető az üres ítélet-összességből, vagyis tétel. ■

Figyelemre méltó az, hogy a Kalmár-féle teljességi tétel és az előtte álló kijelentés bizonyításából kiolvasható az, hogy egy tautológiának miként lehet előállítani egy bizonyítását.

Példa. Legyenek $\mathbf{A}$ és $\mathbf{B}$ ítéletek; megmutatjuk, hogy $(\neg(\mathbf{A} \Rightarrow \mathbf{B}))\Leftrightarrow(\mathbf{A} \wedge (\neg\mathbf{B}))$ az ítéletkalkulusnak tétele (ez az *implikáció negációjának szabálya*). A Kalmár-féle teljességi tétel alapján elég azt igazolni, hogy a $(\neg(\mathbf{A} \Rightarrow \mathbf{B}))\Leftrightarrow(\mathbf{A}\wedge(\neg\mathbf{B}))$ ítélet tautológia. Legyen $\mathfrak{v}$ tetszőleges értékelés, és tekintsük a következő logikai táblázatot.

$\bar{\mathfrak{v}}(\mathbf{A})$	$\bar{\mathfrak{v}}(\mathbf{B})$	$\bar{\mathfrak{v}}(\neg(\mathbf{A} \Rightarrow \mathbf{B}))$	$\bar{\mathfrak{v}}(\mathbf{A} \wedge (\neg\mathbf{B})))$	$\bar{\mathfrak{v}}((\neg(\mathbf{A} \Rightarrow \mathbf{B}))\Leftrightarrow(\mathbf{A} \wedge (\neg\mathbf{B})))$
i	**i**	**h**	**h**	**i**
i	**h**	**i**	**i**	**i**
h	**i**	**h**	**h**	**i**
h	**h**	**h**	**h**	**i**

Ebből azonnal látható, hogy $(\neg(\mathbf{A} \Rightarrow \mathbf{B}))\Leftrightarrow(\mathbf{A} \wedge (\neg\mathbf{B}))$ tautológia, tehát az ítéletkalkulusnak tétele. Ennek az ítéletnek levezetését előállítani sokkal nehezebb volna, mint ezt a logikai táblázatot kiértékelni.

2. fejezet

Axiomatikus matematikai elméletek

2.1. Formális matematikai nyelvek

A *formális matematikai nyelvek* definíciója három lépésben történik. Először értelmezzük a nyelv *szimbólum-rendszerét*, majd a nyelv *kifejezéseit*, végül megadunk egy szabályt, amelynek alkalmazásával a nyelv kifejezései közül kiválaszthatóak az "értelmes kifejezések": az *objektumok* és a *formulák*. Tehát hasonló eljárást követünk, mint az ítéletkalkulusban, azonban itt a kifejezések értelmességének definícója *kétféle* értelmes kifejezésre vezet, míg az ítéletkalkulus nyelvében csak az ítéletek voltak az értelmes kifejezések.

A továbbiakban kizárólag formális matematikai nyelvekről lesz szó, ezért általában a "formális" jelzőt elhagyjuk.

A matematikai nyelvek szimbólum-rendszere négy részből áll: a *változók*, a *logikai operátorok*, a *logikai függvényjelek* és a *matematikai függvényjelek* összességéből.

2.1.1. Definíció. (**A matematikai nyelvek szimbólumai.**) *Egy matematikai nyelv szimbólumai a következők:*

- **Változók***: a latin ábécé kis és nagybetűi, azzal a megállapodással, hogy minden változó vesszővel ellátva szintén változó.*
- **Logikai operátorok***: a $\neg$, $\vee$, ε és $\square$ jelek.*
- **Logikai függvényjelek***: az* $=$ (**egyenlőség**) *jel, valamint olyan szimbólumok, amelyek a változóktól és a logikai operátoroktól különböznek. Minden logikai függvényjelhez hozzá van rendelve egy nem nulla szám, amit a függvényjel* **súlyának** *nevezünk. Az $=$ jel súlya definíció szerint kettő.*
- **Matematikai függvényjelek***: olyan szimbólumok, amelyek a változóktól, a logikai operátoroktól és a logikai függvényjelektől különböznek. Minden matematikai függvényjelhez hozzá van rendelve egy szám, amit a függvényjel* **súlyának** *nevezünk.*

A matematikai nyelv logikai (*illetve matematikai*) *függvényjeleit a hozzájuk rendelt súllyal együtt a nyelv* **logikai** (*illetve* **matematikai**) **függvényeinek** *nevezzük. Az $=$ jeltől különböző logikai függvényeket* **logikai sajátfüggvényeknek** *nevezzük. A nulla súlyú matematikai függvényeket a matematikai nyelv* **konstansainak** *nevezzük. Egy logikai* (*illetve matematikai*) *függvényt n-változósnak nevezünk, ha a függvényjel súlya az n szám.*

A változók definíciójában előírjuk, hogy minden vesszőzött változó szintén változó legyen. Ezzel biztosítjuk korlátlan mennyiségű változó létezését. Ha csak a latin ábécé betűit tekintenénk változóknak, akkor elvileg előfordulhatna olyan bonyolult matematikai kijelentés vagy objektum, amely azért nem volna formalizálható, mert a rendelkezésre álló változók nem elegendőek a kijelentés vagy objektum formalizálására.

A definícióból látható, hogy a matematikai nyelvek szimbólum-rendszerei egymástól csak a logikai sajátfüggvények és a matematikai függvények készletében különböznek. Tehát egy konkrét matematikai nyelv szimbólum-rendszerének meghatározása azt jelenti, hogy a logikai és matematikai függvényeinek összességét rögzítjük. Az $=$ jel minden matematikai nyelvnek logikai függvénye, tehát a legegyszerűbb matematikai nyelv az, amelynek sem logikai sajátfüggvénye, sem matematikai függvénye nincs.

A *zárójelek* és a *szóköz-jel* nem tartoznak hozzá az matematikai nyelvek szimbólumkészletéhez, azonban bizonyos kifejezések *jelöléséhez* célszerű a zárójelek alkalmazása, továbbá bonyolult kifejezések felépítése esetleg világosabbá tehető a szóköz-jel alkalmazásával.

A matematikai nyelvek szimbólum-rendszerében szereplő logikai és matematikai függvény-fogalomnak semmi köze nincs a (később bevezetésre kerülő) halmazelméleti függvény-fogalomhoz. Súlyos félreértésre vezet e kétféle függvény-fogalom összekeverése, hiszen a halmazelméleti függvényeket egy speciális matematikai nyelvben (a halmazelmélet nyelvében) értelmezzük. A matematikai nyelvek esetében egyszerűen csak *elnevezésről* van szó; a logikai és matematikai függvények egyszerűen szimbólumok, amelyekre *úgy hivatkozunk*, mint logikai és matematikai függvények.

Megjegyezzük még, hogy a matematikai nyelvek logikai, illetve matematikai függvényeinek összességére nem követeljük meg azok *végességét*, bár minden fontos konkrét matematikai nyelvben csak véges sok logikai és matematikai függvény van.

Példák. 1) A *halmazelmélet* matematikai nyelvében egyáltalán nincs matematikai függvény, így konstansa sincs, ugyanakkor az egyetlen logikai sajátfüggvénye a kettő súlyú (vagyis kétváltozós) $\in$ (*elem*) szimbólum.

2) Az *aritmetika* matematikai nyelvének nincs logikai sajátfüggvénye, de van négy matematikai függvénye: a nulla súlyú $\mathbf{0}$ (*nulla*) függvény, az egy súlyú (vagyis egyváltozós) $\#$ (*szukcesszor*) függvény, a kétváltozós $+$ (*összeadás*), valamint a szintén kétváltozós $\cdot$ (*szorzás*) függvény. Ebben a nyelvben a $\mathbf{0}$ szimbólum az egyetlen konstans.

3) A *síkgeometria* matematikai nyelvének nincs matematikai függvénye, így konstansa sincs, de van két három súlyú (azaz háromváltozós) logikai sajátfüggvénye: a $\mathfrak{Gr}$ *illeszkedés-függvény* és a $\mathfrak{Zw}$ *közbensőpont-függvény.*

2.1.2. Definíció. (**A matematikai nyelvek kifejezései.**) *Egy matematikai nyelv* **kifejezésének** *nevezünk minden olyan karakterláncot, amelynek karakterei a nyelv szimbólumai, és amelyben egyes, változóktól különböző, karakterpárok a karakterlánc felett haladó vonallal vannak összekötve.* **Zártaknak** *nevezzük azokat a kifejezéseket, amelyekben nem szerepel változó.*

Matematikai nyelv két kifejezését akkor mondjuk *azonosnak*, ha karakterről-karakterre megegyeznek, és mindkét kifejezésben ugyanazok a karakterpárok vannak a karakterlánc felett haladó vonallal összekötve. A nem azonos kifejezéseket *különbözőeknek* nevezzük. Két kifejezés azonosságának a tényét úgy fejezzük ki, hogy leírjuk a két kifejezést, és közéjük tesszük az $\equiv$ (*azonosság*) vagy *grafikus egyenlőség* jelét. Egyidejűleg kikötjük, hogy a $\equiv$ szimbólum egyetlen matematikai nyelvben sem lehet logikai vagy matematikai függvényjel.

Vigyázzunk az *azonosság* és az *egyenlőség* fogalmának pontos megkülönböztetésére! Például az aritmetika matematikai nyelvében a $\mathbf{2}+\mathbf{1}$ szimbólummal jelölt kifejezés *nem azonos* a $\mathbf{3}$-mal jelölt kifejezéssel, mert a definíciók szerint $\mathbf{2}+\mathbf{1} \equiv +\#\#\mathbf{0}\#\mathbf{0}$ és $\mathbf{3} \equiv \#\#\#\mathbf{0}$; ugyanakkor az aritmetikában "igaz" a $\mathbf{2}+\mathbf{1} = \mathbf{3}$ kijelentés, tehát ezek a kifejezések *egyenlőek*. Az egyenlőség és azonosság közötti lényeges különbség az, hogy két kifejezés azonossága csak a szintaktikus szerkezetükön múlik, ugyanakkor az egyenlőségük függ annak az elméletnek az igazság-fogalmától, amelynek nyelvében előállítottuk őket. Erre a kérdésre még visszatérünk az 5. pontban.

Megállapodunk abban, hogy matematikai nyelv tetszőleges változójának (illetve kifejezésének) *jelölésére* vastagon írt, esetleg vesszőkkel ellátott latin kisbetűket (illetve nagybetűket) használunk. Tehát $\mathbf{x}$ (illetve $\mathbf{A}$) tetszőleges változót (illetve kifejezést) jelöl, ami egyáltalán nem szükségképpen azonos az x (illetve A) betűvel.

Csakúgy, mint az ítéletkalkulus nyelvének esetében, itt is nagy különbség van egy *kifejezés*, valamint a *kifejezés jelölése* között. A matematikai nyelvek kifejezéseinek előállításához csak a matematikai nyelvek szimbólumait alkalmazhatjuk, ugyanakkor egy kifejezés jelölése céljából bármely olyan szimbólum használható, amelyből egyértelműen rekonstruálható az a kifejezés, amelynek a jelöléséről van szó. Például a zárójeleket gyakran használjuk a kifejezések jelölésekor, holott azok nem szimbólumai a matematikai nyelveknek. Azonban a gördülékenyebb fogalmazás kedvéért néha elmosódik a különbség a kifejezés és annak jelölése között. A továbbiakban sokszor mondjuk azt, hogy "$\mathbf{A}$ a matematikai nyelv kifejezése", holott valójában úgy kellene fogalmazni, hogy "$\mathbf{A}$ *jelöli* az ítéletkalkulusnak egy kifejezését".

A továbbiakban gyakran előfordul az a kijelentés, hogy "egy $\mathbf{x}$ változó *szerepel* az $\mathbf{A}$ kifejezésben". Intuitíve világos ennek a kijelentésnek az értelme, továbbá az is nyilvánvaló, hogy az $\mathbf{x}$ változó és az $\mathbf{A}$ kifejezés karaktereinek összehasonlításával dönthető el e kijelentés helyessége. Világos, hogy egy $\mathbf{x}$ változó az $\mathbf{A}$ kifejezésben több karakterpozícióban is szerepelhet; minden ilyen szereplést az $\mathbf{x}$ változó *előfordulásának* nevezzük az $\mathbf{A}$ kifejezésben.

Egy matematikai nyelv kifejezéseinek összességén a következő formális manipulációk hajthatók végre:

– két kifejezés egymás mellé illesztése (*konkatenáció*); ha $\mathbf{A}$ és $\mathbf{B}$ kifejezések, akkor az ezek konkatenálásával nyert kifejezést $\mathbf{AB}$ jelöli;

– változó *helyettesítése* egy kifejezésben valamely kifejezéssel; ha $\mathbf{T}$, $\mathbf{A}$ kifejezések és $\mathbf{x}$ változó, akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}$ jelöli azt a kifejezést, amit úgy kapunk, hogy az $\mathbf{A}$-ban az $\mathbf{x}$ minden előfordulása helyére a $\mathbf{T}$ kifejezést helyettesítjük;

– kifejezés két karakterének *összekötése* egy vonallal, amely a kifejezés felett halad;

– karakter *törlése* egy kifejezésben.

Megjegyezzük, hogy ha $\mathbf{A}$, $\mathbf{T}$ kifejezések és $\mathbf{x}$ változó egy matematikai nyelvben, akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}$ előállításakor az $\mathbf{x}$ minden $\mathbf{A}$-beli előfordulása helyére *egyszerre* helyettesítjük be $\mathbf{T}$-t és nem egymás után; ez akkor fontos körülmény, ha $\mathbf{x}$ szerepel $\mathbf{T}$-ben.

Jelölés. (**A Hilbert-féle ε-szimbólum.**) Legyen $\mathbf{A}$ kifejezés és $\mathbf{x}$ változó egy matematikai nyelvben. Ekkor $\varepsilon_{\mathbf{x}}(\mathbf{A})$ jelöli azt a kifejezést, amelyet úgy kapunk, hogy az $\varepsilon\mathbf{A}$ kifejezésben $\mathbf{x}$ minden előfordulása helyére a $\square$ szimbólumot helyettesítjük, és ε-t összekötjük az így bevezetett $\square$ jellel egy olyan vonallal, amely a karakterlánc felett halad.

Például az $\varepsilon_{\mathbf{x}}(\neg = \mathbf{xy})$-szel jelölt kifejezés az $\overline{\varepsilon\neg = \Box}\ \mathbf{y}$ karakterlánc.

Z

Vigyázzunk arra, hogy ha $\mathbf{x}$ szerepel $\mathbf{A}$-ban, akkor $\varepsilon_{\mathbf{x}}(\mathbf{A})$ *nem azonos* az $\varepsilon(\Box|\mathbf{x})\mathbf{A}$ kifejezéssel. A kettő között az a különbség, hogy $\varepsilon_{\mathbf{x}}(\mathbf{A})$-ban az $\mathbf{x}$ helyére tett $\Box$ szimbólumokat *összekötjük* ε-nal egy olyan vonallal, amely a kifejezés felett halad, míg $\varepsilon(\Box|\mathbf{x})\mathbf{A}$-ból ezek az összekötő vonalak hiányoznak. Tehát az $\varepsilon_{\mathbf{x}}(\mathbf{A})$-val jelölt kifejezésben nem szerepel az $\mathbf{x}$ változó (ugyanúgy, mint $\varepsilon(\Box|\mathbf{x})\mathbf{A}$-ban sem), azonban $\varepsilon_{\mathbf{x}}(\mathbf{A})$-ból rekonstruálható az, hogy a $\Box$ szimbólummal való helyettesítés előtt mely karakterpozíciókban volt jelen $\mathbf{A}$-ban az $\mathbf{x}$ változó, ugyanakkor az $\varepsilon(\Box|\mathbf{x})\mathbf{A}$ kifejezésből úgy tűnik el az $\mathbf{x}$ változó, hogy annak eredeti $\mathbf{A}$-beli pozíciói már felderíthetetlenek.

Természetesen felvetődik a kérdés, hogy mi az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ kifejezés *értelme*? A matematikai nyelvek elmélete kifejtésének jelenlegi szintjén ez a kérdés még nem válaszolható meg. Ezen a szinten még a matematikai nyelvek egyetlen kifejezésének sincs *értelme*; a kifejezések *értelmességének* fogalmát később vezetjük be. Annyit előzetesen is érdemes megemlíteni, hogy a Hilbert által bevezetett ε-szimbólum segítségével lehet majd *értelmezni* az *egzisztenciális* és *univerzális kvantorokat* úgy, hogy azok mind szintaktikus, mind szemantikus szempontból úgy viselkedjenek, ahogy azt a mindennapi matematikai gyakorlatban elvárjuk tőlük.

2.1.3. Állítás. (**A helyettesítések felcserélésének szabálya.**) *Legyenek* $\mathbf{A}$, $\mathbf{T}$ *és* $\mathbf{S}$ *kifejezések, továbbá* $\mathbf{x}$ *és* $\mathbf{y}$ *különböző változók egy matematikai nyelvben. Ha* $\mathbf{x}$ *nem szerepel* $\mathbf{S}$*-ben, akkor*

$$(\mathbf{S}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv ((\mathbf{S}|\mathbf{y})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A}).$$

Bizonyítás. Az $(\mathbf{S}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})$ kifejezés előállításának első lépéseként az $\mathbf{A}$ kifejezésben az $\mathbf{x}$ minden előfordulása helyére a $\mathbf{T}$ kifejezést helyettesítjük. Az így nyert $(\mathbf{T}|\mathbf{x})\mathbf{A}$ kifejezésben az $\mathbf{y}$ változó minden olyan helyen szerepel, ahol eredetileg $\mathbf{A}$-ban szerepelt, továbbá azokon a helyeken is, amelyek a $\mathbf{T}$ egyes előfordulásaiban vannak, az $\mathbf{x}$ kicserélése után. Ezért az $\mathbf{S}$ behelyettesítése az $\mathbf{y}$ helyére a $(\mathbf{T}|\mathbf{x})\mathbf{A}$ kifejezésben azt eredményezi, hogy $\mathbf{S}$ kerül az $\mathbf{y}$ minden eredeti $\mathbf{A}$-beli előfordulása helyére és mindazokra a helyekre $\mathbf{T}$-ben, ahol $\mathbf{T}$-ben előfordulnak, az $\mathbf{x}$ változó $\mathbf{T}$-re való kicserélése után. Az $\mathbf{x}$ és $\mathbf{y}$ változók különbözőek, és $\mathbf{x}$ nem szerepel $\mathbf{S}$-ben, ezért ez nyilvánvalóan az $((\mathbf{S}|\mathbf{y})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A})$ kifejezés. ■

Az előző állításban lényeges, hogy $\mathbf{x}$ *nem szerepel* $\mathbf{S}$-ben. Ha nem így van, akkor előfordulhat az, hogy $\mathbf{x}$ szerepel $(\mathbf{S}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})$-ben, de nem szerepel $((\mathbf{S}|\mathbf{y})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A})$-ban, így ezek a kifejezések különbözőek. Például, ha $\mathbf{x}$ és $\mathbf{y}$ különböző változók, valamint $\mathbf{z}$ olyan változó, amely $\mathbf{x}$-től és $\mathbf{y}$-tól különbözik, és $\mathbf{S} \equiv \mathbf{x}$, $\mathbf{T} \equiv \mathbf{z}$ és $\mathbf{A} \equiv \mathbf{y}$, akkor

$$(\mathbf{S}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv (\mathbf{x}|\mathbf{y})\,((\mathbf{z}|\mathbf{x})\mathbf{y}) \equiv (\mathbf{x}|\mathbf{y})\mathbf{y} \equiv \mathbf{x},$$
$$((\mathbf{S}|\mathbf{y})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A}) \equiv ((\mathbf{x}|\mathbf{y})\mathbf{z}|\mathbf{x})((\mathbf{x}|\mathbf{y})\mathbf{y}) \equiv (\mathbf{z}|\mathbf{x})\mathbf{x} \equiv \mathbf{z},$$

ezért $(\mathbf{S}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})$ és $((\mathbf{S}|\mathbf{y})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A})$ különbözőek.

Ugyanakkor az is fontos, hogy $\mathbf{x}$ és $\mathbf{y}$ *különbözőek* legyenek, ha ugyanis $\mathbf{T}$ és $\mathbf{S}$ olyan kifejezések, amelyekben $\mathbf{x}$ nem szerepel, akkor

$$(\mathbf{S}|\mathbf{x})((\mathbf{T}|\mathbf{x})\mathbf{x}) \equiv (\mathbf{S}|\mathbf{x})\mathbf{T} \equiv \mathbf{T}$$
$$((\mathbf{S}|\mathbf{x})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{x})\mathbf{x}) \equiv (\mathbf{T}|\mathbf{x})\mathbf{S} \equiv \mathbf{S},$$

tehát ha $\mathbf{T}$ és $\mathbf{S}$ különbözőek, akkor az $\mathbf{A} \equiv \mathbf{x}$ választással kapjuk, hogy a $(\mathbf{S}|\mathbf{x})((\mathbf{T}|\mathbf{x})\mathbf{A})$ és $((\mathbf{S}|\mathbf{x})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{x})\mathbf{A})$ kifejezések különbözőek.

Ezért a helyettesítések felcserélésének szabályát csak azzal a feltétellel alkalmazhatjuk, hogy $\mathbf{x}$ és $\mathbf{y}$ különbözőek, és $\mathbf{x}$ nem szerepel $\mathbf{S}$-ben.

2.1.4. Állítás. (**A helyettesítések tranzitivitásának szabálya.**) *Legyenek* $\mathbf{A}$, $\mathbf{T}$ *kifejezések, valamint* $\mathbf{x}$ *és* $\mathbf{y}$ *változók egy matematikai nyelvben. Ha* $\mathbf{y}$ *nem szerepel* $\mathbf{A}$*-ban, akkor*

$$(\mathbf{T}|\mathbf{x})\mathbf{A} \equiv (\mathbf{T}|\mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}).$$

Bizonyítás. Az $\mathbf{y}$ változó nem szerepel $\mathbf{A}$-ban, ezért az $(\mathbf{y}|\mathbf{x})\mathbf{A}$ kifejezésben $\mathbf{y}$ azokon és csakis azokon a helyeken szerepel, ahol $\mathbf{A}$-ban az $\mathbf{x}$ szerepel. Tehát , $(\mathbf{y}|\mathbf{x})\mathbf{A}$-ban az $\mathbf{y}$ minden előfordulása helyére a $\mathbf{T}$-t helyettesítve ugyanazt a kifejezést kapjuk, mint amikor az $\mathbf{x}$ minden $\mathbf{A}$-beli előfordulása helyére a $\mathbf{T}$-t helyettesítjük. ■

Az előző állításban lényeges, hogy $\mathbf{y}$ ne szerepeljen $\mathbf{A}$-ban. Például ha $\mathbf{x}$ és $\mathbf{y}$ különbözőek, akkor

$$(\mathbf{T}|\mathbf{y})((\mathbf{y}|\mathbf{x})(\mathbf{x}\mathbf{y})) \equiv (\mathbf{T}|\mathbf{y})(\mathbf{y}\mathbf{y}) \equiv \mathbf{T}\mathbf{T},$$
$$(\mathbf{T}|\mathbf{x})(\mathbf{x}\mathbf{y}) \equiv \mathbf{T}\mathbf{y},$$

ezért ha $\mathbf{T}$ különbözik $\mathbf{y}$-tól, akkor az $\mathbf{A} \equiv \mathbf{x}\mathbf{y}$ választással kapjuk, hogy a $(\mathbf{T}|\mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A})$ és $(\mathbf{T}|\mathbf{x})\mathbf{A}$ kifejezések különbözőek. Tehát fel kell tenni, hogy $\mathbf{y}$ nem szerepel $\mathbf{A}$-ban, azonban $\mathbf{x} \equiv \mathbf{y}$ megengedhető, hiszen ekkor nyilvánvaló, hogy

$$(\mathbf{T}|\mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}) \equiv (\mathbf{T}|\mathbf{x})((\mathbf{x}|\mathbf{x})\mathbf{A}) \equiv (\mathbf{T}|\mathbf{x})\mathbf{A}.$$

2.1.5. Állítás. (**A helyettesítés szabálya ε-kifejezésekben.**) *Legyenek* $\mathbf{A}$, $\mathbf{T}$ *kifejezések és* $\mathbf{x}$, $\mathbf{y}$ *különböző változók egy matematikai nyelvben. Ha* $\mathbf{x}$ *nem szerepel* $\mathbf{T}$*-ben, akkor*

$$(\mathbf{T}|\mathbf{y})\varepsilon_{\mathbf{x}}(\mathbf{A}) \equiv \varepsilon_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A}).$$

Bizonyítás. Az $\mathbf{x}$ és $\mathbf{y}$ változók különbözőek, és $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben, ezért a $(\mathbf{T}|\mathbf{y})\mathbf{A}$ kifejezésben az $\mathbf{x}$ azokon és csakis azokon a helyeken szerepel, ahol $\mathbf{A}$-ban szerepel. A $(\mathbf{T}|\mathbf{y})\mathbf{A}$ kifejezésből úgy nyerjük $\varepsilon_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A})$-t, hogy $\varepsilon(\mathbf{T}|\mathbf{y})\mathbf{A}$-ban az $\mathbf{x}$ minden előfordulása helyére $\square$-t helyettesítünk és ε-t összekötjük a $\square$ jellel egy olyan vonallal, amely $\varepsilon(\mathbf{T}|\mathbf{y})\mathbf{A}$ felett halad. Ekkor az $\mathbf{x}$ minden $\mathbf{A}$-beli előfordulása helyére $\square$ kerül és megjelenik egy $(\mathbf{T}|\mathbf{y})(\varepsilon\mathbf{A})$ felett haladó összekötő vonal ε és $\square$ között. Nyilvánvaló, hogy az így nyert kifejezés éppen $(\mathbf{T}|\mathbf{y})\varepsilon_{\mathbf{x}}(\mathbf{A})$. ■

Az előző állításban lényeges, hogy $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben, különben előfordulhat, hogy $\mathbf{x}$ szerepel $(\mathbf{T}|\mathbf{y})\varepsilon_{\mathbf{x}}(\mathbf{A})$-ban, de természetesen nem szerepel $\varepsilon_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A})$-ban. Ugyanakkor azt sem szabad megengedni, hogy $\mathbf{x}$ és $\mathbf{y}$ azonosak legyenek, mert ekkor $(\mathbf{T}|\mathbf{y})\varepsilon_{\mathbf{x}}(\mathbf{A}) \equiv \varepsilon_{\mathbf{x}}(\mathbf{A})$, de $(\mathbf{T}|\mathbf{x})\mathbf{A}$ lehet az $\mathbf{A}$-tól annyira különböző, hogy $\varepsilon_{\mathbf{x}}(\mathbf{A})$ és $\varepsilon_{\mathbf{x}}((\mathbf{T}|\mathbf{x})\mathbf{A})$ különbözőek.

2.1.6. Állítás. (**A helyettesítések tranzitivitásának szabálya ε-kifejezésekben.**) *Legyen* $\mathbf{A}$ *kifejezés és* $\mathbf{x}$ *változó egy matematikai nyelvben. Ha* $\mathbf{y}$ *olyan változó, amely nem szerepel* $\mathbf{A}$*-ban, akkor*

$$\varepsilon_{\mathbf{x}}(\mathbf{A}) \equiv \varepsilon_{\mathbf{y}}((\mathbf{y}|\mathbf{x})\mathbf{A}).$$

Bizonyítás. Az $\mathbf{y}$ változó nem szerepel $\mathbf{A}$-ban, ezért az $\varepsilon(\mathbf{y}|\mathbf{x})\mathbf{A}$ kifejezésben az $\mathbf{y}$ azokon és csakis azokon a helyeken szerepel, ahol $\mathbf{A}$-ban az $\mathbf{x}$ szerepel. Tehát $\varepsilon(\mathbf{y}|\mathbf{x})\mathbf{A}$-ban az $\mathbf{y}$ minden előfordulása helyére $\Box$-t helyettesítve és az ε jelet $\Box$-szel összekötve egy $\varepsilon(\mathbf{y}|\mathbf{x})\mathbf{A}$ felett haladó vonallal ugyanazt a kifejezést kapjuk, mint amikor az $\mathbf{x}$ minden $\varepsilon\mathbf{A}$-beli előfordulása helyére a $\Box$-t helyettesítjük, majd az ε jelet $\Box$-szel összekötjük egy $\varepsilon\mathbf{A}$ felett haladó vonallal. Az előbbi kifejezés azonos $\varepsilon_{\mathbf{y}}((\mathbf{y}|\mathbf{x})\mathbf{A})$-val, míg az utóbbi azonos $\varepsilon_{\mathbf{x}}(\mathbf{A})$-val. ■

Az előző állításban lényeges, hogy $\mathbf{y}$ nem szerepel $\mathbf{A}$-ban, mert ekkor különböző $\mathbf{x}$ és $\mathbf{y}$ esetén az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ kifejezésben szükségképpen szerepel az $\mathbf{y}$ változó, de ez biztosan nem szerepelhet $\varepsilon_{\mathbf{y}}((\mathbf{y}|\mathbf{x})\mathbf{A})$-ban.

Most megfogalmazzuk azt a meglehetősen bonyolult szabályt, amelynek segítségével kijelölhetőek egy matematikai nyelv *értelmes kifejezései*; vagyis a *kifejezések értelmességének definícióját* fogjuk megadni. Látjuk majd, hogy kétféle lényegesen különböző értelmes kifejezés létezik: az *objektumok* és a *formulák*. Az objektumok (illetve formulák) a természetes matematikai nyelven megfogalmazható matematikai dolgok (illetve állítások) formális megfelelői (*formalizáltjai*). Kiderül, hogy az objektumokat és formulákat nem egymástól függetlenül értelmezzük, hasonlóan ahhoz, ahogy a természetes matematikai nyelvben tesszük.

2.1.7. Definíció. *Egy matematikai nyelv kifejezését*

– **elsőfajúnak** *nevezzük, ha változó, vagy az ε szimbólummal, vagy matematikai függvényjellel kezdődik;*

– **másodfajúnak** *nevezzük, ha a $\neg$ és $\vee$ szimbólumok valamelyikével, vagy logikai függvényjellel kezdődik;*

2.1.8. Definíció. (**A matematikai nyelvek objektumai és formulái.**) *Egy matematikai nyelv* **objektum-formula konstrukciójának** *nevezzük a nyelv kifejezéseinek bármely olyan $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ n-esét, amelyre minden $1 \leq k \leq n$ esetén a következő feltételek valamelyike teljesül:*

(1) *$\mathbf{A}_k$ változó vagy konstans;*

(2) *létezik olyan $1 \leq j < k$ szám, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \neg\mathbf{A}_j$;*

(3) *léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_i$ és $\mathbf{A}_j$ másodfajúak és $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$;*

(4) *létezik olyan $1 \leq j < k$ szám és létezik olyan $\mathbf{x}$ változó, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \varepsilon_{\mathbf{x}}(\mathbf{A}_j)$;*

(5) *létezik olyan m-változós f logikai vagy matematikai függvény és léteznek olyan $1 \leq j_1, \ldots, j_m < k$ számok, hogy minden $1 \leq p \leq m$ számra $\mathbf{A}_{j_p}$ elsőfajú és $\mathbf{A}_k \equiv \mathsf{f}\mathbf{A}_{j_1} \ldots \mathbf{A}_{j_m}$.*

Egy matematikai nyelv $\mathbf{A}$ kifejezését **objektumnak** (*illetve* **formulának**) *nevezzük, ha $\mathbf{A}$ elsőfajú (illetve másodfajú) és létezik a nyelvnek olyan $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ objektum-formula konstrukciója, hogy $\mathbf{A} \equiv \mathbf{A}_n$.*

A definícióból látható, hogy egy matematikai nyelv formulája olyan kifejezés, amely vagy logikai függvényjellel, vagy a $\neg$ és $\vee$ szimbólumok valamelyikével kezdődik. Ugyanakkor minden változó és minden konstans objektum, továbbá egy változótól különböző objektum első karaktere matematikai függvényjel vagy az ε szimbólum.

Természetesen léteznek olyan kifejezések, amelyek se nem elsőfajúak, se nem másodfajúak. Például minden $\Box$-sel kezdődő kifejezés ilyen, továbbá, ha $\mathbf{x}$ változó és $\mathbf{A}$

tetszőleges kifejezés, akkor az $\mathbf{xA}$ kifejezés is ilyen.

A $\vee$ logikai operátorral kapcsolatban gyakran alkalmazzuk az *infix jelölési konvenciót*, ami azt jelenti, hogy ha $\mathbf{A}$ és $\mathbf{B}$ kifejezések egy matematikai nyelvben, akkor a $\vee\mathbf{AB}$ kifejezést az $\mathbf{A} \vee \mathbf{B}$ jellel *jelöljük*. Természetesen az infix jelölés alkalmazásakor elkerülhetetlenné válik a zárójelek helyes használata.

2.1.9. Definíció. *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *kifejezések egy matematikai nyelvben, akkor*

- $\mathbf{A} \Rightarrow \mathbf{B}$ *jelöli a* $\vee\neg\mathbf{AB}$ *kifejezést, vagyis* $\mathbf{A} \Rightarrow \mathbf{B} \equiv (\neg\mathbf{A}) \vee \mathbf{B}$*;*
- $\mathbf{A} \wedge \mathbf{B}$ *jelöli a* $\neg\vee\neg\mathbf{A}\neg\mathbf{B}$ *kifejezést, vagyis* $\mathbf{A} \wedge \mathbf{B} \equiv \neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$*;*
- $\mathbf{A}\Leftrightarrow\mathbf{B}$ *jelöli a* $\neg\vee\neg\vee\neg\mathbf{AB}\neg\vee\neg\mathbf{BA}$ *kifejezést, azaz* $\mathbf{A}\Leftrightarrow\mathbf{B} \equiv (\mathbf{A} \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow \mathbf{A})$*;*

A $\Rightarrow$*,* $\wedge$*,* $\Leftrightarrow$ *szimbólumot rendre* **implikációnak**, **konjunkciónak**, **ekvivalenciának** *nevezzük. Az* $\wedge$ *szimbólum helyett az & szimbólumot is használjuk.*

Természetesen megköveteljük, hogy matematikai nyelv egyetlen logikai vagy matematikai függvénye se legyen azonos a $\Rightarrow$, $\wedge$ és $\Leftrightarrow$ szimbólumok egyikével sem.

2.1.10. Állítás. *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák egy matematikai nyelvben akkor a* $\neg\mathbf{A}$*,* $\mathbf{A} \vee \mathbf{B}$*,* $\mathbf{A} \Rightarrow \mathbf{B}$*,* $\mathbf{A} \wedge \mathbf{B}$ *és* $\mathbf{A}\Leftrightarrow\mathbf{B}$ *kifejezések szintén formulák. Ha* f *n-változós logikai (illetve matematikai) függvény és* $\mathbf{T}_1, \ldots, \mathbf{T}_n$ *objektumok egy matematikai nyelvben, akkor* $\mathsf{f}\mathbf{T}_1 \ldots \mathbf{T}_n$ *formula (illetve objektum). Ha* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó egy matematikai nyelvben, akkor* $\varepsilon_{\mathbf{x}}(\mathbf{A})$ *objektum.*

Bizonyítás. Legyenek $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ és $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m)$ olyan objektum-formula konstrukciók, hogy $\mathbf{A} \equiv \mathbf{A}_n$ és $\mathbf{B} \equiv \mathbf{B}_m$, továbbá tegyük fel, hogy $\mathbf{A}$ és $\mathbf{B}$ másodfajú kifejezések (vagyis formulák). Nyilvánvaló, hogy

$$(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \neg\mathbf{A}_n),$$
$$(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m, \vee\mathbf{A}_n\mathbf{B}_m)$$

objektum-formula konstrukciók, $\neg\mathbf{A} \equiv \neg\mathbf{A}_n$, $\mathbf{A} \vee \mathbf{B} \equiv \vee\mathbf{A}_n\mathbf{B}_m$ és $\neg\mathbf{A}_n$, $\vee\mathbf{A}_n\mathbf{B}_m$ másodfajú kifejezések, ezért $\neg\mathbf{A}$ és $\mathbf{A} \vee \mathbf{B}$ formulák. Az implikáció, konjunkció és ekvivalencia értelmezése alapján ebből adódik, hogy az $\mathbf{A} \Rightarrow \mathbf{B}$, $\mathbf{A} \wedge \mathbf{B}$ és $\mathbf{A}\Leftrightarrow\mathbf{B}$ kifejezések szintén formulák.

Legyen f n-változós logikai vagy matematikai függvény és legyenek $\mathbf{T}_1, \ldots, \mathbf{T}_n$ objektumok. Minden $1 \le k \le n$ számra legyen $(\mathbf{A}_{k,1}, \mathbf{A}_{k,2}, \ldots, \mathbf{A}_{k,m_k})$ olyan objektum-formula konstrukció, hogy $\mathbf{T}_k \equiv \mathbf{A}_{k,m_k}$. Nyilvánvaló, hogy a

$$(\mathbf{A}_{1,1}, \mathbf{A}_{1,2}, \ldots, \mathbf{A}_{1,m_1}, \ldots \mathbf{A}_{n,1}, \mathbf{A}_{n,2}, \ldots, \mathbf{A}_{n,m_n}, \mathsf{f}\mathbf{A}_{1,m_1} \ldots \mathbf{A}_{n,m_n})$$

olyan objektum-formula konstrukció, amelyre $\mathsf{f}\mathbf{T}_1 \ldots \mathbf{T}_n \equiv \mathsf{f}\mathbf{A}_{1,m_1} \ldots \mathbf{A}_{n,m_n}$. Ha f logikai (illetve matematikai) függvény, akkor $s\mathbf{T}_1 \ldots \mathbf{T}_n$ másodfajú (illetve elsőfajú) kifejezés, ezért $s\mathbf{T}_1 \ldots \mathbf{T}_n$ formula (illetve objektum).

Legyen $\mathbf{A}$ formula, $\mathbf{x}$ változó, és $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ olyan objektum-formula konstrukció, hogy $\mathbf{A} \equiv \mathbf{A}_n$. Nyilvánvaló, hogy

$$(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \varepsilon_{\mathbf{x}}(\mathbf{A}_n))$$

objektum-formula konstrukció, hiszen $\mathbf{A}_n$ másodfajú, továbbá $\varepsilon_{\mathbf{x}}(\mathbf{A}_n) \equiv \varepsilon_{\mathbf{x}}(\mathbf{A})$ és $\varepsilon_{\mathbf{x}}(\mathbf{A})$ elsőfajú kifejezés, ezért $\varepsilon_{\mathbf{x}}(\mathbf{A})$ objektum. ■

A logikai és matematikai függvényjelek alkalmazásakor gyakran alkalmazzuk a *funkcionális jelölést*, ami azt jelenti, hogy ha $\mathfrak{f}$ n-változós logikai vagy matematikai függvény és $\mathbf{T}_1, \ldots, \mathbf{T}_n$ kifejezések, akkor az $\mathfrak{f}\mathbf{T}_1 \ldots \mathbf{T}_n$ szimbólum helyett azt írjuk, hogy $\mathfrak{f}(\mathbf{T}_1, \ldots, \mathbf{T}_n)$. Ez a jelölés azt sugallja, hogy minden $\mathfrak{f}$ n-változós logikai vagy matematikai függvényhez hozzárendelhető egy olyan függvény, amely a matematikai nyelv minden $(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ kifejezés n-eséhez az $\mathfrak{f}(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ kifejezést rendeli. Az előző állításból látható, hogy ha $\mathfrak{f}$ n-változós logikai (illetve matematikai) függvény, akkor $\mathfrak{f}$-hez hozzárendelhető az a függvény, amely a matematikai nyelv minden $(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ objektum n-eséhez az $\mathfrak{f}(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ formulát (illetve objektumot) rendeli. Mivel a matematikai nyelvekre alapozott matematikai elméletek (amelyekről a 2.3. pontban lesz szó) a nyelv logikai és matematikai függvényeire vonatkozó kijelentések vizsgálatával foglalkoznak; a matematikai elméleteket *függvénykalkulusoknak* is szokták nevezni.

Kétváltozós logikai és matematikai függvények esetében az *infix jelölés* is használatos, ami azt jelenti, hogy ha $\mathfrak{f}$ kétváltozós logikai vagy matematikai függvény és $\mathbf{T}$, $\mathbf{S}$ kifejezések, akkor $\mathfrak{f}\mathbf{TS}$ vagy $\mathfrak{f}(\mathbf{T}, \mathbf{S})$ helyett azt írjuk, hogy $\mathbf{T}\ \mathfrak{f}\ \mathbf{S}$. Szinte mindig infix jelölést alkalmazunk az $=$ függvény esetében, tehát ha $\mathbf{T}$, $\mathbf{S}$ kifejezések, akkor $= \mathbf{TS}$ helyett azt írjuk, hogy $\mathbf{T} = \mathbf{S}$, továbbá a $\neg = \mathbf{TS}$ kifejezést a $\mathbf{T} \neq \mathbf{S}$ szimbólummal jelöljük.

2.1.11. Tétel. (**A helyettesítés tétele.**) *Ha* $\mathbf{A}$ *formula* (*illetve objektum*), $\mathbf{T}$ *objektum és* $\mathbf{x}$ *változó, akkor* $(\mathbf{T}|\mathbf{x})\mathbf{A}$ *formula* (*illetve objektum*).

Bizonyítás. (I) Először megmutatjuk, hogy ha $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ objektum-formula konstrukció és $\mathbf{x}$, $\mathbf{y}$ olyan változók, hogy $\mathbf{y}$ nem szerepel az $\mathbf{A}_k$ $(1 \leq k \leq n)$ kifejezések egyikében sem, akkor $((\mathbf{y}|\mathbf{x})\mathbf{A}_1, (\mathbf{y}|\mathbf{x})\mathbf{A}_2, \ldots, (\mathbf{y}|\mathbf{x})\mathbf{A}_n)$ szintén objektum-formula konstrukció. Legyen $1 \leq k \leq n$ rögzítve.

Tegyük fel, hogy $\mathbf{A}_k$-ra (1) teljesül. Ha $\mathbf{A}_k$ változó, akkor $\mathbf{A}_k \equiv \mathbf{x}$ esetén $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{y}$, ugyanakkor ha $\mathbf{A}_k$ nem azonos $\mathbf{x}$-szel, akkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{A}_k$, tehát $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ változó. Ha $\mathbf{A}_k$ konstans, akkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{A}_k$, mert konstansban nem szerepel változó, így $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ konstans. Tehát $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$-ra (1) teljesül.

Tegyük fel, hogy $\mathbf{A}_k$-ra (2) teljesül, és legyen $1 \leq j < k$ olyan szám, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \neg\mathbf{A}_j$. Ekkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \neg(\mathbf{y}|\mathbf{x})\mathbf{A}_j$ és $(\mathbf{y}|\mathbf{x})\mathbf{A}_j$ másodfajú, ezért $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$-ra (2) teljesül.

Tegyük fel, hogy $\mathbf{A}_k$-ra (3) teljesül, és legyenek $1 \leq i, j < k$ olyan számok, hogy $\mathbf{A}_i$ és $\mathbf{A}_j$ másodfajúak és $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$. Ekkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \vee(\mathbf{y}|\mathbf{x})\mathbf{A}_i(\mathbf{y}|\mathbf{x})A_j$ és $(\mathbf{y}|\mathbf{x})\mathbf{A}_i$, valamint $(\mathbf{y}|\mathbf{x})\mathbf{A}_j$ másodfajúak, ezért $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$-ra (3) teljesül.

Tegyük fel, hogy $\mathbf{A}_k$-ra (4) teljesül, és legyen $1 \leq j < k$ olyan szám és $\mathbf{z}$ olyan változó, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \varepsilon_{\mathbf{z}}(\mathbf{A}_j)$. Ekkor három eset lehetséges.

• $\mathbf{z}$ különbözik $\mathbf{x}$-től és $\mathbf{y}$-tól; ekkor az ε-kifejezésekre vonatkozó helyettesítési szabály szerint $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv (\mathbf{y}|\mathbf{x})\varepsilon_{\mathbf{z}}(\mathbf{A}_j) \equiv \varepsilon_{\mathbf{z}}((\mathbf{y}|\mathbf{x})\mathbf{A}_j)$, tehát $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$-ra (4) teljesül.

• $\mathbf{z}$ különbözik $\mathbf{y}$-tól és $\mathbf{z} \equiv \mathbf{x}$; ekkor $\mathbf{x}$ nem szerepel $\mathbf{A}_k$-ban, hiszen $\mathbf{A}_k \equiv \varepsilon_{\mathbf{z}}(\mathbf{A}_j)$ és $\mathbf{z}$ nem szerepel $\varepsilon_{\mathbf{z}}(\mathbf{A}_j)$-ben. Ezért $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{A}_k \equiv \varepsilon_{\mathbf{x}}(\mathbf{A}_j)$ és a feltevés szerint $\mathbf{y}$ nem szerepel $\mathbf{A}_j$-ben, így az ε-kifejezésekre vonatkozó helyettesítések tranzitivitásának szabályát alkalmazva $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \varepsilon_{\mathbf{x}}(\mathbf{A}_j) \equiv \varepsilon_{\mathbf{y}}((\mathbf{y}|\mathbf{x})\mathbf{A}_j)$, így $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$-ra (4) teljesül.

• $\mathbf{z} \equiv \mathbf{y}$; ekkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv (\mathbf{y}|\mathbf{x})\varepsilon_{\mathbf{z}}(\mathbf{A}_j) \equiv \varepsilon_{\mathbf{y}}(\mathbf{A}_j) \equiv (\mathbf{y}|\mathbf{x})(\varepsilon\mathbf{A}_j) \equiv \varepsilon(\mathbf{y}|\mathbf{x})\mathbf{A}_j$, mert $\mathbf{y}$ nem szerepel $\mathbf{A}_j$-ben, ugyanakkor $\varepsilon(\mathbf{y}|\mathbf{x})\mathbf{A}_j \equiv \varepsilon_u((\mathbf{y}|\mathbf{x})\mathbf{A}_j)$, ahol $\mathbf{u}$ tetszőleges olyan változó, amely $\mathbf{y}$-tól különbözik és nem szerepel $\mathbf{A}_j$-ben; tehát $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$-ra (4) teljesül.

Tegyük fel, hogy $\mathbf{A}_k$-ra (5) teljesül, és legyen $\mathfrak{f}$ olyan m-változós logikai (illetve matematikai) függvény és legyenek $1 \le j_1, \ldots, j_m < k$ olyan számok, hogy minden $1 \le p \le m$ számra $\mathbf{A}_{j_p}$ elsőfajú és $\mathbf{A}_k \equiv \mathfrak{f}\mathbf{A}_{j_1} \ldots \mathbf{A}_{j_m}$. Az $\mathbf{x}$ változó nem szerepel $\mathfrak{f}$-ben, így $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathfrak{f}(\mathbf{y}|\mathbf{x})\mathbf{A}_{j_1} \ldots (\mathbf{y}|\mathbf{x})\mathbf{A}_{j_m}$, ezért $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$-ra (5) teljesül.

(II) Most megmutatjuk, hogy ha $\mathbf{A}$ formula (illetve objektum) és $\mathbf{x}$, $\mathbf{y}$ változók, akkor az $(\mathbf{y}|\mathbf{x})\mathbf{A}$ kifejezés formula (illetve objektum). Ehhez legyen $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ olyan objektum-formula konstrukció, hogy $\mathbf{A} \equiv \mathbf{A}_n$. Azt fogjuk bizonyítani, hogy minden $1 \le k \le n$ számra: ha $\mathbf{A}_k$ formula (illetve objektum), akkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ szintén formula (illetve objektum).

Az $\mathbf{A}_1$ kifejezés csakis változó vagy konstans lehet; ekkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_1$ is változó vagy konstans, tehát objektum.

Legyen a $1 \le k \le n$ szám rögítve, és tegyük fel, hogy minden $1 \le j < k$ számra: ha $\mathbf{A}_j$ formula (illetve objektum), akkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_j$ szintén formula (illetve objektum). Meg fogjuk mutatni, hogy ha $\mathbf{A}_k$ formula (illetve objektum), akkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ szintén formula (illetve objektum).

Tegyük fel először, hogy $\mathbf{A}_k$ formula. Ekkor $\mathbf{A}_k$ másodfajú, és a következő esetek lehetségesek:

- $\mathbf{A}_k$-ra (2) teljesül; legyen $1 \le j < k$ olyan szám, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \neg\mathbf{A}_j$. Ekkor $\mathbf{A}_j$ formula, tehát a hipotézis alapján $(\mathbf{y}|\mathbf{x})\mathbf{A}_j$ formula, továbbá $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \neg((\mathbf{y}|\mathbf{x})\mathbf{A}_j)$, így $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ formula.
- $\mathbf{A}_k$-ra (3) teljesül; legyenek $1 \le i, j < k$ olyan számok, hogy $\mathbf{A}_i$ és $\mathbf{A}_j$ másodfajúak és $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$. Ekkor $\mathbf{A}_i$ és $\mathbf{A}_j$ formulák, tehát a hipotézis alapján $(\mathbf{y}|\mathbf{x})\mathbf{A}_i$ és $(\mathbf{y}|\mathbf{x})\mathbf{A}_j$ formulák, továbbá $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \vee((\mathbf{y}|\mathbf{x})\mathbf{A}_i)((\mathbf{y}|\mathbf{x})\mathbf{A}_j)$, így $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ formula.
- $\mathbf{A}_k$-ra (5) teljesül; legyen $\mathfrak{f}$ olyan m-változós logikai függvény és tegyük fel, hogy $1 \le j_1, \ldots, j_m < k$ olyan számok, hogy minden $1 \le p \le m$ számra $\mathbf{A}_{j_p}$ elsőfajú és $\mathbf{A}_k \equiv \mathfrak{f}\mathbf{A}_{j_1} \ldots \mathbf{A}_{j_m}$. Ekkor minden $1 \le p \le m$ számra $\mathbf{A}_{j_p}$ objektum, tehát a hipotézis alapján minden $1 \le p \le m$ számra $(\mathbf{y}|\mathbf{x})\mathbf{A}_{j_p}$ objektum. Ugyanakkor nyilvánvaló, hogy $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathfrak{f}((\mathbf{y}|\mathbf{x})\mathbf{A}_{j_1}) \ldots ((\mathbf{y}|\mathbf{x})\mathbf{A}_{j_m})$, tehát az előző állítás alapján $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ formula.

Tegyük most fel, hogy $\mathbf{A}_k$ objektum. Ekkor $\mathbf{A}_k$ elsőfajú, és a következő esetek lehetségesek:

- $\mathbf{A}_k$-ra (1) teljesül, vagyis $\mathbf{A}_k$ változó vagy konstans. Ekkor $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ is változó vagy konstans, tehát objektum.
- $\mathbf{A}_k$-ra (4) teljesül; legyen $1 \le j < k$ olyan szám és $\mathbf{z}$ olyan változó, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \varepsilon_{\mathbf{z}}(\mathbf{A}_j)$. Ekkor $\mathbf{A}_j$ formula, tehát a hipotézis alapján $(\mathbf{y}|\mathbf{x})\mathbf{A}_j$ is formula. Három eset lehetséges:

– $\mathbf{z}$ különbözik $\mathbf{x}$-től és $\mathbf{y}$-tól; ekkor az ε-kifejezésekre vonatkozó helyettesítési szabály szerint $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv (\mathbf{y}|\mathbf{x})\varepsilon_{\mathbf{z}}(\mathbf{A}_j) \equiv \varepsilon_{\mathbf{z}}((\mathbf{y}|\mathbf{x})\mathbf{A}_j)$, tehát az előző állítás szerint $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ objektum.

– $\mathbf{z}$ különbözik $\mathbf{y}$-tól és $\mathbf{z} \equiv \mathbf{x}$; ekkor $\mathbf{x}$ nem szerepel $\mathbf{A}_k$-ban, hiszen $\mathbf{A}_k \equiv \varepsilon_{\mathbf{z}}(\mathbf{A}_j)$ és $\mathbf{z}$ nem szerepel $\varepsilon_{\mathbf{z}}(\mathbf{A}_j)$-ben. Ezért $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{A}_k$, tehát $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ objektum.

– $\mathbf{z} \equiv \mathbf{y}$; ekkor legyen $\mathbf{u}$ olyan változó, amely $\mathbf{x}$-től és $\mathbf{y}$-tól különbözik, továbbá nem szerepel az $\mathbf{A}_1, \ldots, \mathbf{A}_j$ kifejezések egyikében sem. Az (I) alapján $((\mathbf{u}|\mathbf{y})\mathbf{A}_1, \ldots, (\mathbf{u}|\mathbf{y})\mathbf{A}_j)$ objektum-formula konstrukció, és szintén az (I) szerint $((\mathbf{y}|\mathbf{x})(\mathbf{u}|\mathbf{y})\mathbf{A}_1, \ldots, (\mathbf{y}|\mathbf{x})(\mathbf{u}|\mathbf{y})\mathbf{A}_j)$ is objektum-formula konstrukció, hiszen $\mathbf{y}$ nem szerepel az $(\mathbf{u}|\mathbf{y})\mathbf{A}_1, \ldots, (\mathbf{u}|\mathbf{y})\mathbf{A}_j$ kifejezések egyikében sem. Világos, hogy $(\mathbf{u}|\mathbf{y})\mathbf{A}_j$ és $(\mathbf{y}|\mathbf{x})(\mathbf{u}|\mathbf{y})\mathbf{A}_j$ másodfajú kifejezések, mert $\mathbf{A}_j$ másodfajú, hiszen formula. Ezért $(\mathbf{y}|\mathbf{x})(\mathbf{u}|\mathbf{y})\mathbf{A}_j$ is formula, ugyanakkor az ε-

kifejezésekre vonatkozó helyettesítések tranzitivitásának szabálya és az ε-kifejezésekre vonatkozó helyettesítés szabály szerint

$$(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv (\mathbf{y}|\mathbf{x})\varepsilon_z(\mathbf{A}_j) \equiv \varepsilon_y(\mathbf{A}_j) \equiv (\mathbf{y}|\mathbf{x})\varepsilon_u((\mathbf{u}|\mathbf{y})\mathbf{A}_j) \equiv \varepsilon_u((\mathbf{y}|\mathbf{x})(\mathbf{u}|\mathbf{y})\mathbf{A}_j),$$

mert $\mathbf{u}$ különbözik $\mathbf{x}$-től és $\mathbf{y}$-tól, és $\mathbf{u}$ nem szerepel $\mathbf{A}_j$-ben. Ebből következik, hogy $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ objektum.

• $\mathbf{A}_k$-ra (5) teljesül; legyen $\mathfrak{f}$ olyan m-változós matematikai függvény és tegyük fel, hogy $1 \leq j_1, \ldots, j_m < k$ olyan számok, hogy minden $1 \leq p \leq m$ számra $\mathbf{A}_{j_p}$ elsőfajú és $\mathbf{A}_k \equiv \mathfrak{f}\mathbf{A}_{j_1} \ldots \mathbf{A}_{j_m}$. Ekkor minden $1 \leq p \leq m$ számra $\mathbf{A}_{j_p}$ objektum, tehát a hipotézis alapján minden $1 \leq p \leq m$ számra $(\mathbf{y}|\mathbf{x})\mathbf{A}_{j_p}$ objektum. Ugyanakkor nyilvánvaló, hogy $(\mathbf{y}|\mathbf{x})\mathbf{A}_k \equiv \mathfrak{f}((\mathbf{y}|\mathbf{x})\mathbf{A}_{j_1}) \ldots ((\mathbf{y}|\mathbf{x})\mathbf{A}_{j_m})$, így az előző állítás alapján $(\mathbf{y}|\mathbf{x})\mathbf{A}_k$ objektum.

(III) Legyen $\mathbf{A}$ formula (illetve objektum), $\mathbf{T}$ objektum, $\mathbf{x}$ változó, és $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ olyan objektum-formula konstrukció, hogy $\mathbf{A} \equiv \mathbf{A}_n$. Tegyük fel továbbá, hogy egyetlen $\mathbf{T}$-ben szereplő változó sem szerepel az $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ kifejezések egyikében sem. Megmutatjuk, hogy ekkor a $(\mathbf{T}|\mathbf{x})\mathbf{A}$ kifejezés formula (illetve objektum). Azt fogjuk bizonyítani, hogy minden $1 \leq k \leq n$ számra: ha $\mathbf{A}_k$ formula (illetve objektum), akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ formula (illetve objektum).

Az $\mathbf{A}_1$ kifejezés csakis változó vagy konstans lehet; ekkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_1$ is változó vagy konstans, tehát objektum.

Legyen a $1 \leq k \leq n$ szám rögítve, és tegyük fel, hogy minden $1 \leq j < k$ számra: ha $\mathbf{A}_j$ formula (illetve objektum), akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$ szintén formula (illetve objektum). Megmutatjuk, hogy ha $\mathbf{A}_k$ formula (illetve objektum), akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ szintén formula (illetve objektum).

Tegyük fel először, hogy $\mathbf{A}_k$ formula. Ekkor $\mathbf{A}_k$ másodfajú, és a következő esetek lehetségesek:

• $\mathbf{A}_k$-ra (2) teljesül; legyen $1 \leq j < k$ olyan szám, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \neg\mathbf{A}_j$. Ekkor $\mathbf{A}_j$ formula, tehát a hipotézis alapján $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$ formula, továbbá $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \neg((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$, így $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ formula.

• $\mathbf{A}_k$-ra (3) teljesül; legyenek $1 \leq i, j < k$ olyan számok, hogy $\mathbf{A}_i$ és $\mathbf{A}_j$ másodfajúak és $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$. Ekkor $\mathbf{A}_i$ és $\mathbf{A}_j$ formulák, tehát a hipotézis alapján $(\mathbf{T}|\mathbf{x})\mathbf{A}_i$ és $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$ formulák, továbbá $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \vee((\mathbf{T}|\mathbf{x})\mathbf{A}_i)((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$, így $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ formula.

• $\mathbf{A}_k$-ra (5) teljesül; legyen $\mathfrak{f}$ olyan m-változós logikai függvény és tegyük fel, hogy $1 \leq j_1, \ldots, j_m < k$ olyan számok, hogy minden $1 \leq p \leq m$ számra $\mathbf{A}_{j_p}$ elsőfajú és $\mathbf{A}_k \equiv \mathfrak{f}\mathbf{A}_{j_1} \ldots \mathbf{A}_{j_m}$. Ekkor minden $1 \leq p \leq m$ számra $\mathbf{A}_{j_p}$ objektum, tehát a hipotézis alapján minden $1 \leq p \leq m$ számra $(\mathbf{T}|\mathbf{x})\mathbf{A}_{j_p}$ objektum. Ugyanakkor nyilvánvaló, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \mathfrak{f}((\mathbf{T}|\mathbf{x})\mathbf{A}_{j_1}) \ldots ((\mathbf{T}|\mathbf{x})\mathbf{A}_{j_m})$, tehát az előző állítás alapján $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ formula.

Tegyük most fel, hogy $\mathbf{A}_k$ objektum. Ekkor $\mathbf{A}_k$ elsőfajú, és a következő esetek lehetségesek:

• $\mathbf{A}_k$-ra (1) teljesül, vagyis $\mathbf{A}_k$ változó vagy konstans. Ekkor $\mathbf{A}_1 \equiv \mathbf{x}$ esetén $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{T}$, tehát $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ objektum, ugyanakkor, ha $\mathbf{A}_1$ nem azonos $\mathbf{x}$-szel, akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{A}_k$, tehát $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ konstans, így objektum.

• $\mathbf{A}_k$-ra (4) teljesül; legyen $1 \leq j < k$ olyan szám és $\mathbf{z}$ olyan változó, hogy $\mathbf{A}_j$ másodfajú és $\mathbf{A}_k \equiv \varepsilon_{\mathbf{z}}(\mathbf{A}_j)$. Ekkor $\mathbf{A}_j$ formula, tehát a hipotézis alapján $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$ is formula. Három eset lehetséges:

– $\mathbf{z}$ különbözik $\mathbf{x}$-től és nem szerepel $\mathbf{T}$-ben; ekkor az ε-kifejezésekre vonatkozó helyettesítési szabály szerint $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv (\mathbf{T}|\mathbf{x})\varepsilon_{\mathbf{z}}(\mathbf{A}_j) \equiv \varepsilon_{\mathbf{z}}((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$, tehát az előző állítás szerint $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ objektum.

– $\mathbf{z} \equiv \mathbf{x}$; ekkor $\mathbf{x}$ nem szerepel $\mathbf{A}_k$-ban, hiszen $\mathbf{A}_k \equiv \varepsilon_{\mathbf{z}}(\mathbf{A}_j)$ és $\mathbf{z}$ nem szerepel $\varepsilon_{\mathbf{z}}(\mathbf{A}_j)$-ben. Ezért $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \mathbf{A}_k$, így $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ objektum.

– $\mathbf{z}$ szerepel $\mathbf{T}$-ben; ekkor a fekltevés szerint $\mathbf{z}$ nem szerepel az $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ kifejezések egyikében sem, így $\mathbf{A}_k \equiv \varepsilon_{\mathbf{z}}(\mathbf{A}_j) \equiv \varepsilon\mathbf{A}_j$, tehát $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \varepsilon((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$. Ha $\mathbf{u}$ olyan változó, amely $\mathbf{T}$-ben és $\mathbf{A}_j$-ben nem szerepel, akkor $\mathbf{u}$ nem szerepel $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$-ben sem, következésképpen $\varepsilon(\mathbf{T}|\mathbf{x})\mathbf{A}_j \equiv \varepsilon_u((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$. De tudjuk, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$ formula, tehát az előző állítás szerint $\varepsilon_u((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$ objektum, így $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ objektum.

- $\mathbf{A}_k$-ra (5) teljesül; legyen $\mathfrak{f}$ olyan m-változós matematikai függvény és tegyük fel, hogy $1 \le j_1, \ldots, j_m < k$ olyan számok, hogy minden $1 \le p \le m$ számra $\mathbf{A}_{j_p}$ elsőfajú és $\mathbf{A}_k \equiv \mathfrak{f}\mathbf{A}_{j_1} \ldots \mathbf{A}_{j_m}$. Ekkor minden $1 \le p \le m$ számra $\mathbf{A}_{j_p}$ objektum, tehát a hipotézis alapján minden $1 \le p \le m$ számra $(\mathbf{T}|\mathbf{x})\mathbf{A}_{j_p}$ objektum. Ugyanakkor nyilvánvaló, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \mathfrak{f}((\mathbf{T}|\mathbf{x})\mathbf{A}_{j_1}) \ldots ((\mathbf{T}|\mathbf{x})\mathbf{A}_{j_m})$, tehát az előző állítás alapján $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ objektum.

(IV) Áttérve az általános esetre; legyen $\mathbf{A}$ formula (illetve objektum), $\mathbf{T}$ objektum, $\mathbf{x}$ változó és $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ olyan objektum-formula konstrukció, hogy $\mathbf{A} \equiv \mathbf{A}_n$.

Ha $\mathbf{T}$-ben nem szerepel változó, akkor a (III) feltételei teljesülnek, így a $(\mathbf{T}|\mathbf{x})\mathbf{A}$ kifejezés formula (illetve objektum).

Tegyük fel, hogy $\mathbf{T}$-ben szerepel valamelyik változó, és jelölje $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ az összes $\mathbf{T}$-ben szereplő változót. Legyen $(\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m)$ olyan változó m-es, hogy minden $1 \le k \le m$ esetén $\mathbf{y}_k$ az $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ változók mindegyikétől különbözik és $\mathbf{y}_k$ nem szerepel az $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ kifejezések egyikében sem. A (II) alapján $(\mathbf{y}_1|\mathbf{x}_1) \ldots (\mathbf{y}_m|\mathbf{x}_m)\mathbf{T}$ objektum, továbbá a helyettesítések felcserélésének szabálya szerint

$$(\mathbf{T}|\mathbf{x})\mathbf{A} \equiv (\mathbf{x}_1|\mathbf{y}_1) \ldots (\mathbf{x}_m|\mathbf{y}_m)(((\mathbf{y}_1|\mathbf{x}_1) \ldots (\mathbf{y}_m|\mathbf{x}_m)\mathbf{T}|\mathbf{x})\mathbf{A})$$

Tehát ha $\mathbf{T}'$ jelöli az $(\mathbf{y}_1|\mathbf{x}_1) \ldots (\mathbf{y}_m|\mathbf{x}_m)\mathbf{T}$ objektumot, és $(\mathbf{T}'|\mathbf{x})\mathbf{A}$ formula (illetve objektum) volna, akkor a (II) alapján kapnánk, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}$ formula (illetve objektum). De a $\mathbf{T}'$ objektumban szereplő változók nem szerepelnek az $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ kifejezések egyikében sem, tehát a (III) szerint $(\mathbf{T}'|\mathbf{x})\mathbf{A}$ formula (illetve objektum). ■

Világos, hogy az imént bizonyított tételnek az az értelme, hogy egy változót objektummal helyettesítve formulában (illetve objektumban) formulát (illetve objektumot) nyerünk. Ez azt is mutatja, hogy ha $\mathbf{A}$ *nem zárt* formula (illetve objektum) egy matematikai nyelvben és $\mathbf{x}_1, \ldots, \mathbf{x}_n$ az $\mathbf{A}$-ben szereplő különböző változók, akkor $\mathbf{A}$-val kapcsolatba hozható az a függvény, amely a matematikai nyelv minden $(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ objektum n-eséhez azt a formulát (illetve objektumot) rendeli, amit úgy kapunk, hogy $\mathbf{A}$-ban minden $1 \le k \le n$ számra $\mathbf{x}_k$ helyére $\mathbf{T}_k$-t helyettesítünk *egyszerre*; ezt a formulát (illetve objektumot) a $(\mathbf{T}_1, \ldots, \mathbf{T}_n|\mathbf{x}_1, \ldots, \mathbf{x}_n)\mathbf{A}$ vagy $\mathbf{A}(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ szimbólummal jelöljük.

2.2. Egzisztenciális és univerzális kvantor

2.2.1. Definíció. (**A kvantorok értelmezése.**) *Ha* $\mathbf{A}$ *kifejezés és* $\mathbf{x}$ *változó egy matematikai nyelvben, akkor*

- $(\exists\mathbf{x})\mathbf{A}$ *jelöli az* $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ *kifejezést;*
- $(\forall\mathbf{x})\mathbf{A}$ *jelöli a* $\neg((\exists\mathbf{x})(\neg\mathbf{A}))$ *kifejezést.*

A $\exists$ (*illetve* $\forall$) *szimbólumot* **egzisztenciális** (*illetve* **univerzális**) **kvantornak** *nevezzük.*

Tehát, ha $\mathbf{A}$ kifejezés és $\mathbf{x}$ változó egy matematikai nyelvben, akkor a definíció alapján

$$(\forall \mathbf{x})\mathbf{A} \equiv \neg((\exists \mathbf{x})(\neg \mathbf{A})) \equiv \neg((\varepsilon_{\mathbf{x}}(\neg \mathbf{A})|\mathbf{x})(\neg \mathbf{A})) \equiv (\varepsilon_{\mathbf{x}}(\neg \mathbf{A})|\mathbf{x})(\neg\neg \mathbf{A}) \equiv \neg\neg(\varepsilon_{\mathbf{x}}(\neg \mathbf{A})|\mathbf{x})\mathbf{A}.$$

Az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ és $\varepsilon_{\mathbf{x}}(\neg \mathbf{A})$ kifejezésekben nem szerepel az $\mathbf{x}$ változó, ezért $\mathbf{x}$ sem a $(\exists \mathbf{x})\mathbf{A}$, sem a $(\forall \mathbf{x})\mathbf{A}$ kifejezésben nem szerepel.

Fontos látni azt, hogy az egzisztenciális és univerzális kvantorok nem tartoznak hozzá a matematikai nyelvek szimbólum-rendszeréhez. Léteznek olyan formális nyelvek (például az *elsőrendű nyelvek*), amelyekben a $\exists$ és $\forall$ szimbólumok logikai operátorok. Az általunk vizsgált matematikai nyelvek szintaxisa szempontjából a kvantoroknak egyelőre csak az a jelentősége, hogy bonyolultabb kifejezések egyszerűsített jelölését teszik lehetővé. Szemantikus szempontból viszont nagyon nagy jelentőségük van; ez majd kiderül a matematikai elméletek tárgyalásakor. Most néhány kijelentést bizonyítunk a kvantoros kifejezések szintaktikus tulajdonságaival kapcsolatban, valamint értelmezzük a *feltételes* (vagy másnéven *restringált*) *kvantorokat.*

2.2.2. Állítás. *Ha* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó egy matematikai nyelvben, akkor a* $(\exists \mathbf{x})\mathbf{A}$ *és* $(\forall \mathbf{x})\mathbf{A}$ *kifejezések formulák.*

Bizonyítás. Az $\mathbf{A}$, $\neg \mathbf{A}$ és $\neg\neg \mathbf{A}$ kifejezések formulák, ezért az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ és $\varepsilon_{\mathbf{x}}(\neg \mathbf{A})$ kifejezések objektumok, így a helyettesítés tétele alapján $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ (vagyis $(\exists \mathbf{x})\mathbf{A}$) és $(\varepsilon_{\mathbf{x}}(\neg \mathbf{A})|\mathbf{x})(\neg\neg \mathbf{A})$ (vagyis $(\forall \mathbf{x})\mathbf{A}$) formula. ■

2.2.3. Állítás. (**A változók helyettesítésének szabálya kvantoros kifejezésekben.**) *Legyenek* $\mathbf{A}$, $\mathbf{T}$ *kifejezések és* $\mathbf{x}$, $\mathbf{y}$ *különböző változók egy matematikai nyelvben. Ha* $\mathbf{x}$ *nem szerepel* $\mathbf{T}$*-ben, akkor*

$$(\mathbf{T}|\mathbf{y})((\exists \mathbf{x})\mathbf{A}) \equiv (\exists \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}),$$
$$(\mathbf{T}|\mathbf{y})((\forall \mathbf{x})\mathbf{A}) \equiv (\forall \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}).$$

Bizonyítás. Az ε-kifejezésekre vonatkozó helyettesítési szabály szerint

$$(\mathbf{T}|\mathbf{y})(\varepsilon_{\mathbf{x}}(\mathbf{A})) \equiv \varepsilon_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A}),$$

tehát az egzisztenciális kvantor definíciója és a helyettesítések felcserélésének szabálya alapján

$$\begin{aligned}(\mathbf{T}|\mathbf{y})((\exists \mathbf{x})\mathbf{A}) &\equiv (\mathbf{T}|\mathbf{y})((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}) \equiv ((\mathbf{T}|\mathbf{y})(\varepsilon_{\mathbf{x}}(\mathbf{A}))|\mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}) \equiv \\ &\equiv (\varepsilon_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A})|\mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}) \equiv (\exists \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}).\end{aligned}$$

Ebből következik, hogy

$$\begin{aligned}(\mathbf{T}|\mathbf{y})((\forall \mathbf{x})\mathbf{A}) &\equiv (\mathbf{T}|\mathbf{y})(\neg((\exists \mathbf{x})(\neg \mathbf{A}))) \equiv \neg((\mathbf{T}|\mathbf{y})((\exists \mathbf{x})(\neg \mathbf{A}))) \equiv \\ &\equiv \neg((\exists \mathbf{x})((\mathbf{T}|\mathbf{y})(\neg \mathbf{A}))) \equiv \neg((\exists \mathbf{x})(\neg((\mathbf{T}|\mathbf{y})\mathbf{A}))) \equiv (\forall \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}),\end{aligned}$$

amint állítottuk. ■

2.2.4. Állítás. (**A kvantoros kifejezésekre vonatkozó helyettesítések tranzitivitásának szabálya.**) *Legyenek* $\mathbf{x}$*,* $\mathbf{y}$ *változók és* $\mathbf{A}$ *kifejezés egy matematikai nyelvben. Ha* $\mathbf{y}$ *nem szerepel* $\mathbf{A}$*-ban, akkor*

$$(\exists \mathbf{x})\mathbf{A} \equiv (\exists \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}),$$
$$(\forall \mathbf{x})\mathbf{A} \equiv (\forall \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}).$$

Bizonyítás. Feltehető, hogy $\mathbf{y}$ különbözik $\mathbf{x}$-től. Alkalmazva a helyettesítések tranzitivitásának szabályát ε-kifejezésekben azt kapjuk, hogy $\varepsilon_{\mathbf{y}}((\mathbf{y}|\mathbf{x})\mathbf{A}) \equiv \varepsilon_{\mathbf{x}}(\mathbf{A})$, ugyanakkor $\mathbf{x}$ nem szerepel $\varepsilon_{\mathbf{x}}(\mathbf{A})$-ban és $\mathbf{y}$ nem szerepel $\mathbf{A}$-ban, tehát a helyettesítések felcserélésének szabálya szerint

$$(\exists \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}) \equiv (\varepsilon_{\mathbf{y}}((\mathbf{y}|\mathbf{x})\mathbf{A})|\mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}) \equiv (\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}) \equiv$$

$$\equiv ((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{y})\mathbf{y}|\mathbf{x})((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{y})\mathbf{A}) \equiv (\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A} \equiv (\exists \mathbf{x})\mathbf{A}.$$

Ebből következik, hogy

$$(\forall \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}) \equiv \neg((\exists \mathbf{x})(\neg((\mathbf{y}|\mathbf{x})\mathbf{A}))) \equiv \neg((\exists \mathbf{x})((\mathbf{y}|\mathbf{x})(\neg \mathbf{A}))) \equiv \neg((\exists \mathbf{x})(\neg \mathbf{A})) \equiv (\forall \mathbf{x})\mathbf{A},$$

amint állítottuk. ■

2.2.5. Definíció. (**A feltételes kvantorok értelmezése.**) *Ha* $\mathbf{A}$*,* $\mathbf{B}$ *kifejezések és* $\mathbf{x}$ *változó egy matematikai nyelvben, akkor*

- $(\exists_{\mathbf{B}} \mathbf{x})\mathbf{A}$ *jelöli a* $(\exists \mathbf{x})(\mathbf{B} \wedge \mathbf{A})$ *kifejezést;*
- $(\forall_{\mathbf{B}} \mathbf{x})\mathbf{A}$ *jelöli a* $\neg((\exists_{\mathbf{B}} \mathbf{x})(\neg \mathbf{A}))$ *kifejezést.*

A $\exists_{\mathbf{B}}$ *(illetve* $\forall_{\mathbf{B}}$*) jelet* $\mathbf{B}$**-feltételű egzisztenciális** (*illetve* **univerzális**) **kvantornak** *nevezzük.*

Az előzőek alapján nyilvánvaló, hogy ha $\mathbf{A}$, $\mathbf{B}$ formulák és $\mathbf{x}$ változó egy matematikai nyelvben, akkor $(\exists_{\mathbf{B}} \mathbf{x})\mathbf{A}$ szintén formula, így $(\forall_{\mathbf{B}} \mathbf{x})\mathbf{A}$ is formula. Továbbá, a konjunkció és az implikáció értelmezése alapján

$$(\forall_{\mathbf{B}} \mathbf{x})\mathbf{A} \equiv \neg((\exists_{\mathbf{B}} \mathbf{x})(\neg \mathbf{A})) \equiv \neg((\exists \mathbf{x})(\mathbf{B} \wedge (\neg \mathbf{A}))) \equiv$$
$$\equiv \neg((\exists \mathbf{x})(\neg((\neg \mathbf{B}) \vee (\neg(\neg \mathbf{A}))))) \equiv (\forall \mathbf{x})(\mathbf{B} \Rightarrow (\neg\neg \mathbf{A})).$$

A feltételes kvantorok értelmezése, valamint a kvantoros kifejezésekre vonatkozó helyettesítési szabályok alapján kapjuk, hogy ha $\mathbf{x}$, $\mathbf{y}$ különböző változók és $\mathbf{A}$, $\mathbf{B}$, $\mathbf{T}$ kifejezések egy matematikai nyelvben, és $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben, akkor

$$(\mathbf{T}|\mathbf{y})((\exists_{\mathbf{B}} \mathbf{x})\mathbf{A}) \equiv (\exists_{(\mathbf{T}|\mathbf{y})\mathbf{B}} \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}),$$
$$(\mathbf{T}|\mathbf{y})((\forall_{\mathbf{B}} \mathbf{x})\mathbf{A}) \equiv (\forall_{(\mathbf{T}|\mathbf{y})\mathbf{B}} \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}),$$

tehát ha $\mathbf{y}$ nem szerepel $\mathbf{B}$-ben (a *feltételben*), akkor

$$(\mathbf{T}|\mathbf{y})((\exists_{\mathbf{B}} \mathbf{x})\mathbf{A}) \equiv (\exists_{\mathbf{B}} \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}),$$
$$(\mathbf{T}|\mathbf{y})((\forall_{\mathbf{B}} \mathbf{x})\mathbf{A}) \equiv (\forall_{\mathbf{B}} \mathbf{x})((\mathbf{T}|\mathbf{y})\mathbf{A}).$$

2.3. A matematikai elméletek axiómarendszere

Egy *axiomatikus matematikai elmélet* definíciója két lépésben történik. Először rögzítünk egy formális matematikai nyelvet, amelyet a szóban forgó matematikai elmélet nyelvének nevezünk, majd megadunk egy konkrét (axiomatikus) szabályt, amelynek segítségével a nyelv formulái közül kiválaszthatók a *tételek*, vagyis az elmélet *igaznak* minősített formulái.

A továbbiakban kizárólag axiomatikus matematikai elméletekről lesz szó, ezért az "axiomatikus" jelzőt elhagyjuk.

A matematikai elméletek nyelve elméletről-elméletre változhat. Az elmélethez tartozó nyelvben adjuk meg azokat a logikai és matematikai függvényeket, amelyek segítségével megfogalmazhatók az elmélet *értelmes* kifejezései: az objektumok és a formulák. Természetesen az elmélet nyelvében sok olyan kifejezés is létezik, amely nem objektum és nem formula. A matematikai elméletekben az objektumok és a formulák szerepe hasonló. Az objektumok azért fontosak, mert ezek segítségével lehet nem triviális (tartalmas) formulákat előállítani. A formulák azért fontosak, mert ezek segítségével lehet nem triviális (bonyolult szerkezetű) objektumokat előállítani. Ugyanakkor a formulák azok az értelmes kifejezések, amelyekre az *axiomatikus igazság-fogalmat* értelmezhetjük.

A matematikai elméletekben az igazság-fogalom többféleképpen bevezethető; itt az *axiomatikus* igazság-fogalomról lesz szó. Ennek pontos meghatározásához (ugyanúgy, mint az ítéletkalkulusban) előírjuk a matematikai elmélet formuláinak egy összességét (az *axiómarendszert*), majd megadjuk azt a szabályt, amelynek alkalmazásával az *axiómákból* (vagyis az axiómarendszer elemeiből) előállíthatók a *tételek* (vagyis az *igaz* fomulák). Az ítéletkalkulushoz képest a matematikai elméletek esetében annyival bonyolultabb a helyzet, hogy az axiómarendszer nagymértékben *strukturált*, míg az ítéletkalkulusban az axiómarendszer egyszerűen egy ítélet-összesség volt. Valójában az ítéletkalkulus Hilbert–Ackermann-féle axiómarendszerében is megfigyelhető bizonyos strukturáltság, hiszen ott is minden axióma négy *ítélet-típus* valamelyike lehet. Azonban az ítéletkalkulus esetében ennek nincs különösebb jelentősége, ugyanakkor a matematikai elméletek axiómarendszerének strukturáltsága elvi jelentőségű.

2.3.1. Definíció. *Egy matematikai nyelv formuláinak* $\mathfrak{S}$ *összességét* **formula-sémának** *nevezzük, ha az* $\mathfrak{S}$ *minden* $\mathbf{A}$ *elemére, minden* $\mathbf{x}$ *változóra és minden* $\mathbf{T}$ *objektumra a* $(\mathbf{T}|\mathbf{x})\mathbf{A}$ *formula is eleme* $\mathfrak{S}$*-nek.*

A formula-sémákra előírt követelményt *helyettesítés-invarianciának* is nevezhetjük. Világos, hogy ha $\mathfrak{S}$ olyan formulák összessége, amelyekben egyetlen változó sem szerepel, akkor $\mathfrak{S}$ formula-séma. Az ilyen típusú formula-sémákat *triviálisaknak* mondjuk. Most bevezetjük a matematikai nyelvek hét legfontosabb nem triviális formula-sémáját.

2.3.2. Definíció. (**A logikai formula-sémák értelmezése.**) *Egy matematikai nyelvben*

- $\mathfrak{S}_1$ *jelöli az* $(\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}$ *alakú formulák összességét, ahol* $\mathbf{A}$ *formula;*
- $\mathfrak{S}_2$ *jelöli az* $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ *alakú formulák összességét, ahol* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák;*

- $\mathfrak{S}_3$ *jelöli az* $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})$ *alakú formulák összességét, ahol* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák;*
- $\mathfrak{S}_4$ *jelöli az* $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{B}))$ *alakú formulák összességét, ahol* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák;*
- $\mathfrak{S}_5$ *jelöli a* $((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{A})$ *alakú formulák összességét, ahol* $\mathbf{x}$ *változó,* $\mathbf{T}$ *objektum és* $\mathbf{A}$ *formula;*
- $\mathfrak{S}_6$ *jelöli a* $(\mathbf{T}{=}\mathbf{S}) \Rightarrow (((\mathbf{T}|\mathbf{x})\mathbf{A}) \Leftrightarrow ((\mathbf{S}|\mathbf{x})\mathbf{A}))$ *alakú formulák összességét, ahol* $\mathbf{x}$ *változó,* $\mathbf{T}$, $\mathbf{S}$ *objektumok és* $\mathbf{A}$ *formula;*
- $\mathfrak{S}_7$ *jelöli a* $((\forall \mathbf{x})(\mathbf{A} \Leftrightarrow \mathbf{B})) \Rightarrow (\varepsilon_{\mathbf{x}}(\mathbf{A}) = \varepsilon_{\mathbf{x}}(\mathbf{B}))$ *alakú formulák összességét, ahol* $\mathbf{x}$ *változó és* $\mathbf{A}$, $\mathbf{B}$ *formulák.*

2.3.3. Állítás. *Bármely matematikai nyelvben* $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{S}_6$ *és* $\mathfrak{S}_7$ *formula-sémák.*

Bizonyítás. Legyen $\mathbf{y}$ változó és $\mathbf{R}$ objektum egy rögzített matematikai nyelvben.

(I) Ha $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ formulák, akkor

$$
\begin{aligned}
(\mathbf{R}|\mathbf{y})((\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}) &\equiv (\mathbf{A}' \vee \mathbf{A}') \Rightarrow \mathbf{A}', \\
(\mathbf{R}|\mathbf{y})(\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})) &\equiv (\mathbf{A}' \Rightarrow (\mathbf{A}' \vee \mathbf{B}'), \\
(\mathbf{R}|\mathbf{y})((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})) &\equiv (\mathbf{A}' \vee \mathbf{B}') \Rightarrow (\mathbf{B}' \vee \mathbf{A}') \\
(\mathbf{R}|\mathbf{y})((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{B}))) &\equiv (\mathbf{A}' \Rightarrow \mathbf{B}') \Rightarrow ((\mathbf{C}' \vee \mathbf{A}') \Rightarrow (\mathbf{C}' \vee \mathbf{B}')),
\end{aligned}
$$

ahol $\mathbf{A}' \equiv (\mathbf{R}|\mathbf{y})\mathbf{A}$, $\mathbf{B}' \equiv (\mathbf{R}|\mathbf{y})\mathbf{B}$ és $\mathbf{C}' \equiv (\mathbf{R}|\mathbf{y})\mathbf{C}$. A helyettesítés tétele alapján $\mathbf{A}'$, $\mathbf{B}'$ és $\mathbf{C}'$ formulák, ezért $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$ és $\mathfrak{S}_4$ formula-sémák.

(II) Tegyük fel, hogy $\mathbf{x}$ változó, $\mathbf{A}$ formula és legyen $\mathbf{D} \equiv ((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{A})$. Megmutatjuk, hogy $(\mathbf{R}|\mathbf{y})\mathbf{D}$ eleme $\mathfrak{S}_5$-nek. Nyivánvaló, hogy

$$
(\mathbf{R}|\mathbf{y})\mathbf{D} \equiv (\mathbf{R}|\mathbf{y})(((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{A})) \equiv ((\mathbf{R}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{R}|\mathbf{y})((\exists \mathbf{x})(\mathbf{A})).
$$

Legyen $\mathbf{x}'$ olyan változó, amely $\mathbf{y}$-tól különbözik és nem szerepel az $\mathbf{A}$ és $\mathbf{R}$ kifejezésekben. Ekkor a helyettesítések tranzitivitásának és felcserélésének szabálya szerint

$$
(\mathbf{R}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv (\mathbf{R}|\mathbf{y})((\mathbf{T}|\mathbf{x}')(\mathbf{x}'|\mathbf{x})\mathbf{A}) \equiv (((\mathbf{R}|\mathbf{y})\mathbf{T})|\mathbf{x}')((\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})).
$$

Ugyanakkor a kvantorokra vonatkozó helyettesítések tranzitivitásának és felcserélésének szabálya szerint

$$
(\mathbf{R}|\mathbf{y})((\exists \mathbf{x})(\mathbf{A})) \equiv (\mathbf{R}|\mathbf{y})((\exists \mathbf{x}')((\mathbf{x}'|\mathbf{x})\mathbf{A})) \equiv (\exists \mathbf{x}')((\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})).
$$

Ebből következik, hogy

$$
(\mathbf{R}|\mathbf{y})\mathbf{D} \equiv ((\mathbf{T}'|\mathbf{x}')\mathbf{A}') \Rightarrow (\exists \mathbf{x}')(\mathbf{A}'),
$$

ahol $\mathbf{T}' \equiv (\mathbf{R}|\mathbf{y})\mathbf{T}$ és $\mathbf{A}' \equiv (\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})$. A helyettesítés tétele alapján $\mathbf{T}'$ objektum és $\mathbf{A}'$ formula, így $(\mathbf{R}|\mathbf{x})\mathbf{D}$ eleme $\mathfrak{S}_5$-nek.

(III) Legyen $\mathbf{x}$ változó, $\mathbf{A}$ formula, $\mathbf{T}$ és $\mathbf{S}$ objektum, továbbá

$$
\mathbf{D} \equiv (\mathbf{T}{=}\mathbf{S}) \Rightarrow (((\mathbf{T}|\mathbf{x})\mathbf{A}) \Leftrightarrow ((\mathbf{S}|\mathbf{x})\mathbf{A})).
$$

Nyilvánvaló, hogy

$$
(\mathbf{R}|\mathbf{y})\mathbf{D} \equiv (((\mathbf{R}|\mathbf{y})\mathbf{T}) = ((\mathbf{R}|\mathbf{y})\mathbf{S})) \Rightarrow (((\mathbf{R}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})) \Leftrightarrow ((\mathbf{R}|\mathbf{y})((\mathbf{S}|\mathbf{x})\mathbf{A}))).
$$

Legyen $\mathbf{x}'$ olyan változó, amely $\mathbf{y}$-tól különbözik, és az $\mathbf{A}$, $\mathbf{R}$ kifejezésekben nem szerepel. Ekkor a helyettesítések tranzitivitásának és felcserélésének szabálya szerint

$$(\mathbf{R}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv (\mathbf{R}|\mathbf{y})((\mathbf{T}|\mathbf{x}')((\mathbf{x}'|\mathbf{x})\mathbf{A})) \equiv (((\mathbf{R}|\mathbf{y})\mathbf{T})|\mathbf{x}')((\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})),$$

$$(\mathbf{R}|\mathbf{y})((\mathbf{S}|\mathbf{x})\mathbf{A}) \equiv (\mathbf{R}|\mathbf{y})((\mathbf{S}|\mathbf{x}')((\mathbf{x}'|\mathbf{x})\mathbf{A})) \equiv (((\mathbf{R}|\mathbf{y})\mathbf{S})|\mathbf{x}')((\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})).$$

Ebből következik, hogy

$$(\mathbf{R}|\mathbf{y})\mathbf{D} \equiv (\mathbf{T}'{=}\mathbf{S}') \Rightarrow (((\mathbf{T}'|\mathbf{x}')\mathbf{A}')\Leftrightarrow((\mathbf{S}|\mathbf{x}')\mathbf{A}')),$$

ahol $\mathbf{T}'{\equiv}(\mathbf{R}|\mathbf{y})\mathbf{T}$, $\mathbf{S}'{\equiv}(\mathbf{R}|\mathbf{y})\mathbf{S}$ és $\mathbf{A}'{\equiv}(\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})$. A helyettesítés tétele alapján $\mathbf{T}'$ és $\mathbf{S}'$ objektumok, valamint $\mathbf{A}'$ formula, így $(\mathbf{R}|\mathbf{y})\mathbf{D}$ eleme $\mathfrak{S}_6$-nak.

(IV) Legyen $\mathbf{x}$ változó, $\mathbf{A}$, $\mathbf{B}$ formula, továbbá

$$\mathbf{D} \equiv ((\forall\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{B})) \Rightarrow (\varepsilon_{\mathbf{x}}(\mathbf{A}){=}\varepsilon_{\mathbf{x}}(\mathbf{B})).$$

Nyilvánvaló, hogy

$$(\mathbf{R}|\mathbf{y})\mathbf{D} \equiv ((\mathbf{R}|\mathbf{y})((\forall\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{B}))) \Rightarrow ((\mathbf{R}|\mathbf{y})(\varepsilon_{\mathbf{x}}(\mathbf{A})){=}(\mathbf{R}|\mathbf{y})(\varepsilon_{\mathbf{x}}(\mathbf{B}))).$$

Legyen $\mathbf{x}'$ olyan változó, amely $\mathbf{y}$-tól különbözik és nem szerepel az $\mathbf{A}$, $\mathbf{B}$, $\mathbf{R}$ kifejezések egyikében sem. Ekkor a kvantoros kifejezésekre vonatkozó helyettesítések tranzitivitásának és felcserélésének szabályát alkalmazva kapjuk, hogy

$$(\mathbf{R}|\mathbf{y})((\forall\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{B})) \equiv (\mathbf{R}|\mathbf{y})((\forall\mathbf{x}')((\mathbf{x}'|\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{B}))) \equiv$$
$$\equiv(\mathbf{R}|\mathbf{y})((\forall\mathbf{x}')(((\mathbf{x}'|\mathbf{x})\mathbf{A})\Leftrightarrow((\mathbf{x}'|\mathbf{x})\mathbf{B})))\equiv(\forall\mathbf{x}')((\mathbf{R}|\mathbf{y})(((\mathbf{x}'|\mathbf{x})\mathbf{A})\Leftrightarrow((\mathbf{x}'|\mathbf{x})\mathbf{B})))) \equiv$$
$$\equiv (\forall\mathbf{x}')(((\mathbf{R}|\mathbf{y})(\mathbf{x}'|\mathbf{x})\mathbf{A}))\Leftrightarrow((\mathbf{R}|\mathbf{y})(\mathbf{x}'|\mathbf{x})\mathbf{B}))).$$

Ugyanakkor a helyettesítések tranzitivitásának és felcserélésének szabályát alkalmazva ε-kifejezésekben kapjuk, hogy

$$(\mathbf{R}|\mathbf{y})(\varepsilon_{\mathbf{x}}(\mathbf{A})) \equiv (\mathbf{R}|\mathbf{y})(\varepsilon_{\mathbf{x}'}((\mathbf{x}'|\mathbf{x})\mathbf{A})) \equiv \varepsilon_{\mathbf{x}'}((\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A}))),$$

$$(\mathbf{R}|\mathbf{y})(\varepsilon_{\mathbf{x}}(\mathbf{B})) \equiv (\mathbf{R}|\mathbf{y})(\varepsilon_{\mathbf{x}'}((\mathbf{x}'|\mathbf{x})\mathbf{B})) \equiv \varepsilon_{\mathbf{x}'}((\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{B}))).$$

Ebből következik, hogy

$$(\mathbf{R}|\mathbf{y})\mathbf{D} \equiv ((\forall\mathbf{x}')(\mathbf{A}'\Leftrightarrow\mathbf{B}')) \Rightarrow (\varepsilon_{\mathbf{x}'}(\mathbf{A}'){=}\varepsilon_{\mathbf{x}'}(\mathbf{B}')),$$

ahol $\mathbf{A}'{\equiv}(\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A}))$ és $\mathbf{B}'{\equiv}(\mathbf{R}|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{B}))$. A helyettesítés tétele alapján $\mathbf{A}'$ és $\mathbf{B}'$ formulák, ezért $(\mathbf{R}|\mathbf{y})$ eleme $\mathfrak{S}_7$-nek. ■

2.3.4. Definíció. (**A matematikai elméletek értelmezése.**) *Egy* **matematikai elméletnek** *három összetevője van.*

- *Egy matematikai nyelv, amit a matematikai elmélet nyelvének nevezünk.*
- *A választott matematikai nyelv formula-sémáinak bármely olyan összessége, amelynek eleme az $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{S}_6$ és $\mathfrak{S}_7$ formula-séma. Az így kijelölt formula-sémákat a matematikai elmélet* **axióma-sémáinak** *nevezzük. Az $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{S}_6$ és $\mathfrak{S}_7$ formula-sémákat a matematikai elmélet* **logikai axióma-sémáinak** *nevezzük, míg a nem logikai axióma-sémákat a matematikai elmélet* **matematikai axióma-sémáinak** *nevezzük. A matematikai elmélet logikai (illetve matematikai) axióma-sémáinak elemeit a matematikai elmélet* **logikai** (*illetve* **matematikai**) **axiómáinak** *nevezzük.*
- *A választott matematikai nyelv formuláinak egy tetszőleges véges összessége. Az így kijelölt formulákat a matematikai elmélet* **explicit axiómáinak** *nevezzük.*

A matematikai elmélet **axiómáinak** *nevezzük a logikai axiómáit, matematikai axiómáit és az explicit axiómáit.*

Tehát egy matematikai elmélet *specifikálása* azt jelenti, hogy rögzítjük az elmélet nyelvét (vagyis megadjuk a nyelv logikai sajátfüggvényeit és a matematikai függvényeit), továbbá meghatározzuk az axiómáit (vagyis felsoroljuk az explicit axiómáit és megadjuk a matematikai axióma-sémáit). Ebből látható, hogy a lehető legegyszerűbb matematikai elmélet az, amelynek nincs logikai sajátfüggvénye, nincs matematikai függvénye, nincs matematikai axióma-sémája és nincs explicit axiómája. De még ez az elmélet sem teljesen triviális, mert a nyelvének szimbóluma az $=$ logikai függvény, továbbá vannak logikai axióma-sémái: az $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{S}_6$ és $\mathfrak{S}_7$ formula-sémák. Valamivel bonyolultabb matematikai elmélet az, amelynek nyelve tetszőleges matematikai nyelv, de nincs matematikai axióma-sémája és nincs explicit-axiómája; ezekkel részletesebben foglalkozunk majd a 3. fejezetben.

Jelölés. Ha $\mathfrak{T}$ matematikai elmélet, akkor $\mathfrak{T}_0$ jelöli azt a matematikai elméletet, amelynek nyelve megegyezik a $\mathfrak{T}$ nyelvével, de $\mathfrak{T}_0$-nak nincs matematikai axióma-sémája és nincs explicit axiómája. (Tehát $\mathfrak{T}_0$ úgy áll elő $\mathfrak{T}$-ből, hogy megtartva a $\mathfrak{T}$ matematikai nyelvét, töröljük a $\mathfrak{T}$ matematikai axióma-sémáit és explicit axiómáit.)

Gyakran előfordul az, hogy egy matematikai elmélet explicit axiómáiban semmilyen változó nem szerepel. Ekkor az explicit axiómák összessége nyilvánvalóan triviális formula-séma (azaz helyettesítés-invariáns). Ilyen matematikai elmélet például a halmazelmélet, az aritmetika és a síkgeometria. Ez azonban nem jelenti azt, hogy szükségtelen volna olyan matematikai elméletekkel foglalkozni, amelyek explicit axiómáiban szerepelnek változók. Rövidesen látni fogjuk, hogy az alapvető bizonyítási módszerekben (például a dedukció-tétel vagy az indirekt bizonyítás alkalmazásakor) az eredeti matematikai elmélet mellett olyan elméleteket vezetünk be, amelyek explicit axiómáiban szerepelhetnek változók, akkor is, ha az eredeti elmélet explicit axiómáiban egyáltalán nem szerepel változó.

Matematikai elméletben csak *véges sok* explicit axiómát engedünk meg. Ez biztosítja azt, hogy bármely véges sok változóhoz létezzen olyan változó, amely az adott változók mindegyikétől különbözik és nem szerepel az elmélet egyetlen explicit axiómájában sem. Ennek a ténynek néhány állítás bizonyításában jelentősége van.

Matematikai elméletekben különleges szerepe van azoknak a változóknak, amelyek az elmélet explicit axiómáiban szerepelnek. Egy explicit axióma megfogalmaz egy konkrét állítást, amely a benne szereplő változókra vonatkozik, vagyis ezek a változók eleve rendelkeznek egy nem triviális tulajdonsággal (ti. azzal, amit az őket tartalmazó explicit axióma fejez ki). Ezért az explicit axiómákban szereplő változók úgy viselkednek, mintha adott tulajdonságú konstansok volnának, és vigyázni kell akkor, amikor ilyen változót alkalmazunk más formulákban.

2.3.5. Definíció. (**A tétel fogalma.**) *A* $\mathfrak{T}$ *matematikai elmélet* $\mathbf{A}$ *formulája* **bizonyításának** (*vagy* **levezetésének**) *nevezzük a* $\mathfrak{T}$ *formuláinak bármely olyan* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ *n-esét, amelyre* $\mathbf{A}_n \equiv \mathbf{A}$ *és minden* $1 \le k \le n$ *számra a következő feltételek valamelyike teljesül:*

- $\mathbf{A}_k$ *axiómája* $\mathfrak{T}$*-nek, vagyis* $\mathbf{A}_k$ *logikai axióma, matematikai axióma vagy explicit axióma;*
- *léteznek olyan* $1 \le i, j < k$ *számok, hogy* $\mathbf{A}_j \equiv (\mathbf{A}_i \Rightarrow \mathbf{A}_k)$*.*

A $\mathfrak{T}$ *matematikai elmélet* $\mathbf{A}$ *formuláját* **tételnek** (*vagy* **bizonyíthatónak**, *vagy* **levezethetőnek**) *nevezzük, ha létezik* $\mathbf{A}$*-nak bizonyítása* $\mathfrak{T}$*-ben. A* $\mathfrak{T}$ *matematikai elmélet* $\mathbf{A}$

formuláját **cáfolhatónak** *nevezzük* $\mathfrak{T}$*-ben, ha* $\neg\mathbf{A}$ *tétel* $\mathfrak{T}$*-ben.*

2.3.6. Definíció. (**A logikai tétel fogalma.**) *A* $\mathfrak{T}$ *matematikai elmélet* $\mathbf{A}$ *formulája* **logikai bizonyításának** (*vagy* **logikai levezetésének**) *nevezzük a* $\mathfrak{T}$ *formuláinak bármely olyan* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ *n-esét, amelyre* $\mathbf{A}_n \equiv \mathbf{A}$ *és minden* $1 \leq k \leq n$ *számra a következő feltételek valamelyike teljesül:*

- $\mathbf{A}_k$ *logikai axiómája* $\mathfrak{T}$*-nek, vagyis* $\mathbf{A}_k$ *eleme az* $\mathfrak{S}_1$*,* $\mathfrak{S}_2$*,* $\mathfrak{S}_3$*,* $\mathfrak{S}_4$*,* $\mathfrak{S}_5$*,* $\mathfrak{S}_6$ *és* $\mathfrak{S}_7$ *formula-sémák valamelyikének;*
- *léteznek olyan* $1 \leq i, j < k$ *számok, hogy* $\mathbf{A}_j \equiv (\mathbf{A}_i \Rightarrow \mathbf{A}_k)$*.*

A $\mathfrak{T}$ *matematikai elmélet* $\mathbf{A}$ *formuláját* **logikai tételnek** (*vagy* **logikailag bizonyíthatónak**, *vagy* **logikailag levezethetőnek**) *nevezzük, ha létezik* $\mathbf{A}$*-nak logikai bizonyítása* $\mathfrak{T}$*-ben. A* $\mathfrak{T}$ *matematikai elmélet* $\mathbf{A}$ *formuláját* **logikailag cáfolhatónak** *nevezzük* $\mathfrak{T}$*-ben, ha* $\neg\mathbf{A}$ *logikai tétel* $\mathfrak{T}$*-ben.*

Nyilvánvaló, hogy egy matematikai elmélet minden logikai tétele egyben tétel is, de ennek megfordítása általában nem igaz. Előfordulhat az, hogy egy matematikai elmélet valamely formulájának létezik bizonyítása, de bármelyik bizonyításában szerepel nem logikai axióma; ilyenkor a formula nem logikai tétel. A definícióból látható, hogy a logikai tételek abban az értelemben tisztán logikai tényeket fejeznek ki, hogy van olyan bizonyításuk, amely csakis az elmélet logikai axiómáira hivatkozik. Világos továbbá, hogy egy $\mathfrak{T}$ matematikai elmélet $\mathbf{A}$ formulája pontosan akkor logikai tétel $\mathfrak{T}$-ben, ha $\mathbf{A}$ tétel $\mathfrak{T}_0$-ban.

A definíció szerint egy matematikai elmélet formulája pontosan akkor *nem tétel*, ha nem létezik levezetése az elméletben. Azt, hogy egy formula *tétel*, egyszer és mindenkorra eldönthetjük azzal, hogy megadjuk egy levezetését, ami *véges sok* lépésben lehetséges. Ezzel szemben annak bizonyításához, hogy egy formula *nem tétel*, el kell gondolni az elmélet lehetséges levezetéseinek *végtelen* összességét, és meg kell mutatni, hogy az adott formula ezek egyikében sem szerepel; ez véges sok lépésben nem lehetséges. Semmiféle *finit módszer* nem adható annak bizonyítására, hogy egy formula nem tétel. Azonban *infinit módszer* létezhet; ilyen például az *értékelések módszere*, amelynek alkalmazásával igazolni fogjuk, hogy minden predikátumkalkulusnak van olyan formulája, amely nem tétel (3.4.2. és 3.4.3.).

Egy természetes nyelven kifejtett (nem formális) matematikai elmélet kijelentését *igaznak* mondjuk, ha a kijelentés formalizáltja a megfelelő formális axiomatikus matematikai elméletben *tétel*. De amikor azt állítjuk, hogy egy kijelentés *nem igaz*, akkor egyáltalán nem arra gondolunk, hogy a szóban forgó kijelentés formalizáltja a megfelelő formális axiomatikus matematikai elméletben *nem tétel*, hanem ezen azt értjük, hogy az illető formula *negációja tétel*, vagyis a formula *cáfolható*. Ez azt jelenti, hogy a naiv matematikai elméletek igazság-fogalma és a formális axiomatikus matematikai elméletek tétel-fogalma *nem teljesen egyenértékű*. Ezt úgy is felfoghatjuk, hogy a kétféle igazság-fogalom egyenértékű, de ekkor a természetes matematikai nyelv "nem igaz" kijelentése nem az "igaz" kijelentés tagadása, vagyis ekkor a naiv logika tagadás-fogalma nem egyenértékű a negációval.

2.4. A matematikai elméletek bizonyítási módszerei

Most bemutatjuk a matematikai elméletek néhány alapvetően fontos bizonyítási módszerét.

2.4.1. Tétel. (**A leválasztás szabálya: modus ponens.**) *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, továbbá az* $\mathbf{A}$ *és* $\mathbf{A} \Rightarrow \mathbf{B}$ *formulák* (*logikai*) *tételek* $\mathfrak{T}$*-ben, akkor* $\mathbf{B}$ *is* (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Ha $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ az $\mathbf{A}$ formula és $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m)$ az $\mathbf{A} \Rightarrow \mathbf{B}$ formula (logikai) bizonyítása $\mathfrak{T}$-ben, akkor nyilvánvaló, hogy

$$(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m, \mathbf{B})$$

a $\mathbf{B}$ formula (logikai) bizonyítása $\mathfrak{T}$-ben, mert $\mathbf{B}_m \equiv \mathbf{A}_n \Rightarrow \mathbf{B}$. ■

2.4.2. Tétel. (**A tételek helyettesítés-invarianciája.**) *Legyen* $\mathbf{A}$ *formula a* $\mathfrak{T}$ *matematikai elméletben. Ha* $\mathbf{A}$ *tétel* $\mathfrak{T}$*-ben és* $\mathbf{x}$ *olyan változó, amely nem szerepel a* $\mathfrak{T}$ *egyetlen explicit axiómájában sem, akkor bármely* $\mathbf{T}$ *objektumra a* $(\mathbf{T}|\mathbf{x})\mathbf{A}$ *formula is tétel* $\mathfrak{T}$*-ben. Ha* $\mathbf{A}$ *logikai tétel* $\mathfrak{T}$*-ben, akkor bármely* $\mathbf{x}$ *változóra és bármely* $\mathbf{T}$ *objektumra a* $(\mathbf{T}|\mathbf{x})\mathbf{A}$ *formula is logikai tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Legyen $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ az $\mathbf{A}$ formula bizonyítása $\mathfrak{T}$-ben. Megmutatjuk, hogy ekkor minden $1 \leq k \leq n$ számra $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ tétel $\mathfrak{T}$-ben, így aztán $\mathbf{A}_n \equiv \mathbf{A}$ miatt $(\mathbf{T}|\mathbf{x})\mathbf{A}$ is tétel $\mathfrak{T}$-ben.

Az $\mathbf{A}_1$ formula szükségképpen axiómája $\mathfrak{T}$-nek, tehát $\mathbf{A}_1$ vagy eleme a $\mathfrak{T}$ valamelyik axióma-sémájának, vagy explicit axióma. Az első esetben a formula-sémák helyettesítés-invarianciája miatt $(\mathbf{T}|\mathbf{x})\mathbf{A}_1$ axiómája $\mathfrak{T}$-nek, így tétel. A második esetben $(\mathbf{T}|\mathbf{x})\mathbf{A}_1 \equiv \mathbf{A}_1$, mert a feltevés szerint $\mathbf{x}$ nem szerepel a $\mathfrak{T}$ egyetlen explicit axiómájában sem, tehát $(\mathbf{T}|\mathbf{x})\mathbf{A}_1$ ismét axiómája $\mathfrak{T}$-nek, így tétel.

Legyen a $1 \leq k \leq n$ szám rögzítve, és tegyük fel, hogy minden $1 \leq j < k$ számra $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$ tétel $\mathfrak{T}$-ben. Ha $\mathbf{A}_k$ axiómája $\mathfrak{T}$-nek, akkor az előzőekhez hasonlóan kapjuk, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ axiómája $\mathfrak{T}$-nek, így tétel. Ha léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_j \equiv \mathbf{A}_i \Rightarrow \mathbf{A}_k$, akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_j \equiv ((\mathbf{T}|\mathbf{x})\mathbf{A}_i) \Rightarrow ((\mathbf{T}|\mathbf{x})\mathbf{A}_k)$, és a hipotézis szerint a $(\mathbf{T}|\mathbf{x})\mathbf{A}_i$ és $(\mathbf{T}|\mathbf{x})\mathbf{A}_j$ formulák tételek $\mathfrak{T}$-ben, így a leválasztás szabálya alapján $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ tétel $\mathfrak{T}$-ben.

Tegyük fel, hogy $\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben, vagyis tétel $\mathfrak{T}_0$-ban, és legyen $\mathbf{x}$ tetszőleges változó, valamint $\mathbf{T}$ tetszőleges objektum $\mathfrak{T}$-ben. Ekkor $\mathbf{x}$ nem szerepel a $\mathfrak{T}_0$ egyetlen explicit axiómájában sem, hiszen $\mathfrak{T}_0$-nak *nincs* explicit axiómája, továbbá $\mathbf{T}$ objektuma $\mathfrak{T}_0$-nak, hiszen a $\mathfrak{T}$ és $\mathfrak{T}_0$ elméletek nyelve azonos. Ezért az előzőek alapján $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben. ■

Az előző tétel bizonyításában láttuk, hogy ha $\mathbf{A}$ *logikai tétel* $\mathfrak{T}$-ben, akkor *bármely* $\mathbf{x}$ változóra és bármely $\mathbf{T}$ objektumra a $(\mathbf{T}|\mathbf{x})\mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben, még akkor is, ha az $\mathbf{x}$ változó szerepel a $\mathfrak{T}$ valamelyik explicit axiómájában. De ha $\mathbf{A}$ csak *tétel*, és az $\mathbf{x}$ változó *szerepel* a $\mathfrak{T}$ valamelyik explicit axiómájában, akkor létezhet olyan $\mathbf{T}$ objektum, amelyre $(\mathbf{T}|\mathbf{x})\mathbf{A}$ nem tétel $\mathfrak{T}$-ben. A bizonyításból láthatóan ennek az az oka, hogy egy explicit axiómában változó helyére objektumot helyettesítve általában nem kapunk tételt, vagyis az explicit axiómák összessége általában *nem helyettesítés-invariáns.* Természetesen ez a probléma nem vetődik fel olyan matematikai elméletek esetében, amelyek explicit axiómáiban nem szerepelnek változók, amilyen például a halmazelmélet, az aritmetika és a síkgeometria.

2.4.3. Tétel. (**Láncszabály: syllogismus.**) *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, továbbá* $\mathbf{A} \Rightarrow \mathbf{B}$ *és* $\mathbf{B} \Rightarrow \mathbf{C}$ (*logikai*) *tételek* $\mathfrak{T}$*-ben, akkor* $\mathbf{A} \Rightarrow \mathbf{C}$ *is* (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Legyen $(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$ az $\mathbf{A} \Rightarrow \mathbf{B}$, és $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m)$ a $\mathbf{B} \Rightarrow \mathbf{C}$ formula (logikai) bizonyítása $\mathfrak{T}$-ben. Ekkor

$$\Big(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m, (\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})),$$
$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}), \mathbf{A} \Rightarrow \mathbf{C}\Big)$$

az $\mathbf{A} \Rightarrow \mathbf{C}$ formula (logikai) bizonyítása $\mathfrak{T}$-ben, ugyanis az implikáció értelmezése szerint

$$(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}))$$

azonos a $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\neg\mathbf{A} \vee \mathbf{B}) \Rightarrow (\neg\mathbf{A} \vee \mathbf{C}))$ formulával, ami eleme $\mathfrak{S}_4$-nek, tehát logikai axióma, továbbá a feltételek alapján $\mathbf{B}_m \equiv \mathbf{B} \Rightarrow \mathbf{C}$ és $\mathbf{A}_n \equiv \mathbf{A} \Rightarrow \mathbf{B}$. ■

2.4.4. Állítás. (**A kizárt harmadik elve: tertium non datur.**) *Ha* $\mathbf{A}$ *formula a* $\mathfrak{T}$ *matematikai elméletben, akkor* $(\neg\mathbf{A}) \vee \mathbf{A}$*, vagyis* $\mathbf{A} \Rightarrow \mathbf{A}$ *logikai tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Az $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_2$-nek, és az $(\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}$ formula eleme $\mathfrak{S}_1$-nek, tehát ezek a formulák logikai tételek $\mathfrak{T}$-ben, így a láncszabály alkalmazásával kapjuk, hogy $\mathbf{A} \Rightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben. ■

2.4.5. Tétel. (**Az esetszétválasztás szabálya: alternatio.**) *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, és az* $\mathbf{A} \vee \mathbf{B}$, $\mathbf{A} \Rightarrow \mathbf{C}$, $\mathbf{B} \Rightarrow \mathbf{C}$ *formulák* (*logikai*) *tételek* $\mathfrak{T}$*-ben, akkor* $\mathbf{C}$ *is* (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee \mathbf{C}))$ formula eleme $\mathfrak{S}_4$-nek, és a feltevés szerint $\mathbf{B} \Rightarrow \mathbf{C}$ (logikai) tétel $\mathfrak{T}$-ben, így a leválasztás szabálya alapján kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee \mathbf{C})$ is (logikai) tétel $\mathfrak{T}$-ben. Az $(\mathbf{A} \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_3$-nak, tehát a láncszabály szerint $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{C} \vee \mathbf{A})$ is (logikai) tétel $\mathfrak{T}$-ben. A feltevés szerint $\mathbf{A} \vee \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, tehát ismét a leválasztás szabálya alapján kapjuk, hogy $\mathbf{C} \vee \mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. De az $(\mathbf{A} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{C}))$ formula eleme $\mathfrak{S}_4$-nek, és a feltevés szerint $\mathbf{A} \Rightarrow \mathbf{C}$ (logikai) tétel $\mathfrak{T}$-ben, ezért a leválasztás szabálya alapján $(\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{C})$ (logikai) tétel $\mathfrak{T}$-ben. Ebből a leválasztás szabálya alapján adódik, hogy $\mathbf{C} \vee \mathbf{C}$ (logikai) tétel $\mathfrak{T}$-ben. Végül, $(\mathbf{C} \vee \mathbf{C}) \Rightarrow \mathbf{C}$ eleme $\mathfrak{S}_1$-nek, tehát a leválasztás szabálya szerint $\mathbf{C}$ (logikai) tétel $\mathfrak{T}$-ben. ■

Vigyázzunk arra, hogy ha $\mathbf{A}$ és $\mathbf{B}$ olyan formulák a $\mathfrak{T}$ matematikai elméletben, hogy $\mathbf{A} \vee \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, akkor szó sincs arról, hogy $\mathbf{A}$ vagy $\mathbf{B}$ (logikai) tétel volna $\mathfrak{T}$-ben.

2.4.6. Állítás. (**Visszavezetés a lehetetlenre: reductio ad absurdum.**) *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, továbbá* $(\neg\mathbf{B}) \Rightarrow \mathbf{A}$ *és* $\mathbf{B} \Rightarrow \mathbf{A}$ (*logikai*) *tételek* $\mathfrak{T}$*-ben, akkor* $\mathbf{A}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A kizárt harmadik elve alapján a $(\neg\mathbf{B}) \vee \mathbf{B}$ formula logikai tétel $\mathfrak{T}$-ben, ezért az esetszétválasztás szabálya szerint $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. ■

2.4.7. Állítás. (**Igaz bármiből következik: verum sequitur ex quodlibet.**) *Ha* $\mathbf{A}$ (*logikai*) *tétel a* $\mathfrak{T}$ *matematikai elméletben, akkor minden* $\mathbf{B}$ *formulára a* $\mathbf{B} \Rightarrow \mathbf{A}$ *formula* (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Az $\mathbf{A} \Rightarrow (\mathbf{A} \vee (\neg\mathbf{B}))$ formula eleme $\mathfrak{S}_2$-nek, és az $(\mathbf{A} \vee (\neg\mathbf{B})) \Rightarrow ((\neg\mathbf{B}) \vee \mathbf{A})$ formula eleme $\mathfrak{S}_3$-nak, vagyis ezek a formulák logikai tételek $\mathfrak{T}$-ben. A láncszabály szerint $\mathbf{A} \Rightarrow ((\neg\mathbf{B}) \vee \mathbf{A})$, vagyis $\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})$ is logikai tétel $\mathfrak{T}$-ben. Ha $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, akkor a leválasztás szabályát alkalmazva ebből következik, hogy $\mathbf{B} \Rightarrow \mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. ■

2.4.8. Állítás. (**Hamisból bármi következik: ex falso sequitur quodlibet.**) *Ha* $\mathbf{A}$ (*logikailag*) *cáfolható formula a* $\mathfrak{T}$ *matematikai elméletben* (*vagyis* $\neg\mathbf{A}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben*), *akkor minden* $\mathbf{B}$ *formulára az* $\mathbf{A} \Rightarrow \mathbf{B}$ *formula* (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A $\neg\mathbf{A} \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B})$ formula eleme $\mathfrak{S}_2$-nek, és a hipotézis szerint $\neg\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, így a leválasztás szabálya szerint $(\neg\mathbf{A}) \vee \mathbf{B}$ is (logikai) tétel $\mathfrak{T}$-ben. Az implikáció definíciója szerint ez azt jelenti, hogy $\mathbf{A} \Rightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. ■

2.4.9. Állítás. (**A kettős negáció szabálya.**) *Ha* $\mathbf{A}$ *formula a* $\mathfrak{T}$ *matematikai elméletben, akkor az*

$$\mathbf{A} \Rightarrow (\neg\neg\mathbf{A}),$$
$$(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. A kizárt harmadik elve alapján a $(\neg\neg\mathbf{A}) \vee (\neg\mathbf{A})$ formula tétel $\mathfrak{T}$-ben. A

$$((\neg\neg\mathbf{A}) \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\neg\mathbf{A}))$$

formula eleme $\mathfrak{S}_3$-nak, tehát logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabálya szerint $(\neg\mathbf{A}) \vee (\neg\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben. Az implikáció értelmezése alapján $((\neg\mathbf{A}) \vee (\neg\neg\mathbf{A})) \equiv (\mathbf{A} \Rightarrow (\neg\neg\mathbf{A}))$, tehát $\mathbf{A} \Rightarrow (\neg\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben.

Ebből következik, hogy $(\neg\mathbf{A}) \Rightarrow (\neg\neg\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben. Ugyanakkor a

$$((\neg\mathbf{A}) \Rightarrow (\neg\neg\neg\mathbf{A})) \Rightarrow ((\mathbf{A} \vee (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \vee (\neg\neg\neg\mathbf{A})))$$

formula eleme $\mathfrak{S}_4$-nek, így a leválasztás szabálya szerint $(\mathbf{A} \vee (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \vee (\neg\neg\neg\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. A $((\neg\mathbf{A}) \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee (\neg\mathbf{A}))$ és a $(\mathbf{A} \vee (\neg\neg\neg\mathbf{A})) \Rightarrow ((\neg\neg\neg\mathbf{A}) \vee \mathbf{A})$ formulák elemei $\mathfrak{S}_3$-nak, tehát logikai axiómák, így kétszer alkalmazva a láncszabályt kapjuk, hogy $((\neg\mathbf{A}) \vee \mathbf{A}) \Rightarrow ((\neg\neg\neg\mathbf{A}) \vee \mathbf{A})$ logikai tétel $\mathfrak{T}$-ben. A kizárt harmadik elve alapján $(\neg\mathbf{A}) \vee \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\neg\neg\neg\mathbf{A}) \vee \mathbf{A}$, vagyis $(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben. ■

2.4.10. Állítás. (**A kettős negáció elve.**) *Ha* $\mathbf{A}$ *formula a* $\mathfrak{T}$ *matematikai elméletben, akkor* $\mathbf{A}$ *pontosan akkor* (*logikai*) *tétel* $\mathfrak{T}$*-ben, ha* $\neg\neg\mathbf{A}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A kettős negáció szabálya szerint $\mathbf{A} \Rightarrow (\neg\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, tehát ha $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, akkor a leválasztás szabálya szerint $\neg\neg\mathbf{A}$ szintén (logikai) tétel $\mathfrak{T}$-ben.

A kettős negáció szabálya szerint $(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben, tehát ha $\neg\neg\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, akkor a leválasztás szabálya szerint $\mathbf{A}$ szintén (logikai) tétel $\mathfrak{T}$-ben. ■

2.4.11. Állítás. *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, és tegyük fel, hogy* $\mathbf{A} \vee \mathbf{B}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

a) *Ha* $\neg\mathbf{B}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben, akkor* $\mathbf{A}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

b) *Ha* $\neg\mathbf{A}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben, akkor* $\mathbf{B}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. a) A $(\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee (\neg\neg\mathbf{B})))$ formula eleme $\mathfrak{S}_4$-nek, tehát logikai axióma, és a kettős negáció szabálya szerint $\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee (\neg\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Mivel a hipotézis szerint $\mathbf{A} \vee \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, így a leválasztás szabálya szerint $\mathbf{A} \vee (\neg\neg\mathbf{B})$ (logikai) tétel $\mathfrak{T}$-ben. Az $(\mathbf{A} \vee (\neg\neg\mathbf{B})) \Rightarrow ((\neg\neg\mathbf{B}) \vee \mathbf{A})$ formula eleme $\mathfrak{S}_3$-nak, tehát logikai axióma, így ismét a leválasztás szabályát alkalmazva kapjuk, hogy $(\neg\neg\mathbf{B}) \vee \mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. Az implikáció definíciója szerint $(\neg\neg\mathbf{B}) \vee \mathbf{A} \equiv (\neg\mathbf{B}) \Rightarrow \mathbf{A}$, tehát $(\neg\mathbf{B}) \Rightarrow \mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, és a hipotézis alapján $\neg\mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, amiből a leválasztás szabályát alkalmazva következik, hogy $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben.

b) Az $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_3$-nak, tehát logikai axióma, és a hipotézis szerint $\mathbf{A} \vee \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, így a leválasztás szabálya szerint $\mathbf{B} \vee \mathbf{A}$ is (logikai) tétel $\mathfrak{T}$-ben. Ezért az a) kijelentést alkalmazva az $\mathbf{A}$ és $\mathbf{B}$ formulák felcserélésével kapjuk a b) kijelentést. ■

2.4.12. Állítás. (**A kontrapozíció szabálya: modus tollens.**) *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor az*

$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})),$$
$$((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. A $(\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})) \Rightarrow (((\neg\mathbf{A}) \vee \mathbf{B}) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})))$ formula eleme $\mathfrak{S}_4$-nek, tehát logikai tétel $\mathfrak{T}$-ben, és a kettős negáció szabálya szerint $\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})$ is logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabályát, valamint az implikáció értelmezését alkalmazva kapjuk, hogy $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. A $((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})) \Rightarrow ((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A}))$ formula eleme $\mathfrak{S}_3$-nak, így a láncszabály szerint $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. Az implikáció értelmezése alapján $((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A})) \equiv ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$, amiből azonnal kapjuk, hogy $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben.

A kettős negáció szabálya szerint $(\neg\neg\mathbf{B}) \Rightarrow \mathbf{B}$ logikai tétel $\mathfrak{T}$-ben, és

$$((\neg\neg\mathbf{B}) \Rightarrow \mathbf{B}) \Rightarrow (((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B}))$$

eleme $\mathfrak{S}_4$-nek, így logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. Ugyanakkor a $((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\neg\mathbf{B}))$ formula eleme $\mathfrak{S}_3$-nak, így a láncszabály szerint $((\neg\neg\mathbf{B}) \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. Az implikáció értelmezése alapján ez azt jelenti, hogy $((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. ■

2.4.13. Állítás. (**A kontrapozíció elve.**) *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Az* $\mathbf{A} \Rightarrow \mathbf{B}$ *formula pontosan akkor* (*logikai*) *tétel* $\mathfrak{T}$*-ben, ha* $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A kontrapozíció szabálya szerint $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben, tehát ha $\mathbf{A} \Rightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, akkor a leválasztás szabálya szerint $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ (logikai) tétel $\mathfrak{T}$-ben.

A kontrapozíció szabálya szerint $((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben, tehát ha $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ (logikai) tétel $\mathfrak{T}$-ben, akkor a leválasztás szabálya szerint $\mathbf{A} \Rightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. ■

2.4.14. Állítás. *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, továbbá* $\mathbf{A} \Rightarrow \mathbf{B}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben, akkor a* $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})$ *formula is* (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A kontrapozíció szabálya szerint $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben, tehát a feltevés és a leválasztás szabálya alapján $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ (logikai) tétel $\mathfrak{T}$-ben. A $((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow ((\mathbf{C} \vee (\neg\mathbf{B})) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{A})))$ formula eleme $\mathfrak{S}_4$-nek, tehát a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{C} \vee (\neg\mathbf{B})) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{A}))$ (logikai) tétel $\mathfrak{T}$-ben. Azonban a $((\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{B}))$ formula eleme $\mathfrak{S}_3$-nak, így a láncszabály szerint $((\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee (\neg\mathbf{A}))$ (logikai) tétel $\mathfrak{T}$-ben. A $(\mathbf{C} \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{C})$ formula szintén eleme $\mathfrak{S}_3$-nak, tehát ismét a láncszabályt alkalmazva kapjuk, hogy $((\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{C})$ logikai tétel $\mathfrak{T}$-ben. Az implikáció értelmezése alapján ez azonos a $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})$ formulával. ■

2.4.15. Definíció. *Ha* $\mathfrak{T}$ *matematikai elmélet és* $\mathbf{A}$ *formulája* $\mathfrak{T}$*-nek, akkor* $\mathfrak{T}[\mathbf{A}]$ *jelöli azt a matematikai elméletet, amelyet* $\mathfrak{T}$*-ből úgy nyerünk, hogy a* $\mathfrak{T}$ *explicit axiómái mellé felvesszük* $\mathbf{A}$*-t is explicit axiómaként.*

Tehát a $\mathfrak{T}[\mathbf{A}]$ matematikai elmélet nyelve azonos a $\mathfrak{T}$ matematikai elmélet nyelvével, továbbá a matematikai axióma-sémái azonosak a $\mathfrak{T}$ matematikai axióma-sémáival, és az explicit axiómái azonosak a $\mathfrak{T}$ explicit axiómáival, valamint $\mathbf{A}$-val.

2.4.16. Tétel. (**Dedukció-tétel.**) *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Ha a* $\mathbf{B}$ *formula tétel a* $\mathfrak{T}[\mathbf{A}]$ *matematikai elméletben, akkor az* $\mathbf{A} \Rightarrow \mathbf{B}$ *formula tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Legyen $(\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_n)$ a $\mathbf{B}$ formula bizonyítása $\mathfrak{T}[\mathbf{A}]$-ban. Megmutatjuk, hogy minden $1 \leq k \leq n$ számra az $\mathbf{A} \Rightarrow \mathbf{B}_k$ formula tétel $\mathfrak{T}$-ben, amiből következik, hogy $\mathbf{A} \Rightarrow \mathbf{B}$ is tétel $\mathfrak{T}$-ben, hiszen $\mathbf{B}_n \equiv \mathbf{B}$.

A $\mathbf{B}_1$ formula szükségképpen axióma $\mathfrak{T}[\mathbf{A}]$-ban, tehát vagy axiómája $\mathfrak{T}$-nek, vagy azonos $\mathbf{A}$-val. Az első esetben $\mathbf{B}_1$ tétel $\mathfrak{T}$-ben, így $\mathbf{A} \Rightarrow \mathbf{B}_1$ is tétel $\mathfrak{T}$-ben (igaz bármiből következik). A második esetben $\mathbf{A} \Rightarrow \mathbf{B}_1 \equiv \mathbf{A} \Rightarrow \mathbf{A}$, és $\mathbf{A} \Rightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben (a kizárt harmadik elve), így $\mathbf{A} \Rightarrow \mathbf{B}_1$ tétel $\mathfrak{T}$-ben.

Tegyük fel, hogy $1 \leq k \leq n$ olyan szám, hogy minden $1 \leq j < k$ számra $\mathbf{A} \Rightarrow \mathbf{B}_j$ tétel $\mathfrak{T}$-ben; megmutatjuk, hogy ekkor $\mathbf{A} \Rightarrow \mathbf{B}_k$ is tétel $\mathfrak{T}$-ben. Ha $\mathbf{B}_k$ axióma $\mathfrak{T}[\mathbf{A}]$-ban, akkor az előző érvelést megismételve $\mathbf{B}_1$ helyett $\mathbf{B}_k$-ra kapjuk, hogy $\mathbf{A} \Rightarrow \mathbf{B}_k$ tétel $\mathfrak{T}$-ben. Ha $\mathbf{B}_k$ nem axióma $\mathfrak{T}[\mathbf{A}]$-ban, akkor legyenek $1 \leq i, j < k$ olyan számok, amelyekre $\mathbf{B}_j \equiv \mathbf{B}_i \Rightarrow \mathbf{B}_k$. A hipotézisünk szerint $\mathbf{A} \Rightarrow \mathbf{B}_i$ tétel $\mathfrak{T}$-ben, tehát az előző állítás alapján $(\mathbf{B}_i \Rightarrow \mathbf{B}_k) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ is tétel $\mathfrak{T}$-ben. Ugyancsak a hipotézis alapján $\mathbf{A} \Rightarrow (\mathbf{B}_i \Rightarrow \mathbf{B}_k)$ tétel $\mathfrak{T}$-ben, így a láncszabály alkalmazásával kapjuk, hogy $\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ tétel $\mathfrak{T}$-ben. A $(\neg\mathbf{A}) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B}_k)$ formula eleme $\mathfrak{S}_2$-nek, és ez azonos a $(\neg\mathbf{A}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ formulával, tehát $(\neg\mathbf{A}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ tétel $\mathfrak{T}$-ben. Ez azt jelenti, hogy az $\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ és $(\neg\mathbf{A}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_k)$ formulák tételek $\mathfrak{T}$-ben, így a reductio ad absurdum elve alapján az $\mathbf{A} \Rightarrow \mathbf{B}_k$ formula tétel a $\mathfrak{T}$ elméletben.

Ebből következik, hogy az $\mathbf{A} \Rightarrow \mathbf{B}_n$ formula is tétel $\mathfrak{T}$-ben, így $\mathbf{B}_n \equiv \mathbf{B}$ miatt az $\mathbf{A} \Rightarrow \mathbf{B}$ formula tétel $\mathfrak{T}$-ben. ■

A mindennapi matematikai gyakorlatban a dedukció-tételt a következőképpen alkalmazzuk. Legyenek $\mathbf{A}$ és $\mathbf{B}$ azok a formulák a $\mathfrak{T}$ matematikai elméletben, amelyekre bizonyítani akarjuk azt, hogy $\mathbf{A} \Rightarrow \mathbf{B}$ tétel $\mathfrak{T}$-ben. Ekkor így fogalmazunk: "Tegyük fel, hogy $\mathbf{A}$ igaz; megmutatjuk, hogy ekkor $\mathbf{B}$ igaz." Ezen azt értjük, hogy $\mathfrak{T}$-ről áttérünk a $\mathfrak{T}[\mathbf{A}]$ matematikai elméletre, amelyben $\mathbf{A}$ abban az értelemben igaz, hogy tétel (sőt explicit axióma); majd igazoljuk a $\mathbf{B}$ formula levezethetőségét a $\mathfrak{T}[\mathbf{A}]$ matematikai elméletben. Ha ez sikerül, akkor a dedukció-tétel alapján állíthatjuk, hogy $\mathbf{A} \Rightarrow \mathbf{B}$ tétel $\mathfrak{T}$-ben. Ezt a tényállást a természetes nyelven így fejezzük ki: "Tehát $\mathbf{A}$-ból következik $\mathbf{B}$." A dedukció-tétel alkalmazásával magyarázatot kapunk arra, hogy a $\Rightarrow$ szimbólumot miért tekintjük a *következtetés* jelének. Ez világosan kiderül a következő tételből.

2.4.17. Tétel. (**Az implikáció logikai alaptulajdonsága.**) *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Az* $\mathbf{A} \Rightarrow \mathbf{B}$ *formula pontosan akkor tétel* $\mathfrak{T}$*-ben, ha* $\mathbf{B}$ *tétel a* $\mathfrak{T}[\mathbf{A}]$ *matematikai elméletben.*

Bizonyítás. Ha $\mathbf{A} \Rightarrow \mathbf{B}$ tétel $\mathfrak{T}$-ben, akkor tétel a $\mathfrak{T}[\mathbf{A}]$ matematikai elméletben is, amelyben $\mathbf{A}$ szintén tétel (sőt explicit axióma), így a leválasztás szabálya szerint $\mathbf{B}$ tétel $\mathfrak{T}[\mathbf{A}]$-ban. Megfordítva, ha $\mathbf{B}$ tétel $\mathfrak{T}[\mathbf{A}]$-ban, akkor a dedukció-tétel alapján $\mathbf{A} \Rightarrow \mathbf{B}$ tétel $\mathfrak{T}$-ben. ■

2.4.18. Állítás. *Legyenek* $\mathbf{A}$*,* $\mathbf{A}'$*,* $\mathbf{B}$ *és* $\mathbf{B}'$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Ha* $\mathbf{A} \Rightarrow \mathbf{A}'$ *és* $\mathbf{B} \Rightarrow \mathbf{B}'$ (*logikai*) *tételek* $\mathfrak{T}$*-ben, akkor* $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A}' \vee \mathbf{B}')$ *és* $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow (\mathbf{A}' \wedge \mathbf{B}')$ (*logikai*) *tételek* $\mathfrak{T}$*-ben.*

Bizonyítás. A $(\mathbf{B} \Rightarrow \mathbf{B}') \Rightarrow ((\mathbf{A}' \vee \mathbf{B}) \Rightarrow (\mathbf{A}' \vee \mathbf{B}'))$ formula eleme $\mathfrak{S}_4$-nek, amiből leválasztással kapjuk, hogy $(\mathbf{A}' \vee \mathbf{B}) \Rightarrow (\mathbf{A}' \vee \mathbf{B}')$ (logikai) tétel $\mathfrak{T}$-ben. Továbbá, az $(\mathbf{A} \Rightarrow \mathbf{A}') \Rightarrow ((\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{B} \vee \mathbf{A}'))$ formula szintén eleme $\mathfrak{S}_4$-nek, amiből a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{B} \vee \mathbf{A}')$ (logikai) tétel $\mathfrak{T}$-ben. De az $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})$ és $(\mathbf{B} \vee \mathbf{A}') \Rightarrow (\mathbf{A}' \vee \mathbf{B})$ formulák elemei $\mathfrak{S}_3$-nak, így háromszor alkalmazva a láncszabályt kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A}' \vee \mathbf{B}')$ (logikai) tétel $\mathfrak{T}$-ben.

A kontrapozíció szabálya szerint $(\mathbf{A} \Rightarrow \mathbf{A}') \Rightarrow ((\neg\mathbf{A}') \Rightarrow (\neg\mathbf{A}))$ és $(\mathbf{B} \Rightarrow \mathbf{B}') \Rightarrow ((\neg\mathbf{B}') \Rightarrow (\neg\mathbf{B}))$ logikai tételek $\mathfrak{T}$-ben, amiből a leválasztás szabályát alkalmazva következik, hogy $(\neg\mathbf{A}') \Rightarrow (\neg\mathbf{A})$ és $(\neg\mathbf{B}') \Rightarrow (\neg\mathbf{B})$ logikai tételek $\mathfrak{T}$-ben. A bizonyítás első részéből következik, hogy $((\neg\mathbf{A}') \vee (\neg\mathbf{B}')) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$ (logikai) tétel $\mathfrak{T}$-ben. Ismét a kontrapozíció szabályát alkalmazva kapjuk, hogy

$$(((\neg\mathbf{A}') \vee (\neg\mathbf{B}')) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\mathbf{B}))) \Rightarrow ((\neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))) \Rightarrow (\neg((\neg\mathbf{A}') \vee (\neg\mathbf{B}'))))$$

logikai $\mathfrak{T}$-ben, tehát a leválasztás szabályát alkalmazva kapjuk, hogy

$$(\neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))) \Rightarrow (\neg((\neg\mathbf{A}') \vee (\neg\mathbf{B}')))$$

(logikai) tétel $\mathfrak{T}$-ben. A konjunkció értelmezése szerint ez pontosan azt jelenti, hogy $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow (\mathbf{A}' \wedge \mathbf{B}')$ (logikai) tétel $\mathfrak{T}$-ben. ■

2.4.19. Definíció. *Azt mondjuk, hogy a* $\mathfrak{T}'$ *matematikai elmélet* **bővítése** *a* $\mathfrak{T}$ *matematikai elméletnek, ha a* $\mathfrak{T}$ *nyelvének minden logikai és matematikai függvénye a* $\mathfrak{T}'$ *nyelvének is logikai és matematikai függvénye, továbbá a* $\mathfrak{T}$ *minden matematikai axióma-sémája a* $\mathfrak{T}'$*-nek is matematikai axióma-sémája, valamint a* $\mathfrak{T}$ *minden explicit axiómája a* $\mathfrak{T}'$*-nek is explicit axiómája. Azt mondjuk, hogy a* $\mathfrak{T}$ *matematikai elmélet* **részelmélete** *a* $\mathfrak{T}'$ *matematikai elméletnek, ha* $\mathfrak{T}'$ *bővítése* $\mathfrak{T}$*-nek.*

Tegyük fel, hogy a $\mathfrak{T}'$ matematikai elmélet bővítése a $\mathfrak{T}$ matematikai elméletnek. Nyilvánvaló, hogy a $\mathfrak{T}$ minden kifejezése (objektuma, formulája) a $\mathfrak{T}'$-nek is kifejezése (objektuma, formulája), továbbá a $\mathfrak{T}$ minden (logikai) tétele $\mathfrak{T}'$-nek is (logikai) tétele. Azonban előfordulhat, hogy $\mathfrak{T}'$-nek van olyan kifejezése (például objektuma vagy formulája), amely $\mathfrak{T}$-nek nem kifejezése. Létezhet továbbá $\mathfrak{T}$-nek olyan formulája, amely tétel $\mathfrak{T}'$-ben, de *nem tétel* $\mathfrak{T}$-ben.

A definíció alapján nyilvánvaló, hogy ha $\mathfrak{T}$ matematikai elmélet, akkor $\mathfrak{T}$ bővítése $\mathfrak{T}_0$-nak, vagyis $\mathfrak{T}_0$ részelmélete $\mathfrak{T}$-nek.

Nyilvánvaló, hogy ha $\mathfrak{T}$ matematikai elmélet és $\mathbf{A}$ formulája $\mathfrak{T}$-nek, akkor $\mathfrak{T}[\mathbf{A}]$ bővítése a $\mathfrak{T}$ matematikai elméletnek. Ha $\mathbf{A}$ és $\mathbf{B}$ formulái a $\mathfrak{T}$ matematikai elméletnek, akkor a $\mathfrak{T}[\mathbf{A}][\mathbf{B}]$ matematikai elméletet a $\mathfrak{T}[\mathbf{A},\mathbf{B}]$ szimbólummal jelöljük. Természetesen ennél általánosabb bővítések is elgondolhatók, de a mindennapi matematikai alkalmazásokban általában elegendő a $\mathfrak{T}[\mathbf{A}]$ és $\mathfrak{T}[\mathbf{A},\mathbf{B}]$ alakú bővítéseket tekinteni.

Ha $\mathfrak{T}$ matematikai elmélet és $\mathbf{A}$ formulája $\mathfrak{T}$-nek, akkor az $\mathbf{A}$-ban szereplő változók szerepelnek a $\mathfrak{T}[\mathbf{A}]$ matematikai elmélet valamelyik explicit axiómájában (ti. $\mathbf{A}$-ban biztosan szerepelnek), tehát a $\mathfrak{T}[\mathbf{A}]$ elmélet explicit axiómáiban szerepelhetnek változók akkor is, ha az eredeti $\mathfrak{T}$ matematikai elmélet explicit axiómáiban nem szerepel változó.

2.4.20. Definíció. *Azt mondjuk, hogy a* $\mathfrak{T}$ *matematikai elmélet* **ellentmondásos**, *ha van olyan* $\mathbf{A}$ *formulája* $\mathfrak{T}$*-nek, hogy* $\mathbf{A}$ *és* $\neg\mathbf{A}$ *tételek* $\mathfrak{T}$*-ben. A nem ellentmondásos matematikai elméleteket* **ellentmondásmenteseknek** *nevezzük.*

Tehát egy $\mathfrak{T}$ matematikai elmélet pontosan akkor ellentmondásmentes, ha *nem létezik* $\mathfrak{T}$-nek olyan $\mathbf{A}$ formulája, hogy $\mathbf{A}$ és $\neg\mathbf{A}$ *mindketten* tételek $\mathfrak{T}$-ben.

2.4.21. Állítás. *Ha a* $\mathfrak{T}$ *matematikai elmélet ellentmondásos, akkor* $\mathfrak{T}$ *minden formulája tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Legyen $\mathbf{B}$ olyan formula, hogy $\mathbf{B}$ és $\neg\mathbf{B}$ tételek $\mathfrak{T}$. Legyen $\mathbf{A}$ tetszőleges formulája $\mathfrak{T}$-nek. A $(\neg\mathbf{B}) \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})$ formula azonos a $(\neg\mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \vee \mathbf{A})$ formulával, és az utóbbi eleme $\mathfrak{S}_2$-nek, tehát logikai tétel $\mathfrak{T}$-ben. Kétszer alkalmazva a leválasztás szabályát kapjuk, hogy $\mathbf{A}$ tétel $\mathfrak{T}$-ben. ■

Az előző állítás *elvi szempontból* rendkívül fontos. Azt mutatja, hogy ha egy matematikai elmélettel kapcsolatos alapfeladatnak tekintjük az elmélet tételeinek meghatározását, akkor ellentmondásos elmélet esetében ez a probléma triviálisan megoldható: az elmélet *minden* formulája tétel, és persze bármely formulájának a negációja is tétel. Sőt, ekkor az elmélet minden formulájának létezik egy standard levezetése, az amelyik az előző állítás bizonyításában szerepel. Ezért az ellentmondásos matematikai elméletek *értéktelenek*. Ez az oka annak, hogy a matematikai logikában különösen nagy hangsúlyt kap a matematikai elméletek ellentmondásmentességének vizsgálata.

2.4.22. Állítás. *Legyen* $\mathbf{A}$ *formulája a* $\mathfrak{T}$ *matematikai elméletnek.*

a) *Ha* $\mathbf{A}$ *nem cáfolható* $\mathfrak{T}$*-ben* (*vagyis* $\neg\mathbf{A}$ *nem tétel* $\mathfrak{T}$*-ben*), *akkor a* $\mathfrak{T}$ *és* $\mathfrak{T}[\mathbf{A}]$ *matematikai elméletek ellentmondásmentesek.*

b) *Ha* $\mathbf{A}$ *nem bizonyítható* $\mathfrak{T}$*-ben* (*vagyis* $\mathbf{A}$ *nem tétel* $\mathfrak{T}$*-ben*), *akkor a* $\mathfrak{T}$ *és* $\mathfrak{T}[\neg\mathbf{A}]$ *matematikai elméletek ellentmondásmentesek.*

c) *Ha* $\mathbf{A}$ *nem bizonyítható és nem cáfolható* $\mathfrak{T}$*-ben, akkor a* $\mathfrak{T}$*,* $\mathfrak{T}[\mathbf{A}]$ *és* $\mathfrak{T}[\neg\mathbf{A}]$ *matematikai elméletek ellentmondásmentesek.*

Bizonyítás. A c) állítás nyilvánvalóan következik a)-ból és b)-ből. Az a) és b) állítás premisszáiból következik, hogy *létezik* $\mathfrak{T}$-nek olyan formulája, amely nem tétel $\mathfrak{T}$-ben, így az előző állítás alapján $\mathfrak{T}$ ellentmondásmentes.

Tegyük fel, hogy $\mathfrak{T}[\mathbf{A}]$ *ellentmondásos*, és legyen $\mathbf{B}$ olyan formula, hogy $\mathbf{B}$ és $\neg\mathbf{B}$ tétel $\mathfrak{T}[\mathbf{A}]$-ban. A dedukció-tétel alapján ekkor $\mathbf{A} \Rightarrow \mathbf{B}$ és $\mathbf{A} \Rightarrow (\neg\mathbf{B})$ tétel $\mathfrak{T}$-ben. Ebből a kontrapozíció elve alapján kapjuk, hogy $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ és $(\neg\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ szintén tétel $\mathfrak{T}$-ben. Ezért a reductio ad absurdum elve alapján $\neg\mathbf{A}$ tétel $\mathfrak{T}$-ben, vagyis $\mathbf{A}$ *cáfolható* $\mathfrak{T}$-ben. Tehát ha $\mathbf{A}$ *nem cáfolható* $\mathfrak{T}$-ben, akkor $\mathfrak{T}[\mathbf{A}]$ *ellentmondásmentes*. Ezzel az a) állítást igazoltuk.

Ha a $\mathfrak{T}$ matematikai elmélet $\mathbf{A}$ formulája *nem bizonyítható* $\mathfrak{T}$-ben, akkor a kettős negáció elve szerint $\neg\neg\mathbf{A}$ sem bizonyítható, vagyis $\neg\mathbf{A}$ *nem cáfolható* $\mathfrak{T}$-ben, így az első állításból következik, hogy a $\mathfrak{T}[\neg\mathbf{A}]$ elmélet *ellentmondásmentes*, ami a b) állítást igazolja. ■

2.4.23. Tétel. (**Az indirekt bizonyítás elve.**) *Ha* $\mathbf{A}$ *formula a* $\mathfrak{T}$ *matematikai elméletben és a* $\mathfrak{T}[\neg\mathbf{A}]$ *matematikai elmélet ellentmondásos, akkor* $\mathbf{A}$ *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Nyilvánvalóan következik az előző állítás b) pontjából. ■

A mindennapi matematikai gyakorlatban az indirekt bizonyítás elvét a következőképpen alkalmazzuk. Legyen $\mathbf{A}$ az a formula a $\mathfrak{T}$ matematikai elméletben, amelyről be akarjuk bizonyítani, hogy tétel $\mathfrak{T}$-ben.

– Először így fogalmazunk: "Tegyük fel, hogy $\mathbf{A}$ nem igaz." Ezen azt értjük, hogy $\mathfrak{T}$-ről áttérünk a $\mathfrak{T}[\neg\mathbf{A}]$ elméletre, amelyben $\mathbf{A}$ abban az értelemben *nem igaz*, hogy $\neg\mathbf{A}$ tétel benne, sőt explicit axióma.

– Ezután azt mondjuk, hogy "Megmutatjuk, hogy ekkor ellentmondásra jutunk." Ez azt jelenti, hogy igazoljuk a $\mathfrak{T}[\neg\mathbf{A}]$ elmélet ellentmondásosságát, vagyis előállítunk olyan formulát, amely a negációjával együtt bebizonyítható $\mathfrak{T}[\neg\mathbf{A}]$-ban.

– Végül kijelentjük, hogy "Tehát $\mathbf{A}$ igaz.", ami azt jelenti, hogy az indirekt bizonyítás elve alapján $\mathbf{A}$ tétel a $\mathfrak{T}$ matematikai elméletben.

2.5. A logikai operátorok tulajdonságai

2.5.1. Állítás. *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor* $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{A}$ *és* $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{B}$ *logikai tételek* $\mathfrak{T}$*-ben.*

Bizonyítás. A $(\neg\mathbf{A}) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$ formula eleme $\mathfrak{S}_2$-nek, tehát logikai tétel $\mathfrak{T}$-ben. Ezért a kontrapozíció elve alapján $(\neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))) \Rightarrow (\neg\neg\mathbf{A})$ szintén logikai tétel $\mathfrak{T}$-ben. A konjunkció definíciója szerint $\mathbf{A} \wedge \mathbf{B} \equiv \neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$, tehát $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow (\neg\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben. A kettős negáció szabálya szerint $(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben, tehát a láncszabályt alkalmazva kapjuk, hogy $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben.

A $((\neg\mathbf{B}) \vee (\neg\mathbf{A})) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$ formula eleme $\mathfrak{S}_3$-nak, tehát logikai tétel $\mathfrak{T}$-ben. Ugyanakkor a $(\neg\mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \vee (\neg\mathbf{A}))$ formula eleme $\mathfrak{S}_2$-nek, tehát szintén logikai tétel $\mathfrak{T}$-ben. Ebből a láncszabály alkalmazásával kapjuk, hogy $(\neg\mathbf{B}) \Rightarrow ((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Tehát a kontrapozíció elve alapján $(\neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))) \Rightarrow (\neg\neg\mathbf{B})$ szintén logikai tétel $\mathfrak{T}$-ben. Ismét a konjunkció definíciójára hivatkozva ebből adódik, hogy $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow (\neg\neg\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. A kettős negáció szabálya szerint $(\neg\neg\mathbf{B}) \Rightarrow \mathbf{B}$ logikai tétel $\mathfrak{T}$-ben, tehát a láncszabályt alkalmazva kapjuk, hogy $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{B}$ logikai tétel $\mathfrak{T}$-ben. ■

2.5.2. Tétel. (**A konjunkció logikai alaptulajdonsága.**) *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Az* $\mathbf{A} \wedge \mathbf{B}$ *formula pontosan akkor* (*logikai*) *tétel* $\mathfrak{T}$*-ben, ha* $\mathbf{A}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben és* $\mathbf{B}$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Tegyük fel, hogy $\mathbf{A} \wedge \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. Az előző állítás szerint $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{A}$ és $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{B}$ logikai tétel $\mathfrak{T}$-ben, ezért a leválasztás szabálya alapján $\mathbf{A}$ és $\mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben.

Megfordítva, tegyük fel, hogy $\mathbf{A}$ és $\mathbf{B}$ tétel $\mathfrak{T}$-ben. Jelölje $\mathfrak{T}'$ a $\mathfrak{T}[\neg(\mathbf{A} \wedge \mathbf{B})]$ elméletet. A konjunkció értelmezése alapján $\neg\neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$ tétel (sőt explicit axióma) $\mathfrak{T}'$-ben, következésképpen a kettős negáció elve alapján $(\neg\mathbf{A}) \vee (\neg\mathbf{B})$ tétel $\mathfrak{T}'$-ben. Ugyanakkor $(\neg\mathbf{A}) \vee (\neg\mathbf{B}) \equiv \mathbf{A} \Rightarrow (\neg\mathbf{B})$, tehát $\mathbf{A}$ és $\mathbf{A} \Rightarrow (\neg\mathbf{B})$ tételek $\mathfrak{T}'$-ben, így a leválasztás szabálya szerint $\neg\mathbf{B}$ tétel $\mathfrak{T}'$-ben. A feltevés szerint $\mathbf{B}$ is tétel $\mathfrak{T}'$-ben, tehát a $\mathfrak{T}'$ matematikai elmélet ellentmondásos. Az indirekt bizonyítás elve alapján $\mathbf{A} \wedge \mathbf{B}$ tétel a $\mathfrak{T}$ matematikai elméletben.

Ha $\mathbf{A}$ és $\mathbf{B}$ logikai tétel $\mathfrak{T}$-ben, akkor $\mathbf{A}$ és $\mathbf{B}$ tétel $\mathfrak{T}_0$-ban, tehát az előző bekezdés alapján $\mathbf{A} \wedge \mathbf{B}$ tétel a $\mathfrak{T}_0$-ban, vagyis $\mathbf{A} \wedge \mathbf{B}$ logikai tétel a $\mathfrak{T}$ matematikai elméletben. ■

2.5.3. Következmény. *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor az*

$$\mathbf{A} \Leftrightarrow (\neg\neg\mathbf{A})$$
$$(\mathbf{A} \Rightarrow \mathbf{B}) \Leftrightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. A kettős negáció szabálya szerint az $\mathbf{A} \Rightarrow (\neg\neg\mathbf{A})$ és $(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$ formulák logikai tételek $\mathfrak{T}$-ben, így a konjunkció logikai alaptulajdonsága szerint $(\mathbf{A} \Rightarrow (\neg\neg\mathbf{A})) \wedge ((\neg\neg\mathbf{A}) \Rightarrow \mathbf{A})$, vagyis az $\mathbf{A} \Leftrightarrow (\neg\neg\mathbf{A})$ formula logikai tétel $\mathfrak{T}$-ben.

A kontrapozíció szabálya szerint az $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ és $((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$ formulák logikai tételek $\mathfrak{T}$-ben, így a konjunkció logikai alaptulajdonsága szerint $((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))) \wedge (((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}))$, vagyis az $(\mathbf{A} \Rightarrow \mathbf{B}) \Leftrightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ formula logikai tétel $\mathfrak{T}$-ben. ■

2.5.4. Következmény. *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor az* $\mathbf{A} \Leftrightarrow \mathbf{B}$ *formula pontosan akkor* (*logikai*) *tétel* $\mathfrak{T}$*-ben, ha* $(\neg\mathbf{A}) \Leftrightarrow (\neg\mathbf{B})$ (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Tegyük fel, hogy $\mathbf{A} \Leftrightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. Ekkor a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \Rightarrow \mathbf{B}$ és $\mathbf{B} \Rightarrow \mathbf{A}$ (logikai) tételek $\mathfrak{T}$-ben. A kontrapozíció szabálya szerint az $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ és $(\mathbf{B} \Rightarrow \mathbf{A}) \Rightarrow ((\neg\mathbf{A}) \Rightarrow (\neg\mathbf{B}))$ formulák logikai tételek $\mathfrak{T}$-ben, így kétszer alkalmazva a leválasztás szabályát kapjuk, hogy $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ és $(\neg\mathbf{A}) \Rightarrow (\neg\mathbf{B})$ (logikai) tételek $\mathfrak{T}$-ben. Ezért a konjunkció logikai alaptulajdonsága szerint $((\neg\mathbf{A}) \Rightarrow (\neg\mathbf{B})) \wedge ((\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A}))$ (logikai) tétel $\mathfrak{T}$-ben, és ez a formula azonos a $(\neg\mathbf{A}) \Leftrightarrow (\neg\mathbf{B})$ formulával.

Megfordítva, tegyük fel, hogy $(\neg\mathbf{A}) \Leftrightarrow (\neg\mathbf{B})$ (logikai) tétel $\mathfrak{T}$-ben. Az előző bekezdés szerint ekkor $(\neg\neg\mathbf{A}) \Leftrightarrow (\neg\neg\mathbf{B})$ (logikai) tétel $\mathfrak{T}$-ben, tehát a konjunkció logikai alaptulajdonságát alkalmazva kapjuk, hogy $(\neg\neg\mathbf{A}) \Rightarrow (\neg\neg\mathbf{B})$ és $(\neg\neg\mathbf{B}) \Rightarrow (\neg\neg\mathbf{A})$ (logikai) tételek $\mathfrak{T}$-ben. A kettős negáció szabálya szerint az $\mathbf{A} \Rightarrow (\neg\neg\mathbf{A})$ és $(\neg\neg\mathbf{B}) \Rightarrow \mathbf{B}$ formulák logikai tételek $\mathfrak{T}$-ben, így kétszer alkalmazva a láncszabályt kapjuk, hogy $\mathbf{A} \Rightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. Szintén a kettős negáció szabálya szerint a $\mathbf{B} \Rightarrow (\neg\neg\mathbf{B})$ és $(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$ formulák logikai tételek $\mathfrak{T}$-ben, így kétszer alkalmazva a láncszabályt kapjuk, hogy $\mathbf{B} \Rightarrow \mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. Ezért a konjunkció logikai alaptulajdonsága szerint az $\mathbf{A} \Leftrightarrow \mathbf{B}$ formula (logikai) tétel $\mathfrak{T}$-ben. ■

2.5.5. Tétel. (**Az ekvivalencia logikai alaptulajdonsága.**) *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Az* $\mathbf{A}\Leftrightarrow\mathbf{B}$ *formula pontosan akkor tétel* $\mathfrak{T}$*-ben, ha* $\mathbf{B}$ *tétel* $\mathfrak{T}[\mathbf{A}]$*-ban és* $\mathbf{A}$ *tétel* $\mathfrak{T}[\mathbf{B}]$*-ben. Az* $\mathbf{A}\Leftrightarrow\mathbf{B}$ *formula pontosan akkor logikai tétel* $\mathfrak{T}$*-ben, ha az* $\mathbf{A} \Rightarrow \mathbf{B}$ *és* $\mathbf{B} \Rightarrow \mathbf{A}$ *formulák logikai tételek* $\mathfrak{T}$*-ben.*

Bizonyítás. Az ekvivalencia értelmezése szerint $\mathbf{A}\Leftrightarrow\mathbf{B}\equiv(\mathbf{A} \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow \mathbf{A})$, ezért a konjunkció logikai alaptulajdonsága szerint az $\mathbf{A}\Leftrightarrow\mathbf{B}$ formula pontosan akkor (logikai) tétel $\mathfrak{T}$-ben, ha $\mathbf{A} \Rightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben és $\mathbf{B} \Rightarrow \mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. Az implikáció logikai alaptulajdonsága szerint $\mathbf{A} \Rightarrow \mathbf{B}$ pontosan akkor tétel $\mathfrak{T}$-ben, ha $\mathbf{B}$ tétel $\mathfrak{T}[\mathbf{A}]$-ban, és $\mathbf{B} \Rightarrow \mathbf{A}$ pontosan akkor tétel $\mathfrak{T}$-ben, ha $\mathbf{A}$ tétel $\mathfrak{T}[\mathbf{B}]$-ben. ■

2.5.6. Következmény. *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor az*

$$((\mathbf{A} \vee \mathbf{B}) \Rightarrow \mathbf{C}) \Leftrightarrow ((\mathbf{A} \Rightarrow \mathbf{C}) \wedge (\mathbf{B} \Rightarrow \mathbf{C}))$$

formula logikai tétel $\mathfrak{T}$*-ben.*

Bizonyítás. Az ekvivalencia logikai alaptulajdonsága szerint elég azt igazolni, hogy $(\mathbf{A} \Rightarrow \mathbf{C}) \wedge (\mathbf{B} \Rightarrow \mathbf{C})$ tétel a $\mathfrak{T}' \equiv \mathfrak{T}_0[(\mathbf{A} \vee \mathbf{B}) \Rightarrow \mathbf{C}]$ matematikai elméletben, és $(\mathbf{A} \vee \mathbf{B}) \Rightarrow \mathbf{C}$ tétel a $\mathfrak{T}'' \equiv \mathfrak{T}_0[(\mathbf{A} \Rightarrow \mathbf{C}) \wedge (\mathbf{B} \Rightarrow \mathbf{C})]$ matematikai elméletben.

Az $(\mathbf{A}\vee\mathbf{B}) \Rightarrow \mathbf{C}$ formula explicit axióma a $\mathfrak{T}'$ matematikai elméletben és az $\mathbf{A} \Rightarrow (\mathbf{A}\vee\mathbf{B})$ formula eleme $\mathfrak{S}_2$-nek, így a láncszabály szerint $\mathbf{A} \Rightarrow \mathbf{C}$ tétel $\mathfrak{T}'$-ben. A $\mathbf{B} \Rightarrow (\mathbf{B} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_2$-nek és $(\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee \mathbf{B})$ eleme $\mathfrak{S}_3$-nak, így a láncszabály szerint $\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ tétel $\mathfrak{T}'$, tehát ismét alkalmazva a láncszabályt kapjuk, hogy $\mathbf{B} \Rightarrow \mathbf{C}$ is tétel $\mathfrak{T}'$-ben. Ezért a konjunkció logikai alaptulajdonsága szerint $(\mathbf{A} \Rightarrow \mathbf{C}) \wedge (\mathbf{B} \Rightarrow \mathbf{C})$ tétel a $\mathfrak{T}'$ matematikai elméletben.

Az $(\mathbf{A} \Rightarrow \mathbf{C}) \wedge (\mathbf{B} \Rightarrow \mathbf{C})$ formula explicit axióma a $\mathfrak{T}''$ matematikai elméletben, tehát a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \Rightarrow \mathbf{C}$ és $\mathbf{B} \Rightarrow \mathbf{C}$ tételek $\mathfrak{T}''$-ben. A $(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee \mathbf{C}))$ formula eleme $\mathfrak{S}_4$-nek, ezért a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee \mathbf{C})$ tétel $\mathfrak{T}''$-ben. Az $(\mathbf{A} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{C}))$ formula eleme $\mathfrak{S}_4$-nek, ezért a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{C})$ tétel $\mathfrak{T}''$-ben. Az $(\mathbf{A} \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_2$-nek, így kétszer alkalmazva a láncszabályt kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{C} \vee \mathbf{C})$ tétel $\mathfrak{T}''$-ben. A $(\mathbf{C} \vee \mathbf{C}) \Rightarrow \mathbf{C}$ formula eleme $\mathfrak{S}_1$-nek, ezért utoljára alkalmazva a láncszabályt kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Rightarrow \mathbf{C}$ tétel a $\mathfrak{T}''$ matematikai elméletben. ■

2.5.7. Következmény. *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor az*

$$(\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Leftrightarrow ((\mathbf{A} \wedge \neg\mathbf{B}) \Rightarrow \mathbf{C})$$
$$(\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Leftrightarrow ((\mathbf{A} \wedge \neg\mathbf{C}) \Rightarrow \mathbf{B})$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. (I) Az ekvivalencia logikai alaptulajdonsága szerint az első állítás bizonyításához elegendő azt igazolni, hogy $(\mathbf{A} \wedge \neg\mathbf{B}) \Rightarrow \mathbf{C}$ tétel a $\mathfrak{T}' \equiv \mathfrak{T}_0[\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})]$ matematikai elméletben, és $\mathbf{A}\Rightarrow(\mathbf{B} \vee \mathbf{C})$ tétel a $\mathfrak{T}'' \equiv \mathfrak{T}_0[(\mathbf{A} \wedge \neg\mathbf{B}) \Rightarrow \mathbf{C}]$ matematikai elméletben.

Legyen $\mathfrak{T}^* \equiv \mathfrak{T}'[\mathbf{A} \wedge \neg\mathbf{B}]$. Ekkor $\mathbf{A} \wedge \neg\mathbf{B}$ tétel $\mathfrak{T}^*$-ban, így a konjunkció logikai alaptulajdonsága szerint $\mathbf{A}$ és $\neg\mathbf{B}$ tétel $\mathfrak{T}^*$-ban. Mivel $\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})$ is tétel $\mathfrak{T}^*$-ban, így a leválasztás szabálya szerint $\mathbf{B} \vee \mathbf{C}$ tétel $\mathfrak{T}^*$-ban. A $(\mathbf{B} \Rightarrow \neg\neg\mathbf{B}) \Rightarrow ((\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{C} \vee \neg\neg\mathbf{B}))$ formula eleme $\mathfrak{S}_4$-nek, és a kettős negáció szabálya szerint $\mathbf{B} \Rightarrow \neg\neg\mathbf{B}$ tétel $\mathfrak{T}^*$-ban, ezért a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{C} \vee \neg\neg\mathbf{B})$ tétel $\mathfrak{T}^*$-ban. A $(\mathbf{B} \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \mathbf{B})$ formula eleme $\mathfrak{S}_3$-nak, így a láncszabály alkalmazásával kapjuk, hogy $(\mathbf{B} \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \neg\neg\mathbf{B})$ tétel $\mathfrak{T}^*$-ban. Ugyanakkor $\mathbf{B} \vee \mathbf{C}$ tétel $\mathfrak{T}^*$-ban, így ebből a leválasztás szabálya alapján adódik, hogy $\mathbf{C} \vee \neg\neg\mathbf{B}$ tétel $\mathfrak{T}^*$-ban. A $(\mathbf{C} \vee \neg\neg\mathbf{B}) \Rightarrow ((\neg\neg\mathbf{B}) \vee \mathbf{C})$ formula eleme $\mathfrak{S}_2$-nek, így a leválasztás szabályának alkalmazásával kapjuk, hogy $(\neg\neg\mathbf{B}) \vee \mathbf{C}$ tétel $\mathfrak{T}^*$-ban. Ez a formula azonos a $(\neg\mathbf{B}) \Rightarrow \mathbf{C}$ formulával, és mivel $\neg\mathbf{B}$ tétel $\mathfrak{T}^*$-ban, ebből a leválasztás szabályának alkalmazásával kapjuk, hogy $\mathbf{C}$ tétel $\mathfrak{T}^*$-ban. A definíció szerint $\mathfrak{T}^* \equiv \mathfrak{T}'[\mathbf{A} \wedge \neg\mathbf{B}]$, tehát ebből a dedukció-tétel alapján következik, hogy $(\mathbf{A} \wedge \neg\mathbf{B}) \Rightarrow \mathbf{C}$ tétel $\mathfrak{T}'$-ben.

Legyen $\mathfrak{T}^{**} \equiv (\mathfrak{T}''[\mathbf{A}])[\neg\mathbf{B}]$. Ekkor $\mathbf{A}$, $\neg\mathbf{B}$ és $(\mathbf{A} \wedge \neg\mathbf{B}) \Rightarrow \mathbf{C}$ tételek $\mathfrak{T}^{**}$-ban. A konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \wedge \neg\mathbf{B}$ tétel $\mathfrak{T}^{**}$-ban, így a leválasztás szabályának alkalmazásával kapjuk, hogy $\mathbf{C}$ tétel $\mathfrak{T}^{**}$-ban. A $\mathfrak{T}^{**}$ elmélet definíciója és a dedukció-tétel alapján ebből következik, hogy $(\neg\mathbf{B}) \Rightarrow \mathbf{C}$ tétel $\mathfrak{T}''[\mathbf{A}]$-ban. Ugyanakkor $((\neg\mathbf{B}) \Rightarrow \mathbf{C}) \equiv ((\neg\neg\mathbf{B}) \vee \mathbf{C})$, tehát $(\neg\neg\mathbf{B}) \vee \mathbf{C}$ tétel $\mathfrak{T}''[\mathbf{A}]$-ban. A $((\neg\neg\mathbf{B}) \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{C} \vee (\neg\neg\mathbf{B})) \Rightarrow (\mathbf{C} \vee \mathbf{B}))$ formula eleme $\mathfrak{S}_4$-nek, így a kettős negáció és a leválasztás szabálya alapján kapjuk, hogy $(\mathbf{C} \vee (\neg\neg\mathbf{B})) \Rightarrow (\mathbf{C} \vee \mathbf{B})$ tétel $\mathfrak{T}''[\mathbf{A}]$-ban. A $((\neg\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee (\neg\neg\mathbf{B}))$ formula eleme $\mathfrak{S}_2$-nek, így a láncszabály szerint $((\neg\neg\mathbf{B}) \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \mathbf{B})$ tétel $\mathfrak{T}''[\mathbf{A}]$-ban. Ebből ismét alkalmazva a leválasztás szabályát kapjuk, hogy $\mathbf{C} \vee \mathbf{B}$ tétel $\mathfrak{T}''[\mathbf{A}]$-ban. Mivel $(\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{C})$ szintén eleme $\mathfrak{S}_2$-nek, így a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{B} \vee \mathbf{C}$ tétel $\mathfrak{T}''[\mathbf{A}]$-ban. Ebből a dedukció-tétel alapján következik, hogy $\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})$ tétel $\mathfrak{T}''$-ben.

Ezzel igazoltuk, hogy az $(\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Leftrightarrow ((\mathbf{A} \wedge \neg\mathbf{B}) \Rightarrow \mathbf{C})$ formula logikai tétel a $\mathfrak{T}$ matematikai elméletben.

(II) Az (I) állítást alkalmazva a $\mathbf{B}$ és $\mathbf{C}$ formulák felcserélésével kapjuk, hogy

$$(\mathbf{A} \Rightarrow (\mathbf{C} \vee \mathbf{B})) \Leftrightarrow ((\mathbf{A} \wedge \neg\mathbf{C}) \Rightarrow \mathbf{B})$$

logikai tétel $\mathfrak{T}$-ben. Ebből az ekvivalencia definíciója és a konjunkció alaptulajdonságának alkalmazásával kapjuk, hogy a

$$\begin{aligned} (\mathbf{A} \Rightarrow (\mathbf{C} \vee \mathbf{B})) &\Rightarrow ((\mathbf{A} \wedge \neg\mathbf{C}) \Rightarrow \mathbf{B}) \\ ((\mathbf{A} \wedge \neg\mathbf{C}) \Rightarrow \mathbf{B}) &\Rightarrow (\mathbf{A} \Rightarrow (\mathbf{C} \vee \mathbf{B})) \end{aligned}$$

formulák szintén logikai tételek $\mathfrak{T}$-ben.

A $(\mathbf{B} \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \mathbf{B})$ formula eleme $\mathfrak{S}_2$-nek, és a $((\mathbf{B} \vee \mathbf{C}) \Rightarrow (\mathbf{C} \vee \mathbf{B})) \Rightarrow ((\neg\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})) \Rightarrow ((\neg\mathbf{A} \vee (\mathbf{C} \vee \mathbf{B})))$ formula eleme $\mathfrak{S}_4$-nek, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\neg\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})) \Rightarrow ((\neg\mathbf{A} \vee (\mathbf{C} \vee \mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Az implikáció definíciója szerint ez azt jelenti, hogy $(\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Rightarrow (\mathbf{A} \Rightarrow (\mathbf{C} \vee \mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, így a láncszabály szerint $(\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Rightarrow ((\mathbf{A} \wedge \neg\mathbf{C}) \Rightarrow \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben.

A $(\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{C})$ formula eleme $\mathfrak{S}_2$-nek, és a $((\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Rightarrow ((\neg\mathbf{A} \vee (\mathbf{C} \vee \mathbf{B})) \Rightarrow (\neg\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})))$ formula eleme $\mathfrak{S}_4$-nek, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\neg\mathbf{A} \vee (\mathbf{C} \vee \mathbf{B})) \Rightarrow (\neg\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben. Az implikáció definíciója szerint ez azt jelenti, hogy $(\mathbf{A} \Rightarrow (\mathbf{C} \vee \mathbf{B})) \Rightarrow (\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben, így a láncszabály szerint $((\mathbf{A} \wedge \neg\mathbf{C}) \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben.

Ebből a konjunkció logikai alaptulajdonsága és az ekvivalencia definíciója alapján kapjuk, hogy $(\mathbf{A} \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Leftrightarrow ((\mathbf{A} \wedge \neg\mathbf{C}) \Rightarrow \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. ■

A 2.5.2. és 2.5.5. tételeket komoly okkal minősítettük *logikai alaptulajdonságoknak.* A nem formális (naiv) logikában az "és" (illetve "ekvivalens") logikai operációkkal kapcsolatban határozott elvárásainak vannak, és az előző tételek éppen azt fejezik ki, hogy a formális logika igazság-fogalma és az $\wedge$ (illetve $\Leftrightarrow$) szimólumai eleget tesznek a természetes követelményeknek. Pontosabban, a nem formális logikában elvárjuk, hogy ha $\mathbf{A}$ és $\mathbf{B}$ kijelentések, akkor az "$\mathbf{A}$ és $\mathbf{B}$" (illetve "$\mathbf{A}$ ekvivalens $\mathbf{B}$-vel") kijelelentés pontosan akkor legyen igaz, ha "$\mathbf{A}$ igaz és $\mathbf{B}$ igaz" (illetve "$\mathbf{A}$-ból következik $\mathbf{B}$ és $\mathbf{B}$-ből következik $\mathbf{A}$"). A konjunkció és ekvivalencia logikai alaptulajdonsága szerint ez teljesül a formális axiomatikus matematikai elméletekben, ha az "és" (illetve "ekvivalens") kifejezést az $\wedge$ (illetve $\Leftrightarrow$) szimbólummal formalizáljuk, és az "igaz" fogalmat a "tétel" fogalommal helyettesítjük.

Vegyük észre, hogy a *diszjunkcióval* kapcsolatban nem fogalmaztunk meg logikai alaptulajdonságot. Ennek komoly oka van. Könnyen belátható, hogy ha $\mathbf{A}$ és $\mathbf{B}$ formulák a $\mathfrak{T}$ matematikai elméletben, és $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, *vagy* $\mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, akkor $\mathbf{A} \vee \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. Valóban, ha $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, akkor $\mathbf{A} \vee \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, mert az $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ formula eleme $\mathfrak{S}_2$-nek, és elég a leválasztás szabályát alkalmazni. Másfelől, $\mathbf{B} \Rightarrow (\mathbf{B} \vee \mathbf{A})$ eleme $\mathfrak{S}_2$-nek, és $(\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee \mathbf{B})$ eleme $\mathfrak{S}_3$-nak, így a láncszabály szerint $\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben, tehát ha $\mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben, akkor ismét a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{A} \vee \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. Azonban abból, hogy az $\mathbf{A} \vee \mathbf{B}$ formula (logikai) tétel $\mathfrak{T}$-ben, *egyáltalán nem következik* az, hogy $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, *vagy* $\mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben! Például, a kizárt harmadik elve alapján a $(\neg\mathbf{A}) \vee \mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben, de ha $\mathfrak{T}$ predikátumkalkulus (3.1.1.), akkor látni fogjuk, hogy $\mathbf{A}$ megválasztható úgy, hogy sem $\neg\mathbf{A}$, sem $\mathbf{A}$ ne legyen tétel $\mathfrak{T}$-ben (3.4.3.).

2.5.8. Állítás. **(Az ekvivalencia logikai tulajdonságai.)** *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$\mathbf{A} \Leftrightarrow \mathbf{A}, \qquad (\textit{reflexivitás})$$

$$(\mathbf{A}\Leftrightarrow\mathbf{B}) \Leftrightarrow (\mathbf{B}\Leftrightarrow\mathbf{A}), \qquad (\textit{szimmetrikusság})$$

$$((\mathbf{A}\Leftrightarrow\mathbf{B}) \wedge (\mathbf{B}\Leftrightarrow\mathbf{C})) \Rightarrow (\mathbf{A}\Leftrightarrow\mathbf{C}). \qquad (\textit{tranzitivitás})$$

Bizonyítás. Az $\mathbf{A} \Rightarrow \mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben, ezért a konjunkció logikai alaptulajdonsága szerint $(\mathbf{A} \Rightarrow \mathbf{A}) \wedge (\mathbf{A} \Rightarrow \mathbf{A})$ is logikai tétel $\mathfrak{T}$-ben, vagyis az ekvivalencia értelmezése szerint $\mathbf{A}\Leftrightarrow\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben.

Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[\mathbf{A}\Leftrightarrow\mathbf{B}]$ elméletet. Ebben $\mathbf{A}\Leftrightarrow\mathbf{B}$, vagyis $(\mathbf{A} \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow \mathbf{A})$ tétel (sőt explicit axióma), ezért a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \Rightarrow \mathbf{B}$ és $\mathbf{B} \Rightarrow \mathbf{A}$ tételek $\mathfrak{T}'$-ben. Ez azt jelenti, hogy $\mathbf{B} \Rightarrow \mathbf{A}$ és $\mathbf{A} \Rightarrow \mathbf{B}$ tételek $\mathfrak{T}'$-ben, tehát a konjunkció logikai alaptulajdonsága szerint $(\mathbf{B} \Rightarrow \mathbf{A}) \wedge (\mathbf{A} \Rightarrow \mathbf{B})$, azaz $\mathbf{B}\Leftrightarrow\mathbf{A}$ tétel $\mathfrak{T}'$-ben. Tehát $\mathbf{B}\Leftrightarrow\mathbf{A}$ tétel a $\mathfrak{T}_0[\mathbf{A}\Leftrightarrow\mathbf{B}]$ matematikai elméletben. Ez bármely két $\mathbf{A}$ és $\mathbf{B}$ formulára igaz, ezért az $\mathbf{A}$ és $\mathbf{B}$ felcserélésével kapjuk, hogy $\mathbf{A}\Leftrightarrow\mathbf{B}$ is tétel a $\mathfrak{T}_0[\mathbf{B}\Leftrightarrow\mathbf{A}]$ matematikai elméletben. Az ekvivalencia logikai alaptulajdonsága szerint ez azt jelenti, hogy $(\mathbf{A}\Leftrightarrow\mathbf{B})\Leftrightarrow(\mathbf{B}\Leftrightarrow\mathbf{A})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[(\mathbf{A}\Leftrightarrow\mathbf{B}) \wedge (\mathbf{B}\Leftrightarrow\mathbf{C})]$ elméletet. Ebben $(\mathbf{A}\Leftrightarrow\mathbf{B}) \wedge (\mathbf{B}\Leftrightarrow\mathbf{C})$ tétel (sőt explicit axióma), ezért a konjunkció logikai alaptulajdonsága szerint $\mathbf{A}\Leftrightarrow\mathbf{B}$ és $\mathbf{B}\Leftrightarrow\mathbf{C}$ tételek $\mathfrak{T}'$-ben. Az ekvivalencia értelmezése és ismét a konjunkció logikai alaptulajdonsága szerint az $\mathbf{A} \Rightarrow \mathbf{B}$, $\mathbf{B} \Rightarrow \mathbf{A}$, $\mathbf{B} \Rightarrow \mathbf{C}$ és $\mathbf{C} \Rightarrow \mathbf{B}$ formulák mind tételek $\mathfrak{T}'$-ben. A láncszabályt kétszer alkalmazva kapjuk, hogy $\mathbf{A} \Rightarrow \mathbf{C}$ és $\mathbf{C} \Rightarrow \mathbf{A}$ tétel $\mathfrak{T}'$-ben, tehát a konjunkció logikai alaptulajdonsága és az ekvivalencia értelmezése alapján $\mathbf{A}\Leftrightarrow\mathbf{C}$ tétel $\mathfrak{T}'$-ben. Ezért a dedukció-tétel szerint $((\mathbf{A}\Leftrightarrow\mathbf{B}) \wedge (\mathbf{B}\Leftrightarrow\mathbf{C})) \Rightarrow (\mathbf{A}\Leftrightarrow\mathbf{C})$ tétel $\mathfrak{T}_0$-ban, vagyis ez logikai tétel $\mathfrak{T}$-ben. ∎

2.5.9. Állítás. *Legyenek* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{A}'$ *és* $\mathbf{B}'$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Ha* $\mathbf{A}\Leftrightarrow\mathbf{A}'$ *(logikai) tétel* $\mathfrak{T}$*-ben, akkor* $(\neg\mathbf{A})\Leftrightarrow(\neg\mathbf{A}')$ *is (logikai) tétel* $\mathfrak{T}$*-ben. Ha* $\mathbf{A}\Leftrightarrow\mathbf{A}'$ *és* $\mathbf{B}\Leftrightarrow\mathbf{B}'$ *(logikai) tételek* $\mathfrak{T}$*-ben, akkor az* $(\mathbf{A} \vee \mathbf{B})\Leftrightarrow(\mathbf{A}' \vee \mathbf{B}')$, $(\mathbf{A} \Rightarrow \mathbf{B})\Leftrightarrow(\mathbf{A}' \Rightarrow \mathbf{B}')$, $(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow(\mathbf{A}' \wedge \mathbf{B}')$ *és* $(\mathbf{A}\Leftrightarrow\mathbf{B})\Leftrightarrow(\mathbf{A}'\Leftrightarrow\mathbf{B}')$ *formulák (logikai) tételek* $\mathfrak{T}$*-ben.*

Bizonyítás. Tegyük fel, hogy $\mathbf{A}\Leftrightarrow\mathbf{A}'$ (logikai) tétel $\mathfrak{T}$-ben. Ekkor az ekvivalencia értelmezése és a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \Rightarrow \mathbf{A}'$ és $\mathbf{A}' \Rightarrow \mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, és a kontrapozíció szabálya szerint $(\mathbf{A} \Rightarrow \mathbf{A}') \Rightarrow ((\neg\mathbf{A}') \Rightarrow (\neg\mathbf{A}))$ és $(\mathbf{A}' \Rightarrow \mathbf{A}) \Rightarrow ((\neg\mathbf{A}) \Rightarrow (\neg\mathbf{A}'))$ logikai tétel $\mathfrak{T}$-ben. Ebből a leválasztás szabályát alkalmazva kapjuk, hogy $(\neg\mathbf{A}') \Rightarrow (\neg\mathbf{A})$ és $(\neg\mathbf{A}) \Rightarrow (\neg\mathbf{A}')$ (logikai) tétel $\mathfrak{T}$-ben. Tehát $(\neg\mathbf{A}) \Rightarrow (\neg\mathbf{A}')$ és $(\neg\mathbf{A}') \Rightarrow (\neg\mathbf{A})$ (logikai) tétel $\mathfrak{T}$-ben, így a konjunkció logikai alaptulajdonsága és az ekvivalencia értelmezése alapján $(\neg\mathbf{A})\Leftrightarrow(\neg\mathbf{A}')$ (logikai) tétel $\mathfrak{T}$-ben.

Tegyük fel, hogy $\mathbf{A}\Leftrightarrow\mathbf{A}'$ és $\mathbf{B}\Leftrightarrow\mathbf{B}'$ (logikai) tételek $\mathfrak{T}$-ben. Ekkor $\mathbf{A} \Rightarrow \mathbf{A}'$, $\mathbf{A}' \Rightarrow \mathbf{A}$, $\mathbf{B} \Rightarrow \mathbf{B}'$ és $\mathbf{B}' \Rightarrow \mathbf{B}$ (logikai) tételek $\mathfrak{T}$-ben, így 2.4.18. szerint $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A}' \vee \mathbf{B}')$ és $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow (\mathbf{A}' \wedge \mathbf{B}')$ (logikai) tételek $\mathfrak{T}$-ben, ugyanakkor $(\mathbf{A}' \vee \mathbf{B}') \Rightarrow (\mathbf{A} \vee \mathbf{B})$ és $(\mathbf{A}' \wedge \mathbf{B}') \Rightarrow (\mathbf{A} \wedge \mathbf{B})$ is (logikai) tételek $\mathfrak{T}$-ben. Így a konjunkció logikai alaptulajdonsága és az ekvivalencia értelmezése alapján $(\mathbf{A} \vee \mathbf{B})\Leftrightarrow(\mathbf{A}' \vee \mathbf{B}')$ és $(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow(\mathbf{A}' \wedge \mathbf{B}')$ (logikai) tételek $\mathfrak{T}$-ben.

Ismét tegyük fel, hogy $\mathbf{A}\Leftrightarrow\mathbf{A}'$ és $\mathbf{B}\Leftrightarrow\mathbf{B}'$ (logikai) tételek $\mathfrak{T}$-ben. Az első bekezdés alapján $(\neg\mathbf{A})\Leftrightarrow(\neg\mathbf{A}')$ (logikai) tétel $\mathfrak{T}$-ben, így a második bekezdésből adódik, hogy $((\neg\mathbf{A}) \vee \mathbf{B})\Leftrightarrow((\neg\mathbf{A}') \vee \mathbf{B}')$ (logikai) tétel $\mathfrak{T}$-ben; ez pontosan azt jelenti, hogy $(\mathbf{A} \Rightarrow \mathbf{B})\Leftrightarrow(\mathbf{A}' \Rightarrow \mathbf{B}')$ (logikai) tétel $\mathfrak{T}$-ben. Ebből látható, hogy $(\mathbf{B} \Rightarrow \mathbf{A})\Leftrightarrow(\mathbf{B}' \Rightarrow \mathbf{A}')$ szintén (logikai) tétel $\mathfrak{T}$-ben. Ezért a második bekezdés szerint $((\mathbf{A} \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow \mathbf{A}))\Leftrightarrow((\mathbf{A}' \Rightarrow \mathbf{B}') \wedge (\mathbf{B}' \Rightarrow \mathbf{A}'))$ (logikai) tétel $\mathfrak{T}$-ben. Az ekvivalencia definícója alapján ez éppen azt jelenti, hogy $(\mathbf{A}\Leftrightarrow\mathbf{B})\Leftrightarrow(\mathbf{A}'\Leftrightarrow\mathbf{B}')$ (logikai) tétel $\mathfrak{T}$-ben. ∎

2.5.10. Állítás. **(Az implikáció negációja.)** *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor*

$$\neg(\mathbf{A} \Rightarrow \mathbf{B}) \Leftrightarrow (\mathbf{A} \wedge (\neg\mathbf{B}))$$

logikai tétel $\mathfrak{T}$*-ben.*

Bizonyítás. Az ekvivalencia reflexivitása szerint $\mathbf{A}\Leftrightarrow\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben és a 2.5.3. állítás szerint $\mathbf{B}\Leftrightarrow(\neg\neg\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben, így 2.5.9. miatt $(\mathbf{A} \Rightarrow \mathbf{B})\Leftrightarrow(\mathbf{A} \Rightarrow (\neg\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Ebből ismét 2.5.9. alkalmazásával kapjuk, hogy $(\neg(\mathbf{A} \Rightarrow \mathbf{B}))\Leftrightarrow(\neg(\mathbf{A} \Rightarrow (\neg\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. Ugyanakkor, a konjunkció és az implikáció értelmezése alapján $\neg(\mathbf{A} \Rightarrow (\neg\neg\mathbf{B})) \equiv (\mathbf{A} \wedge (\neg\mathbf{B}))$. ∎

2.5.11. Állítás. **(A konjunkció és diszjunkció logikai tulajdonságai.)** *Ha* $\mathbf{A}$, $\mathbf{B}$

és $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor az*

$$\begin{array}{cc} \mathbf{A} \Leftrightarrow \mathbf{A} \wedge \mathbf{A} & \mathbf{A} \Leftrightarrow \mathbf{A} \vee \mathbf{A} \\ \mathbf{A} \wedge \mathbf{B} \Leftrightarrow \mathbf{B} \wedge \mathbf{A} & \mathbf{A} \vee \mathbf{B} \Leftrightarrow \mathbf{B} \vee \mathbf{A} \\ \multicolumn{2}{c}{(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C} \Leftrightarrow \mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C}),} \\ \multicolumn{2}{c}{(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C} \Leftrightarrow \mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})} \end{array}$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. (I) A 2.5.1. állítás szerint $(\mathbf{A} \wedge \mathbf{A}) \Rightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben. Megfordítva, $\mathbf{A}$ tétel a $\mathfrak{T}_0[\mathbf{A}]$ elméletben, ezért a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \wedge \mathbf{A}$ is tétel ebben az elméletben, így a dedukció-tétel alkalmazásával kapjuk, hogy $\mathbf{A} \Rightarrow (\mathbf{A} \wedge \mathbf{A})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$. Ebből az ekvivalencia logikai alaptulajdonságát alkalmazva nyerjük, hogy $(\mathbf{A} \wedge \mathbf{A}) \Leftrightarrow \mathbf{A}$ logikai tétel $\mathfrak{T}$-ben.

Az $(\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}$ formula eleme $\mathfrak{S}_1$-nek, és az $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_2$-nek, ezért a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \Leftrightarrow (\mathbf{A} \vee \mathbf{A})$ logikai tétel $\mathfrak{T}$.

(II) Az $\mathbf{A} \wedge \mathbf{B}$ formula tétel $\mathfrak{T}_0[\mathbf{A} \wedge \mathbf{B}]$-ben, tehát $\mathbf{A}$ és $\mathbf{B}$ tétel ebben az elméletben. Ezért a konjunkció logikai alaptulajdonsága szerint $\mathbf{B} \wedge \mathbf{A}$ tétel ebben az elméletben, így a dedukció-tétel alapján $(\mathbf{A} \wedge \mathbf{B}) \Rightarrow (\mathbf{B} \wedge \mathbf{A})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben. Ez a $\mathfrak{T}$ elmélet bármely két $\mathbf{A}$ és $\mathbf{B}$ formulájára igaz, így $\mathbf{A}$ és $\mathbf{B}$ felcserélésével kapjuk, hogy $(\mathbf{B} \wedge \mathbf{A}) \Rightarrow (\mathbf{A} \wedge \mathbf{B})$ is logikai tétel $\mathfrak{T}$-ben. Ebből az ekvivalencia logikai alaptulajdonságának alkalmazásával kapjuk, hogy $(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow (\mathbf{B} \wedge \mathbf{A})$ logikai tétel $\mathfrak{T}$-ben.

Az $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})$ és $(\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee \mathbf{B})$ formulák elemei $\mathfrak{S}_3$-nak, tehát logikai tételek $\mathfrak{T}$-ben, így a konjunkció logikai alaptulajdonságának alkalmazásával kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow (\mathbf{B} \vee \mathbf{A})$ logikai tétel $\mathfrak{T}$-ben.

(III) Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})]$ elméletet. Az $\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})$ formula tétel $\mathfrak{T}'$-ben (sőt explicit axióma), tehát a konjunkció logikai alaptulajdonsága szerint $\mathbf{A}$ és $\mathbf{B} \wedge \mathbf{C}$ tételek $\mathfrak{T}'$-ben. Ismét a konjunkció logikai alaptulajdonságát alkalmazva kapjuk, hogy $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ tételek $\mathfrak{T}'$-ben. Mivel $\mathbf{A}$ és $\mathbf{B}$ tételek $\mathfrak{T}'$-ben, a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \wedge \mathbf{B}$ tétel $\mathfrak{T}'$-ben. Ugyanakkor $\mathbf{C}$ is tétel $\mathfrak{T}'$-ben, tehát a konjunkció logikai alaptulajdonsága szerint $(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}$ tétel $\mathfrak{T}'$-ben. A dedukció-tétel alapján kapjuk, hogy $(\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})) \Rightarrow ((\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

Jelölje $\mathfrak{T}''$ a $\mathfrak{T}_0[(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C})]$ elméletet. Az $(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}$ formula tétel $\mathfrak{T}''$-ben (sőt explicit axióma), tehát a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \wedge \mathbf{B}$ és $\mathbf{C}$ tételek $\mathfrak{T}''$-ben. Ismét a konjunkció logikai alaptulajdonságát alkalmazva kapjuk, hogy $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ tételek $\mathfrak{T}''$-ben. Mivel $\mathbf{B}$ és $\mathbf{C}$ tételek $\mathfrak{T}''$-ben, a konjunkció logikai alaptulajdonsága szerint $\mathbf{B} \wedge \mathbf{C}$ tétel $\mathfrak{T}''$-ben. Ugyanakkor $\mathbf{A}$ is tétel $\mathfrak{T}''$-ben, tehát a konjunkció logikai alaptulajdonsága szerint $\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})$ tétel $\mathfrak{T}''$-ben. A dedukció-tétel alapján kapjuk, hogy $((\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}) \Rightarrow (\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C}))$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

A két előző bekezdés eredményének és a konjunkció logikai alaptulajdonságának alkalmazásával kapjuk, hogy $(((\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}) \Rightarrow (\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C}))) \wedge (((\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})) \Rightarrow ((\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}))),$ vagyis $((\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}) \Leftrightarrow (\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben.

(IV) A $\mathbf{B} \Rightarrow (\mathbf{B} \vee \mathbf{C})$ formula $\mathfrak{S}_2$-nek és a $(\mathbf{B} \Rightarrow (\mathbf{B} \vee \mathbf{C})) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})))$ formula $\mathfrak{S}_4$-nek eleme, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben, vagyis tétel $\mathfrak{T}_0$-ban. Tehát, ha $\mathfrak{T}'$ jelöli a $\mathfrak{T}_0[(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C}]$ elméletet, akkor $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}))$ tétel $\mathfrak{T}'$-ben, továbbá $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C}$ tétel (sőt explicit axióma) $\mathfrak{T}'$-ben. Ugyanakkor, a $\mathbf{C} \Rightarrow \mathbf{C} \vee \mathbf{B}$ és $(\mathbf{B} \vee \mathbf{C}) \Rightarrow ((\mathbf{B} \vee \mathbf{C}) \vee \mathbf{A})$ formulák elemei $\mathfrak{S}_2$-nek, valamint a $(\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{C})$ és $((\mathbf{B} \vee \mathbf{C}) \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}))$ formulák elemei $\mathfrak{S}_3$-nak, így háromszor alkalmazva a láncszabályt kapjuk, hogy $\mathbf{C} \Rightarrow (\mathbf{A}\vee(\mathbf{B}\vee\mathbf{C}))$ tétel $\mathfrak{T}'$-ben. Ezért az esetszétválasztás szabálya szerint $\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$ is tétel $\mathfrak{T}'$-ben, így a dedukció-tételt alkalmazva kapjuk, hogy $((\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C}) \Rightarrow (\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}))$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

Az $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ és $(\mathbf{A} \vee \mathbf{B}) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C})$ formulák elemei $\mathfrak{S}_2$-nek, tehát a láncszabály szerint $\mathbf{A} \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C})$ logikai tétel $\mathfrak{T}$-ben, vagyis tétel $\mathfrak{T}_0$-ban. Tehát, ha $\mathfrak{T}''$ jelöli a $\mathfrak{T}_0[\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})]$ elméletet, akkor $\mathbf{A} \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C})$ tétel $\mathfrak{T}''$-ben, továbbá $\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$ tétel (sőt explicit axióma) $\mathfrak{T}''$-ben. Ugyanakkor, a $\mathbf{B} \Rightarrow (\mathbf{B} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_2$-nek, és a $(\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee \mathbf{B})$ formula eleme $\mathfrak{S}_3$-nak, így a láncszabály alkalmazásával kapjuk, hogy $\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ tétel $\mathfrak{T}''$-ben. Tobábbá, a $(\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})) \Rightarrow ((\mathbf{C} \vee \mathbf{B}) \Rightarrow (\mathbf{C} \vee (\mathbf{A} \vee \mathbf{B}))$ formula eleme $\mathfrak{S}_4$-nek, amiből a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{C}\vee\mathbf{B}) \Rightarrow (\mathbf{C}\vee(\mathbf{A}\vee\mathbf{B}))$ tétel $\mathfrak{T}''$-ben. Mivel a $(\mathbf{B}\vee\mathbf{C}) \Rightarrow (\mathbf{C}\vee\mathbf{B})$ és $(\mathbf{C} \vee (\mathbf{A} \vee \mathbf{B})) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C})$ formulák elemei $\mathfrak{S}_3$-nak, így kétszer alkalmazva a láncszabályt kapjuk, hogy $(\mathbf{B} \vee \mathbf{C}) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C})$ tétel $\mathfrak{T}''$-ben. Ezzel megmutattuk, hogy az $\mathbf{A} \Rightarrow ((\mathbf{A}\vee\mathbf{B})\vee\mathbf{C})$ és $\mathbf{A}\vee(\mathbf{B}\vee\mathbf{C})$ formulák mellett a $(\mathbf{B}\vee\mathbf{C}) \Rightarrow ((\mathbf{A}\vee\mathbf{B})\vee\mathbf{C})$ formula is tétel $\mathfrak{T}''$-ben, ezért az esetszétválasztás szabálya szerint $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C}$ is tétel $\mathfrak{T}''$-ben. Ebből a dedukció-tételt alkalmazva nyerjük, hogy $(\mathbf{A}\vee(\mathbf{B}\vee\mathbf{C})) \Rightarrow ((\mathbf{A}\vee\mathbf{B})\vee\mathbf{C})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

A két előző bekezdés eredményének és a konjunkció logikai alaptulajdonságának alkalmazásával kapjuk, hogy $(((\mathbf{A}\vee\mathbf{B})\vee\mathbf{C}) \Rightarrow (\mathbf{A}\vee(\mathbf{B}\vee\mathbf{C})))\wedge((\mathbf{A}\vee(\mathbf{B}\vee\mathbf{C})) \Rightarrow ((\mathbf{A}\vee\mathbf{B})\vee\mathbf{C}))$, vagyis $((\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C})\Leftrightarrow(\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben. ■

A következő állítás a konjunkció és diszjunkció negációjának szabályát fogalmazza meg.

2.5.12. Állítás. (**de Morgan-tétel.**) *Ha* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor a*

$$\neg(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow (\neg\mathbf{A}) \vee (\neg\mathbf{B})$$
$$\neg(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow (\neg\mathbf{A}) \wedge (\neg\mathbf{B})$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. A konjunkció értelmezése alapján $\neg(\mathbf{A}\wedge\mathbf{B})\equiv\neg\neg((\neg\mathbf{A})\vee(\neg\mathbf{B}))$ és 2.5.3. miatt $\neg\neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))\Leftrightarrow((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, így $\neg(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben.

A 2.5.3. állítás szerint $\mathbf{A}\Leftrightarrow(\neg\neg\mathbf{A})$ és $\mathbf{B}\Leftrightarrow(\neg\neg\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben, így 2.5.9.-ből következik, hogy $(\mathbf{A} \vee \mathbf{B})\Leftrightarrow((\neg\neg\mathbf{A}) \vee (\neg\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. 2.5.9.-ből következik, hogy $\neg(\mathbf{A}\vee\mathbf{B})\Leftrightarrow\neg((\neg\neg\mathbf{A})\vee(\neg\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Ugyanakkor a konjunkció értelmezése szerint $(\neg\mathbf{A}) \wedge (\neg\mathbf{B})\equiv\neg((\neg\neg\mathbf{A}) \vee (\neg\neg\mathbf{B}))$, következésképpen $\neg(\mathbf{A} \vee \mathbf{B})\Leftrightarrow(\neg\mathbf{A}) \wedge (\neg\mathbf{B})$ is logikai tétel $\mathfrak{T}$-ben. ■

2.5.13. Állítás. (**Disztributivitás-formulák.**) *Ha* $\mathbf{A}$, $\mathbf{B}$ *és* $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor az*

$$\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) \Leftrightarrow (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$$
$$\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) \Leftrightarrow (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. Az implikáció és a konjunkció értelmezése alapján

$$\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) \equiv \neg(\mathbf{A} \Rightarrow (\neg(\mathbf{B} \vee \mathbf{C}))),$$
$$(\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C}) \equiv (\neg(\mathbf{A} \Rightarrow (\neg\mathbf{B}))) \vee (\neg(\mathbf{A} \Rightarrow (\neg\mathbf{C}))),$$

ugyanakkor a de Morgan-tétel alapján

$$((\neg(\mathbf{A} \Rightarrow (\neg\mathbf{B}))) \vee (\neg(\mathbf{A} \Rightarrow (\neg\mathbf{C})))) \Leftrightarrow \neg((\mathbf{A} \Rightarrow (\neg\mathbf{B})) \wedge (\mathbf{A} \Rightarrow (\neg\mathbf{C})))$$

logikai tétel $\mathfrak{T}$-ben. Ezért az ekvivalencia tranzitivitásából következik, hogy ha a

$$\neg(\mathbf{A} \Rightarrow (\neg(\mathbf{B} \vee \mathbf{C}))) \Leftrightarrow \neg((\mathbf{A} \Rightarrow (\neg\mathbf{B})) \wedge (\mathbf{A} \Rightarrow (\neg\mathbf{C})))$$

formula logikai tétel $\mathfrak{T}$-ben, akkor az $(\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C})\Leftrightarrow((\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C}))$ formula is logikai tétel $\mathfrak{T}$-ben. Tehát az első állításunk bizonyításához 2.5.4. alapján elegendő azt igazolni, hogy az

$$(\mathbf{A} \Rightarrow (\neg(\mathbf{B} \vee \mathbf{C}))) \Leftrightarrow ((\mathbf{A} \Rightarrow (\neg\mathbf{B})) \wedge (\mathbf{A} \Rightarrow (\neg\mathbf{C})))$$

formula logikai tétel $\mathfrak{T}$-ben. Ez viszont könnyen igazolható.

Valóban, a $\mathfrak{T}_0[(\mathbf{A} \Rightarrow (\neg\mathbf{B}))\wedge(\mathbf{A} \Rightarrow (\neg\mathbf{C})), \mathbf{A}]$ elméletben az $\mathbf{A}$, $\mathbf{A} \Rightarrow (\neg\mathbf{B})$ és $\mathbf{A} \Rightarrow (\neg\mathbf{C})$ formulák tételek, tehát a leválasztás szabálya szerint $\neg\mathbf{B}$ és $\neg\mathbf{C}$, így ezekkel együtt $(\neg\mathbf{B}) \wedge (\neg\mathbf{C})$ tétel ebben az elméletben. Ezért a de Morgan-tétel alapján $\neg(\mathbf{B} \vee \mathbf{C})$ is tétel ebben az elméletben, tehát kétszer alkalmazva a dedukció-tételt kapjuk, hogy $((\mathbf{A} \Rightarrow (\neg\mathbf{B})) \wedge (\mathbf{A} \Rightarrow (\neg\mathbf{C}))) \Rightarrow (\mathbf{A} \Rightarrow (\neg(\mathbf{B} \vee \mathbf{C})))$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben. Megfordítva, a $\mathfrak{T}_0[\mathbf{A} \Rightarrow (\neg(\mathbf{B}\vee\mathbf{C})), \mathbf{A}]$ elméletben a de Morgan-tétel és a láncszabály szerint $\mathbf{A} \Rightarrow ((\neg\mathbf{B})\wedge(\neg\mathbf{C}))$ és $\mathbf{A}$ tétel, így a leválasztás szabályát alkalmazva kapjuk, hogy $\neg\mathbf{B}$ és $\neg\mathbf{C}$ tételek ebben az elméletben. A dedukció-tétel alapján $\mathbf{A} \Rightarrow (\neg\mathbf{B})$ és $\mathbf{A} \Rightarrow (\neg\mathbf{C})$ tételek a $\mathfrak{T}_0[\mathbf{A} \Rightarrow (\neg(\mathbf{B} \vee \mathbf{C}))]$ elméletben, tehát $(\mathbf{A} \Rightarrow (\neg\mathbf{B})) \wedge (\mathbf{A} \Rightarrow (\neg\mathbf{C}))$ is tétel ebben az elméletben. Ismét a dedukció-tételre hivatkozva ebből következik, hogy $(\mathbf{A} \Rightarrow (\neg(\mathbf{B} \vee \mathbf{C}))) \Rightarrow ((\mathbf{A} \Rightarrow (\neg\mathbf{B})) \wedge (\mathbf{A} \Rightarrow (\neg\mathbf{C})))$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

A de Morgan-tétel alapján $\neg(\mathbf{A}\vee\mathbf{B})\Leftrightarrow((\neg\mathbf{A})\wedge(\neg\mathbf{B}))$ és $\neg(\mathbf{A}\vee\mathbf{C})\Leftrightarrow((\neg\mathbf{A})\wedge(\neg\mathbf{C}))$ logikai tételek $\mathfrak{T}$-ben. Ebből következik, hogy $(\neg(\mathbf{A}\vee\mathbf{B})\vee\neg(\mathbf{A}\vee\mathbf{C}))\Leftrightarrow(((\neg\mathbf{A})\wedge(\neg\mathbf{B}))\vee((\neg\mathbf{A})\wedge(\neg\mathbf{C})))$ logikai tétel $\mathfrak{T}$-ben. A de Morgan-tételt és a konjunkció definícióját alkalmazva kapjuk, hogy $((\mathbf{A}\vee\mathbf{B})\wedge(\mathbf{A}\vee\mathbf{C}))\Leftrightarrow\neg(((\neg\mathbf{A})\wedge(\neg\mathbf{B}))\vee((\neg\mathbf{A})\wedge(\neg\mathbf{C})))$ logikai tétel $\mathfrak{T}$-ben, hiszen $(\mathbf{A}\vee\mathbf{B})\wedge(\mathbf{A}\vee\mathbf{C}) \equiv \neg(\neg(\mathbf{A}\vee\mathbf{B})\vee\neg(\mathbf{A}\vee\mathbf{C}))$. Az előzőek szerint $(((\neg\mathbf{A})\wedge(\neg\mathbf{B}))\vee((\neg\mathbf{A})\wedge(\neg\mathbf{C})))\Leftrightarrow((\neg\mathbf{A})\wedge((\neg\mathbf{B})\vee(\neg\mathbf{C})))$ logikai tétel $\mathfrak{T}$-ben. A de Morgan-tétel szerint $((\neg\mathbf{B}) \vee (\neg\mathbf{C}))\Leftrightarrow(\neg(\mathbf{B} \wedge \mathbf{C}))$ és $((\neg\mathbf{A}) \wedge (\neg(\mathbf{B} \wedge \mathbf{C})))\Leftrightarrow(\neg(\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C})))$ logikai tétel $\mathfrak{T}$-ben, ezért az előző bekezdés eredménye szerint $((\neg\mathbf{A})\wedge(\neg(\mathbf{B}\wedge\mathbf{C})))\Leftrightarrow(\neg(\mathbf{A}\vee(\mathbf{B}\wedge\mathbf{C})))$ logikai tétel $\mathfrak{T}$-ben. Mivel $\neg\neg(\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}))\Leftrightarrow(\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben, így $(\neg(((\neg\mathbf{A}) \wedge (\neg\mathbf{B})) \vee ((\neg\mathbf{A}) \wedge (\neg\mathbf{C}))))\Leftrightarrow(\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}))$ logikai tétel $\mathfrak{T}$-ben, tehát $(\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}))\Leftrightarrow((\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C}))$ szintén logikai tétel a $\mathfrak{T}$ elméletben. ■

2.5.14. Állítás. *Legyen* $\mathbf{A}$ *formula a* $\mathfrak{T}$ *matematikai elméletben.*

a) *Ha* $\mathbf{A}$ *(logikailag) cáfolható* $\mathfrak{T}$*-ben, vagyis* $\neg\mathbf{A}$ *(logikai) tétel* $\mathfrak{T}$*-ben, akkor* $\mathfrak{T}$ *minden* $\mathbf{B}$ *formulájára az* $(\mathbf{A} \vee \mathbf{B})\Leftrightarrow\mathbf{B}$ *formula (logikai) tétel* $\mathfrak{T}$*-ben.*

b) *Ha* $\mathbf{A}$ *(logikai) tétel* $\mathfrak{T}$*-ben, akkor* $\mathfrak{T}$ *minden* $\mathbf{B}$ *formulájára az* $(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow\mathbf{B}$ *formula (logikai) tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. a) Tegyük fel, hogy $\neg\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, és legyen $\mathbf{B}$ tetszőleges formula a $\mathfrak{T}$ matematikai elméletben.

A $(\neg\mathbf{A}) \Rightarrow ((\neg\mathbf{A}) \vee \mathbf{B})$ formula eleme $\mathfrak{S}_2$-nek, tehát logikai axióma, így a leválasztás szabálya szerint $(\neg\mathbf{A}) \vee \mathbf{B}$ vagyis $\mathbf{A} \Rightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben. Az $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{B} \vee \mathbf{B}))$ formula eleme $\mathfrak{S}_4$-nek, tehát logikai axióma, így a leválasztás szabálya szerint $(\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{B} \vee \mathbf{B})$ (logikai) tétel $\mathfrak{T}$-ben. Az $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})$ formula eleme $\mathfrak{S}_3$-nak, tehát logikai axióma, így a láncszabály szerint $(\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{B})$ (logikai) tétel $\mathfrak{T}$-ben. A $(\mathbf{B} \vee \mathbf{B}) \Rightarrow \mathbf{B}$ formula eleme $\mathfrak{S}_1$-nek, tehát logikai axióma, így a láncszabály szerint $(\mathbf{A} \vee \mathbf{B}) \Rightarrow \mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben.

Ugyanakkor, $\mathbf{B} \Rightarrow (\mathbf{B} \vee \mathbf{A})$ eleme $\mathfrak{S}_2$-nek, tehát logikai axióma, és $(\mathbf{B} \vee \mathbf{A}) \Rightarrow (\mathbf{A} \vee \mathbf{B})$ eleme $\mathfrak{S}_3$-nak, tehát szintén logikai axióma, így a láncszabály szerint $\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ logikai tétel $\mathfrak{T}$-ben.

A két előző bekezdésből és a konjunkció logikai alaptulajdonságából következik, hogy az $((\mathbf{A} \vee \mathbf{B}) \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B}))$ formula (logikai) tétel $\mathfrak{T}$-ben, vagyis az ekvivalencia definíciója alapján $(\mathbf{A} \vee \mathbf{B})\Leftrightarrow\mathbf{B}$ (logikai) tétel $\mathfrak{T}$-ben.

b) Tegyük fel, hogy $\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, és legyen $\mathbf{B}$ tetszőleges formula a $\mathfrak{T}$ matematikai elméletben.

A kettős negáció elve szerint $\neg\neg\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, vagyis a $\neg\mathbf{A}$ formula (logikailag) cáfolható $\mathfrak{T}$-ben, így az a) állítást alkalmazva $\mathbf{A}$ helyett $\neg\mathbf{A}$-ra és $\mathbf{B}$ helyett $\neg\mathbf{B}$-re kapjuk, hogy az $((\neg\mathbf{A}) \vee (\neg\mathbf{B}))\Leftrightarrow(\neg\mathbf{B})$ formula (logikai) tétel $\mathfrak{T}$-ben. Ezért a konjunkció logikai alaptulajdonságának második következményéből kapjuk, hogy $\neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))\Leftrightarrow(\neg\neg\mathbf{B})$ (logikai) tétel $\mathfrak{T}$-ben. Mivel $\mathbf{A} \wedge \mathbf{B} \equiv \neg((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$, ez nyilvánvalóan azt jelenti, hogy $(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow(\neg\neg\mathbf{B})$. A konjunkció logikai alaptulajdonságának első következménye szerint $\mathbf{B}\Leftrightarrow(\neg\neg\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben, így az ekvivalencia szimmetrikussága és tranzitivitása folytán az $(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow\mathbf{B}$ formula (logikai) tétel $\mathfrak{T}$-ben. ■

2.6. A kvantorok logikai alaptulajdonságai

2.6.1. Tétel. (**Az egzisztenciális kvantor logikai alaptulajdonsága.**) *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben. A* $(\exists\mathbf{x})\mathbf{A}$ *formula pontosan akkor* (*logikai*) *tétel* $\mathfrak{T}$*-ben, ha létezik olyan* $\mathbf{T}$ *objektum* $\mathfrak{T}$*-ben, hogy a* $(\mathbf{T}|\mathbf{x})\mathbf{A}$ *formula* (*logikai*) *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Az egzisztenciális kvantor definíciója szerint $(\exists\mathbf{x})\mathbf{A} \equiv (\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$, így ha $(\exists\mathbf{x})\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, akkor $\varepsilon_{\mathbf{x}}(\mathbf{A})$ olyan objektum $\mathfrak{T}$-ben, hogy $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben.

Megfordítva, legyen $\mathbf{T}$ olyan objektum $\mathfrak{T}$-ben, amelyre $(\mathbf{T}|\mathbf{x})\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. A $(\mathbf{T}|\mathbf{x})\mathbf{A} \Rightarrow (\exists\mathbf{x})\mathbf{A}$ formula eleme $\mathfrak{S}_5$-nek, tehát logikai tétel $\mathfrak{T}$-ben, amiből a leválasztás szabályát alkalmazva kapjuk, hogy $(\exists\mathbf{x})\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. ■

Ez a tétel szemléleti szempontból rendkívül fontos, mert megvilágítja a $(\exists\mathbf{x})\mathbf{A}$ alakú formulák (az ún. *egzisztenciális formulák*) értelmét. Látható, hogy a $(\exists\mathbf{x})\mathbf{A}$ formula pontosan akkor tétel a $\mathfrak{T}$ matematikai elméletben, ha az elmélet nyelvében található olyan $\mathbf{T}$ objektum, amelyet $\mathbf{A}$-ban $\mathbf{x}$ helyére téve tételt kapunk. Ezért azt a tényállást, hogy "a $(\exists\mathbf{x})\mathbf{A}$ formula tétel", így is megfogalmazhatjuk "létezik olyan objektum, amelyet $\mathbf{A}$-ban $\mathbf{x}$ helyére téve igaz formulát kapunk". Ugyanakkor az egzisztenciális kvantor logikai alaptulajdonsága az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ alakú objektumok (az ún. *ε-objektumok*) értelmét is felfedi. Ugyanis az egzisztenciális kvantor definíciója szerint a $(\exists\mathbf{x})\mathbf{A}$ formula azonos a $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ formulával, tehát $\varepsilon_{\mathbf{x}}(\mathbf{A})$ egy *olyan* (nyelvi szempontból) kitüntetett objektum, amely az $\mathbf{A}$-ban $\mathbf{x}$ helyére téve pontosan akkor eredményez igaz formulát, ha létezik olyan objektum, amelyet $\mathbf{A}$-ban $\mathbf{x}$ helyére téve igaz formulát kapunk.

2.6.2. Állítás. (**A kvantoros kifejezések negációjának szabálya.**) *Ha* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben, akkor a*

$$\neg((\forall\mathbf{x})\mathbf{A}) \Leftrightarrow (\exists\mathbf{x})(\neg\mathbf{A})$$
$$\neg((\exists\mathbf{x})\mathbf{A}) \Leftrightarrow (\forall\mathbf{x})(\neg\mathbf{A})$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. Az univerzális kvantor értelmezése szerint $\neg((\forall\mathbf{x})\mathbf{A})\equiv\neg\neg(\exists\mathbf{x})(\neg\mathbf{A})$, és 2.5.3. alapján $\neg\neg(\exists\mathbf{x})(\neg\mathbf{A})\Leftrightarrow(\exists\mathbf{x})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, így $\neg((\forall\mathbf{x})\mathbf{A})\Leftrightarrow(\exists\mathbf{x})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben.

Az univerzális kvantor értelmezéséből látszik, hogy $(\forall\mathbf{x})(\neg\mathbf{A})\equiv\neg(\exists\mathbf{x})(\neg\neg\mathbf{A})$, ezért a $\neg((\exists\mathbf{x})\mathbf{A})\Leftrightarrow(\forall\mathbf{x})(\neg\mathbf{A})$ formula azonos a $\neg((\exists\mathbf{x})\mathbf{A})\Leftrightarrow\neg(\exists\mathbf{x})(\neg\neg\mathbf{A})$ formulával. A 2.5.4. állításból következik, hogy ez a formula pontosan akkor logikai tétel a $\mathfrak{T}$ elméletben, ha a $((\exists\mathbf{x})\mathbf{A})\Leftrightarrow(\exists\mathbf{x})(\neg\neg\mathbf{A})$ formula logikai tétel $\mathfrak{T}$-ben.

A 2.5.3. állítás szerint $\mathbf{A}\Leftrightarrow(\neg\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, így a tételek helyettesítés-invarianciája és az egzisztenciális kvantor definíciója folytán $((\exists\mathbf{x})\mathbf{A})\Leftrightarrow(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})(\neg\neg\mathbf{A})$ szintén logikai tétel $\mathfrak{T}$-ben. Továbbá, az $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})(\neg\neg\mathbf{A}) \Rightarrow (\exists\mathbf{x}(\neg\neg\mathbf{A}))$ formula eleme $\mathfrak{S}_5$-nek, így 2.5.9. alkalmazásával azonnal kapjuk, hogy $((\exists\mathbf{x})\mathbf{A}) \Rightarrow (\exists\mathbf{x})(\neg\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben.

Megfordítva, 2.5.3. szerint a $(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben, így a tételek helyettesítés-invarianciája és az egzisztenciális kvantor definíciója folytán $((\exists\mathbf{x})(\neg\neg\mathbf{A})) \Rightarrow (\varepsilon_{\mathbf{x}}(\neg\neg\mathbf{A})|\mathbf{x})\mathbf{A}$ szintén logikai tétel $\mathfrak{T}$-ben. Ugyanakkor a $((\varepsilon_{\mathbf{x}}(\neg\neg\mathbf{A})|\mathbf{x})\mathbf{A}) \Rightarrow (\exists\mathbf{x})\mathbf{A}$ formula eleme $\mathfrak{S}_5$-nek, így a láncszabály alkalmazásával kapjuk, hogy $((\exists\mathbf{x})(\neg\neg\mathbf{A})) \Rightarrow (\exists\mathbf{x})\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben.

Az konjunkció logikai alaptulajdonsága szerint a fentiekből nyilvánvalóan következik, hogy $\neg((\exists\mathbf{x})\mathbf{A})\Leftrightarrow(\forall\mathbf{x})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben. ■

2.6.3. Állítás. *Ha* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben, akkor a*

$$((\forall\mathbf{x})\mathbf{A}) \Leftrightarrow (\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}$$

formula logikai tétel $\mathfrak{T}$*-ben.*

Bizonyítás. Az egzisztenciális kvantor értelmezése alapján

$$(\exists\mathbf{x})(\neg\mathbf{A}) \equiv (\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})(\neg\mathbf{A}) \equiv \neg(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A},$$

így az univerzális kvantor definíciója szerint

$$(\forall\mathbf{x})\mathbf{A} \equiv \neg(\exists\mathbf{x})(\neg\mathbf{A}) \equiv \neg\neg(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A},$$

tehát 2.5.3. alapján a $((\forall\mathbf{x})\mathbf{A}) \Leftrightarrow (\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben. ■

2.6.4. Állítás. *Ha* $\mathbf{A}$ *formula,* $\mathbf{x}$ *változó és* $\mathbf{T}$ *objektum a* $\mathfrak{T}$ *matematikai elméletben, akkor a*

$$(\forall\mathbf{x})\mathbf{A} \;\Rightarrow\; (\mathbf{T}|\mathbf{x})\mathbf{A}$$

formula logikai tétel $\mathfrak{T}$*-ben.*

Bizonyítás. A $((\mathbf{T}|\mathbf{x})(\neg\mathbf{A})) \Rightarrow (\exists\mathbf{x})(\neg\mathbf{A})$ formula eleme $\mathfrak{S}_5$-nek, továbbá nyilvánvalóan $(\mathbf{T}|\mathbf{x})(\neg\mathbf{A})\equiv\neg((\mathbf{T}|\mathbf{x})\mathbf{A})$, és $(\exists\mathbf{x})(\neg\mathbf{A})\equiv(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})(\neg\mathbf{A})\equiv\neg((\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A})$. Ez azt jelenti, hogy a $\neg((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow \neg((\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A})$ formula logikai tétel $\mathfrak{T}$-ben. Ezért 2.5.3. alapján $((\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{T}|\mathbf{x})\mathbf{A}$ szintén logikai tétel $\mathfrak{T}$-ben. Az előző állítás szerint $((\forall\mathbf{x})\mathbf{A})\Leftrightarrow(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben, így a láncszabály alkalmazásával kapjuk, hogy a $((\forall\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{T}|\mathbf{x})\mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben. ■

2.6.5. Következmény. *Ha* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben, akkor a*

$$(\forall\mathbf{x})\mathbf{A} \;\Rightarrow\; (\exists\mathbf{x})\mathbf{A}$$

formula logikai tétel $\mathfrak{T}$*-ben.*

Bizonyítás. Az előző állítás szerint $((\forall\mathbf{x})\mathbf{A}) \Rightarrow ((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, és definíció szerint $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A} \equiv (\exists\mathbf{x})\mathbf{A}$. ■

Habár az imént igazolt állítás meghökkentőnek tűnhet: valójában sohasem alkalmazzuk a matematikában. Az állítás gyakorlatban előforduló, nagyon is "ésszerűnek tűnő" változatát később fogalmazzuk meg (2.8.5.).

2.6.6. Tétel. (**Az univerzális kvantor logikai alaptulajdonsága.**) *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben. A* $(\forall\mathbf{x})\mathbf{A}$ *formula pontosan akkor (logikai) tétel* $\mathfrak{T}$*-ben, ha* $\mathfrak{T}$ *minden* $\mathbf{T}$ *objektumára* $(\mathbf{T}|\mathbf{x})\mathbf{A}$ *(logikai) tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Ha a $(\forall\mathbf{x})\mathbf{A}$ formula (logikai) tétel $\mathfrak{T}$-ben, akkor a 2.6.4. állítás és a leválasztás szabálya szerint a $\mathfrak{T}$ minden $\mathbf{T}$ objektumára $(\mathbf{T}|\mathbf{x})\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. Megfordítva, ha $\mathfrak{T}$ minden $\mathbf{T}$ objektumára $(\mathbf{T}|\mathbf{x})\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben, akkor $(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}$ (logikai) tétel $\mathfrak{T}$-ben. Láttuk, hogy $((\forall\mathbf{x})\mathbf{A})\Leftrightarrow(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben, így $(\forall\mathbf{x})\mathbf{A}$ is (logikai) tétel $\mathfrak{T}$-ben. ■

Ez a tétel szemléleti szempontból rendkívül fontos, mert megvilágítja a $(\forall\mathbf{x})\mathbf{A}$ alakú formulák értelmét. Látható, hogy a $(\forall\mathbf{x})\mathbf{A}$ formula pontosan akkor tétel a $\mathfrak{T}$ matematikai elméletben, ha az elmélet nyelvének bármely $\mathbf{T}$ objektumát az $\mathbf{x}$ változó helyére téve $\mathbf{A}$-ban tételt kapunk. Ezért azt a tényállást, hogy "a $(\forall\mathbf{x})\mathbf{A}$ formula tétel" így is megfogalmazhatjuk: "minden objektumot az $\mathbf{A}$-ban $\mathbf{x}$ helyére téve igaz formulát kapunk". Ugyanakkor az univerzális kvantor logikai alaptulajdonsága az ε-objektumok egy érdekes tulajdonságára is rámutat. Láttuk, hogy a $((\forall\mathbf{x})\mathbf{A})\Leftrightarrow(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}$ formula logikai tétel, ezért az ekvivalencia logikai alaptulajdonsága szerint szerint $(\forall\mathbf{x})\mathbf{A}$ pontosan akkor tétel, ha $(\varepsilon_{\mathbf{x}}(\neg\mathbf{A})|\mathbf{x})\mathbf{A}$ tétel. Ez azt jelenti, hogy ha az $\varepsilon_{\mathbf{x}}(\neg\mathbf{A})$ objektumot $\mathbf{A}$-ban az $\mathbf{x}$ helyére téve tételt kapunk, akkor (és csak akkor) az $\mathbf{A}$-ban $\mathbf{x}$ helyére *bármely* objektumot téve tételt kapunk.

2.6.7. Következmény. (**Az általánosítás szabálya.**) *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *olyan változó a* $\mathfrak{T}$ *matematikai elméletben, amely a* $\mathfrak{T}$ *egyetlen explicit axiómájában sem szerepel. Az* $\mathbf{A}$ *formula pontosan akkor tétel* $\mathfrak{T}$*-ben, ha* $(\forall\mathbf{x})\mathbf{A}$ *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A $((\forall\mathbf{x})\mathbf{A}) \Rightarrow \mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben, tehát ha $(\forall\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}$-ben, akkor a leválasztás szabálya szerint $\mathbf{A}$ is tétel $\mathfrak{T}$-ben (még akkor is, ha $\mathbf{x}$ szerepel a $\mathfrak{T}$ valamelyik explicit axiómájában).

Megfordítva, ha $\mathbf{A}$ tétel $\mathfrak{T}$-ben, akkor a tételek helyettesítés-invarianciája folytán bármely $\mathbf{T}$ objektumra $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}$-ben, mert $\mathbf{x}$ a $\mathfrak{T}$ egyetlen explicit axiómájában sem szerepel, így az univerzális kvantor logikai alaptulajdonsága alapján $(\forall \mathbf{x})\mathbf{A}$ tétel a $\mathfrak{T}$ elméletben. ■

Az általánosítás szabálya a nem formális logika egy természetes szabályának formális megfelelője. Ha $\mathbf{A}$ egy kijelentés a nem formális logikában és az $\mathbf{x}$ változó szerepel $\mathbf{A}$-ban, akkor az $\mathbf{A}$ igazság-tartalma $\mathbf{x}$-től függ: bizonyos objektumokat $\mathbf{A}$-ban $\mathbf{x}$ helyére téve igaz, más objektumokat behelyettesítve nem igaz (hamis) kijelentéseket kaphatunk. Ha minden helyettesítés nélkül kijelentjük, hogy "$\mathbf{A}$ igaz", akkor ez a nem formális matematikai logikában nyilvánvalóan azt jelenti, hogy $\mathbf{A}$-ban $\mathbf{x}$ helyére bármely objektumot helyettesítve igaz kijelentéshez jutunk. Az általánosítás szabálya (az univerzális kvantor logikai alaptulajdonságának ismeretében) ugyanezt fejezi ki a formális matematikai logikában. Itt csak arra kell vigyázni, hogy az $\mathbf{x}$ változó az elmélet egyetlen explicit axiómájában se szerepeljen. A nem formális logikában is hallgatólagosan feltesszük, hogy az $\mathbf{x}$ változó *független*, vagyis semmilyen olyan konkrét tulajdonsággal nem rendelkezik, amelyet valamilyen őt tartalmazó, vagyis rá vonatkozó axióma előír.

2.6.8. Következmény. *Legyenek* $\mathbf{A}$ *és* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Ha* $\mathbf{A} \Rightarrow \mathbf{B}$ *(illetve* $\mathbf{A}\Leftrightarrow\mathbf{B}$*) tétel* $\mathfrak{T}$*-ben, és* $\mathbf{x}$ *olyan változó, amely nem szerepel a* $\mathfrak{T}$ *egyetlen explicit axiómájában sem, akkor a* $((\exists \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$ *és* $((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\forall \mathbf{x})\mathbf{B})$ *(illetve a* $((\exists \mathbf{x})\mathbf{A})\Leftrightarrow((\exists \mathbf{x})\mathbf{B})$ *és* $((\forall \mathbf{x})\mathbf{A})\Leftrightarrow((\forall \mathbf{x})\mathbf{B})$*) formulák tételek* $\mathfrak{T}$*-ben. Ha* $\mathbf{A} \Rightarrow \mathbf{B}$ *(illetve* $\mathbf{A}\Leftrightarrow\mathbf{B}$*) logikai tétel* $\mathfrak{T}$*-ben, és* $\mathbf{x}$ *tetszőleges változó, akkor a* $((\exists \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$ *és* $((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\forall \mathbf{x})\mathbf{B})$ *(illetve a* $((\exists \mathbf{x})\mathbf{A})\Leftrightarrow((\exists \mathbf{x})\mathbf{B})$ *és* $((\forall \mathbf{x})\mathbf{A})\Leftrightarrow((\forall \mathbf{x})\mathbf{B})$*) formulák logikai tételek* $\mathfrak{T}$*-ben.*

Bizonyítás. (I) Először tegyük fel, hogy az $\mathbf{x}$ változó a $\mathfrak{T}$ egyetlen explicit axiómájában sem szerepel.

Ha $\mathbf{A} \Rightarrow \mathbf{B}$ tétel $\mathfrak{T}$-ben, akkor a tételek helyettesítés-invarianciája következtében $((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}) \Rightarrow ((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{B})$ tétel $\mathfrak{T}$-ben, vagyis $((\exists \mathbf{x})\mathbf{A}) \Rightarrow ((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{B})$ tétel $\mathfrak{T}$-ben, ugyanakkor $((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{B}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$ eleme $\mathfrak{S}_5$-nek, ezért a láncszabály alkalmazásával kapjuk, hogy $((\exists \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$ tétel $\mathfrak{T}$-ben.

Ha $\mathbf{A} \Rightarrow \mathbf{B}$ tétel $\mathfrak{T}$-ben, akkor 2.5.3. alapján $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$ tétel $\mathfrak{T}$-ben, tehát az előző bekezdés szerint $((\exists \mathbf{x})(\neg\mathbf{B})) \Rightarrow ((\exists \mathbf{x})(\neg\mathbf{A}))$ tétel $\mathfrak{T}$-ben, tehát ismét a 2.5.3. állítást alkalmazva nyerjük, hogy $\neg((\exists \mathbf{x})(\neg\mathbf{A})) \Rightarrow \neg((\exists \mathbf{x})(\neg\mathbf{B}))$ tétel $\mathfrak{T}$-ben, vagyis (az univerzális kvantor értelmezése alapján) $((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\forall \mathbf{x})\mathbf{B})$ tétel $\mathfrak{T}$-ben.

Tegyük fel, hogy $\mathbf{A}\Leftrightarrow\mathbf{B}$ tétel $\mathfrak{T}$-ben. A konjunkció logikai alaptulajdonsága szerint ekkor $\mathbf{A} \Rightarrow \mathbf{B}$ és $\mathbf{B} \Rightarrow \mathbf{A}$ tételek $\mathfrak{T}$-ben. Az előzőekből látható, hogy ekkor a $((\exists \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$, $((\exists \mathbf{x})\mathbf{B}) \Rightarrow ((\exists \mathbf{x})\mathbf{A})$, $((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\forall \mathbf{x})\mathbf{B})$ és $((\forall \mathbf{x})\mathbf{B}) \Rightarrow ((\forall \mathbf{x})\mathbf{A})$ formulák mindegyike tétel $\mathfrak{T}$-ben. Kétszer alkalmazva az ekvivalencia logikai alaptulajdonságát ebből kapjuk, hogy a $((\exists \mathbf{x})\mathbf{A})\Leftrightarrow((\exists \mathbf{x})\mathbf{B})$ és $((\forall \mathbf{x})\mathbf{A})\Leftrightarrow((\forall \mathbf{x})\mathbf{B})$ formulák tételek $\mathfrak{T}$-ben.

(II) Most tegyük fel, hogy $\mathbf{x}$ tetszőleges változó; ekkor $\mathbf{x}$ nem szerepel a $\mathfrak{T}_0$ egyetlen explicit axiómájában sem.

Ha $\mathbf{A} \Rightarrow \mathbf{B}$ logikai tétel $\mathfrak{T}$-ben, akkor tétel $\mathfrak{T}_0$-ban, igy az (I)-ből következik, hogy a $((\exists \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$ és $((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\forall \mathbf{x})\mathbf{B})$ formulák tételek $\mathfrak{T}_0$-ban, tehát logikai tételek $\mathfrak{T}$-ben.

Ha $\mathbf{A}\Leftrightarrow\mathbf{B}$ logikai tétel $\mathfrak{T}$-ben, akkor tétel $\mathfrak{T}_0$-ban, igy az (I)-ből következik, hogy a $((\exists \mathbf{x})\mathbf{A})\Leftrightarrow((\exists \mathbf{x})\mathbf{B})$ és $((\forall \mathbf{x})\mathbf{A})\Leftrightarrow((\forall \mathbf{x})\mathbf{B})$ formulák tételek $\mathfrak{T}_0$-ban, tehát logikai tételek $\mathfrak{T}$-ben. ■

2.7. A kvantorok speciális tulajdonságai

2.7.1. Állítás. (**A kvantorok kapcsolata a diszjunkcióval, konjunkcióval és implikációval.**) *Ha* $\mathbf{x}$ *változó és* $\mathbf{A}$*,* $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$(\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow ((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})$$
$$(\exists \mathbf{x})(\mathbf{A} \wedge \mathbf{B}) \Rightarrow ((\exists \mathbf{x})\mathbf{A}) \wedge ((\exists \mathbf{x})\mathbf{B})$$
$$(\exists \mathbf{x})(\mathbf{A} \Rightarrow \mathbf{B}) \Leftrightarrow ((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$$
$$(((\forall \mathbf{x})\mathbf{A}) \vee ((\forall \mathbf{x})\mathbf{B})) \Rightarrow (\forall \mathbf{x})(\mathbf{A} \vee \mathbf{B})$$
$$(\forall \mathbf{x})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow ((\forall \mathbf{x})\mathbf{A}) \wedge ((\forall \mathbf{x})\mathbf{B})$$
$$(((\exists \mathbf{x})\mathbf{A}) \Rightarrow ((\forall \mathbf{x})\mathbf{B})) \Rightarrow (\forall \mathbf{x})(\mathbf{A} \Rightarrow \mathbf{B}).$$

Bizonyítás. (I) Legyen $\mathfrak{T}'$ a $\mathfrak{T}_0[(\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B})]$ elmélet, és jelölje $\mathbf{T}$ az $\varepsilon_{\mathbf{x}}(\mathbf{A} \vee \mathbf{B})$ objektumot. Az egzisztenciális kvantor értelmezése szerint $(\mathbf{T}|\mathbf{x})(\mathbf{A} \vee \mathbf{B})$ tétel (sőt explicit axióma) $\mathfrak{T}'$-ben, ugyanakkor $(\mathbf{T}|\mathbf{x})(\mathbf{A} \vee \mathbf{B}) \equiv ((\mathbf{T}|\mathbf{x})\mathbf{A}) \vee ((\mathbf{T}|\mathbf{x})\mathbf{B})$. Továbbá, a $((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow (\exists \mathbf{x})\mathbf{A}$ és $((\exists \mathbf{x})\mathbf{A}) \Rightarrow (((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B}))$ formulák logikai tételek, így a láncszabály alkalmazásával kapjuk, hogy $((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow (((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}'$-ben. Továbbá, a $((\mathbf{T}|\mathbf{x})\mathbf{B}) \Rightarrow (\exists \mathbf{x})\mathbf{B}$ és $((\exists \mathbf{x})\mathbf{B}) \Rightarrow (((\exists \mathbf{x})\mathbf{B}) \vee ((\exists \mathbf{x})\mathbf{A}))$ és $(((\exists \mathbf{x})\mathbf{B}) \vee ((\exists \mathbf{x})\mathbf{A})) \Rightarrow (((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B}))$ formulák szintén logikai tételek, tehát a láncszabály kétszeri alkalmazásával kapjuk, hogy $((\mathbf{T}|\mathbf{x})\mathbf{B}) \Rightarrow (((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}'$-ben. Így az esetszétválasztás szabálya szerint $((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})$ tétel $\mathfrak{T}'$-ben. Ezután a dedukció-tétel alkalmazásával arra következtethetünk, hogy $(\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B}) \Rightarrow ((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

Most jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})]$ elméletet. Az $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ formula eleme $\mathfrak{S}_2$-nek, és az $\mathbf{x}$ változó nem szerepel a $((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})$ formulában, tehát nem szerepel a $\mathfrak{T}'$ elmélet egyetlen explicit axiómájában sem, így $((\exists \mathbf{x})\mathbf{A}) \Rightarrow (\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B})$ tétel $\mathfrak{T}'$-ben. A $\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})$ formula tétel $\mathfrak{T}'$-ben, és az $\mathbf{x}$ változó nem szerepel a $\mathfrak{T}'$ egyetlen explicit axiómájában sem, ezért $((\exists \mathbf{x})\mathbf{B}) \Rightarrow (\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B})$ tétel $\mathfrak{T}'$-ben. Ugyanakkor $((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})$ is tétel $\mathfrak{T}'$-ben, így az esetszétválasztás szabálya szerint $(\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B})$ tétel $\mathfrak{T}'$-ben. Ebből a dedukció-tétel alkalmazásával kapjuk, hogy $(((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})) \Rightarrow (\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

Tehát a két előző bekezdés és a konjunkció logikai alaptulajdonsága, valamint az ekvivalencia definíciója szerint a $(\exists \mathbf{x})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow ((\exists \mathbf{x})\mathbf{A}) \vee ((\exists \mathbf{x})\mathbf{B})$ formula logikai tétel $\mathfrak{T}$-ben.

(II) Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[(\exists \mathbf{x})(\mathbf{A} \wedge \mathbf{B})]$ elméletet és $\mathbf{T}$ a $\varepsilon_{\mathbf{x}}(\mathbf{A} \wedge \mathbf{B})$ objektumot. Ekkor $(\mathbf{T}|\mathbf{x})(\mathbf{A} \wedge \mathbf{B})$ tétel $\mathfrak{T}'$-ben és $(\mathbf{T}|\mathbf{x})(\mathbf{A} \wedge \mathbf{B}) \equiv ((\mathbf{T}|\mathbf{x})\mathbf{A}) \wedge ((\mathbf{T}|\mathbf{x})\mathbf{B})$, tehát a konjunkció logikai alaptulajdonsága szerint $(\mathbf{T}|\mathbf{x})\mathbf{A}$ és $(\mathbf{T}|\mathbf{x})\mathbf{B}$ tételek $\mathfrak{T}'$-ben. Ezért $(\exists \mathbf{x})\mathbf{A}$ és $(\exists \mathbf{x})\mathbf{B}$ tétel $\mathfrak{T}'$-ben, így $((\exists \mathbf{x})\mathbf{A}) \wedge ((\exists \mathbf{x})\mathbf{B})$ is tétel $\mathfrak{T}'$-ben. A dedukció-tétel alapján ez azt jelenti, hogy a $(\exists \mathbf{x})(\mathbf{A} \wedge \mathbf{B}) \Rightarrow ((\exists \mathbf{x})\mathbf{A}) \wedge ((\exists \mathbf{x})\mathbf{B})$ formula tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

(III) Az implikáció értelmezése alapján $(\exists \mathbf{x})(\mathbf{A} \Rightarrow \mathbf{B}) \equiv (\exists \mathbf{x})((\neg \mathbf{A}) \vee \mathbf{B})$, és az (I)-ből következik, hogy a $(\exists \mathbf{x})((\neg \mathbf{A}) \vee \mathbf{B}) \Leftrightarrow ((\exists \mathbf{x})(\neg \mathbf{A})) \vee ((\exists \mathbf{x})\mathbf{B})$ formula logikai tétel $\mathfrak{T}$-ben. A kvantoros kifejezések negációjának szabályát alkalmazva kapjuk, hogy $(((\exists \mathbf{x})(\neg \mathbf{A})) \vee ((\exists \mathbf{x})\mathbf{B})) \Leftrightarrow ((\neg((\forall \mathbf{x})\mathbf{A}))) \vee ((\exists \mathbf{x})\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben, és itt a jobb oldalon éppen a $((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B})$ formula áll. Ebből következik, hogy $(\exists \mathbf{x})(\mathbf{A} \Rightarrow \mathbf{B}) \Leftrightarrow (((\forall \mathbf{x})\mathbf{A}) \Rightarrow ((\exists \mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben.

(IV) Az univerzális kvantor értelmezése szerint $((\forall \mathbf{x})\mathbf{A}) \vee ((\forall \mathbf{x})\mathbf{B}) \equiv (\neg(\exists \mathbf{x})(\neg \mathbf{A})) \vee$

$(\neg(\exists\mathbf{x})(\neg\mathbf{B}))$. Ugyanakkor $((\neg(\exists\mathbf{x})(\neg\mathbf{A}))\vee(\neg(\exists\mathbf{x})(\neg\mathbf{B})))\Leftrightarrow\neg(((\exists\mathbf{x})(\neg\mathbf{A}))\wedge((\exists\mathbf{x})(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben a de Morgan-tétel alapján, így a konjunkció logikai alaptulajdonsága szerint a $\neg(((\exists\mathbf{x})(\neg\mathbf{A}))\wedge((\exists\mathbf{x})(\neg\mathbf{B})))\Rightarrow\neg((\exists\mathbf{x}((\neg\mathbf{A})\wedge(\neg\mathbf{B}))))$ formula logikai tétel $\mathfrak{T}$-ben. Ugyanakkor a de Morgan-tétel alapján $((\neg\mathbf{A})\wedge(\neg\mathbf{B}))\Leftrightarrow\neg(\mathbf{A}\vee\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. Az univerzális kvantor értelmezése szerint $\neg((\exists\mathbf{x})((\neg\mathbf{A})\wedge(\neg\mathbf{B})))\equiv(\forall\mathbf{x})(\mathbf{A}\vee\mathbf{B})$, tehát az előzőekből a láncszabály többszöri alkalmazásával következik, hogy a $(((\forall\mathbf{x})\mathbf{A})\vee((\forall\mathbf{x})\mathbf{B}))\Rightarrow(\forall\mathbf{x})(\mathbf{A}\vee\mathbf{B})$ formula logikai tétel $\mathfrak{T}$-ben.

(V) Az univerzális kvantor értelmezése szerint $(\forall\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\equiv\neg((\exists\mathbf{x})(\neg(\mathbf{A}\wedge\mathbf{B})))$, és a de Morgan-tétel alapján $(\neg(\mathbf{A}\wedge\mathbf{B}))\Leftrightarrow((\neg\mathbf{A})\vee(\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, így $((\forall\mathbf{x})(\mathbf{A}\wedge\mathbf{B}))\Leftrightarrow\neg((\exists\mathbf{x})((\neg\mathbf{A})\vee(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. Az (I) állítás és 2.5.4. alapján $(\neg((\exists\mathbf{x})((\neg\mathbf{A})\vee(\neg\mathbf{B}))))\Leftrightarrow\neg(((\exists\mathbf{x})(\neg\mathbf{A}))\vee((\exists\mathbf{x})(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. Azonban $(\neg(((\exists\mathbf{x})(\neg\mathbf{A}))\vee((\exists\mathbf{x})(\neg\mathbf{B}))))\Leftrightarrow((\neg((\exists\mathbf{x})(\neg\mathbf{A})))\wedge(\neg((\exists\mathbf{x})(\neg\mathbf{B}))))$ szintén logikai tétel $\mathfrak{T}$-ben a de Morgan-tétel szerint, és $(\forall\mathbf{x})\mathbf{A}\equiv\neg((\exists\mathbf{x})(\neg\mathbf{A}))$, valamint $(\forall\mathbf{x})\mathbf{B}\equiv\neg((\exists\mathbf{x})(\neg\mathbf{B}))$, ami az előzőek alapján azt jelenti, hogy $(\forall\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Leftrightarrow(((\forall\mathbf{x})\mathbf{A})\wedge((\forall\mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben.

(VI) A definíciók szerint $((\exists\mathbf{x})\mathbf{A})\Rightarrow((\forall\mathbf{x})\mathbf{B})\equiv(\neg((\exists\mathbf{x})\mathbf{A}))\vee(\neg((\exists\mathbf{x})(\neg\mathbf{B})))$, és a de Morgan-tétel szerint $((\neg((\exists\mathbf{x})\mathbf{A}))\vee(\neg((\exists\mathbf{x})(\neg\mathbf{B}))))\Leftrightarrow\neg(((\exists\mathbf{x})\mathbf{A})\wedge((\exists\mathbf{x})(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. A (II) állítás és a kontrapozíció tétele alapján $(\neg(((\exists\mathbf{x})\mathbf{A})\wedge((\exists\mathbf{x})(\neg\mathbf{B}))))\Rightarrow(\neg((\exists\mathbf{x})(\mathbf{A}\wedge(\neg\mathbf{B}))))$ logikai tétel $\mathfrak{T}$-ben. Az implikáció negációjának szabálya szerint $(\mathbf{A}\wedge(\neg\mathbf{B}))\Leftrightarrow(\neg(\mathbf{A}\Rightarrow\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, így $(\neg((\exists\mathbf{x})(\mathbf{A}\wedge(\neg\mathbf{B}))))\Leftrightarrow(\neg((\exists\mathbf{x})(\neg(\mathbf{A}\Rightarrow\mathbf{B}))))$ szintén logikai tétel $\mathfrak{T}$-ben. Továbbá, $\neg((\exists\mathbf{x})(\neg(\mathbf{A}\Rightarrow\mathbf{B})))\equiv(\forall\mathbf{x})(\mathbf{A}\Rightarrow\mathbf{B})$, így a láncszabály többszöri alkalmazásával az előzőekből kapjuk, hogy $(((\exists\mathbf{x})\mathbf{A})\Rightarrow((\forall\mathbf{x})\mathbf{B}))\Rightarrow(\forall\mathbf{x})(\mathbf{A}\Rightarrow\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. ■

2.7.2. Állítás. *Ha* $\mathbf{x}$ *változó és* $\mathbf{A}$, $\mathbf{B}$ *olyan formulák a* $\mathfrak{T}$ *matematikai elméletben, hogy* $\mathbf{x}$ *nem szerepel* $\mathbf{A}$*-ban, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$(\exists\mathbf{x})(\mathbf{A}\vee\mathbf{B})\Leftrightarrow\mathbf{A}\vee(\exists\mathbf{x})\mathbf{B},\qquad(\exists\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Leftrightarrow\mathbf{A}\wedge(\exists\mathbf{x})\mathbf{B},$$
$$(\forall\mathbf{x})(\mathbf{A}\vee\mathbf{B})\Leftrightarrow\mathbf{A}\vee(\forall\mathbf{x})\mathbf{B},\qquad(\forall\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Leftrightarrow\mathbf{A}\wedge(\forall\mathbf{x})\mathbf{B}.$$

Bizonyítás. Azt fogjuk felhasználni, hogy ha az $\mathbf{x}$ változó nem szerepel az $\mathbf{A}$ formulában, akkor az egzisztenciális kvantor definíciója szerint $(\exists\mathbf{x})\mathbf{A}\equiv(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}\equiv\mathbf{A}$.

(I) Az előző állításban beláttuk, hogy $(\exists\mathbf{x})(\mathbf{A}\vee\mathbf{B})\Leftrightarrow(((\exists\mathbf{x})\mathbf{A})\vee((\exists\mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, következésképpen $(\exists\mathbf{x})(\mathbf{A}\vee\mathbf{B})\Leftrightarrow(\mathbf{A}\vee(\exists\mathbf{x})\mathbf{B})$ is logikai tétel $\mathfrak{T}$-ben.

(II) Szintén az előző állításban láttuk, hogy $(\exists\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Rightarrow(((\exists\mathbf{x})\mathbf{A})\wedge((\exists\mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, következésképpen $(\exists\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Rightarrow(\mathbf{A}\wedge(\exists\mathbf{x})\mathbf{B})$ is logikai tétel $\mathfrak{T}$-ben.

Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[\mathbf{A}\wedge(\exists\mathbf{x})\mathbf{B}]$ elméletet és $\mathbf{T}$ az $\varepsilon_{\mathbf{x}}(\mathbf{B})$ objektumot. Az $\mathbf{A}\wedge(\mathbf{T}|\mathbf{x})\mathbf{B}$ formula explicit axióma $\mathfrak{T}'$-ben, és $\mathbf{A}\wedge(\mathbf{T}|\mathbf{x})\mathbf{B}\equiv(\mathbf{T}|\mathbf{x})(\mathbf{A}\wedge\mathbf{B})$, mert $\mathbf{x}$ nem szerepel $\mathbf{A}$-ban. A $(\mathbf{T}|\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Rightarrow(\exists\mathbf{x})(\mathbf{A}\wedge\mathbf{B})$ formula eleme $\mathfrak{S}_5$-nek, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\exists\mathbf{x})(\mathbf{A}\wedge\mathbf{B})$ tétel $\mathfrak{T}'$-ben. A dedukció-tétel alapján az adódik, hogy $(\mathbf{A}\wedge(\exists\mathbf{x})\mathbf{B})\Rightarrow(\exists\mathbf{x})(\mathbf{A}\wedge\mathbf{B})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

Tehát a konjunkció logikai alaptulajdonsága szerint $(\exists\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Leftrightarrow(\mathbf{A}\wedge(\exists\mathbf{x})\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben.

(III) Az univerzális kvantor definíciója szerint $(\forall\mathbf{x})(\mathbf{A}\vee\mathbf{B})\equiv\neg(\exists\mathbf{x})(\neg(\mathbf{A}\vee\mathbf{B}))$, továbbá a de Morgan-tétel szerint $(\neg(\mathbf{A}\vee\mathbf{B}))\Leftrightarrow((\neg\mathbf{A})\wedge(\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, következésképpen $(\forall\mathbf{x})(\mathbf{A}\vee\mathbf{B})\Leftrightarrow(\neg(\exists\mathbf{x})((\neg\mathbf{A})\wedge(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. Az $\mathbf{x}$ változó nem szerepel a $\neg\mathbf{A}$ formulában, ezért (II) és 2.5.4. alkalmazásával arra jutunk, hogy $(\neg(\exists\mathbf{x})((\neg\mathbf{A})\wedge(\neg\mathbf{B})))\Leftrightarrow(\neg((\neg\mathbf{A})\wedge(\exists\mathbf{x})(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. A de Morgan-tétel szerint $(\neg((\neg\mathbf{A})\wedge$

$(\exists\mathbf{x})(\neg\mathbf{B})))\Leftrightarrow((\neg\neg\mathbf{A}) \vee \neg(\exists\mathbf{x})(\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, így az univerzális kvantor értelmezése alapján $(\neg((\neg\mathbf{A}) \wedge (\exists\mathbf{x})(\neg\mathbf{B})))\Leftrightarrow(\mathbf{A} \vee (\forall\mathbf{x})\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. Ez azt jelenti, hogy $(\forall\mathbf{x})(\mathbf{A} \vee \mathbf{B})\Leftrightarrow(\mathbf{A} \vee (\forall\mathbf{x})\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben.

(IV) Az univerzális kvantor definíciója szerint $(\forall\mathbf{x})(\mathbf{A} \wedge \mathbf{B}) \equiv \neg(\exists\mathbf{x})((\neg\mathbf{A}) \vee (\neg\mathbf{B}))$, továbbá $(\neg(\mathbf{A}\wedge\mathbf{B}))\Leftrightarrow((\neg\mathbf{A})\vee(\neg\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, így $(\forall\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Leftrightarrow(\neg(\exists\mathbf{x})((\neg\mathbf{A})\vee(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. Az $\mathbf{x}$ változó nem szerepel a $\neg\mathbf{A}$ formulában, ezért (I) és 2.5.4. alkalmazásával arra jutunk, hogy $(\neg(\exists\mathbf{x})((\neg\mathbf{A}) \vee (\neg\mathbf{B})))\Leftrightarrow(\neg((\neg\mathbf{A}) \vee (\exists\mathbf{x})(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben. A de Morgan-tétel szerint $(\neg((\neg\mathbf{A}) \vee (\exists\mathbf{x})(\neg\mathbf{B})))\Leftrightarrow((\neg\neg\mathbf{A}) \wedge (\neg(\exists\mathbf{x})(\neg\mathbf{B})))$ logikai tétel $\mathfrak{T}$-ben, amiből az univerzális kvantor értelmezése alapján következik, hogy $(\neg((\neg\mathbf{A}) \vee (\exists\mathbf{x})(\neg\mathbf{B})))\Leftrightarrow(\mathbf{A} \wedge (\forall\mathbf{x})(\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Ez azt jelenti, hogy $(\forall\mathbf{x})(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow(\mathbf{A} \wedge (\forall\mathbf{x})\mathbf{B})$ logikai tétel $\mathfrak{T}$-ben. ■

2.7.3. Állítás. *Legyenek* $\mathbf{x}$, $\mathbf{y}$ *különböző változók és* $\mathbf{A}$, $\mathbf{B}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben. Ha* $\mathbf{x}$ *nem szerepel* $\mathbf{B}$*-ben és* $\mathbf{y}$ *nem szerepel* $\mathbf{A}$*-ban, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$\begin{aligned}
&(\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \vee \mathbf{B})\Leftrightarrow((\exists\mathbf{x})\mathbf{A}) \vee ((\exists\mathbf{y})\mathbf{B}), &&(\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow((\exists\mathbf{x})\mathbf{A}) \wedge ((\exists\mathbf{y})\mathbf{B}),\\
&(\exists\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \vee \mathbf{B})\Leftrightarrow((\exists\mathbf{x})\mathbf{A}) \vee ((\forall\mathbf{y})\mathbf{B}), &&(\exists\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow((\exists\mathbf{x})\mathbf{A}) \wedge ((\forall\mathbf{y})\mathbf{B}),\\
&(\forall\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \vee \mathbf{B})\Leftrightarrow((\forall\mathbf{x})\mathbf{A}) \vee ((\forall\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow((\forall\mathbf{x})\mathbf{A}) \wedge ((\forall\mathbf{y})\mathbf{B}),\\
&(\forall\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \vee \mathbf{B})\Leftrightarrow((\forall\mathbf{x})\mathbf{A}) \vee ((\exists\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \wedge \mathbf{B})\Leftrightarrow((\forall\mathbf{x})\mathbf{A}) \wedge ((\exists\mathbf{y})\mathbf{B}).
\end{aligned}$$

Bizonyítás. Az $\mathbf{y}$ változó nem szerepel $\mathbf{A}$-ban, ezért a korábbiak szerint a

$$\begin{aligned}
&(\exists\mathbf{y})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow \mathbf{A} \wedge (\exists\mathbf{y})\mathbf{B}, &&(\forall\mathbf{y})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow \mathbf{A} \wedge (\forall\mathbf{y})\mathbf{B},\\
&(\exists\mathbf{y})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow \mathbf{A} \vee (\exists\mathbf{y})\mathbf{B}, &&(\forall\mathbf{y})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow \mathbf{A} \vee (\forall\mathbf{y})\mathbf{B}
\end{aligned}$$

formulák logikai tételek $\mathfrak{T}$-ben. Ebből következik, hogy a

$$\begin{aligned}
&(\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow (\exists\mathbf{x})(\mathbf{A} \wedge (\exists\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow (\forall\mathbf{x})(\mathbf{A} \wedge (\exists\mathbf{y})\mathbf{B}),\\
&(\exists\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow (\exists\mathbf{x})(\mathbf{A} \wedge (\forall\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow (\forall\mathbf{x})(\mathbf{A} \wedge (\forall\mathbf{y})\mathbf{B}),\\
&(\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow (\exists\mathbf{x})(\mathbf{A} \vee (\exists\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\exists\mathbf{y})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow (\forall\mathbf{x})(\mathbf{A} \vee (\exists\mathbf{y})\mathbf{B}),\\
&(\exists\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow (\exists\mathbf{x})(\mathbf{A} \vee (\forall\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\forall\mathbf{y})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow (\forall\mathbf{x})(\mathbf{A} \vee (\forall\mathbf{y})\mathbf{B})
\end{aligned}$$

formulák logikai tételek $\mathfrak{T}$-ben. Az $\mathbf{x}$ változó nem szerepel a $(\exists\mathbf{y})\mathbf{B}$ és $(\forall\mathbf{y})\mathbf{B}$ formulákban, ezért a

$$\begin{aligned}
&(\exists\mathbf{x})(\mathbf{A} \wedge (\exists\mathbf{y})\mathbf{B}) \Leftrightarrow ((\exists\mathbf{x})\mathbf{A}) \wedge ((\exists\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\mathbf{A} \wedge (\exists\mathbf{y})\mathbf{B}) \Leftrightarrow ((\forall\mathbf{x})\mathbf{A}) \wedge ((\exists\mathbf{y})\mathbf{B}),\\
&(\exists\mathbf{x})(\mathbf{A} \wedge (\forall\mathbf{y})\mathbf{B}) \Leftrightarrow ((\exists\mathbf{x})\mathbf{A}) \wedge ((\forall\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\mathbf{A} \wedge (\forall\mathbf{y})\mathbf{B}) \Leftrightarrow ((\forall\mathbf{x})\mathbf{A}) \wedge ((\forall\mathbf{y})\mathbf{B}),\\
&(\exists\mathbf{x})(\mathbf{A} \vee (\exists\mathbf{y})\mathbf{B}) \Leftrightarrow ((\exists\mathbf{x})\mathbf{A}) \vee ((\exists\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\mathbf{A} \vee (\exists\mathbf{y})\mathbf{B}) \Leftrightarrow ((\forall\mathbf{x})\mathbf{A}) \vee ((\exists\mathbf{y})\mathbf{B}),\\
&(\exists\mathbf{x})(\mathbf{A} \vee (\forall\mathbf{y})\mathbf{B}) \Leftrightarrow ((\exists\mathbf{x})\mathbf{A}) \vee ((\forall\mathbf{y})\mathbf{B}), &&(\forall\mathbf{x})(\mathbf{A} \vee (\forall\mathbf{y})\mathbf{B}) \Leftrightarrow ((\forall\mathbf{x})\mathbf{A}) \vee ((\forall\mathbf{y})\mathbf{B})
\end{aligned}$$

formulák logikai tételek $\mathfrak{T}$-ben, amiből következik az állítás. ■

2.7.4. Állítás. (**A kvantorok felcserélésének tétele.**) *Ha* $\mathbf{x}$, $\mathbf{y}$ *változók, és* $\mathbf{A}$ *formula a* $\mathfrak{T}$ *matematikai elméletben, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$\begin{aligned}
&(\exists\mathbf{x})(\exists\mathbf{y})\mathbf{A} \Leftrightarrow (\exists\mathbf{y})(\exists\mathbf{x})\mathbf{A},\\
&(\forall\mathbf{x})(\forall\mathbf{y})\mathbf{A} \Leftrightarrow (\forall\mathbf{y})(\forall\mathbf{x})\mathbf{A},\\
&(\exists\mathbf{x})(\forall\mathbf{y})\mathbf{A} \Rightarrow (\forall\mathbf{y})(\exists\mathbf{x})\mathbf{A}.
\end{aligned}$$

Bizonyítás. (I) Tegyük fel, hogy $\mathbf{x}$ és $\mathbf{y}$ különböző változók. Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[(\exists\mathbf{x})(\exists\mathbf{y})\mathbf{A}]$ elméletet, továbbá jelölje $\mathbf{T}$ az $\varepsilon_{\mathbf{x}}((\exists\mathbf{y})\mathbf{A})$ és $\mathbf{S}$ az $\varepsilon_{\mathbf{y}}((\mathbf{T}|\mathbf{x})\mathbf{A})$ objektumot. Ekkor $(\mathbf{T}|\mathbf{x})((\exists\mathbf{y})\mathbf{A})$ explicit axiómája $\mathfrak{T}'$-nek, és $\mathbf{x}$, $\mathbf{y}$ különböző változók, valamint $\mathbf{y}$ nem szerepel $\mathbf{T}$-ben, hiszen a $(\exists\mathbf{y})\mathbf{A}$ kifejezésben sem szerepel. Ezért a kvantoros kifejezésekre vonatkozó helyettesítési szabály szerint $(\mathbf{T}|\mathbf{x})((\exists\mathbf{y})\mathbf{A}) \equiv (\exists\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})$, így $(\exists\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})$ tétel $\mathfrak{T}'$-ben. Az egzisztenciális kvantor értelmezése alapján ez azt jelenti, hogy $(\mathbf{S}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})$ tétel $\mathfrak{T}'$-ben. Itt $\mathbf{x}$ és $\mathbf{y}$ különbözőek, és $\mathbf{x}$ nem szerepel $\mathbf{S}$-ben, mert nem szerepel $\mathbf{T}$-ben, így a $(\mathbf{T}|\mathbf{x})\mathbf{A}$ kifejezésben sem. Most a helyettesítések felcserélésének szabályát alkalmazva kapjuk, hogy $(\mathbf{S}|\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv ((\mathbf{S}|\mathbf{y})\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A}) \equiv (\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A})$, mert $\mathbf{y}$ nem szerepel $\mathbf{T}$-ben. A $(\mathbf{T}|\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A}) \Rightarrow (\exists\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A})$ formula eleme $\mathfrak{S}_5$-nek, amiből a leválasztás szabályát alkalmazva kapjuk, hogy $(\exists\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A})$ tétel $\mathfrak{T}'$-ben. Ugyanakkor $\mathbf{x}$ és $\mathbf{y}$ különböző változók, valamint $\mathbf{x}$ nem szerepel $\mathbf{S}$-ben, ezért a kvantoros kifejezésekre vonatkozó helyettesítés szabálya szerint $(\exists\mathbf{x})((\mathbf{S}|\mathbf{y})\mathbf{A}) \equiv (\mathbf{S}|\mathbf{y})((\exists\mathbf{x})\mathbf{A})$, így $(\mathbf{S}|\mathbf{y})((\exists\mathbf{x})\mathbf{A})$ tétel $\mathfrak{T}'$-ben. Az $(\mathbf{S}|\mathbf{y})((\exists\mathbf{x})\mathbf{A}) \Rightarrow (\exists\mathbf{y})(\exists\mathbf{x})\mathbf{A}$ formula eleme $\mathfrak{S}_5$-nek, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\exists\mathbf{y})(\exists\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}'$-ben. A dedukció-tétel alkalmazva kapjuk, hogy $(\exists\mathbf{x})(\exists\mathbf{y})\mathbf{A} \Rightarrow (\exists\mathbf{y})(\exists\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

Ez tetszőleges $\mathbf{A}$ formulára és különböző $\mathbf{x}$, $\mathbf{y}$ változókra igaz, ezért a $(\exists\mathbf{y})(\exists\mathbf{x})\mathbf{A} \Rightarrow (\exists\mathbf{x})(\exists\mathbf{y})\mathbf{A}$ formula is logikai tétel $\mathfrak{T}$-ben, így a konjunkció logikai alaptulajdonsága szerint a $(\exists\mathbf{x})(\exists\mathbf{y})\mathbf{A}\Leftrightarrow(\exists\mathbf{y})(\exists\mathbf{x})\mathbf{A}$ formula logikai tétel $\mathfrak{T}$-ben.

(II) Tegyük fel, hogy $\mathbf{x}$ és $\mathbf{y}$ különböző változók. Az univerzális kvantor definíciója szerint $(\forall\mathbf{x})(\forall\mathbf{y})\mathbf{A} \equiv \neg(\exists\mathbf{x})(\neg\neg(\exists\mathbf{y})(\neg\mathbf{A}))$. Azonban 2.5.3. alapján $(\neg\neg(\exists\mathbf{y})(\neg\mathbf{A}))\Leftrightarrow(\exists\mathbf{y})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, amiből következik, hogy $(\exists\mathbf{x})(\neg\neg(\exists\mathbf{y})(\neg\mathbf{A}))\Leftrightarrow(\exists\mathbf{x})(\exists\mathbf{y})(\neg\mathbf{A})$ is logikai tétel $\mathfrak{T}$-ben. Ez azt jelenti, hogy $(\forall\mathbf{x})(\forall\mathbf{y})\mathbf{A}\Leftrightarrow\neg(\exists\mathbf{x})(\exists\mathbf{y})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben. Ez tetszőleges $\mathbf{A}$ formulára és különböző $\mathbf{x}$, $\mathbf{y}$ változókra igaz, következésképpen $(\forall\mathbf{y})(\forall\mathbf{x})\mathbf{A}\Leftrightarrow\neg(\exists\mathbf{y})(\exists\mathbf{x})(\neg\mathbf{A})$ szintén logikai tétel $\mathfrak{T}$-ben. Az (I) állítás alapján $(\exists\mathbf{x})(\exists\mathbf{y})(\neg\mathbf{A})\Leftrightarrow(\exists\mathbf{y})(\exists\mathbf{x})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, így $\neg(\exists\mathbf{x})(\exists\mathbf{y})(\neg\mathbf{A})\Leftrightarrow\neg(\exists\mathbf{y})(\exists\mathbf{x})(\neg\mathbf{A})$ szintén logikai tétel $\mathfrak{T}$-ben. Ebből kapjuk, hogy $(\forall\mathbf{x})(\forall\mathbf{y})\mathbf{A}\Leftrightarrow(\forall\mathbf{y})(\forall\mathbf{x})\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben.

(III) Tegyük fel, hogy $\mathbf{x}$ és $\mathbf{y}$ különböző változók. Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[(\exists\mathbf{x})(\forall\mathbf{y})\mathbf{A}]$ elméletet, és legyen $\mathbf{T}$ az $\varepsilon_{\mathbf{x}}((\forall\mathbf{y})\mathbf{A})$ objektum. A $\mathfrak{T}'$ definíciója szerint $(\mathbf{T}|\mathbf{x})((\forall\mathbf{y})\mathbf{A})$ explicit axióma $\mathfrak{T}'$-ben. Az $\mathbf{y}$ változó nem szerepel $\mathbf{T}$-ben, mert nem szerepel a $(\forall\mathbf{y})\mathbf{A}$ formulában. Ezért $(\mathbf{T}|\mathbf{x})((\forall\mathbf{y})\mathbf{A}) \equiv (\forall\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A})$, és a $(\forall\mathbf{y})((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow ((\mathbf{T}|\mathbf{x})\mathbf{A})$ formula logikai tétel $\mathfrak{T}'$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}'$-ben. A $(\mathbf{T}|\mathbf{x})\mathbf{A} \Rightarrow (\exists\mathbf{x})\mathbf{A}$ formula eleme $\mathfrak{S}_5$-nek, ezért ismét a leválasztás szabályát alkalmazva kapjuk, hogy $(\exists\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}'$-ben. Az $\mathbf{y}$ változó nem szerepel a $\mathfrak{T}'$ egyetlen explicit axiómájában sem (vagyis a $(\exists\mathbf{x})(\forall\mathbf{y})\mathbf{A}$ formulában), tehát az általánosítás szabálya szerint $(\forall\mathbf{y})(\exists\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}'$-ben. Ebből a dedukció-tétel alapján következik, hogy $(\exists\mathbf{x})(\forall\mathbf{y})\mathbf{A} \Rightarrow (\forall\mathbf{y})(\exists\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben.

(IV) Utoljára feltesszük, hogy $\mathbf{x} \equiv \mathbf{y}$. Ekkor az első két formula triviálisan logikai tétel $\mathfrak{T}$-ben, hiszen az $\Leftrightarrow$ operátor mindkét oldalán ugyanaz a formula áll és az ekvivalencia reflexív. A $(\forall\mathbf{x})\mathbf{A}$ formulában nem szerepel az $\mathbf{x}$ változó, ezért az egzisztenciális kvantor definíciója szerint $(\exists\mathbf{x})(\forall\mathbf{x})\mathbf{A} \equiv (\forall\mathbf{x})\mathbf{A}$. Továbbá, a $(\exists\mathbf{x})\mathbf{A}$ formulában nem szerepel az $\mathbf{x}$ változó, ezért az univerzális kvantor definíciója szerint

$$(\forall\mathbf{x})(\exists\mathbf{x})\mathbf{A} \equiv (\varepsilon_{\mathbf{x}}(\neg((\exists\mathbf{x})\mathbf{A}))|\mathbf{x})\neg\neg((\exists\mathbf{x})\mathbf{A}) \equiv \neg\neg((\exists\mathbf{x})\mathbf{A}).$$

A kettős negáció szabálya szerint $((\exists\mathbf{x})\mathbf{A}) \Rightarrow \neg\neg((\exists\mathbf{x})\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, ugyanakkor a 2.6.5. állítás alapján $((\forall\mathbf{x})\mathbf{A}) \Rightarrow ((\exists\mathbf{x})\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, így a láncszabályt alkalmazva kapjuk, hogy $((\forall \mathbf{x})\mathbf{A}) \Rightarrow \neg\neg((\exists \mathbf{x})\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben. Az előzőek alapján ez pontosan azt jelenti, hogy $(\exists \mathbf{x})(\forall \mathbf{x})\mathbf{A} \Rightarrow (\forall \mathbf{x})(\exists \mathbf{x})\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben. ∎

2.8. A feltételes kvantorok tulajdonságai

2.8.1. Állítás. *Ha* **A**, **B** *formulák és* **x** *változó a* $\mathfrak{T}$ *matematikai elméletben, akkor a*

$$(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A} \Leftrightarrow (\forall \mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A})$$

formula logikai tétel $\mathfrak{T}$*-ben.*

Bizonyítás. A feltételes kvantorok definíciója (2.2.5.) után álló bekezdésben láttuk, hogy $(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A} \equiv (\forall \mathbf{x})(\mathbf{B} \Rightarrow (\neg\neg\mathbf{A}))$, így elég azt igazolni, hogy a $(\forall \mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A}) \Leftrightarrow (\forall \mathbf{x})(\mathbf{B} \Rightarrow (\neg\neg\mathbf{A}))$ formula logikai tétel $\mathfrak{T}$-ben. Ez viszont nyilvánvaló, mert 2.5.3. szerint $(\mathbf{B} \Rightarrow \mathbf{A}) \Leftrightarrow (\mathbf{B} \Rightarrow (\neg\neg\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. ∎

2.8.2. Állítás. (**A feltételes kvantoros kifejezések negációja.**) *Ha* **A**, **B** *formulák és* **x** *változó a* $\mathfrak{T}$ *matematikai elméletben, akkor a*

$$\neg((\exists_{\mathbf{B}}\mathbf{x})\mathbf{A}) \Leftrightarrow (\forall_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A}) \tag{2.1}$$

$$\neg((\forall_{\mathbf{B}}\mathbf{x})\mathbf{A}) \Leftrightarrow (\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A}) \tag{2.2}$$

formulák logikai tételek $\mathfrak{T}$*-ben.*

Bizonyítás. A definíció szerint $(\forall_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A}) \equiv \neg(\exists_{\mathbf{B}}\mathbf{x})(\neg\neg\mathbf{A}) \equiv \neg(\exists \mathbf{x})(\mathbf{B} \wedge (\neg\neg\mathbf{A}))$. A 2.5.3. állítás alapján $(\mathbf{B} \wedge (\neg\neg\mathbf{A})) \Leftrightarrow (\mathbf{B} \wedge \mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, így $(\exists \mathbf{x})(\mathbf{B} \wedge (\neg\neg\mathbf{A})) \Leftrightarrow (\exists \mathbf{x})(\mathbf{B} \wedge \mathbf{A})$ is logikai tétel $\mathfrak{T}$-ben. Ezután a 2.5.4. állítást alkalmazva kapjuk, hogy $(\neg(\exists \mathbf{x})(\mathbf{B} \wedge (\neg\neg\mathbf{A}))) \Leftrightarrow (\neg(\exists \mathbf{x})(\mathbf{B} \wedge \mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben, ami azt jelenti, hogy $(\forall_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A}) \Leftrightarrow \neg((\exists_{\mathbf{B}}\mathbf{x})\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben.

A definíció szerint $\neg((\forall_{\mathbf{B}}\mathbf{x})\mathbf{A}) \equiv \neg\neg(\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})$, és a 2.5.3. állítás alapján világos, hogy $(\neg\neg(\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})) \Leftrightarrow (\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, így $(\neg((\forall_{\mathbf{B}}\mathbf{x})\mathbf{A})) \Leftrightarrow (\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})$ szintén logikai tétel $\mathfrak{T}$-ben. ∎

2.8.3. Állítás. (**A feltételes kvantorok kapcsolata a diszjunkcióval, konjunkcióval és implikációval.**) *Ha* **x** *változó és* **A**, **B**, **C** *formulák a* $\mathfrak{T}$ *matematikai elméletben, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$(\exists_{\mathbf{C}}\mathbf{x})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow ((\exists_{\mathbf{C}}\mathbf{x})\mathbf{A}) \vee ((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}), \quad (\exists_{\mathbf{C}}\mathbf{x})(\mathbf{A} \wedge \mathbf{B}) \Rightarrow ((\exists_{\mathbf{C}}\mathbf{x})\mathbf{A}) \wedge ((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}),$$
$$(\exists_{\mathbf{C}}\mathbf{x})(\mathbf{A} \Rightarrow \mathbf{B}) \Leftrightarrow ((\forall_{\mathbf{C}}\mathbf{x})\mathbf{A}) \Rightarrow ((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}),$$
$$((\forall_{\mathbf{C}}\mathbf{x})\mathbf{A}) \vee ((\forall_{\mathbf{C}}\mathbf{x})\mathbf{B}) \Rightarrow (\forall_{\mathbf{C}}\mathbf{x})(\mathbf{A} \vee \mathbf{B}), \quad (\forall_{\mathbf{C}}\mathbf{x})(\mathbf{A} \wedge \mathbf{B}) \Leftrightarrow ((\forall_{\mathbf{C}}\mathbf{x})\mathbf{A}) \wedge ((\forall_{\mathbf{C}}\mathbf{x})\mathbf{B}),$$
$$(((\exists_{\mathbf{C}}\mathbf{x})\mathbf{A}) \Rightarrow ((\forall_{\mathbf{C}}\mathbf{x})\mathbf{B})) \Rightarrow (\forall_{\mathbf{C}}\mathbf{x})(\mathbf{A} \Rightarrow \mathbf{B}).$$

Bizonyítás. Tudjuk, hogy $(\mathbf{C} \wedge (\mathbf{A} \vee \mathbf{B})) \Leftrightarrow ((\mathbf{C} \wedge \mathbf{A}) \vee (\mathbf{C} \wedge \mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, amiből következik, hogy $(\exists \mathbf{x})(\mathbf{C} \wedge (\mathbf{A} \vee \mathbf{B})) \Leftrightarrow (\exists \mathbf{x})((\mathbf{C} \wedge \mathbf{A}) \vee (\mathbf{C} \wedge \mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Ugyanakkor láttuk, hogy a $(\exists \mathbf{x})((\mathbf{C} \wedge \mathbf{A}) \vee (\mathbf{C} \wedge \mathbf{B})) \Leftrightarrow (((\exists \mathbf{x})(\mathbf{C} \wedge \mathbf{A})) \vee ((\exists \mathbf{x})(\mathbf{C} \wedge \mathbf{B})))$ formula logikai tétel $\mathfrak{T}$-ben, amiből kapjuk, hogy $(\exists_{\mathbf{C}}\mathbf{x})(\mathbf{A} \vee \mathbf{B}) \Leftrightarrow (((\exists_{\mathbf{C}}\mathbf{x})\mathbf{A}) \vee ((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben.

Tudjuk továbbá, hogy $(\mathbf{C} \wedge (\mathbf{A} \wedge \mathbf{B})) \Leftrightarrow ((\mathbf{C} \wedge \mathbf{A}) \wedge (\mathbf{C} \wedge \mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben, amiből következik, hogy $(\exists \mathbf{x})(\mathbf{C} \wedge (\mathbf{A} \wedge \mathbf{B})) \Leftrightarrow (\exists \mathbf{x})((\mathbf{C} \wedge \mathbf{A}) \wedge (\mathbf{C} \wedge \mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Igazoltuk, hogy $(\exists \mathbf{x})((\mathbf{C} \wedge \mathbf{A}) \wedge (\mathbf{C} \wedge \mathbf{B})) \Rightarrow (((\exists \mathbf{x})(\mathbf{C} \wedge \mathbf{A})) \wedge ((\exists \mathbf{x})(\mathbf{C} \wedge \mathbf{A})))$ logikai tétel

$\mathfrak{T}$-ben, tehát $(\exists_{\mathbf{C}}\mathbf{x})(\mathbf{A}\wedge\mathbf{B})\Rightarrow(((\exists_{\mathbf{C}}\mathbf{x})\mathbf{A})\wedge((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben.

Az implikáció definíciója szerint $(\exists_{\mathbf{C}}\mathbf{x})(\mathbf{A}\Rightarrow\mathbf{B})\equiv(\exists_{\mathbf{C}}\mathbf{x})((\neg\mathbf{A})\vee\mathbf{B})$, és igazoltuk, hogy $(\exists_{\mathbf{C}}\mathbf{x})((\neg\mathbf{A})\vee\mathbf{B})\Leftrightarrow(((\exists_{\mathbf{C}}\mathbf{x})(\neg\mathbf{A}))\vee((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. A feltételes kvantoros kifejezések negációjának szabályát alkalmazva kapjuk, hogy $((\exists_{\mathbf{C}}\mathbf{x})(\neg\mathbf{A}))\Leftrightarrow(\neg(\forall_{\mathbf{C}}\mathbf{x})\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, amiből következik, hogy $(\exists_{\mathbf{C}}\mathbf{x})((\neg\mathbf{A})\vee\mathbf{B})\Leftrightarrow((\neg((\forall_{\mathbf{C}}\mathbf{x})\mathbf{A}))\vee((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}))$ logikai tétel $\mathfrak{T}$-ben. Az implikáció definíciója szerint ez pontosan azt jelenti, hogy a $(\exists_{\mathbf{C}}\mathbf{x})(\mathbf{A}\Rightarrow\mathbf{B})\Leftrightarrow(((\forall_{\mathbf{C}}\mathbf{x})\mathbf{A})\Rightarrow((\exists_{\mathbf{C}}\mathbf{x})\mathbf{B}))$ formula logikai tétel $\mathfrak{T}$-ben.

Ezzel a feltételes egzisztenciális kvantorokra vonatkozó állításokat igazoltuk. Ezekből a feltételes kvantoros kifejezések negációjának szabályát alkalmazva könnyen megkapjuk a feltételes univerzális kvantorokra vonatkozó állításokat. ∎

2.8.4. Állítás. (**A feltételes kvantorok felcserélésének tétele.**) *Ha* $\mathbf{x}$, $\mathbf{y}$ *különböző változók, és* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *formulák a* $\mathfrak{T}$ *matematikai elméletben, és* $\mathbf{x}$ *nem szerepel* $\mathbf{C}$*-ben, valamint* $\mathbf{y}$ *nem szerepel* $\mathbf{B}$*-ben, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$(\exists_{\mathbf{B}}\mathbf{x})(\exists_{\mathbf{C}}\mathbf{y})\mathbf{A}\Leftrightarrow(\exists_{\mathbf{C}}\mathbf{y})(\exists_{\mathbf{B}}\mathbf{x})\mathbf{A},$$
$$(\forall_{\mathbf{B}}\mathbf{x})(\forall_{\mathbf{C}}\mathbf{y})\mathbf{A}\Leftrightarrow(\forall_{\mathbf{C}}\mathbf{y})(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A},$$
$$(\exists_{\mathbf{B}}\mathbf{x})(\forall_{\mathbf{C}}\mathbf{y})\mathbf{A}\Rightarrow(\forall_{\mathbf{C}}\mathbf{y})(\exists_{\mathbf{B}}\mathbf{x})\mathbf{A}.$$

Bizonyítás. (I) Definíció szerint $(\exists_{\mathbf{B}}\mathbf{x})(\exists_{\mathbf{C}}\mathbf{y})\mathbf{A}\equiv(\exists\mathbf{x})(\mathbf{B}\wedge(\exists\mathbf{y})(\mathbf{C}\wedge\mathbf{A}))$. Az $\mathbf{y}$ nem szerepel $\mathbf{B}$-ben, így $(\mathbf{B}\wedge(\exists\mathbf{y})(\mathbf{C}\wedge\mathbf{A}))\Leftrightarrow(\exists\mathbf{y})(\mathbf{B}\wedge(\mathbf{C}\wedge\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. Ugyanakkor a korábbi eredmények szerint $(\mathbf{B}\wedge(\mathbf{C}\wedge\mathbf{A}))\Leftrightarrow(\mathbf{C}\wedge(\mathbf{B}\wedge\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben, így $(\exists\mathbf{y})(\mathbf{B}\wedge(\mathbf{C}\wedge\mathbf{A}))\Leftrightarrow(\exists\mathbf{y})(\mathbf{C}\wedge(\mathbf{B}\wedge\mathbf{A}))$ szintén logikai tétel $\mathfrak{T}$-ben. Ezért $(\exists_{\mathbf{B}}\mathbf{x})(\exists_{\mathbf{C}}\mathbf{y})\mathbf{A}\Leftrightarrow(\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{C}\wedge(\mathbf{B}\wedge\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. A kvantorok felcserélésének tétele alapján $(\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{C}\wedge(\mathbf{B}\wedge\mathbf{A}))\Leftrightarrow(\exists\mathbf{y})(\exists\mathbf{x})(\mathbf{C}\wedge(\mathbf{B}\wedge\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. De $\mathbf{x}$ nem szerepel $\mathbf{C}$-ben, ezért $(\exists\mathbf{x})(\mathbf{C}\wedge(\mathbf{B}\wedge\mathbf{A}))\Leftrightarrow(\mathbf{C}\wedge(\exists\mathbf{x})(\mathbf{B}\wedge\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. Ebből kapjuk, hogy $(\exists\mathbf{y})(\exists\mathbf{x})(\mathbf{C}\wedge(\mathbf{B}\wedge\mathbf{A}))\Leftrightarrow(\exists\mathbf{y})(\mathbf{C}\wedge(\exists\mathbf{x})(\mathbf{B}\wedge\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. A definíció szerint világos, hogy $(\exists\mathbf{y})(\mathbf{C}\wedge(\exists\mathbf{x})(\mathbf{B}\wedge\mathbf{A}))\equiv(\exists_{\mathbf{C}}\mathbf{y})(\exists_{\mathbf{B}}\mathbf{x})\mathbf{A}$, tehát $(\exists_{\mathbf{B}}\mathbf{x})(\exists_{\mathbf{C}}\mathbf{y})\mathbf{A}\Leftrightarrow(\exists_{\mathbf{C}}\mathbf{y})(\exists_{\mathbf{B}}\mathbf{x})\mathbf{A}$ logikai tétel $\mathfrak{T}$-ben.

(II) A definíció szerint $(\forall_{\mathbf{B}}\mathbf{x})(\forall_{\mathbf{C}}\mathbf{y})\mathbf{A}\equiv\neg(\exists_{\mathbf{B}}\mathbf{x})(\neg\neg(\exists_{\mathbf{C}}\mathbf{y})(\neg\mathbf{A}))$, és hasonlóan látható, hogy $(\forall_{\mathbf{C}}\mathbf{y})(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A}\equiv\neg(\exists_{\mathbf{C}}\mathbf{y})(\neg\neg(\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A}))$, ezért a 2.5.4. állítás alapján elég azt igazolni, hogy $((\exists_{\mathbf{B}}\mathbf{x})(\neg\neg(\exists_{\mathbf{C}}\mathbf{y})(\neg\mathbf{A})))\Leftrightarrow((\exists_{\mathbf{C}}\mathbf{y})(\neg\neg(\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben. A 2.5.3. állítás szerint $\neg\neg(\exists_{\mathbf{C}}\mathbf{y})(\neg\mathbf{A})\Leftrightarrow(\exists_{\mathbf{C}}\mathbf{y})(\neg\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, következésképpen $((\exists_{\mathbf{B}}\mathbf{x})(\neg\neg(\exists_{\mathbf{C}}\mathbf{y})(\neg\mathbf{A})))\Leftrightarrow((\exists_{\mathbf{B}}\mathbf{x})((\exists_{\mathbf{C}}\mathbf{y})(\neg\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben. Hasonlóan kapjuk, hogy $((\exists_{\mathbf{C}}\mathbf{y})(\neg\neg(\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})))\Leftrightarrow((\exists_{\mathbf{C}}\mathbf{y})((\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben. Az (I) alapján $((\exists_{\mathbf{B}}\mathbf{x})((\exists_{\mathbf{C}}\mathbf{y})(\neg\mathbf{A})))\Leftrightarrow((\exists_{\mathbf{C}}\mathbf{y})((\exists_{\mathbf{B}}\mathbf{x})(\neg\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben, ezért $((\forall_{\mathbf{B}}\mathbf{x})(\forall_{\mathbf{C}}\mathbf{y})\mathbf{A})\Leftrightarrow((\forall_{\mathbf{C}}\mathbf{y})(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A})$ szintén logikai tétel $\mathfrak{T}$-ben.

(III) A $((\forall_{\mathbf{C}}\mathbf{y})\mathbf{A})\Leftrightarrow((\forall\mathbf{y})(\mathbf{C}\Rightarrow\mathbf{A}))$ formula logikai tétel $\mathfrak{T}$-ben, következésképpen a $((\exists_{\mathbf{B}}\mathbf{x})(\forall_{\mathbf{C}}\mathbf{y})\mathbf{A})\Leftrightarrow((\exists\mathbf{x})(\mathbf{B}\wedge(\forall\mathbf{y})(\mathbf{C}\Rightarrow\mathbf{A})))$ formula szintén logikai tétel $\mathfrak{T}$-ben. Az $\mathbf{y}$ nem szerepel $\mathbf{B}$-ben, így $(\mathbf{B}\wedge(\forall\mathbf{y})(\mathbf{C}\Rightarrow\mathbf{A}))\Leftrightarrow((\forall\mathbf{y})(\mathbf{B}\wedge(\mathbf{C}\Rightarrow\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben, így $((\exists_{\mathbf{B}}\mathbf{x})(\forall_{\mathbf{C}}\mathbf{y})\mathbf{A})\Leftrightarrow((\exists\mathbf{x})(\forall\mathbf{y})(\mathbf{B}\wedge(\mathbf{C}\Rightarrow\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben. A kvantorok felcserélésének tétele szerint $((\exists\mathbf{x})(\forall\mathbf{y})(\mathbf{B}\wedge(\mathbf{C}\Rightarrow\mathbf{A})))\Rightarrow((\forall\mathbf{y})(\exists\mathbf{x})(\mathbf{B}\wedge(\mathbf{C}\Rightarrow\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben. Ez azt jelenti, hogy ha bebizonyítjuk, hogy $((\forall\mathbf{y})(\exists\mathbf{x})(\mathbf{B}\wedge(\mathbf{C}\Rightarrow\mathbf{A})))\Rightarrow((\forall_{\mathbf{C}}\mathbf{y})(\exists_{\mathbf{B}}\mathbf{x})\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, akkor a láncszabály alapján az állítást igazoltuk. Ehhez észrevesszük, hogy $((\forall_{\mathbf{C}}\mathbf{y})(\exists_{\mathbf{B}}\mathbf{x})\mathbf{A})\Leftrightarrow((\forall\mathbf{y})(\mathbf{C}\Rightarrow(\exists\mathbf{x})(\mathbf{B}\wedge\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben, ezért elegendő volna azt igazolni, hogy $((\forall\mathbf{y})(\exists\mathbf{x})(\mathbf{B}\wedge(\mathbf{C}\Rightarrow\mathbf{A})))\Rightarrow((\forall\mathbf{y})(\mathbf{C}\Rightarrow(\exists\mathbf{x})(\mathbf{B}\wedge\mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben. Ehhez pedig elég azt belátni, hogy $((\exists\mathbf{x})(\mathbf{B}\wedge(\mathbf{C}\Rightarrow\mathbf{A})))\Rightarrow(\mathbf{C}\Rightarrow(\exists\mathbf{x})(\mathbf{B}\wedge\mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. Az $\mathbf{x}$ változó nem szerepel $\mathbf{C}$-ben, így $((\neg\mathbf{C})\vee(\exists\mathbf{x})(\mathbf{B}\wedge\mathbf{A}))\Leftrightarrow((\exists\mathbf{x})((\neg\mathbf{C})\vee(\mathbf{B}\wedge\mathbf{A})))$, vagyis

$(\mathbf{C} \Rightarrow (\exists\mathbf{x})(\mathbf{B} \wedge \mathbf{A})) \Leftrightarrow ((\exists\mathbf{x})(\mathbf{C} \Rightarrow (\mathbf{B} \wedge \mathbf{A})))$ logikai tétel $\mathfrak{T}$-ben. Ez azt mutatja, hogy elég azt igazolni, hogy $(\mathbf{B} \wedge (\mathbf{C} \Rightarrow \mathbf{A})) \Rightarrow (\mathbf{C} \Rightarrow (\mathbf{B} \wedge \mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben, vagyis tétel $\mathfrak{T}_0$-ban. Ez viszont nyilvánvaló, mert ha $\mathfrak{T}'$ jelöli a $\mathfrak{T}_0[\mathbf{B} \wedge (\mathbf{C} \Rightarrow \mathbf{A}), \mathbf{C}]$ elméletet, akkor világos, hogy $\mathbf{B}$, $\mathbf{C} \Rightarrow \mathbf{A}$ és $\mathbf{C}$ tételek $\mathfrak{T}'$-ben, tehát a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{A}$ is tétel $\mathfrak{T}'$-ben, így a $\mathbf{B} \wedge \mathbf{A}$ formula is tétel $\mathfrak{T}'$-ben, amiből a dedukció-tétel kétszeri alkalmazásával kapjuk, hogy $(\mathbf{B} \wedge (\mathbf{C} \Rightarrow \mathbf{A})) \Rightarrow (\mathbf{C} \Rightarrow (\mathbf{B} \wedge \mathbf{A}))$ logikai tétel $\mathfrak{T}$-ben. ■

2.8.5. Állítás. *Legyen* $\mathbf{x}$ *változó és* $\mathbf{B}$ *formula a* $\mathfrak{T}$ *matematikai elméletben. Ha a* $(\exists\mathbf{x})\mathbf{B}$ *formula (logikai) tétel* $\mathfrak{T}$*-ben, akkor a* $\mathfrak{T}$ *matematikai elmélet minden* $\mathbf{A}$ *formulájára a*

$$(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A} \;\Rightarrow\; (\exists_{\mathbf{B}}\mathbf{x})\mathbf{A}$$

formula (logikai) tétel $\mathfrak{T}$*-ben.*

Bizonyítás. (I) Tegyük fel hogy $(\exists\mathbf{x})\mathbf{B}$ tétel $\mathfrak{T}$-ben, és legyen $\mathbf{A}$ tetszőleges formulája a $\mathfrak{T}$ matematikai elméletnek. Jelölje $\mathfrak{T}'$ a $\mathfrak{T}[(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A}]$ matematikai elméletet, amelyben $(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A}$ explicit axióma, tehát tétel. Tudjuk, hogy $(\forall_{\mathbf{B}}\mathbf{x})\mathbf{A} \Leftrightarrow (\forall\mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A})$ logikai tétel $\mathfrak{T}'$-ben, tehát $(\forall\mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A})$ tétel $\mathfrak{T}'$-ben. Ugyanakkor, a hipotézis szerint $(\exists\mathbf{x})\mathbf{B}$ tétel $\mathfrak{T}$-ben, így $\mathfrak{T}'$-ben is, ami az egzisztenciális kvantor definíciója szerint azt jelenti, hogy $(\mathbf{T}|\mathbf{x})\mathbf{B}$ tétel $\mathfrak{T}'$-ben, ahol $\mathbf{T} \equiv \varepsilon_{\mathbf{x}}(\mathbf{B})$. Az univerzális kvantor logikai alaptulajdonsága szerint $(\forall\mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A}) \Rightarrow (\mathbf{T}|\mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A})$ logikai tétel $\mathfrak{T}'$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{T}|\mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A})$ tétel $\mathfrak{T}'$-ben. Mivel $(\mathbf{T}|\mathbf{x})(\mathbf{B} \Rightarrow \mathbf{A}) \equiv ((\mathbf{T}|\mathbf{x})\mathbf{B}) \Rightarrow ((\mathbf{T}|\mathbf{x})\mathbf{A})$, így ismét a leválasztás szabályát alkalmazva adódik, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}'$-ben. Tehát a konjunkció logikai alaptulajdonsága szerint $((\mathbf{T}|\mathbf{x})\mathbf{B}) \wedge ((\mathbf{T}|\mathbf{x})\mathbf{A})$ tétel $\mathfrak{T}'$-ben. Mivel $((\mathbf{T}|\mathbf{x})\mathbf{B}) \wedge ((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv (\mathbf{T}|\mathbf{x})(\mathbf{B} \wedge \mathbf{A})$ és a $((\mathbf{T}|\mathbf{x})(\mathbf{B} \wedge \mathbf{A})) \Rightarrow (\exists\mathbf{x})(\mathbf{B} \wedge \mathbf{A})$ formula eleme $\mathfrak{S}_5$-nek, tehát axióma $\mathfrak{T}'$-ben, így a leválasztás szabálya szerint $(\exists\mathbf{x})(\mathbf{B} \wedge \mathbf{A})$, vagyis $(\exists_{\mathbf{B}}\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}'$-ben. Ebből a dedukció-tétel alkalmazásával kapjuk, hogy $((\forall_{\mathbf{B}}\mathbf{x})\mathbf{A}) \Rightarrow ((\exists_{\mathbf{B}}\mathbf{x})\mathbf{A})$ tétel $\mathfrak{T}$-ben.

(II) Tegyük fel hogy $(\exists\mathbf{x})\mathbf{B}$ logikai tétel $\mathfrak{T}$-ben, és legyen $\mathbf{A}$ tetszőleges formulája a $\mathfrak{T}$ matematikai elméletnek. Ekkor $(\exists\mathbf{x})\mathbf{B}$ tétel a $\mathfrak{T}_0$ predikátumkalkulusban, és $\mathbf{A}$ formulája a $\mathfrak{T}_0$ predikátumkalkulusnak is, így (I) alapján $((\forall_{\mathbf{B}}\mathbf{x})\mathbf{A}) \Rightarrow ((\exists_{\mathbf{B}}\mathbf{x})\mathbf{A})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben. ■

Vigyázzunk arra, hogy az előző állításban nélkülözhetetlen az a mellékfeltétel, hogy a $(\exists\mathbf{x})\mathbf{B}$ egzisztenciális formula (logikai) tétel legyen $\mathfrak{T}$-ben. Z

2.9. Az egyenlőség logikai tulajdonságai

Most az $=$ jellel kapcsolatos alapvető logikai tulajdonságokat fogjuk megvizsgálni. Érdemes bevezetni a következő elnevezést:

2.9.1. Definíció. *Legyenek* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumok a* $\mathfrak{T}$ *matematikai elméletben. Azt mondjuk, hogy* $\mathbf{T}$ *és* $\mathbf{S}$ **egyenlő** $\mathfrak{T}$*-ben, ha a* $\mathbf{T} = \mathbf{S}$ *formula tétel* $\mathfrak{T}$*-ben. A* $\mathbf{T} = \mathbf{S}$ *alakú formulákat* **egyenlőségeknek** *nevezzük.*

Világosan látható, hogy két objektum egyenlősége lényegesen függ annak a matematikai elméletnek az igazság-fogalmától, amelynek nyelvében a két objektum egyenlőségét (mint formulát) megfogalmaztuk.

2.9.2. Tétel. (**Az egyenlőség logikai tulajdonságai.**) *Ha* $\mathbf{T}$*,* $\mathbf{S}$ *és* $\mathbf{R}$ *objektumok a* $\mathfrak{T}$ *matematikai elméletben, akkor a következő formulák logikai tételek* $\mathfrak{T}$*-ben:*

$$\mathbf{T} = \mathbf{T},$$
$$\mathbf{T} = \mathbf{S} \Leftrightarrow \mathbf{S} = \mathbf{T},$$
$$(\ (\mathbf{T} = \mathbf{S})\ \wedge\ (\mathbf{S} = \mathbf{R})\ )\ \Rightarrow\ \mathbf{T} = \mathbf{R}.$$

Bizonyítás. (I) Legyen $\mathbf{x}$ tetszőleges változó, és jelölje $\mathbf{A}$ a $\neg(\mathbf{x} = \mathbf{x})$ formulát. A $((\forall\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{A})) \Rightarrow (\varepsilon_{\mathbf{x}}(\mathbf{A}) = \varepsilon_{\mathbf{x}}(\mathbf{A}))$ formula eleme $\mathfrak{S}_7$-nek, tehát logikai tétel $\mathfrak{T}$-ben, ugyanakkor $\mathbf{A}\Leftrightarrow\mathbf{A}$ is logikai tétel $\mathfrak{T}$-ben, így a tételek helyettesítés-invarianciájának szabálya szerint az $(\varepsilon_{\mathbf{x}}(\neg(\mathbf{A}\Leftrightarrow\mathbf{A}))|\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{A})$ formula is logikai tétel $\mathfrak{T}$-ben. De $((\varepsilon_{\mathbf{x}}(\neg(\mathbf{A}\Leftrightarrow\mathbf{A}))|\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{A}))\Leftrightarrow(\forall\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{A})$ logikai tétel $\mathfrak{T}$-ben, tehát $(\forall\mathbf{x})(\mathbf{A}\Leftrightarrow\mathbf{A})$ szintén logikai tétel $\mathfrak{T}$-ben. A leválasztás szabályát alkalmazva kapjuk, hogy az $\varepsilon_{\mathbf{x}}(\mathbf{A}) = \varepsilon_{\mathbf{x}}(\mathbf{A})$ formula logikai tétel $\mathfrak{T}$-ben. Ugyanakkor ez a formula azonos az $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})(\mathbf{x} = \mathbf{x})$ formulával, ami nem más, mint az $(\varepsilon_{\mathbf{x}}(\neg(\mathbf{x} = \mathbf{x}))|\mathbf{x})(\mathbf{x} = \mathbf{x})$ formula. Tudjuk, hogy $((\forall\mathbf{x})(\mathbf{x} = \mathbf{x}))\Leftrightarrow(\varepsilon_{\mathbf{x}}(\neg(\mathbf{x} = \mathbf{x}))|\mathbf{x})(\mathbf{x} = \mathbf{x})$ logikai tétel $\mathfrak{T}$-ben, ezért az előzőek alapján $(\forall\mathbf{x})(\mathbf{x} = \mathbf{x})$ logikai tétel $\mathfrak{T}$-ben. Ha $\mathbf{T}$ tetszőleges objektum, akkor a $(\forall\mathbf{x})(\mathbf{x} = \mathbf{x}) \Rightarrow (\mathbf{T}|\mathbf{x})(\mathbf{x} = \mathbf{x})$ formula logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy a $(\mathbf{T}|\mathbf{x})(\mathbf{x} = \mathbf{x})$ formula logikai tétel $\mathfrak{T}$-ben, tehát $(\mathbf{T}|\mathbf{x})(\mathbf{x} = \mathbf{x}) \equiv (\mathbf{T} = \mathbf{T})$ miatt $\mathbf{T} = \mathbf{T}$ logikai tétel $\mathfrak{T}$-ben.

(II) Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[\mathbf{T} = \mathbf{S}]$ elméletet, és legyen $\mathbf{x}$ olyan változó, amely $\mathbf{T}$-ben nem szerepel. A $(\mathbf{T} = \mathbf{S}) \Rightarrow ((\mathbf{T}|\mathbf{x})(\mathbf{x} = \mathbf{T})\Leftrightarrow(\mathbf{S}|\mathbf{x})(\mathbf{x} = \mathbf{T}))$ formula eleme $\mathfrak{S}_6$-nak, tehát tétel $\mathfrak{T}'$-ben. Ugyanakkor $(\mathbf{T}|\mathbf{x})(\mathbf{x} = \mathbf{T}) \equiv (\mathbf{T} = \mathbf{T})$ és $(\mathbf{S}|\mathbf{x})(\mathbf{x} = \mathbf{T}) \equiv (\mathbf{S} = \mathbf{T})$, mert $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben. Tehát $(\mathbf{T} = \mathbf{S}) \Rightarrow ((\mathbf{T} = \mathbf{T})\Leftrightarrow(\mathbf{S} = \mathbf{T}))$ tétel $\mathfrak{T}'$-ben. Ebből a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{T} = \mathbf{T})\Leftrightarrow(\mathbf{S} = \mathbf{T})$ tétel $\mathfrak{T}'$-ben. Az ekvivalencia tulajdonságaiból következik, hogy ekkor $(\mathbf{T} = \mathbf{T}) \Rightarrow (\mathbf{S} = \mathbf{T})$ is tétel $\mathfrak{T}'$-ben. Az (I) alapján $\mathbf{T} = \mathbf{T}$ tétel $\mathfrak{T}'$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{S} = \mathbf{T}$ tétel $\mathfrak{T}'$-ben. A dedukció-tételből következik, hogy $(\mathbf{T} = \mathbf{S}) \Rightarrow (\mathbf{S} = \mathbf{T})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben. Ez a $\mathfrak{T}$ bármely két $\mathbf{T}$ és $\mathbf{S}$ objektumára teljesül, tehát a $\mathbf{T}$ és $\mathbf{S}$ felcserélésével kapjuk, hogy $(\mathbf{S} = \mathbf{T}) \Rightarrow (\mathbf{T} = \mathbf{S})$ is logikai tétel $\mathfrak{T}$-ben. Az ekvivalencia logikai tulajdonságai alapján ez azt jelenti, hogy $(\mathbf{T} = \mathbf{S})\Leftrightarrow(\mathbf{S} = \mathbf{T})$ logikai tétel $\mathfrak{T}$-ben.

(III) Jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[(\mathbf{T} = \mathbf{S}) \wedge (\mathbf{S} = \mathbf{R})]$ elméletet. Legyen $\mathbf{x}$ olyan változó, amely nem szerepel $\mathbf{T}$-ben. Az $(\mathbf{S} = \mathbf{R}) \Rightarrow ((\mathbf{S}|\mathbf{x})(\mathbf{T} = \mathbf{x})\Leftrightarrow(\mathbf{R}|\mathbf{x})(\mathbf{T} = \mathbf{x}))$ formula eleme $\mathfrak{S}_6$-nak, tehát tétel $\mathfrak{T}'$-ben. Ugyanakkor $(\mathbf{S}|\mathbf{x})(\mathbf{T} = \mathbf{x}) \equiv (\mathbf{T} = \mathbf{S})$ és $(\mathbf{R}|\mathbf{x})(\mathbf{T} = \mathbf{x}) \equiv (\mathbf{T} = \mathbf{R})$, mert $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben. Tehát $(\mathbf{S} = \mathbf{R}) \Rightarrow ((\mathbf{T} = \mathbf{S})\Leftrightarrow(\mathbf{T} = \mathbf{R}))$ tétel $\mathfrak{T}'$-ben, és $\mathbf{S} = \mathbf{R}$ tétel $\mathfrak{T}'$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{T} = \mathbf{S})\Leftrightarrow(\mathbf{T} = \mathbf{R})$ tétel $\mathfrak{T}'$-ben. Az ekvivalencia tulajdonságai alapján ebből következik, hogy $(\mathbf{T} = \mathbf{S}) \Rightarrow (\mathbf{T} = \mathbf{R})$ tétel $\mathfrak{T}'$-ben. Ugyanakkor $\mathbf{T} = \mathbf{S}$ is tétel $\mathfrak{T}'$-ben, így ismét leválasztást alkalmazva kapjuk, hogy $\mathbf{T} = \mathbf{R}$ tétel $\mathfrak{T}'$-ben. Ebből a dedukció-tétel alkalmazásával következik, hogy a $((\mathbf{T} = \mathbf{S})\wedge(\mathbf{S} = \mathbf{R})) \Rightarrow (\mathbf{T} = \mathbf{R})$ formula tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben. ■

Eddig az $=$ szimbólum egy kitüntetett kétváltozós logikai függvényjelként szerepelt a matematikai nyelvekben. Abból a szempontból kitüntetett, hogy *minden* matematikai nyelv szimbólum-készletében szerepel. A matematikai elméletekben az $=$ jelnek logikai értelmet az $\mathfrak{S}_6$ és $\mathfrak{S}_7$ logikai axióma-sémák adnak. Az imént bizonyított tételből látható, hogy ezek a logikai axióma-sémák (egyéb logikai axiómákkal és szabályokkal együtt) valóban olyan tulajdonságokkal ruházzák fel az $=$ jelet tartalmazó formulákat (vagyis az *egyenlőségeket*), amelyeket az objektumok egyenlőségével kapcsolatban a nem formális logikában is elvárunk. A következő állításban szintén egy ilyen természetes követelmény teljesülését igazoljuk.

2.9.3. Állítás. *Ha* **T***,* **S***,* **R** *objektumok és* **x** *változó a* $\mathfrak{T}$ *matematikai elméletben, akkor*

$$\mathbf{T} = \mathbf{S} \;\Rightarrow\; (\mathbf{T}|\mathbf{x})\mathbf{R} = (\mathbf{S}|\mathbf{x})\mathbf{R}$$

logikai tétel $\mathfrak{T}$*-ben.*

Bizonyítás. Legyenek **y** és **z** olyan különböző változók, amelyek különböznek **x**-től és nem szerepelnek a **T**, **S**, **R** objektumokban, továbbá jelölje $\mathfrak{T}'$ a $\mathfrak{T}_0[\mathbf{y}{=}\mathbf{z}]$ elméletet. A $\mathfrak{T}$ bármely **B** formulájára az $(\mathbf{y} = \mathbf{z}) \Rightarrow ((\mathbf{y}|\mathbf{z})\mathbf{B}{\Leftrightarrow}(\mathbf{z}|\mathbf{z})\mathbf{B})$ formula eleme $\mathfrak{S}_6$-nak, tehát tétel $\mathfrak{T}'$-ben, továbbá $\mathbf{y} = \mathbf{z}$ axióma $\mathfrak{T}'$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{y}|\mathbf{z})\mathbf{B}{\Leftrightarrow}(\mathbf{z}|\mathbf{z})\mathbf{B}$, vagyis $(\mathbf{y}|\mathbf{z})\mathbf{B}{\Leftrightarrow}\mathbf{B}$ tétel $\mathfrak{T}'$-ben. Jelölje **B** az $(\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{z}|\mathbf{x})\mathbf{R}$ formulát. A **z** és **y** változók különbözőek és **z** nem szerepel **R**-ben, ezért $(\mathbf{y}|\mathbf{z})(\mathbf{y}|\mathbf{x})\mathbf{R} \equiv (\mathbf{y}|\mathbf{x})\mathbf{R}$, továbbá az **x** változó különbözik **z**-től és **y**-tól, így $(\mathbf{y}|\mathbf{z})(\mathbf{z}|\mathbf{x})\mathbf{R} \equiv (\mathbf{y}|\mathbf{x})\mathbf{R}$, hiszen **z** nem szerepel **R**-ben. Ez azt jelenti, hogy $(\mathbf{y}|\mathbf{z})\mathbf{B} \equiv ((\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{y}|\mathbf{x})\mathbf{R})$, amivel megmutattuk, hogy $((\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{y}|\mathbf{x})\mathbf{R}){\Leftrightarrow}((\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{z}|\mathbf{x})\mathbf{R})$ tétel $\mathfrak{T}'$-ben. A konjunkció logikai alaptulajdonsága szerint ekkor $((\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{y}|\mathbf{x})\mathbf{R}) \Rightarrow ((\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{z}|\mathbf{x})\mathbf{R})$ tétel $\mathfrak{T}'$-ben, és mivel $(\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{y}|\mathbf{x})\mathbf{R}$ tétel $\mathfrak{T}'$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{z}|\mathbf{x})\mathbf{R}$ tétel $\mathfrak{T}'$-ben. Tehát a dedukció-tételből következik, hogy $(\mathbf{y} = \mathbf{z}) \Rightarrow ((\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{z}|\mathbf{x})\mathbf{R})$ tétel $\mathfrak{T}_0$-ban, vagyis logikai tétel $\mathfrak{T}$-ben. Kétszer egymás után alkalmazva a tételek helyettesítés-invarianciájának szabályát kapjuk, hogy $(\mathbf{T}|\mathbf{y})(\mathbf{S}|\mathbf{z})((\mathbf{y} = \mathbf{z}) \Rightarrow ((\mathbf{y}|\mathbf{x})\mathbf{R} = (\mathbf{z}|\mathbf{x})\mathbf{R}))$ is logikai tétel $\mathfrak{T}$-ben. Természetesen az **y** és **z** változók választása alapján nyilvánvaló, hogy ez a formula azonos a $(\mathbf{T} = \mathbf{S}) \Rightarrow ((\mathbf{T}|\mathbf{x})\mathbf{R} = (\mathbf{S}|\mathbf{x})\mathbf{R})$ formulával. ■

Tehát megmutattuk, hogy ha két objektum egyenlő, akkor ezeket bármely objektum bármely változója helyére behelyettesítve egyenlő objektumokat kapunk. Azt is elvárjuk, hogy ha két objektum egyenlő, akkor ezeket bármely formula bármely változója helyére helyettesítve ekvivalens formulákat kapjunk. Ez valóban így van, és nem is kell bizonyítanunk, mert az $\mathfrak{S}_6$ logikai axióma-sémának pontosan ez az értelme.

Azonban vigyázzunk arra, hogy ha a $\mathfrak{T}$ matematikai elmélet *bármely* **T**, **S**, **R** objektumára és *bármely* **x** változójára a $\mathbf{T} = \mathbf{S} \;\Rightarrow\; (\mathbf{R}|\mathbf{x})\mathbf{T} = (\mathbf{R}|\mathbf{x})\mathbf{S}$ formula tétel $\mathfrak{T}$-ben, akkor az elmélet bármely **T** és **S** objektumára $\mathbf{T} = \mathbf{S}$ tétel $\mathfrak{T}$-ben. Legyenek ugyanis **T** és **S** rögzített objektumok, és vegyünk olyan **x** és **y** változókat, amelyek különböznek egymástól, és nem szerepelnek sem **T**-ben, sem **S**-ben, valamint a $\mathfrak{T}$ explicit axiómáiban sem szerepelnek. A hipotézis szerint az $(\mathbf{x} = \mathbf{y}) \Rightarrow ((\mathbf{S}|\mathbf{y})\mathbf{x} = (\mathbf{S}|\mathbf{y})\mathbf{y})$ formula tétel $\mathfrak{T}$-ben, és természetesen $(\mathbf{S}|\mathbf{y})\mathbf{x} \equiv \mathbf{x}$ (mert **x** és **y** különbözőek), valamint $(\mathbf{S}|\mathbf{y})\mathbf{y} \equiv \mathbf{S}$. Tehát $(\mathbf{x} = \mathbf{y}) \Rightarrow (\mathbf{x} = \mathbf{S})$ tétel $\mathfrak{T}$-ben. Az **x** nem szerepel a $\mathfrak{T}$ explicit axiómáiban, ezért a tételek helyettesítés-invarianciája szerint $(\mathbf{T}|\mathbf{x})((\mathbf{x} = \mathbf{y}) \Rightarrow (\mathbf{x} = \mathbf{S}))$ tétel $\mathfrak{T}$-ben. De $(\mathbf{T}|\mathbf{x})((\mathbf{x} = \mathbf{y}) \Rightarrow (\mathbf{x} = \mathbf{S})) \equiv ((\mathbf{T} = \mathbf{y}) \Rightarrow (\mathbf{T} = \mathbf{S}))$, mert **x** nem szerepel **S**-ben. Tehát $(\mathbf{T} = \mathbf{y}) \Rightarrow (\mathbf{T} = \mathbf{S})$ tétel $\mathfrak{T}$-ben. Az **y** nem szerepel a $\mathfrak{T}$ explicit axiómáiban, ezért a tételek helyettesítés-invarianciája szerint $(\mathbf{T}|\mathbf{y})((\mathbf{T} = \mathbf{y}) \Rightarrow (\mathbf{T} = \mathbf{S}))$ tétel $\mathfrak{T}$-ben. De $(\mathbf{T}|\mathbf{y})((\mathbf{T} = \mathbf{y}) \Rightarrow (\mathbf{T} = \mathbf{S})) \equiv (\mathbf{T} = \mathbf{T}) \Rightarrow (\mathbf{T} = \mathbf{S})$, mert **y** nem szerepel **T**-ben és **S**-ben. Tehát $(\mathbf{T} = \mathbf{T}) \Rightarrow (\mathbf{T} = \mathbf{S})$ és $\mathbf{T} = \mathbf{T}$ tétel a $\mathfrak{T}$ elméletben, amiből a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{T} = \mathbf{S}$ tétel $\mathfrak{T}$-ben.

A matematikai elméletekben gyakran találkozunk különféle *egyenletekkel* és azok *megoldásaival.* Pontosabban a következőről van szó. Legyenek **T** és **S** objektumok a

$\mathfrak{T}$ matematikai elméletben, és $\mathbf{x}$ olyan változó, amely $\mathbf{S}$-ben nem szerepel. Ha $\mathbf{R}$ olyan objektum, amelyre a $(\mathbf{R}|\mathbf{x})\mathbf{T} = \mathbf{S}$ formula tétel $\mathfrak{T}$-ben, akkor azt mondjuk, hogy $\mathbf{R}$ *megoldása* $\mathbf{x}$*-ben a* $\mathbf{T} = \mathbf{S}$ *egyenletnek a* $\mathfrak{T}$ *elméletben.*

A nem formális matematikában sokszor előfordulnak *egyértelműen létező* matematikai objektumok. Ilyenről akkor beszélünk, ha egy $\mathbf{A}$ kijelentésről és annak $\mathbf{x}$ változójáról bebizonyítjuk, hogy "létezik olyan $\mathbf{x}$, hogy $\mathbf{A}$" és "bármely két objektumra igaz az, hogy ha azok $\mathbf{x}$ helyére téve igazzá teszik az $\mathbf{A}$ kijelentést, akkor a két objektum egyenlő". Most ennek a nem formális logikai fogalomnak a formalizálásával foglalkozunk.

2.9.4. Lemma. *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben. Ha* $\mathbf{y}$ *és* $\mathbf{z}$ *olyan különböző változók, amelyek* $\mathbf{x}$*-től különböznek és nem szerepelnek* $\mathbf{A}$*-ban, akkor a*

$$(\forall\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z}))$$

formula független az $\mathbf{y}$ *és* $\mathbf{z}$ *változóktól, tehát ha* $\mathbf{y}'$ *és* $\mathbf{z}'$ *szintén olyan különböző változók, amelyek* $\mathbf{x}$*-től különböznek és nem szerepelnek* $\mathbf{A}$*-ban, akkor*

$$(\forall\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z})\equiv$$
$$\equiv(\forall\mathbf{y}')(\forall\mathbf{z}')(((\mathbf{y}'|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}'|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y}' = \mathbf{z}')).$$

Bizonyítás. Tetszőleges $\mathbf{u}$ és $\mathbf{v}$ változóra legyen

$$\mathbf{B}(\mathbf{u},\mathbf{v}) \equiv ((\mathbf{u}|\mathbf{x})\mathbf{A} \wedge (\mathbf{v}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{u} = \mathbf{v}).$$

Legyenek $\mathbf{y}$ és $\mathbf{z}$ olyan különböző változók, amelyek $\mathbf{x}$-től különböznek és nem szerepelnek $\mathbf{A}$-ban. Válasszunk olyan $\mathbf{u}$ és $\mathbf{v}$ változókat, amelyek különböznek egymástól, $\mathbf{x}$-től, $\mathbf{y}$-tól és $\mathbf{z}$-től, valamint nem szerepelnek $\mathbf{A}$-ban. Ekkor $\mathbf{z}$ nem szerepel $\mathbf{B}(\mathbf{u},\mathbf{v})$-ben, mert $\mathbf{z}$ különbözik $\mathbf{u}$-tól és $\mathbf{v}$-től, valamint $\mathbf{z}$ nem szerepel $\mathbf{A}$-ban. Ezért a kvantoros kifejezésekre vonatkozó helyettesítések tranzitivitásának szabályát alkalmazva $(\forall\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}) \equiv (\forall\mathbf{z})((\mathbf{z}|\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}))$ adódik. A $\mathbf{z}$ különbözik $\mathbf{u}$-tól és $\mathbf{y}$-tól, ezért ha a változók helyettesítésének szabályát alkalmazzuk a kvantoros kifejezésekre, akkor $(\mathbf{y}|\mathbf{u})(\forall\mathbf{z})((\mathbf{z}|\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v})) \equiv (\forall\mathbf{z})((\mathbf{y}|\mathbf{u})(\mathbf{z}|\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}))$ adódik. Ugyanakkor $\mathbf{y}$ nem szerepel a $(\forall\mathbf{z})((\mathbf{z}|\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}))$ formulában, mert különbözik $\mathbf{u}$-tól és $\mathbf{z}$-től, valamint nem szerepel $\mathbf{A}$-ban. Ezért a helyettesítések tranzitivitásának szabályát alkalmazva a kvantoros kifejezésekre kapjuk, hogy

$$(\forall\mathbf{u})(\forall\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}) \equiv (\forall\mathbf{y})((\mathbf{y}|\mathbf{u})(\forall\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v})) \equiv (\forall\mathbf{y})((\mathbf{y}|\mathbf{u})(\forall\mathbf{z})((\mathbf{z}|\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}))) \equiv$$
$$\equiv (\forall\mathbf{y})(\forall\mathbf{z})((\mathbf{y}|\mathbf{u})(\mathbf{z}|\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v})) \equiv (\forall\mathbf{y})(\forall\mathbf{z})\mathbf{B}(\mathbf{y},\mathbf{z}),$$

ahol az utolsó azonosságnál felhasználtuk, hogy $(\mathbf{y}|\mathbf{u})(\mathbf{z}|\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}) \equiv \mathbf{B}(\mathbf{y},\mathbf{z})$.

Ha $\mathbf{y}'$ és $\mathbf{z}'$ szintén olyan különböző változók, amelyek $\mathbf{x}$-től különböznek és nem szerepelnek $\mathbf{A}$-ban, továbbá az $\mathbf{u}$ és $\mathbf{v}$ változókat úgy választjuk meg, hogy különbözzenek egymástól, $\mathbf{x}$-től, $\mathbf{y}$-tól, $\mathbf{z}$-től, $\mathbf{y}'$-től és $\mathbf{z}'$-től, akkor az előzőek szerint

$$(\forall\mathbf{y})(\forall\mathbf{z})\mathbf{B}(\mathbf{y},\mathbf{z}) \equiv (\forall\mathbf{u})(\forall\mathbf{v})\mathbf{B}(\mathbf{u},\mathbf{v}) \equiv (\forall\mathbf{y}')(\forall\mathbf{z}')\mathbf{B}(\mathbf{y}',\mathbf{z}'),$$

és természetesen $\mathbf{B}(\mathbf{y},\mathbf{z}) \equiv ((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z})$, valamint $\mathbf{B}(\mathbf{y}',\mathbf{z}') \equiv ((\mathbf{y}'|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}'|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y}' = \mathbf{z}')$. Ezzel az állítást igazoltuk. ■

2.9.5. Definíció. *Azt mondjuk, hogy a* $\mathfrak{T}$ *matematikai elmélet* $\mathbf{A}$ *formulája az* $\mathbf{x}$ *változóban* **egyértelmű** $\mathfrak{T}$*-ben, ha a* $(\forall\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z}))$ *formula tétel* $\mathfrak{T}$*-ben, ahol* $\mathbf{y}$ *és* $\mathbf{z}$ *tetszőleges olyan különböző változók, amelyek* $\mathbf{x}$*-től különböznek és nem szerepelnek* $\mathbf{A}$*-ban.*

2.9.6. Tétel. *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben. Ha* $\mathbf{A}$ *az* $\mathbf{x}$ *változóban egyértelmű* $\mathfrak{T}$*-ben, akkor* $\mathfrak{T}$ *bármely* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumára a*

$$((\mathbf{T}|\mathbf{x})\mathbf{A}) \wedge ((\mathbf{S}|\mathbf{x})\mathbf{A}) \ \Rightarrow \ \mathbf{T} = \mathbf{S}$$

formula tétel $\mathfrak{T}$*-ben.*

Bizonyítás. Legyenek $\mathbf{y}$ és $\mathbf{z}$ olyan különböző változók, amelyek különböznek $\mathbf{x}$-től és nem szerepelnek sem az $\mathbf{A}$ formulában, sem a $\mathbf{T}$ és $\mathbf{S}$ objektumokban. A $(\forall\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z}))$ formula tétel $\mathfrak{T}$-ben, és a

$$(\forall\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z})) \ \Rightarrow \ (\mathbf{T}|\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z}))$$

formula logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabálya szerint $(\mathbf{T}|\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z}))$ tétel $\mathfrak{T}$-ben. A $\mathbf{z}$ változó $\mathbf{y}$-tól különbözik és nem szerepel $\mathbf{T}$-ben, így a kvantoros kifejezésekre vonatkozó helyettesítési tétel alapján

$$\begin{aligned}(\mathbf{T}|\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z})) &\equiv (\forall\mathbf{z})(\mathbf{T}|\mathbf{y})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z})) \\ &\equiv \ (\forall\mathbf{z})(((\mathbf{T}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{z})),\end{aligned}$$

hiszen $(\mathbf{T}|\mathbf{y})(\mathbf{y}|\mathbf{x})\mathbf{A} \equiv (\mathbf{T}|\mathbf{x})\mathbf{A}$ (mert $\mathbf{y}$ nem szerepel $\mathbf{A}$-ban), $(\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})\mathbf{A} \equiv (\mathbf{z}|\mathbf{x})\mathbf{A}$ (mert $\mathbf{y}$ és $\mathbf{z}$ különbözőek, valamint $\mathbf{y}$ nem szerepel $\mathbf{A}$-ban), és $(\mathbf{T}|\mathbf{y})(\mathbf{y} = \mathbf{z}) \equiv \mathbf{T} = \mathbf{z}$ (mert $\mathbf{y}$ és $\mathbf{z}$ különbözőek). Ez azt jelenti, hogy $(\forall\mathbf{z})(((\mathbf{T}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{z}))$ tétel $\mathfrak{T}$-ben, ugyanakkor a

$$(\forall\mathbf{z})(((\mathbf{T}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{z})) \ \Rightarrow \ (\mathbf{S}|\mathbf{z})(((\mathbf{T}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{z}))$$

formula logikai tétel $\mathfrak{T}$-ben, így a leválasztás szabálya szerint $(\mathbf{S}|\mathbf{z})(((\mathbf{T}|\mathbf{x})\mathbf{A}\wedge(\mathbf{z}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{z}))$ tétel $\mathfrak{T}$-ben. Könnyen látható, hogy

$$(\mathbf{S}|\mathbf{z})(((\mathbf{T}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{z})) \ \equiv \ (((\mathbf{T}|\mathbf{x})\mathbf{A}) \wedge ((\mathbf{S}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{S}),$$

ugyanis nyilvánvalóan $(\mathbf{S}|\mathbf{z})(\mathbf{T}|\mathbf{x})\mathbf{A} \equiv (\mathbf{T}|\mathbf{x})\mathbf{A}$ (mert $\mathbf{z}$ nem szerepel $\mathbf{T}$-ben és $\mathbf{A}$-ban), $(\mathbf{S}|\mathbf{z})(\mathbf{z}|\mathbf{x})\mathbf{A} \equiv (\mathbf{S}|\mathbf{x})\mathbf{A}$ (mert $\mathbf{z}$ nem szerepel $\mathbf{A}$-ban), és $(\mathbf{S}|\mathbf{z})(\mathbf{T}{=}\mathbf{z}) \equiv \mathbf{T}{=}\mathbf{S}$ (mert $\mathbf{z}$ nem szerepel $\mathbf{T}$-ben). Ez azt jelenti, hogy $(((\mathbf{T}|\mathbf{x})\mathbf{A}) \wedge ((\mathbf{S}|\mathbf{x})\mathbf{A})) \Rightarrow (\mathbf{T} = \mathbf{S})$ tétel $\mathfrak{T}$-ben. ■

2.9.7. Következmény. *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben. Tegyük fel, hogy* $\mathbf{A}$ *az* $\mathbf{x}$ *változóban egyértelmű* $\mathfrak{T}$*-ben. Ha* $\mathbf{T}$ *olyan objektum, hogy* $(\mathbf{T}|\mathbf{x})\mathbf{A}$ *tétel* $\mathfrak{T}$*-ben, akkor* $(\exists\mathbf{x})\mathbf{A}$ *tétel* $\mathfrak{T}$*-ben és* $\mathbf{T} = \varepsilon_{\mathbf{x}}(\mathbf{A})$ *tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. A $(\mathbf{T}|\mathbf{x})\mathbf{A} \Rightarrow (\exists\mathbf{x})\mathbf{A}$ formula eleme $\mathfrak{S}_5$-nek, tehát a leválasztás szabályát alkalmazva kapjuk, hogy $(\exists\mathbf{x})\mathbf{A}$, vagyis az $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ formula tétel $\mathfrak{T}$-ben. Tehát a konjunkció logikai alaptulajdonságából következik, hogy $((\mathbf{T}|\mathbf{x})\mathbf{A}) \wedge ((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A})$ tétel $\mathfrak{T}$-ben. Az előző tétel és a leválasztás szabálya alapján $\mathbf{T} = \varepsilon_{\mathbf{x}}(\mathbf{A})$ tétel $\mathfrak{T}$-ben, vagyis $\mathbf{T}$ egyenlő az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ objektummal $\mathfrak{T}$-ben. ■

Az előző állítás rávilágít az ε-szimbólumok egy újabb jelentésére. Korábban láttuk, hogy az egzisztenciális kvantor értelmezéséből adódik az, hogy ha $\mathbf{A}$ formula és $\mathbf{x}$ változó, akkor $\varepsilon_{\mathbf{x}}(\mathbf{A})$ *egy olyan* objektum, amelyet $\mathbf{x}$ helyére téve $\mathbf{A}$-ban pontosan akkor kapunk tételt, ha $(\exists\mathbf{x})\mathbf{A}$ tétel. Most azt is látjuk, hogy ha $(\exists\mathbf{x})\mathbf{A}$ tétel és $\mathbf{A}$ egyértelmű az $\mathbf{x}$ változóban, akkor $\varepsilon_{\mathbf{x}}(\mathbf{A})$ *az az egyetlen* objektum, amelyet $\mathbf{x}$ helyére téve $\mathbf{A}$-ban tételt kapunk. Ezt úgy kell érteni, hogy ekkor $\varepsilon_{\mathbf{x}}(\mathbf{A})$ egyenlő (az adott matematikai elméletben) minden olyan objektummal, amelyet $\mathbf{x}$ helyére téve $\mathbf{A}$-ban tételt kapunk. De vigyázzunk arra, hogy ha $\mathbf{T}$ olyan objektum, amelyre $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel, akkor szó sincs arról, hogy $\mathbf{T}$ és $\varepsilon_{\mathbf{x}}(\mathbf{A})$ *azonos* volna; az azonosság nem logikai kapcsolat, vagyis az független a matematikai elmélet igazság-fogalmától. Ekkor csak annyit állíthatunk, hogy a $\mathbf{T} = \varepsilon_{\mathbf{x}}(\mathbf{A})$ formula tétel az adott matematikai elméletben; ez *logikai kapcsolat* a $\mathbf{T}$ és $\varepsilon_{\mathbf{x}}(\mathbf{A})$ objektumok között.

Jelölés. Ha $\mathbf{A}$ formula és $\mathbf{x}$ változó a $\mathfrak{T}$ matematikai elméletben, akkor $(\exists_1\mathbf{x})\mathbf{A}$ jelöli a

$$((\exists\mathbf{x})\mathbf{A}) \ \wedge\ (\forall\mathbf{y})(\forall\mathbf{z})(((\mathbf{y}|\mathbf{x})\mathbf{A} \wedge (\mathbf{z}|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{y} = \mathbf{z}))$$

formulát, ahol $\mathbf{y}$ és $\mathbf{z}$ tetszőleges olyan különböző változók, amelyek $\mathbf{x}$-től különböznek és nem szerepelnek $\mathbf{A}$-ban.

A fentiek alapján állíthatjuk, hogy a $(\exists_1\mathbf{x})\mathbf{A}$ formula a "létezik egyetlen olyan $\mathbf{x}$, amelyre $\mathbf{A}$" kijelentés formalizáltja. Figyeljük meg, hogy a $(\exists_1\mathbf{x})\mathbf{A}$ kifejezés tisztán formális nyelvi konstrukcióval kapható, tehát az előállításához csak a $\mathfrak{T}$ matematikai elmélet formális matematikai nyelvére van szükség, azonban e formula csak matematikai elméletekben kapja meg azt a jelentést, amelyet elvárunk tőle. Most megmutatjuk, hogy ha a $(\exists_1\mathbf{x})\mathbf{A}$ formula tétel egy matematikai elméletben, akkor az $\mathbf{A}$ formula ekvivalens egy egészen speciális alakú egyenlőséggel.

2.9.8. Állítás. *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a* $\mathfrak{T}$ *matematikai elméletben. Ha a* $(\exists_1\mathbf{x})\mathbf{A}$ *formula tétel* $\mathfrak{T}$*-ben, akkor az* $\mathbf{A}\Leftrightarrow(\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A}))$ *formula tétel* $\mathfrak{T}$*-ben.*

Bizonyítás. Jelölje $\mathfrak{T}'$ a $\mathfrak{T}[\mathbf{A}]$ matematikai elméletet. A $(\exists\mathbf{x})\mathbf{A}$, vagyis $(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ formula tétel $\mathfrak{T}$-ben, tehát $\mathfrak{T}'$-ben is tétel. Ugyanakkor $\mathbf{A}$ tétel $\mathfrak{T}'$-ben (sőt explicit axióma), így az $\mathbf{A} \wedge (\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ formula tétel $\mathfrak{T}'$-ben. De $\mathbf{A} \equiv (\mathbf{x}|\mathbf{x})\mathbf{A}$, és $\mathbf{A}$ az $\mathbf{x}$ változóban egyértelmű $\mathfrak{T}$-ben, tehát $\mathfrak{T}'$-ben is; így az előzőek alapján $((\mathbf{x}|\mathbf{x})\mathbf{A} \wedge (\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A}))$ tétel $\mathfrak{T}'$-ben. Ebből a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A})$ tétel $\mathfrak{T}'$-ben, tehát a dedukció-tétel alapján $\mathbf{A} \Rightarrow (\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A}))$ tétel $\mathfrak{T}$-ben.

Jelölje most $\mathfrak{T}''$ a $\mathfrak{T}[\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A})]$ matematikai elméletet. Világos, hogy az $(\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A})) \Rightarrow (\mathbf{A}\Leftrightarrow(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A})$ formula eleme $\mathfrak{S}_6$-nak, ezért a leválasztás szabályát alkalmazva kapjuk, hogy az $\mathbf{A}\Leftrightarrow(\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}$ formula, vagyis $\mathbf{A}\Leftrightarrow(\exists\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}''$-ben. Ugyanakkor $(\exists\mathbf{x})\mathbf{A}$ tétel $\mathfrak{T}$-ben, így $\mathfrak{T}''$-ben is, ezért $\mathbf{A}$ tétel $\mathfrak{T}''$-ben. A dedukció-tétel alkalmazásával ebből kapjuk, hogy $(\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A})) \Rightarrow \mathbf{A}$ tétel $\mathfrak{T}$-ben.

Tehát a konjunkció logikai alaptulajdonsága szerint az $\mathbf{A}\Leftrightarrow(\mathbf{x} = \varepsilon_{\mathbf{x}}(\mathbf{A}))$ formula tétel $\mathfrak{T}$-ben. ■

2.10. Formális aritmetika és formális síkgeometria

Befejezésként értelmezünk két, önmagában is érdekes, lényegesen nem triviális, konkrét matematikai elméletet; a (formális) *aritmetikát* és a (formális sík-) *geometriát.* Itt ezek csak illusztrációként szolgálnak, de fontos tudni azt, hogy az aritmetikának komoly alkalmazásai vannak a matematikai elméletek ellentmondásmentességének vizsgálatában, továbbá az általunk értelmezett geometria bizonyos változatai (rendszerint bővítései) a matematika egy nevezetes ágának (*a logikai geometriának*) alapját képezik. Az egész matematika alapjául szolgáló *halmazelméletet* a **4.** fejezetben fogjuk értelmezni.

2.10.1. Definíció. Formális aritmetikának, *vagy röviden* **aritmetikának** ($\mathfrak{Ari}$) *nevezzük azt a matematikai elméletet, amelynek*

– *matematikai nyelvében nincs logikai sajátfüggvény, és négy matematikai függvénye van: a nulla súlyú* $\mathbf{0}$ (**nulla**) *függvény, az egyváltozós* $\#$ (**szukcesszor**) *függvény, a kétváltozós* $+$ (**összeadás**) *függvény, valamint a szintén kétváltozós* $\cdot$ (**szorzás**) *függvény (megállapodunk abban, hogy minden* $\mathbf{T}$ *kifejezésre a* $\#\mathbf{T}$ *kifejezést a* $\mathbf{T}^{\#}$ *szimbólummal jelöljük, továbbá a* $+$ *és* $\cdot$ *kétváltozós matematikai függvényekre az infix jelölést alkalmazzuk, vagyis minden* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumra* $+\mathbf{TS}$ *és* $\cdot\mathbf{TS}$ *helyett azt írjuk, hogy* $\mathbf{T}+\mathbf{S}$ *és* $\mathbf{T}\cdot\mathbf{S}$*);*

– *az egyetlen matematikai axióma-sémája a*

$$(\mathbf{0}|\mathbf{x})\mathbf{A} \;\Rightarrow\; (\;(\forall\mathbf{x})(\mathbf{A}\Rightarrow(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A}) \;\Rightarrow\; (\forall\mathbf{x})\mathbf{A}\;)$$

alakú formulák összessége, ahol $\mathbf{x}$ *változó és* $\mathbf{A}$ *formula az aritmetika matematikai nyelvében (ezt nevezzük a* **teljes indukció** *axióma-sémának, és az* $\mathfrak{S}_{\mathrm{ind}}$ *szimbólummal jelöljük);*

– *explicit axiómái a következő formulák:*

$$(\forall x)(\forall y)(x^{\#}=y^{\#}\Leftrightarrow x=y),$$
$$(\forall x)(x^{\#}\neq\mathbf{0}),$$
$$(\forall x)(x+\mathbf{0}=x),$$
$$(\forall x)(\forall y)(x+y^{\#}=(x+y)^{\#}),$$
$$(\forall x)(x\cdot\mathbf{0}=\mathbf{0}),$$
$$(\forall x)(\forall y)(x\cdot y^{\#}=x\cdot y+x).$$

Láthatóan az aritmetika egyetlen explicit axiómájában sem szerepel változó, vagyis az aritmetika formális nyelvének nincs olyan változója, amely konstans volna.

Megmutatjuk, hogy $\mathfrak{S}_{\mathrm{ind}}$ valóban formula-séma. Legyenek $\mathbf{x}$, $\mathbf{y}$ változók, $\mathbf{A}$ formula és $\mathbf{T}$ objektum az aritmetika matematikai nyelvében. Jelölje $\mathbf{B}$ a

$$(\mathbf{0}|\mathbf{x})\mathbf{A} \;\Rightarrow\; (\;(\forall\mathbf{x})(\mathbf{A}\Rightarrow(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A}) \;\Rightarrow\; (\forall\mathbf{x})\mathbf{A}\;)$$

formulát; azt kell igazolni, hogy $(\mathbf{T}|\mathbf{y})\mathbf{B}$ is eleme $\mathfrak{S}_{\mathrm{ind}}$-nek. Legyen $\mathbf{z}$ olyan változó, amely $\mathbf{x}$-től és $\mathbf{y}$-tól különbözik, továbbá nem szerepel az $\mathbf{A}$ és $\mathbf{T}$ kifejezésekben. Ekkor

$$(\mathbf{T}|\mathbf{y})\mathbf{B}\equiv(\mathbf{T}|\mathbf{y})(\mathbf{0}|\mathbf{x})\mathbf{A}\Rightarrow((\mathbf{T}|\mathbf{y})(\forall\mathbf{x})(\mathbf{A}\Rightarrow(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A})\Rightarrow(\mathbf{T}|\mathbf{y})(\forall\mathbf{x})\mathbf{A})\equiv$$
$$\equiv(\mathbf{T}|\mathbf{y})(\mathbf{0}|\mathbf{x})\mathbf{A}\Rightarrow((\mathbf{T}|\mathbf{y})(\forall\mathbf{z})((\mathbf{z}|\mathbf{x})\mathbf{A}\Rightarrow(\mathbf{z}|\mathbf{x})(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A})\Rightarrow(\mathbf{T}|\mathbf{y})(\forall\mathbf{z})((\mathbf{z}|\mathbf{x})\mathbf{A}))\equiv$$
$$\equiv(\mathbf{T}|\mathbf{y})(\mathbf{0}|\mathbf{x})\mathbf{A}\Rightarrow((\forall\mathbf{z})((\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})\mathbf{A}\Rightarrow(\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A})\Rightarrow(\forall\mathbf{z})((\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})\mathbf{A})).$$

Jelölje $\mathbf{A}'$ a $(\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})\mathbf{A}$ formulát; ekkor

$$(\mathbf{T}|\mathbf{y})\mathbf{B}\equiv(\mathbf{T}|\mathbf{y})(\mathbf{0}|\mathbf{x})\mathbf{A}\Rightarrow((\forall\mathbf{z})(\mathbf{A}'\Rightarrow(\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A})\Rightarrow(\forall\mathbf{z})\mathbf{A}').$$

A $\mathbf{z}$ változó nem szerepel $\mathbf{A}$-ban, ezért $(\mathbf{z}|\mathbf{x})(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A}\equiv(\mathbf{z}^{\#}|\mathbf{z})(\mathbf{z}|\mathbf{x})\mathbf{A}$, így

$$(\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})(\mathbf{x}^{\#}|\mathbf{x})\mathbf{A}\equiv(\mathbf{T}|\mathbf{y})(\mathbf{z}^{\#}|\mathbf{z})(\mathbf{z}|\mathbf{x})\mathbf{A}\equiv(\mathbf{z}^{\#}|\mathbf{z})\mathbf{A}'.$$

Továbbá, $\mathbf{z}$ nem szerepel $\mathbf{T}$-ben és $\mathbf{A}$-ban, így $(\mathbf{0}|\mathbf{z})\mathbf{T}\equiv\mathbf{T}$ és $(\mathbf{0}|\mathbf{z})(\mathbf{z}|\mathbf{x})\mathbf{A}\equiv(\mathbf{0}|\mathbf{x})\mathbf{A}$, tehát

$$(\mathbf{0}|\mathbf{z})\mathbf{A}'\equiv(\mathbf{0}|\mathbf{z})(\mathbf{T}|\mathbf{y})(\mathbf{z}|\mathbf{x})\mathbf{A}\equiv((\mathbf{0}|\mathbf{z})\mathbf{T}|\mathbf{y})(\mathbf{0}|\mathbf{z})(\mathbf{z}|\mathbf{x})\mathbf{A}\equiv$$
$$\equiv(\mathbf{T}|\mathbf{y})(\mathbf{0}|\mathbf{z})(\mathbf{z}|\mathbf{x})\mathbf{A}\equiv(\mathbf{T}|\mathbf{y})(\mathbf{0}|\mathbf{x})\mathbf{A}.$$

Ez azt jelenti, hogy

$$(\mathbf{T}|\mathbf{y})\mathbf{B} \equiv (\mathbf{0}|\mathbf{z})\mathbf{A}' \Rightarrow (\ (\forall\mathbf{z})(\mathbf{A}' \Rightarrow (\mathbf{z}^{\#}|\mathbf{z})\mathbf{A}') \ \Rightarrow \ (\forall\mathbf{z})\mathbf{A}'\ ),$$

vagyis $(\mathbf{T}|\mathbf{y})\mathbf{B}$ eleme $\mathfrak{S}_{\mathrm{ind}}$-nek.

Az aritmetika explicit axiómáiból könnyen levezethető, hogy bármely két $\mathbf{T}$ és $\mathbf{S}$ objektumra a következő formulák tételek:

$$(\mathbf{T}^{\#} = \mathbf{S}^{\#}) \Leftrightarrow (\mathbf{T} = \mathbf{S}),$$
$$\mathbf{T}^{\#} \neq \mathbf{0},$$
$$\mathbf{T} + \mathbf{0} = \mathbf{T},$$
$$\mathbf{T} + \mathbf{S}^{\#} = (\mathbf{T} + \mathbf{S})^{\#},$$
$$\mathbf{T} \cdot \mathbf{0} = \mathbf{0},$$
$$\mathbf{T} \cdot \mathbf{S}^{\#} = \mathbf{T} \cdot \mathbf{S} + \mathbf{T}.$$

Ha $\mathbf{T}$ és $\mathbf{S}$ objektumok az aritmetika nyelvében, akkor $\mathbf{T} < \mathbf{S}$ a következő formula rövidítése:

$$(\exists\mathbf{x})((\mathbf{x} \neq \mathbf{0}) \wedge (\mathbf{T} + \mathbf{x} = \mathbf{S})),$$

ahol $\mathbf{x}$ tetszőleges olyan változó, amely $\mathbf{T}$-ben és $\mathbf{S}$-ben nem szerepel. A kvantoros kifejezésekre vonatkozó helyettesítések tranzitivitásának szabálya alapján nyilvánvaló, hogy ha $\mathbf{x}'$ szintén olyan változó, amely $\mathbf{T}$-ben és $\mathbf{S}$-ben nem szerepel, akkor

$$(\exists\mathbf{x})((\mathbf{x} \neq \mathbf{0}) \wedge (\mathbf{T} + \mathbf{x} = \mathbf{S})) \equiv (\exists\mathbf{x}')((\mathbf{x}' \neq \mathbf{0}) \wedge (\mathbf{T} + \mathbf{x}' = \mathbf{S})),$$

tehát a $\mathbf{T} < \mathbf{S}$ formula jól értelmezett.

Az aritmetika zárt, vagyis változót nem tartalmazó objektumait *természetes számoknak* nevezzük, és ha $\mathbf{T}$ természetes szám, akkor a $\mathbf{T}^{\#}$ természetes számot a $\mathbf{T}$ *rákövetkezőjének* nevezzük. A $\mathbf{0}$ objektum egy (explicit axiómák által) kitüntetett tulajdonságokkal rendelkező természetes szám. Az utolsó négy explicit axióma a $+$ *összeadásfüggvény* és a $\cdot$ *szorzásfüggvény* alapvető tulajdonságait írja elő. Az aritmetika nem zárt, vagyis változót tartalmazó objektumait *aritmetikai függvényeknek* nevezzük.

Az aritmetikában bevezetünk néhány zárt, vagyis változót nem tartalmazó objektumot. Definíció szerint: $\mathbf{1} \equiv \mathbf{0}^{\#}$, $\mathbf{2} \equiv \mathbf{1}^{\#}$, $\mathbf{3} \equiv \mathbf{2}^{\#}$, $\mathbf{4} \equiv \mathbf{3}^{\#}$, $\mathbf{5} \equiv \mathbf{4}^{\#}$, s.í.t. Látható, hogy ez az értelmezési eljárás minden határon túl folytatható, csak az a lényeg, hogy minden újabb lépésben olyan szimbólumot vezessünk be, amely az addig bevezetett jelek mindegyikétől különbözik, valamint az aritmetika nyelvének egyetlen szimbólumával sem azonos. Az így bevezethető jeleket elnevezhetjük *konkrét természetes számoknak*, és természetesen gondolhatunk ezek összességére, továbbá ezt az összességet jelölhetjük például az $\mathbb{N}_{\mathfrak{Ari}}$ szimbólummal. Azonban ez az $\mathbb{N}_{\mathfrak{Ari}}$ összesség *nem objektuma* az aritmetikának, vagyis az $\mathfrak{Ari}$ elmélet egyetlen formulájában sem szerepelhet. Ugyanakkor $\mathbb{N}_{\mathfrak{Ari}}$ *nem objektuma* a **4.** fejezetben alaposabb vizsgálat alá kerülő *halmazelméletnek* sem, tehát $\mathbb{N}_{\mathfrak{Ari}}$ *nem halmaz*, így az $\mathfrak{Ens}$ elmélet (vagyis a halmazelmélet) egyetlen formulájában sem szerepelhet. Másként fogalmazva: az $\mathbb{N}_{\mathfrak{Ari}}$ szimbólum sem formális aritmetikai, sem formális halmazelméleti módszerekkel nem kezelhető. Azonban nem formális (vagyis matematikai elméletben nem formalizálható) kijelentéseket mondhatunk rá, de az így nyert állításoknak még az értelmessége is erősen kétséges lehet. Ezt a tényt mindig figyelembe kell venni akkor, amikor az $\mathbb{N}_{\mathfrak{Ari}}$ "objektumra" kijelentéseket mondunk, vagy vele kapcsolatos konstrukciókat hajtunk végre; például amikor olyan (nem halmazelméleti) függvényt vezetünk be, amely az $\mathbb{N}_{\mathfrak{Ari}}$ "összességen" értelmezett vagy az $\mathbb{N}_{\mathfrak{Ari}}$ "összességbe" érkezik.

2.10.2. Definíció. Elemi geometriának ($\mathfrak{Geo}$) *nevezzük azt a matematikai elméletet, amelynek*

– *matematikai nyelvében nincs matematikai függvény, de van két háromváltozós logikai sajátfüggvény: a* $\mathfrak{Gr}$ **illeszkedés-függvény** *és a* $\mathfrak{Zw}$ **közbensőpont-függvény**, *amelyekre a szokásos funkcionális jelölést alkalmazzuk;*

– *nincs matematikai axiómasémája;*

– *explicit axiómái a következő formulák:*

$$
\begin{gathered}
(\forall x)(\forall y)\mathfrak{Gr}(x,x,y),\\
(\forall x)(\forall y)(\forall z)(\ \mathfrak{Gr}(x,y,z)\ \Rightarrow\ (\mathfrak{Gr}(y,x,z)\wedge\mathfrak{Gr}(x,z,y))\ ),\\
(\forall x)(\forall y)(\forall z)(\forall z')(\ (\mathfrak{Gr}(x,y,z)\wedge\mathfrak{Gr}(x,y,z'))\wedge(x\neq y)\ \Rightarrow\ \mathfrak{Gr}(x,z,z')\ ),\\
(\exists x)(\exists y)(\exists z)(\neg\mathfrak{Gr}(x,y,z)),\\
(\forall x)(\forall y)(\forall z)(\ \mathfrak{Zw}(x,y,z)\ \Rightarrow\ \mathfrak{Gr}(x,y,z)\ ),\\
(\forall x)(\forall y)(\neg\mathfrak{Zw}(x,y,y)),\\
(\forall x)(\forall y)(\forall z)(\ \mathfrak{Zw}(x,y,z)\ \Rightarrow\ (\ \mathfrak{Zw}(x,z,y)\wedge(\neg\mathfrak{Zw}(y,x,z))\ )\ ),\\
(\forall x)(\forall y)(\ (x\neq y)\ \Rightarrow\ (\exists z)\mathfrak{Zw}(x,y,z)\ ),\\
(\forall x)(\forall y)(\forall z)(\forall u)(\forall v)(\ (\neg\mathfrak{Gr}(x,y,z)\wedge\mathfrak{Zw}(u,x,y)\wedge\neg\mathfrak{Gr}(v,x,y)\wedge\neg\mathfrak{Gr}(z,u,v))\ \Rightarrow\\
\Rightarrow\ (\exists w)(\ \mathfrak{Gr}(u,v,w)\wedge(\mathfrak{Zw}(w,x,z)\vee\mathfrak{Zw}(w,y,z))\ )\ ),\\
(\forall x)(\forall y)(\forall z)(\neg\mathfrak{Gr}(x,y,z)\Rightarrow(\exists u)(\mathfrak{Par}(x,y;z,u)\wedge(\forall v)(\mathfrak{Par}(x,y;z,v)\Rightarrow\mathfrak{Gr}(z,u,v))))
\end{gathered}
$$

ahol bármely négy **x**, **y**, **u**, **v** *változóra definíció szerint:*

$$\mathfrak{Par}(\mathbf{x},\mathbf{y};\mathbf{u},\mathbf{v})\equiv\neg(\exists\mathbf{w})(\ \mathfrak{Gr}(\mathbf{x},\mathbf{y},\mathbf{w})\wedge\mathfrak{Gr}(\mathbf{u},\mathbf{v},\mathbf{w})\ ),$$

ahol **w** *tetszőleges olyan változó, amely az* **x**, **y**, **u**, **v** *változók mindegyikétől különbözik.*

A $\mathfrak{Geo}$ elmélet zárt, tehát változót nem tartalmazó objektumait *pontoknak* nevezzük, és ha **T**, **S**, **R** pontok, akkor a $\mathfrak{Gr}(\mathbf{T},\mathbf{S},\mathbf{R})$ formulát úgy mondjuk ki, hogy "*a* **T**, **S** *és* **R** *pontok egy egyenesen vannak*", továbbá a $\mathfrak{Zw}(\mathbf{T},\mathbf{S},\mathbf{R})$ formulát úgy mondjuk ki, hogy "*a* **T** *pont az* **S** *és* **R** *pontok közé esik*". Ha **X**, **Y**, **U**, **V** pontok, a $\mathfrak{Par}(\mathbf{X},\mathbf{Y};\mathbf{U},\mathbf{V})$ formulát úgy mondjuk ki, hogy "*az* **X** *és* **Y** *pontok által meghatározott egyenes párhuzamos az* **U** *és* **V** *pontok által meghatározott egyenessel*". Ezeket a kifejezéseket használva könnyen látható, hogy a $\mathfrak{Geo}$ elmélet explicit axiómái az elemi síkgeometriából jól ismert euklidészi axiómák. Például a negyedik axiómának az a tartalma, hogy *létezik három nem egy egyenesre eső pont*, tehát a pontok legalább kétdimenziós sokaságot alkotnak. A tizedik axióma Euklidész párhuzamossági axiómája: *minden egyeneshez, és azon kívüli ponthoz létezik egyetlen olyan egyenes, amely párhuzamos az adott egyenessel, és áthalad az adott ponton.*

3. fejezet

A predikátumkalkulus ellentmondásmentessége

3.1. Elemi formulák és formula-konstrukciók

3.1.1. Definíció. Predikátumkalkulusnak *nevezünk minden olyan matematikai elméletet, amelynek nincs matematikai axióma-sémája és nincs explicit axiómája.*

Tehát nem egyetlen predikátumkalkulus létezik, hiszen a matematikai és logikai függvényeikben különbözhetnek egymástól, így a matematikai nyelvük nem szükségképpen azonos. Azonban minden predikátumkalkulusnak csak az $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{S}_6$ és $\mathfrak{S}_7$ formula-sémák az axióma-sémái, tehát bármely két predikátumkalkulus csak a matematikai nyelvében különbözhet egymástól.

Példa. Ha $\mathfrak{T}$ matematikai elmélet, akkor korábban $\mathfrak{T}_0$ jelölte azt a matematikai elméletet, amelynek matematikai nyelve megegyezik a $\mathfrak{T}$ matematikai nyelvével, és $\mathfrak{T}_0$-nak nincs matematikai axióma-sémája és nincs explicit axiómája. Világos, hogy $\mathfrak{T}_0$ predikátumkalkulus; ezt a $\mathfrak{T}$ *alatt fekvő predikátumkalkulusnak* nevezzük.

Minden matematikai elmélet bővítése az alatta fekvő predikátumkalkulusnak, tehát ha $\mathfrak{T}$ matematikai elmélet, és egy formula tétel $\mathfrak{T}_0$-ban, akkor tétel $\mathfrak{T}$-ben is. Azonban egy $\mathfrak{T}$ matematikai elméletnek létezhet olyan formulája, amely tétel $\mathfrak{T}$-ben, de nem tétel $\mathfrak{T}_0$-ban. Például lehetséges az, hogy a $\mathfrak{T}$ matematikai elmélet ellentmondásos, ezért a $\mathfrak{T}$ minden formulája tétel $\mathfrak{T}$-ben, ugyanakkor látni fogjuk, hogy a $\mathfrak{T}_0$ predikátumkalkulus *mindig ellentmondásmentes.*

A predikátumkalkulusok ellentmondásmentességének bizonyításához szükségünk lesz néhány olyan konstrukcióra és fogalomra, amelyek a matematikai nyelvekkel kapcsolatosak. Ezeket már a **2.1.** pontban is tárgyalhattuk volna, de akkor az a téves képzet alakulhatott volna ki, hogy ezekre a formális nyelvi konstrukciókra és fogalmakra szükség van az axiomatikus matematikai elméletek felépítéséhez, holott láthatóan nem ez a helyzet.

3.1.2. Lemma. *Tegyük fel, hogy* $\mathbf{x}$ *változó és* $\mathbf{A}$, $\mathbf{B}$ *kifejezések egy matematikai nyelvben. Ha* $\varepsilon_{\mathbf{x}}(\mathbf{A}) \equiv \varepsilon_{\mathbf{x}}(\mathbf{B})$, *akkor* $\mathbf{A} \equiv \mathbf{B}$.

Bizonyítás. Az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ kifejezés első ε szimbólumából pontosan annyi összekötő vonal indul ki, és pontosan arra a karakterpozícióra mutat $\varepsilon_{\mathbf{x}}(\mathbf{A})$-ban, mint az $\varepsilon_{\mathbf{x}}(\mathbf{B})$ kifejezésben. Tehát ha az első ε szimbólumból kiinduló összekötő vonalak által mutatott $\square$ jelek helyére mindkét kifejezésben $\mathbf{x}$-et helyettesítünk, és letöröljük az első ε szimbólumot, valamint a belőle kiinduló összekötő vonalakat, akkor ugyanazokra a kifejezésekre jutunk. Nyilvánvaló, hogy ezek a kifejezések éppen $\mathbf{A}$ és $\mathbf{B}$, így $\mathbf{A} \equiv \mathbf{B}$. ■

Az előző lemma bizonyításából látszik, hogy az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ alakú (az ún. *ε-kifejezések*) szintaktikus előállításakor miért kötöttük össze az $\mathbf{A}$ elé írt ε szimbólumot azokkal a $\square$ jelekkel, amelyeket az $\mathbf{x}$ helyére bevezettünk. Ha ezt nem tettük volna, akkor most az $\varepsilon_{\mathbf{x}}(\mathbf{A}) \equiv \varepsilon_{\mathbf{x}}(\mathbf{B})$ összefüggésből nem következtethetnénk arra, hogy $\mathbf{A} \equiv \mathbf{B}$.

3.1.3. Lemma. *Ha* $\mathbf{A}$ *formula vagy objektum, és* $\mathbf{B}$ *kifejezés egy matematikai nyelvben, akkor az* $\mathbf{AB}$ *kifejezés nem formula és nem objektum.*

Bizonyítás. Az $\mathbf{A}$ kifejezés hossza szerinti teljes indukcióval igazoljuk, hogy minden $\mathbf{B}$ kifejezésre, ha $\mathbf{A}$ formula vagy objektum, akkor $\mathbf{AB}$ nem formula és nem objektum.

Ha $\mathbf{A}$ hossza 1, akkor $\mathbf{A}$ változó vagy konstans; ekkor bármely $\mathbf{B}$ kifejezésre $\mathbf{AB}$ nyilvánvalóan nem elsőfajú, így $\mathbf{AB}$ nem lehet objektum; ugyanakkor az első karaktere nem logikai függvény és nem a $\neg$ vagy $\vee$ logikai operátor, következésképpen $\mathbf{AB}$ formula sem lehet.

Tegyük fel, hogy $\mathbf{A}$ formula vagy objektum, továbbá az $\mathbf{A}$ hossza 1-nél nagyobb, és minden $\mathbf{A}$-nál rövidebb $\mathbf{A}'$ kifejezésre igaz az, hogy ha $\mathbf{A}'$ formula vagy objektum, akkor minden $\mathbf{B}$ kifejezésre $\mathbf{A}'\mathbf{B}$ nem formula és nem objektum. Az objektum-formula-konstrukciók értelmezése alapján $\mathbf{A}$-ra a következő esetek közül pontosan az egyik teljesül.

1) Létezik olyan $\mathbf{A}'$ formula, hogy $\mathbf{A} \equiv \neg\mathbf{A}'$. Tegyük fel, hogy $\mathbf{B}$ olyan kifejezés, amelyre $\mathbf{AB}$ formula vagy objektum. Ekkor $\mathbf{AB}$ szükségképpen formula, mert ez másodfajú kifejezés, így létezik olyan $\mathbf{B}'$ formula, amelyre $\neg\mathbf{A}'\mathbf{B} \equiv \mathbf{AB} \equiv \neg\mathbf{B}'$. Ekkor $\mathbf{A}'\mathbf{B} \equiv \mathbf{B}'$, vagyis $\mathbf{A}'\mathbf{B}$ formula, ami az indukciós hipotézis miatt lehetetlen, mert $\mathbf{A}'$ hossza kisebb, mint az $\mathbf{A}$ hossza. Ezért minden $\mathbf{B}$ kifejezésre $\mathbf{AB}$ nem formula és nem objektum.

2) Léteznek olyan $\mathbf{A}'$ és $\mathbf{A}''$ formulák, hogy $\mathbf{A} \equiv \vee\mathbf{A}'\mathbf{A}''$. Tegyük fel, hogy $\mathbf{B}$ olyan kifejezés, amelyre $\mathbf{AB}$ formula vagy objektum. Ekkor $\mathbf{AB}$ szükségképpen formula, mert ez másodfajú kifejezés, így léteznek olyan $\mathbf{B}'$ és $\mathbf{B}''$ formulák, amelyekre $\vee\mathbf{A}'\mathbf{A}''\mathbf{B} \equiv \mathbf{AB} \equiv \vee\mathbf{B}'\mathbf{B}''$. Ekkor $\mathbf{A}'\mathbf{A}''\mathbf{B} \equiv \mathbf{B}'\mathbf{B}''$ és itt az $\mathbf{A}'$, $\mathbf{A}''$, $\mathbf{B}'$ és $\mathbf{B}''$ formulák mindegyikének a hossza kisebb az $\mathbf{A}$ hosszánál. Ha $\mathbf{A}'$ hossza kisebb a $\mathbf{B}'$ hosszánál, akkor van olyan $\mathbf{C}$ kifejezés, hogy $\mathbf{A}'\mathbf{C} \equiv \mathbf{B}'$, vagyis $\mathbf{A}'\mathbf{C}$ formula, ami az indukciós hipotézis miatt lehetetlen. Ha $\mathbf{A}'$ hossza nagyobb a $\mathbf{B}'$ hosszánál, akkor van olyan $\mathbf{C}$ kifejezés, hogy $\mathbf{A}' \equiv \mathbf{B}'\mathbf{C}$, vagyis $\mathbf{B}'\mathbf{C}$ formula, ami az indukciós hipotézis miatt lehetetlen. Ezért $\mathbf{A}'$ és $\mathbf{B}'$ hossza megegyezik, így $\mathbf{A}''\mathbf{B} \equiv \mathbf{B}''$, vagyis $\mathbf{A}''\mathbf{B}$ formula, ami az indukciós hipotézis szerint lehetetlen. Tehát minden $\mathbf{B}$ kifejezésre $\mathbf{AB}$ nem formula és nem objektum.

3) Létezik olyan $\mathbf{x}$ változó és $\mathbf{A}'$ formula, hogy $\mathbf{A} \equiv \varepsilon_{\mathbf{x}}(\mathbf{A}')$. Tegyük fel, hogy $\mathbf{B}$ olyan kifejezés, amelyre $\mathbf{AB}$ formula vagy objektum. Ekkor az $\mathbf{AB}$ kifejezés az ε szimbólummal kezdődik, tehát elsőfajú, így ez a kifejezés objektum. Tehát létezik olyan $\mathbf{y}$ változó és $\mathbf{A}''$ formula, hogy $\varepsilon_{\mathbf{x}}(\mathbf{A}')\mathbf{B} \equiv \varepsilon_{\mathbf{y}}(\mathbf{A}'')$. Legyen $\mathbf{z}$ olyan változó, amely nem szerepel az $\mathbf{A}'$, $\mathbf{A}''$ és $\mathbf{B}$ formulák egyikében sem. Az ε-kifejezésekre vonatkozó helyettesítések tranzitivitásának szabálya szerint

$$\varepsilon_{\mathbf{z}}((\mathbf{z}|\mathbf{y})\mathbf{A}'') \equiv \varepsilon_{\mathbf{y}}(\mathbf{A}'') \equiv \varepsilon_{\mathbf{x}}(\mathbf{A}')\mathbf{B} \equiv \varepsilon_{\mathbf{z}}((\mathbf{z}|\mathbf{x})\mathbf{A}')\mathbf{B} \equiv \varepsilon_{\mathbf{z}}(((\mathbf{z}|\mathbf{x})\mathbf{A}')\mathbf{B}).$$

Az előző lemma szerint ebből $(\mathbf{z}|\mathbf{y})\mathbf{A}'' \equiv ((\mathbf{z}|\mathbf{x})\mathbf{A}')\mathbf{B}$ következik. Ez azt jelenti, hogy $((\mathbf{z}|\mathbf{x})\mathbf{A}')\mathbf{B}$ formula, ami az indukciós hipotézis miatt lehetetlen, mert $(\mathbf{z}|\mathbf{x})\mathbf{A}'$ olyan formula, amelynek a hossza egyenlő az $\mathbf{A}'$ hosszával, és $\mathbf{A}'$ rövidebb $\mathbf{A}$-nál. Tehát minden $\mathbf{B}$ kifejezésre $\mathbf{AB}$ nem formula és nem objektum.

4) Létezik olyan m-változós $\mathfrak{f}$ logikai (illetve matematikai) függvény, és léteznek olyan $\mathbf{T}_1, \dots \mathbf{T}_m$ objektumok, hogy $\mathbf{A} \equiv \mathfrak{f}\mathbf{T}_1 \dots \mathbf{T}_m$. Tegyük fel, hogy $\mathbf{B}$ olyan kifejezés, amelyre $\mathbf{AB}$ formula vagy objektum. Ha $\mathfrak{f}$ logikai (illetve matematikai) függvény, akkor $\mathbf{AB}$ másodfajú (illetve elsőfajú) kifejezés, tehát $\mathbf{AB}$ formula (illetve objektum). Ezért létezik olyan $\mathfrak{f}'$ n-változós logikai (illetve matematikai) függvény, és léteznek olyan $\mathbf{S}_1, \dots, \mathbf{S}_n$ objektumok, hogy $\mathfrak{f}\mathbf{T}_1 \dots \mathbf{T}_m\mathbf{B} \equiv \mathfrak{f}'\mathbf{S}_1 \dots \mathbf{S}_n$. Ekkor $\mathfrak{f} \equiv \mathfrak{f}'$, tehát $m \equiv n$, és $\mathbf{T}_1 \dots \mathbf{T}_m\mathbf{B} \equiv \mathbf{S}_1 \dots \mathbf{S}_m$ teljesül. Az indukciós hipotézis $(m-1)$-szer való egymás utáni alkalmazásával ebből kapjuk, hogy minden $1 \leq k < m$ számra $\mathbf{T}_k \equiv \mathbf{S}_k$, így $\mathbf{T}_m\mathbf{B} \equiv \mathbf{S}_m$, vagyis $\mathbf{T}_m\mathbf{B}$ objektum, ami az indukciós hipotézis alapján lehetetlen. Ebből következik, hogy minden $\mathbf{B}$ kifejezésre $\mathbf{AB}$ nem formula és nem objektum. ■

3.1.4. Állítás. (**A formula-antecedensek egyértelműsége**.) *Legyen* $\mathbf{A}$ *formula egy matematikai nyelvben. Ha* $\mathbf{A}$ *első karaktere a* $\neg$ *logikai operátor, akkor egyértelműen létezik olyan* $\mathbf{B}$ *formula, hogy* $\mathbf{A} \equiv \neg\mathbf{B}$. *Ha* $\mathbf{A}$ *első karaktere a* $\vee$ *logikai operátor, akkor egyértelműen léteznek olyan* $\mathbf{B}$ *és* $\mathbf{C}$ *formulák, amelyre* $\mathbf{A} \equiv \vee\mathbf{BC}$. *Ha* $\mathbf{A}$ *első karaktere az* n*-változós* $\mathfrak{f}$ *logikai függvény, akkor egyértelműen létezik olyan* $(\mathbf{T}_1, \dots, \mathbf{T}_n)$ *objektum* n*-es, hogy* $\mathbf{A} \equiv \mathfrak{f}\mathbf{T}_1 \dots \mathbf{T}_n$.

Bizonyítás. Ha $\mathbf{A}$ első karaktere a $\neg$ logikai operátor, és $\mathbf{B}$, $\mathbf{B}'$ olyan formulák, hogy $\mathbf{A} \equiv \neg\mathbf{B} \equiv \neg\mathbf{B}'$, akkor triviálisan teljesül a $\mathbf{B} \equiv \mathbf{B}'$ azonosság.

Legyen $\mathbf{A}$ első karaktere a $\vee$ logikai operátor, és legyenek $\mathbf{A}'$, $\mathbf{A}''$, $\mathbf{B}'$ és $\mathbf{B}''$ olyan formulák, hogy $\mathbf{A} \equiv \vee\mathbf{A}'\mathbf{A}'' \equiv \vee\mathbf{B}'\mathbf{B}''$. Ekkor nyilvánvalóan $\mathbf{A}'\mathbf{A}'' \equiv \mathbf{B}'\mathbf{B}''$ teljesül. Ha az $\mathbf{A}'$ formula hossza kisebb volna a $\mathbf{B}'$ hosszánál, akkor létezne olyan $\mathbf{C}$ kifejezés, hogy $\mathbf{A}'\mathbf{C} \equiv \mathbf{B}'$, tehát $\mathbf{A}'\mathbf{C}$ formula volna, ami az előző lemma szerint lehetetlen. Ha az $\mathbf{A}'$ formula hossza nagyobb volna a $\mathbf{B}'$ hosszánál, akkor létezne olyan $\mathbf{C}$ kifejezés, hogy $\mathbf{A}' \equiv \mathbf{B}'\mathbf{C}$, tehát $\mathbf{B}'\mathbf{C}$ formula volna, ami az előző lemma szerint lehetetlen. Ezért az $\mathbf{A}'$ és $\mathbf{B}'$ formulák hossza azonos, így $\mathbf{A}' \equiv \mathbf{B}'$. Ebből és az $\mathbf{A}'\mathbf{A}'' \equiv \mathbf{B}'\mathbf{B}''$ összefüggésből azonnal következik, hogy $\mathbf{A}'' \equiv \mathbf{B}''$.

Legyen az $\mathbf{A}$ első karaktere logikai függvény. Tegyük fel, hogy $\mathfrak{f}$ (illetve $\mathfrak{f}'$) olyan n-változós (illetve n'-változós) logikai függvény, továbbá $\mathbf{T}_1, \dots, \mathbf{T}_n$ (illetve $\mathbf{T}'_1, \dots, \mathbf{T}'_{n'}$) olyan objektumok, hogy $\mathbf{A} \equiv \mathfrak{f}\mathbf{T}_1 \dots \mathbf{T}_n \equiv \mathfrak{f}'\mathbf{T}'_1 \dots \mathbf{T}'_{n'}$. Ekkor $\mathfrak{f} \equiv \mathfrak{f}'$, tehát $n \equiv n'$, így $\mathbf{T}_1 \dots \mathbf{T}_n \equiv \mathbf{T}'_1 \dots \mathbf{T}'_n$. Az előző lemma alkalmazásával ebből könnyen látható, hogy minden $1 \leq k \leq n$ számra $\mathbf{T}_k \equiv \mathbf{T}'_k$ teljesül. ■

3.1.5. Definíció. *Ha* $\mathbf{A}$ *olyan formula egy matematikai nyelvben, amelynek első karaktere a* $\neg$ *logikai operátor, akkor az* $\mathbf{A}$ **antecedensének** *nevezzük azt a* $\mathbf{B}$ *formulát, amelyre* $\mathbf{A} \equiv \neg\mathbf{B}$. *Ha* $\mathbf{A}$ *olyan formula egy matematikai nyelvben, amelynek első karaktere a* $\vee$ *logikai operátor, akkor az* $\mathbf{A}$ **antecedenseinek** *nevezzük azokat a* $\mathbf{B}$ *és* $\mathbf{C}$ *formulákat, amelyekre* $\mathbf{A} \equiv \vee\mathbf{BC}$. *Ha* $\mathbf{A}$ *olyan formula, amelynek az első karaktere az* n*-változós* $\mathfrak{f}$ *logikai függvény, akkor az* $\mathbf{A}$ **antecedenseinek** *nevezzük azokat a* $\mathbf{T}_1, \dots, \mathbf{T}_n$ *objektumokat, amelyekre* $\mathbf{A} \equiv \mathfrak{f}\mathbf{T}_1 \dots \mathbf{T}_n$.

Vegyük észre, hogy a formula-antecedensek egyértelműségi tétele nélkül nem lehetne bevezetni a formulák antecedenseinek fogalmát!

3.1.6. Definíció. *Azt mondjuk, hogy egy matematikai nyelv* $\mathbf{A}$ *formulája* **elemi**, *ha az első karaktere logikai függvény. Egy matematikai nyelv kifejezéseinek* $(\mathbf{A}_1, \dots, \mathbf{A}_n)$ n*-esét* **formula-konstrukciónak** *nevezünk, ha minden* $1 \leq j, k \leq n$, $j \neq k$ *esetén az* $\mathbf{A}_j$ *és* $\mathbf{A}_k$ *kifejezések különbözőek, továbbá minden* $1 \leq k \leq n$ *számra a következő feltételek valamelyike teljesül:*

a) $\mathbf{A}_k$ *elemi formula;*

b) *létezik olyan* $1 \leq j < k$ *szám, hogy* $\mathbf{A}_k \equiv \neg\mathbf{A}_j$*;*

c) *léteznek olyan* $1 \leq i, j < k$ *számok, hogy* $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$*.*

Ha $\mathfrak{a}$ *jelöli az* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ *formula-konstrukciót, akkor az* n *számot az* $\mathfrak{a}$ **hosszának** *nevezzük.*

Világos, hogy egy formula pontosan akkor *nem elemi*, ha az első karaktere a $\neg$ vagy $\vee$ logikai operátor.

Az elemi formulákat *irreducibiliseknek* is nevezhetjük, amennyiben a $\neg$ és $\vee$ logikai operátorok segítségével nem állíthatók elő egyszerűbb formulákból azon a módon, ahogy azt a formula-konstrukciók megkövetelik. Világos, hogy a matematikai nyelvek formula-konstrukciói az ítéletkalkulus ítélet-konstrukcióival analógok. Azonban egy ítélet-konstrukcióban a legegyszerűbb tagok az elemi ítéletek, amelyek semmiféle struktúrával nem rendelkeznek. Ugyanakkor a formula-konstrukciókban az elemi formulákból indulunk ki, amelyek egészen bonyolult szerkezetűek is lehetnek. Például; elemi formulákban szerepelhetnek a $\neg$ és $\vee$ logikai operátorok (csak nem az első karakterpozícióban), hiszen ha $\mathbf{T}$ és $\mathbf{S}$ objektumok, akkor $= \mathbf{TS}$ elemi formula, és a $\mathbf{T}$ vagy $\mathbf{S}$ lehet $\varepsilon_{\mathbf{x}}(\mathbf{A})$ alakú, ahol $\mathbf{A}$ tetszőleges formula, tehát $\mathbf{A}$-ban elvileg tetszőleges számú logikai operátor szerepelhet.

Megjegyezzük, hogy ha $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukció egy matematikai nyelvben, akkor minden $1 \leq k \leq n$ számra $(\mathbf{A}_1, \ldots, \mathbf{A}_k)$ szintén formula-konstrukció és $\mathbf{A}_k$ formula. Ez a definíció alapján nyilvánvaló.

3.1.7. Állítás. *Matematikai nyelv minden* $\mathbf{A}$ *formulájához létezik olyan* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ *formula-konstrukció, hogy* $\mathbf{A} \equiv \mathbf{A}_n$*.*

Bizonyítás. Legyen $(\mathbf{B}_1, \ldots, \mathbf{B}_m)$ olyan objektum-formula konstrukció, amelyre $\mathbf{A} \equiv \mathbf{B}_m$. Hagyjuk el ebből az összes elsőfajú kifejezést, és legyen az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ így nyert rendszer. Az $\mathbf{A}$ kifejezés másodfajú és $\mathbf{B}_m \equiv \mathbf{A}$, ezért $\mathbf{A}_n \equiv \mathbf{B}_m \equiv \mathbf{A}$. Ha $1 \leq k \leq n$ tetszőleges szám, akkor van olyan $1 \leq j \leq m$ szám, hogy $\mathbf{A}_k \equiv \mathbf{B}_j$, és $\mathbf{B}_j$ másodfajú tagja a $(\mathbf{B}_1, \ldots, \mathbf{B}_m)$ objektum-formula konstrukciónak, következésképpen az alábbi esetek lehetségesek.

1) Létezik olyan $1 \leq i < j$ szám, hogy $\mathbf{B}_j \equiv \neg\mathbf{B}_i$ és $\mathbf{B}_i$ másodfajú. Ekkor valamely $1 \leq p \leq n$ számra $\mathbf{A}_p \equiv \mathbf{B}_i$ és $p < k$, valamint $\mathbf{A}_k \equiv \mathbf{B}_j \equiv \neg\mathbf{B}_i \equiv \neg\mathbf{A}_p$;

2) Léteznek olyan $1 \leq j_1, j_2 < j$ számok, hogy $\mathbf{B}_j \equiv \vee\mathbf{B}_{j_1}\mathbf{B}_{j_2}$ és $\mathbf{B}_{j_1}$, $\mathbf{B}_{j_2}$ másodfajú kifejezések. Ekkor vannak olyan $1 \leq i_1, i_2 \leq n$ számok, hogy $\mathbf{A}_{i_1} \equiv \mathbf{B}_{j_1}$ és $\mathbf{A}_{i_2} \equiv \mathbf{B}_{j_2}$, továbbá $i_1, i_2 < k$, valamint $\mathbf{A}_k \equiv \mathbf{B}_j \equiv \vee\mathbf{B}_{j_1}\mathbf{B}_{j_2} \equiv \vee\mathbf{A}_{i_1}\mathbf{A}_{i_2}$;

3) Létezik olyan p-változós $\mathfrak{f}$ logikai függvény, és léteznek olyan $1 \leq j_1, \ldots, j_p \leq m$ számok, hogy $\mathbf{B}_j \equiv \mathfrak{f}\mathbf{B}_{j_1} \ldots \mathbf{B}_{j_p}$ és minden $1 \leq q \leq p$ számra $\mathbf{B}_{j_q}$ elsőfajú. Ekkor $\mathbf{B}_{j_1}, \ldots, \mathbf{B}_{j_p}$ objektumok, tehát $\mathbf{B}_j$ elemi formula, vagyis $\mathbf{A}_k$ elemi formula.

Ez azt jelenti, hogy ha az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-rendszerben a többször előforduló tagok közül csak a legkisebb sorszámút tartjuk meg, akkor olyan formula-konstrukciót kapunk, amelynek utolsó tagja azonos $\mathbf{A}$-val. ■

3.2. Matematikai nyelv értékelései

3.2.1. Definíció. *Egy matematikai nyelv* **értékelésének** *nevezünk minden olyan függvényt, amely a nyelv minden elemi formulájához hozzárendeli az* $\mathbf{i}$ *és* $\mathbf{h}$ *betűk közül pon-*

tosan az egyiket.

Tegyük fel, hogy $(\mathbf{A}_1, \dots, \mathbf{A}_n)$ formula-konstrukció és $1 \leq k \leq n$ rögzített szám. Ha $1 \leq i < k$ olyan, hogy $\mathbf{A}_k \equiv \neg\mathbf{A}_i$, akkor i *egyértelműen* van meghatározva, hiszen a formula-antecedensek egyértelműsége miatt $\mathbf{A}_i$ egyértelműen van meghatározva, és a formula-konsktrukciók különböző indexű tagjai különbözőek (a formula-konstrukciók definíciója szerint). Továbbá, ha $1 \leq i, j < k$ olyanok, hogy $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$, akkor i és j szintén *egyértelműen* vannak meghatározva, hiszen a formula-antecedensek egyértelműsége miatt az $\mathbf{A}_i$ és $\mathbf{A}_j$ formulák egyértelműen vannak meghatározva, továbbá a formula-konsktrukciók különböző indexű tagjai különbözők (a formula-konsktrukciók definíciója szerint).

3.2.2. Definíció. *Legyen ω értékelése egy matematikai nyelvnek, és jelölje $\mathfrak{a}$ az*

$$(\mathbf{A}_1, \dots, \mathbf{A}_n)$$

formula-konstrukciót. Minden $1 \leq k \leq n$ számra indukcióval értelmezzük az $\omega_\mathfrak{a}(\mathbf{A}_k)$ értéket, amely az $\mathbf{i}$ és $\mathbf{h}$ betűk valamelyike lesz.

a) *Ha $k = 1$, akkor $\mathbf{A}_1$ szükségképpen elemi formula; legyen ekkor $\omega_\mathfrak{a}(\mathbf{A}_1) \equiv \omega(\mathbf{A}_1)$.*

b) *Ha $1 \leq k \leq n$ olyan, hogy minden $1 \leq j < k$ számra az $\omega_\mathfrak{a}(\mathbf{A}_j)$ betűt már értelmeztük, akkor az $\mathbf{A}_k$ formulára a következő esetek lehetségesek:*

1) *$\mathbf{A}_k$ elemi formula; ekkor legyen $\omega_\mathfrak{a}(\mathbf{A}_k) \equiv \omega(\mathbf{A}_k)$;*

2) *egyértelműen létezik olyan $1 \leq i < k$ szám, hogy $\mathbf{A}_k \equiv \neg\mathbf{A}_i$; ekkor legyen*

$$\omega_\mathfrak{a}(\mathbf{A}_k) \equiv \begin{cases} \mathbf{i} & \text{, } ha\ \omega_\mathfrak{a}(\mathbf{A}_i) \equiv \mathbf{h}, \\ \mathbf{h} & \text{, } ha\ \omega_\mathfrak{a}(\mathbf{A}_i) \equiv \mathbf{i}; \end{cases}$$

3) *egyértelműen léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$; ekkor legyen*

$$\omega_\mathfrak{a}(\mathbf{A}_k) \equiv \begin{cases} \mathbf{h} & \text{, } ha\ \omega_\mathfrak{a}(\mathbf{A}_i) \equiv \omega_\mathfrak{a}(\mathbf{A}_j) \equiv \mathbf{h}, \\ \mathbf{i} & \text{, } egyébként. \end{cases}$$

Jelölés. Vezessük be a következő jelöléseket:

$$\mathfrak{B}_\neg(\mathbf{i}) \equiv \mathbf{h}, \quad \mathfrak{B}_\neg(\mathbf{h}) \equiv \mathbf{i};$$
$$\mathfrak{B}_\vee(\mathbf{i},\mathbf{i}) \equiv \mathfrak{B}_\vee(\mathbf{i},\mathbf{h}) \equiv \mathfrak{B}_\vee(\mathbf{h},\mathbf{i}) \equiv \mathbf{i}, \quad \mathfrak{B}_\vee(\mathbf{h},\mathbf{h}) \equiv \mathbf{h};$$
$$\mathfrak{B}_\Rightarrow(\mathbf{i},\mathbf{i}) \equiv \mathfrak{B}_\Rightarrow(\mathbf{h},\mathbf{i}) \equiv \mathfrak{B}_\Rightarrow(\mathbf{h},\mathbf{h}) \equiv \mathbf{i}, \quad \mathfrak{B}_\Rightarrow(\mathbf{i},\mathbf{h}) \equiv \mathbf{h};$$
$$\mathfrak{B}_\wedge(\mathbf{i},\mathbf{h}) \equiv \mathfrak{B}_\wedge(\mathbf{h},\mathbf{i}) \equiv \mathfrak{B}_\wedge(\mathbf{h},\mathbf{h}) \equiv \mathbf{h}, \quad \mathfrak{B}_\wedge(\mathbf{i},\mathbf{i}) \equiv \mathbf{i};$$
$$\mathfrak{B}_\Leftrightarrow(\mathbf{i},\mathbf{i}) \equiv \mathfrak{B}_\Leftrightarrow(\mathbf{h},\mathbf{h}) \equiv \mathbf{i}, \quad \mathfrak{B}_\Leftrightarrow(\mathbf{i},\mathbf{h}) \equiv \mathfrak{B}_\Leftrightarrow(\mathbf{h},\mathbf{i}) \equiv \mathbf{h}.$$

Ezeket a jelöléseket alkalmazva nyilvánvaló, hogy ha ω értékelése egy matematikai nyelvnek, és $\mathfrak{a}$ jelöli az $(\mathbf{A}_1, \dots, \mathbf{A}_n)$ formula-konstrukciót, akkor minden $1 \leq k \leq n$ számra:

– ha $\mathbf{A}_k$ elemi formula, akkor $\omega_\mathfrak{a}(\mathbf{A}_k) \equiv \omega(\mathbf{A}_k)$;

– ha $1 \leq i < k$ olyan, hogy $\mathbf{A}_k \equiv \neg\mathbf{A}_i$, akkor

$$\omega_\mathfrak{a}(\mathbf{A}_k) \equiv \mathfrak{B}_\neg(\omega_\mathfrak{a}(\mathbf{A}_i));$$

– ha $1 \leq i, j < k$ olyanok, hogy $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$, akkor

$$\omega_\mathfrak{a}(\mathbf{A}_k) \equiv \mathfrak{B}_\vee(\omega_\mathfrak{a}(\mathbf{A}_i), \omega_\mathfrak{a}(\mathbf{A}_j)).$$

3.2.3. Lemma. (**Egyértelműségi lemma**.) *Jelölje* $\mathfrak{a}$ *az* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$*, valamint* $\mathfrak{b}$ *a* $(\mathbf{B}_1, \ldots, \mathbf{B}_m)$ *formula-konstrukciót egy matematikai nyelvben. Ha* $\mathbf{A}_n \equiv \mathbf{B}_m$*, akkor a matematikai nyelv minden* ω *értékelésére* $\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_m)$*.*

Bizonyítás. Megállapodunk abban, hogy ha $\mathfrak{a}$ jelöli az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukciót, akkor minden $1 \leq k \leq n$ számra $\mathfrak{a}(k)$ jelöli az $(\mathbf{A}_1, \ldots, \mathbf{A}_k)$ formula-konstrukciót.

(I) Először megmutatjuk, hogy ha $\mathfrak{a}$ jelöli a $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukciót, akkor a matematikai nyelv minden ω értékelésére és minden $1 \leq k \leq n$ számra $\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$ teljesül. Ezt n szerinti teljes indukcióval igazoljuk.

Az állítás igaz, ha $n = 1$, mert ekkor $1 \leq k \leq n$ esetén $k = 1$, így $\mathfrak{a}(k) \equiv \mathfrak{a}$ miatt a matematikai nyelv minden ω értékelésére $\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$ triviálisan teljesül.

Tegyük fel, hogy az állítás igaz minden olyan formula-konstrukcióra, amelynek hossza kisebb n-nél (ezt a feltevést fogjuk *külső* indukciós hipotézisnek nevezni), és jelölje $\mathfrak{a}$ az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukciót. Legyen továbbá ω a matematikai nyelvnek tetszőleges értékelése. Azt kell igazolni, hogy minden $1 \leq k \leq n$ számra $\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$. Világos, hogy $k = n$ esetén $\mathfrak{a}(k) \equiv \mathfrak{a}$, így $\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$ triviálisan teljesül, tehát elég azokat az $1 \leq k \leq n$ számokat vizsgálni, amelyekre $k < n$.

Ha $k = 1$, akkor $\mathbf{A}_1$ szükségképpen elemi formula, így $\omega_{\mathfrak{a}(1)}(\mathbf{A}_1) \equiv \omega(\mathbf{A}_1) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_1)$.

Tegyük fel, hogy minden $1 \leq i < k$ számra $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_i)$ teljesül (ezt a feltevést fogjuk *belső* indukciós hipotézisnek nevezni). Az $\mathbf{A}_k$ formulára három eset lehetséges.

1) $\mathbf{A}_k$ elemi formula: ekkor $\omega_{\mathfrak{a}(k)}(\mathbf{A}_i) \equiv \omega(\mathbf{A}_k) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$.

2) Van olyan $1 \leq i < k$ szám, hogy $\mathbf{A}_k \equiv \neg\mathbf{A}_k$. Ekkor nyilvánvalóan $\mathfrak{a}(k)(i) \equiv \mathfrak{a}(i)$, és az $\mathfrak{a}(k)$ formula-konstrukciónak n-nél kevesebb tagja van, mert $k < n$, így a külső indukciós hipotézis szerint $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}(k)}(\mathbf{A}_i)$, mert $i < k$: következésképpen $\omega_{\mathfrak{a}(k)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_i)$, így a definíció alapján $\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \mathfrak{B}_{\neg}(\omega_{\mathfrak{a}(k)}(\mathbf{A}_i)) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$.

3) Léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$. Ekkor $i, j < k$ miatt, a belső indukciós hipotézis alapján $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_i)$ és $\omega_{\mathfrak{a}(j)}(\mathbf{A}_j) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_j)$. Továbbá, $\mathfrak{a}(k)(i) \equiv \mathfrak{a}(i)$, $\mathfrak{a}(k)(j) \equiv \mathfrak{a}(j)$, és az $\mathfrak{a}(k)$ formula-konstrukciónak n-nél kevesebb tagja van, mert $k < n$, így a külső indukciós hipotézis szerint $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}(k)}(\mathbf{A}_i)$ és $\omega_{\mathfrak{a}(j)}(\mathbf{A}_j) \equiv \omega_{\mathfrak{a}(k)}(\mathbf{A}_j)$, mert $i, j < k$. Ezért $\omega_{\mathfrak{a}(k)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_i)$ és $\omega_{\mathfrak{a}(k)}(\mathbf{A}_j) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_j)$, amiből a definíció alapján következik, hogy

$$\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \mathfrak{B}_{\vee}(\omega_{\mathfrak{a}(k)}(\mathbf{A}_i), \omega_{\mathfrak{a}(k)}(\mathbf{A}_j)) \equiv \mathfrak{B}_{\vee}(\omega_{\mathfrak{a}}(\mathbf{A}_i), \omega_{\mathfrak{a}}(\mathbf{A}_j)) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k).$$

Ezzel megmutattuk, hogy a külső és belső indukciós hipotézis teljesülése esetén $\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$. Ezért a külső indukciós hipotézis teljesülése esetén minden $1 \leq k \leq n$ számra $\omega_{\mathfrak{a}(k)}(\mathbf{A}_k) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_k)$. Ez azt jelenti, hogy az (I) elején megfogalmazott állítás tetszőleges formula-konstrukcióra és értékelésre igaz.

(II) Most n szerinti teljes indukcióval bizonyítjuk az állítást.

Ha $n = 1$, akkor $\mathbf{A}_n$ szükségképpen elemi formula, így $\mathbf{A}_n \equiv \mathbf{B}_m$ miatt $\mathbf{B}_m$ is elemi formula, amiből a definíció alapján következik, hogy $\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \omega(\mathbf{A}_n) \equiv \omega(\mathbf{B}_m) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_m)$.

Tegyük fel, hogy az állítás minden olyan $\mathfrak{a}$ formula-konstrukcióra igaz, amelynek hossza kisebb n-nél. Jelölje $\mathfrak{a}$ az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukciót. Ekkor $\mathbf{A}_n$-re a következő esetek lehetségesek.

1) $\mathbf{A}_n$ elemi formula. Ekkor $\mathbf{A}_n \equiv \mathbf{B}_m$ miatt $\mathbf{B}_m$ is elemi formula, amiből a definíció alapján következik, hogy $\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \omega(\mathbf{A}_n) \equiv \omega(\mathbf{B}_m) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_m)$.

2) Van olyan $1 \le i < n$ szám, hogy $\mathbf{A}_n \equiv \neg\mathbf{A}_i$. Ekkor $\mathbf{A}_n \equiv \mathbf{B}_m$ miatt egyértelműen létezik olyan $1 \le j \le m$ szám, hogy $\mathbf{B}_m \equiv \neg\mathbf{B}_j$. Világos, hogy az (I) szerint $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_i)$ és $\omega_{\mathfrak{b}(j)}(\mathbf{B}_j) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_j)$. Ugyanakkor a definíció alapján

$$\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \mathfrak{B}_{\neg}(\omega_{\mathfrak{a}}(\mathbf{A}_i)) \equiv \mathfrak{B}_{\neg}(\omega_{\mathfrak{a}(i)}(\mathbf{A}_i)),$$
$$\omega_{\mathfrak{b}}(\mathbf{B}_m) \equiv \mathfrak{B}_{\neg}(\omega_{\mathfrak{b}}(\mathbf{B}_j)) \equiv \mathfrak{B}_{\neg}(\omega_{\mathfrak{b}(j)}(\mathbf{B}_j)).$$

De $i < n$ miatt az $\mathfrak{a}(i)$ formula-konstrukciónak n-nél kevesebb tagja van, valamint a formula-antecedensek egyértelműsége szerint $\mathbf{A}_i \equiv \mathbf{B}_j$, ezért az indukciós hipotézis alapján $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{b}(j)}(\mathbf{B}_j)$, így a fentiek alapján $\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_m)$.

3) Léteznek olyan $1 \le i, j < n$ számok, hogy $\mathbf{A}_n \equiv \vee\mathbf{A}_i\mathbf{A}_j$. Ekkor $\mathbf{A}_n \equiv \mathbf{B}_m$ miatt egyértelműen léteznek olyan $1 \le i', j' < m$ számok, hogy $\mathbf{B}_m \equiv \vee\mathbf{B}_{i'}\mathbf{B}_{j'}$. A formula-antecedensek egyértelműsége alapján $\mathbf{A}_i \equiv \mathbf{B}_{i'}$ és $\mathbf{A}_j \equiv \mathbf{B}_{j'}$. Világos, hogy az (I) szerint $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_i)$, $\omega_{\mathfrak{a}(j)}(\mathbf{A}_j) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_j)$, $\omega_{\mathfrak{b}(i')}(\mathbf{B}_{i'}) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_{i'})$ és $\omega_{\mathfrak{b}(j')}(\mathbf{B}_{j'}) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_{j'})$. Ugyanakkor a definíció alapján

$$\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \mathfrak{B}_{\vee}(\omega_{\mathfrak{a}}(\mathbf{A}_i), \omega_{\mathfrak{a}}(\mathbf{A}_j)) \equiv \mathfrak{B}_{\vee}(\omega_{\mathfrak{a}(i)}(\mathbf{A}_i), \omega_{\mathfrak{a}(j)}(\mathbf{A}_j)),$$
$$\omega_{\mathfrak{b}}(\mathbf{B}_m) \equiv \mathfrak{B}_{\vee}(\omega_{\mathfrak{b}}(\mathbf{B}_{i'}), \omega_{\mathfrak{b}}(\mathbf{B}_{j'})) \equiv \mathfrak{B}_{\vee}(\omega_{\mathfrak{b}(i')}(\mathbf{B}_{i'}), \omega_{\mathfrak{b}(j')}(\mathbf{B}_{j'})).$$

De $i, j < n$ miatt az $\mathfrak{a}(i)$ és $\mathfrak{a}(j)$ formula-konstrukciók hossza kisebb n-nél, valamint $\mathbf{A}_i \equiv \mathbf{B}_{i'}$ és $\mathbf{A}_j \equiv \mathbf{B}_{j'}$, ezért az indukciós hipotézis alapján $\omega_{\mathfrak{a}(i)}(\mathbf{A}_i) \equiv \omega_{\mathfrak{b}(i')}(\mathbf{B}_{i'})$ és $\omega_{\mathfrak{a}(j)}(\mathbf{A}_j) \equiv \omega_{\mathfrak{b}(j')}(\mathbf{B}_{j'})$, így a fentiek szerint $\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_m)$. ■

3.2.4. Állítás. (**Az értékelések kiterjesztésének tétele**.) *Ha ω értékelése egy matematikai nyelvnek, akkor egyértelműen létezik olyan $\overline{\omega}$ függvény, amely a nyelv minden formulájához hozzárendeli az* **i** *és* **h** *betűk közül pontosan az egyiket, és rendelkezik azzal a tulajdonsággal, hogy minden* $\mathbf{A}$ *formulára és minden* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ *formula-konstrukcióra, ha* $\mathbf{A} \equiv \mathbf{A}_n$*, akkor* $\overline{\omega}(\mathbf{A}) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_n)$*, ahol* $\mathfrak{a}$ *jelöli az* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ *formula-konstrukciót.*

Bizonyítás. Láttuk, hogy az $\mathbf{A}$ formulához *van olyan* $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukció, amelyre $\mathbf{A} \equiv \mathbf{A}_n$, ezért $\omega_{\mathfrak{a}}(\mathbf{A}_n)$ jól értelmezett, ha $\mathfrak{a}$ jelöli az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukciót. Az egyértelműségi lemmából következik, hogy ez az $\omega_{\mathfrak{a}}(\mathbf{A}_n)$ érték (amely az **i** és **h** értékek valamelyikével azonos) *független* az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukció választásától, hiszen ha $\mathfrak{b}$ jelöl egy olyan $(\mathbf{B}_1, \ldots, \mathbf{B}_m)$ formula-konstrukciót, amelyre $\mathbf{A} \equiv \mathbf{B}_m$, akkor $\omega_{\mathfrak{a}}(\mathbf{A}_n) \equiv \omega_{\mathfrak{b}}(\mathbf{B}_m)$; jelölje $\overline{\omega}(\mathbf{A})$ ezt az értéket. Ekkor $\overline{\omega}(\mathbf{A})$ az **i** és **h** értékek egyikével azonos, és a definíciója szerint rendelkezik azzal a tulajdonsággal, hogy minden $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukcióra, ha $\mathbf{A} \equiv \mathbf{A}_n$, akkor $\overline{\omega}(\mathbf{A}) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_n)$, ahol $\mathfrak{a}$ jelöli az $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ formula-konstrukciót. ■

Elnevezés. Ha ω értékelése egy matematikai nyelvnek, akkor az előző állításban értelmezett $\overline{\omega}$ függvényt az ω **kiterjesztésének** nevezzük.

A definíció alapján világos, hogy ha ω értékelése egy matematikai nyelvnek és $\mathbf{A}$ elemi formula, akkor $\overline{\omega}(\mathbf{A}) \equiv \omega(\mathbf{A})$, tehát $\overline{\omega}$ valóban az ω függvény kiterjesztése az elemi formulák összességéről a formulák összességére.

3.2.5. Lemma. *Ha ω értékelése egy matematikai nyelvnek, akkor bármely két* $\mathbf{A}$ *és* $\mathbf{B}$

formulára

$$\begin{aligned}\overline{\omega}(\neg\mathbf{A}) &\equiv \mathfrak{B}_{\neg}(\overline{\omega}(\mathbf{A})),\\ \overline{\omega}(\mathbf{A}\vee\mathbf{B}) &\equiv \mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{A}),\overline{\omega}(\mathbf{B})),\\ \overline{\omega}(\mathbf{A}\Rightarrow\mathbf{B}) &\equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A}),\overline{\omega}(\mathbf{B})),\\ \overline{\omega}(\mathbf{A}\wedge\mathbf{B}) &\equiv \mathfrak{B}_{\wedge}(\overline{\omega}(\mathbf{A}),\overline{\omega}(\mathbf{B})),\\ \overline{\omega}(\mathbf{A}\Leftrightarrow\mathbf{B}) &\equiv \mathfrak{B}_{\Leftrightarrow}(\overline{\omega}(\mathbf{A}),\overline{\omega}(\mathbf{B})).\end{aligned}$$

Bizonyítás. (I) Jelöljön $\mathfrak{a}$ egy olyan $(\mathbf{A}_1,\ldots,\mathbf{A}_n)$ formula-konstrukciót, amelyre $\mathbf{A}_n\equiv\mathbf{A}$, és jelölje $\mathfrak{c}$ az $(\mathbf{A}_1,\ldots,\mathbf{A}_n,\neg\mathbf{A}_n)$ formula $(n+1)$-est. Ez szintén formula-konstrukció, mert ha létezne olyan $1\le m\le n+1$ szám, hogy $\mathbf{A}_m\equiv\neg\mathbf{A}_n$, akkor $m\ne n$, hiszen $\mathbf{A}_n$ és $\neg\mathbf{A}_n$ hossza különböző, és létezne olyan $1\le k<m$ szám, hogy $\mathbf{A}_m\equiv\neg\mathbf{A}_k$, így $\mathbf{A}_k\equiv\mathbf{A}_n$ teljesülne, ami lehetetlen, mert az $\mathfrak{a}$ formula-konstrukció különböző indexű tagjai különbözőek. Az egyértelműségi lemma bizonyításának (I) része alapján $\omega_{\mathfrak{c}}(\mathbf{A})\equiv\omega_{\mathfrak{a}}(\mathbf{A})$, mert $\mathfrak{c}(n)\equiv\mathfrak{a}$, ezért az $\overline{\omega}$ értelmezése szerint

$$\overline{\omega}(\neg\mathbf{A})\equiv\omega_{\mathfrak{c}}(\neg\mathbf{A})\equiv\mathfrak{B}_{\neg}(\omega_{\mathfrak{c}}(\mathbf{A}))\equiv\mathfrak{B}_{\neg}(\omega_{\mathfrak{a}}(\mathbf{A}))\equiv\mathfrak{B}_{\neg}(\overline{\omega}(\mathbf{A})).$$

(II) Jelöljön $\mathfrak{a}$ egy olyan $(\mathbf{A}_1,\ldots,\mathbf{A}_n)$ formula-konstrukciót, amelyre $\mathbf{A}_n\equiv\mathbf{A}$, és jelöljön $\mathfrak{b}$ egy olyan $(\mathbf{B}_1,\ldots,\mathbf{B}_m)$ formula-konstrukciót, amelyre $\mathbf{B}_m\equiv\mathbf{B}$. Ekkor két eset lehetséges.

1) Van olyan $1\le k\le n$ szám, hogy $\mathbf{B}\equiv\mathbf{A}_k$. Jelölje $\mathfrak{c}$ az $(\mathbf{A}_1,\ldots,\mathbf{A}_n,\vee\mathbf{AB})$ formula $(n+1)$-est. Ha $\vee\mathbf{AB}$ azonos volna az $\mathbf{A}_1,\ldots,\mathbf{A}_n$ formulák valamelyikével, akkor léteznének olyan $1\le i,j<n$ számok, hogy $\vee\mathbf{AB}\equiv\vee\mathbf{A}_i\mathbf{A}_j$; ekkor a formula-antecedensek egyértelműsége miatt $\mathbf{A}_n\equiv\mathbf{A}\equiv\mathbf{A}_i$, ami lehetetlen, mert i és n különbözőek. Ezért $\mathfrak{c}$ szintén formula-konstrukció, és világos, hogy $\mathfrak{c}(n)\equiv\mathfrak{a}$ és $\mathfrak{c}(k)$ olyan formula-konstrukció, amelynek utolsó tagja azonos $\mathbf{A}_k$-val, vagyis $\mathbf{B}$-vel. Ezért az $\overline{\omega}$ értelmezése és az egyértelműségi lemma bizonyításának (I) része alapján $\overline{\omega}(\mathbf{A})\equiv\omega_{\mathfrak{a}}(\mathbf{A})\equiv\omega_{\mathfrak{c}(n)}(\mathbf{A}_n)\equiv\omega_{\mathfrak{c}}(\mathbf{A})$, és $\overline{\omega}(\mathbf{B})\equiv\omega_{\mathfrak{c}(k)}(\mathbf{A}_k)\equiv\omega_{\mathfrak{c}}(\mathbf{B})$. Ezért az $\overline{\omega}$ értelmezése szerint

$$\overline{\omega}(\mathbf{A}\vee\mathbf{B})\equiv\omega_{\mathfrak{c}}(\mathbf{A}\vee\mathbf{B})\equiv\mathfrak{B}_{\vee}(\omega_{\mathfrak{c}}(\mathbf{A}),\omega_{\mathfrak{c}}(\mathbf{B}))\equiv\mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{A}),\overline{\omega}(\mathbf{B}))$$

teljesül. (Láthatóan ebben az esetben a $\mathfrak{b}$ formula-konstrukciónak semmilyen szerep nem jutott.)

2) Minden $1\le k\le n$ számra $\mathbf{B}$ különbözik $\mathbf{A}_k$-tól. Hagyjuk el a $(\mathbf{B}_1,\ldots,\mathbf{B}_m)$ formula-konstrukcióból azokat a formulákat, amelyek valamelyik $1\le k\le n$ számra az $\mathbf{A}_k$-val azonosak, és az így nyert formula-rendszert jelölje $(\mathbf{B}'_1,\ldots,\mathbf{B}'_p)$. Világos, hogy $\mathbf{B}'_p\equiv\mathbf{B}$. Jelölje $\mathfrak{c}$ az $(\mathbf{A}_1,\ldots,\mathbf{A}_n,\mathbf{B}'_1,\ldots,\mathbf{B}'_p,\vee\mathbf{AB})$ formula $(n+p+1)$-est. Az előzőekhez hasonlóan könnyen látható, hogy ez is formula-konstrukció. Továbbá, $\mathfrak{c}(n)\equiv\mathfrak{a}$, és $\mathfrak{c}(n+p)$ olyan formula-konstrukció, amelynek utolsó tagja azonos $\mathbf{B}'_p$-vel, vagyis $\mathbf{B}$-vel. Ezért az $\overline{\omega}$ értelmezése és az egyértelműségi lemma bizonyításának (I) része alapján $\overline{\omega}(\mathbf{A})\equiv\omega_{\mathfrak{a}}(\mathbf{A})\equiv\omega_{\mathfrak{c}(n)}(\mathbf{A}_n)\equiv\omega_{\mathfrak{c}}(\mathbf{A}_n)$, és $\overline{\omega}(\mathbf{B})\equiv\omega_{\mathfrak{c}(n+p)}(\mathbf{B}'_p)\equiv\omega_{\mathfrak{c}}(\mathbf{B})$. Ezért az $\overline{\omega}$ értelmezése alapján ismét

$$\overline{\omega}(\mathbf{A}\vee\mathbf{B})\equiv\omega_{\mathfrak{c}}(\mathbf{A}\vee\mathbf{B})\equiv\mathfrak{B}_{\vee}(\omega_{\mathfrak{c}}(\mathbf{A}),\omega_{\mathfrak{c}}(\mathbf{B}))\equiv\mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{A}),\overline{\omega}(\mathbf{B}))$$

teljesül.

(III) Könnyen ellenőrizhető (például megfelelő logikai táblázatok felírásával), hogy ha $\mathbf{b}$

és **c** az **i** vagy **h** értékek bármelyikét jelölik, akkor

$$\mathfrak{B}_{\Rightarrow}(\mathbf{b},\mathbf{c}) \equiv \mathfrak{B}_{\vee}(\mathfrak{B}_{\neg}(\mathbf{b}),\mathbf{c}),$$
$$\mathfrak{B}_{\wedge}(\mathbf{b},\mathbf{c}) \equiv \mathfrak{B}_{\neg}(\mathfrak{B}_{\vee}(\mathfrak{B}_{\neg}(\mathbf{b}),\mathfrak{B}_{\neg}(\mathbf{c}))),$$
$$\mathfrak{B}_{\Leftrightarrow}(\mathbf{b},\mathbf{c}) \equiv \mathfrak{B}_{\neg}(\mathfrak{B}_{\vee}(\mathfrak{B}_{\neg}(\mathfrak{B}_{\vee}(\mathfrak{B}_{\neg}(\mathbf{b}),\mathbf{c})),\mathfrak{B}_{\neg}(\mathfrak{B}_{\vee}(\mathfrak{B}_{\neg}(\mathbf{c}),\mathbf{b})))).$$

Ezekből (I) és (II) alkalmazásával könnyen kapjuk az $\overline{\omega}(\mathbf{A} \Rightarrow \mathbf{B})$, $\overline{\omega}(\mathbf{A} \wedge \mathbf{B})$ és $\overline{\omega}(\mathbf{A} \Leftrightarrow \mathbf{B})$ értékekre vonatkozó állításokat. ■

3.3. Helyettesítés-invariáns értékelések

A következő definíció előtt megjegyezzük, hogy ha **A** elemi formulája, **x** változója és **T** objektuma egy matematikai nyelvnek, akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}$ szintén elemi formula, mert ennek az első karaktere megegyezik **A** első karakterével, ami logikai függvényjel, és a logikai függvényjelek minden változótól különböznek.

3.3.1. Definíció. *Egy matematikai nyelv ω értékelését* **helyettesítés-invariánsnak** *nevezzük, ha a nyelv minden* **A** *elemi formulájára, minden* **x** *változójára és minden* **T** *objektumára $\omega((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv \omega(\mathbf{A})$ teljesül.*

Például egy matematikai nyelv helyettesítés-invariáns értékelése az a függvény, amely a nyelv minden elemi formulájához az **i** (illetve **h**) értéket rendeli; ezeket *homogén értékeléseknek* nevezzük.

3.3.2. Állítás. *Ha ω helyettesítés-invariáns értékelése egy matematikai nyelvnek, akkor a nyelv minden* **A** *formulájára, minden* **x** *változójára és minden* **T** *objektumára $\overline{\omega}((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv \overline{\omega}(\mathbf{A})$ teljesül.*

Bizonyítás. Legyen **A** formula, **x** változó, **T** objektum és jelöljön $\mathfrak{a}$ egy olyan $(\mathbf{A}_1,\ldots,\mathbf{A}_n)$ formula-konstrukciót, amelyre $\mathbf{A}_n \equiv \mathbf{A}$. Az $\overline{\omega}$ függvény értelmezése alapján $\overline{\omega}(\mathbf{A}) \equiv \omega_{\mathfrak{a}}(\mathbf{A}_n)$.

A $((\mathbf{T}|\mathbf{x})\mathbf{A}_1,\ldots,(\mathbf{T}|\mathbf{x})\mathbf{A}_n)$ formula n-es szintén formula-konstrukció, mert ha $1 \leq k \leq n$ tetszőleges szám, akkor

– ha $\mathbf{A}_k$ elemi formula, akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ elemi formula;

– ha $1 \leq i < k$ olyan szám, hogy $\mathbf{A}_k \equiv \neg\mathbf{A}_i$, akkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \neg((\mathbf{T}|\mathbf{x})\mathbf{A}_k)$;

– ha $1 \leq i,j < k$ olyan számok, hogy $\mathbf{A}_k \equiv \vee\mathbf{A}_i\mathbf{A}_j$, akkor teljesül az, hogy $(\mathbf{T}|\mathbf{x})\mathbf{A}_k \equiv \vee((\mathbf{T}|\mathbf{x})\mathbf{A}_i)((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$.

Jelölje $(\mathbf{T}|\mathbf{x})\mathfrak{a}$ a $((\mathbf{T}|\mathbf{x})\mathbf{A}_1,\ldots,(\mathbf{T}|\mathbf{x})\mathbf{A}_n)$ formula-konstrukciót. Ekkor $(\mathbf{T}|\mathbf{x})\mathbf{A}_n \equiv (\mathbf{T}|\mathbf{x})\mathbf{A}$, így az $\overline{\omega}$ függvény értelmezése alapján $\overline{\omega}((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv \omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_n)$. Ezért elég azt igazolni, hogy minden $1 \leq k \leq n$ számra $\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_k) \equiv \overline{\omega}(\mathbf{A}_k)$.

Ha $k = 1$, akkor $\mathbf{A}_1$ és $(\mathbf{T}|\mathbf{x})\mathbf{A}_1$ elemi formulák, így az ω helyettesítés-invarianciája folytán

$$\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_1) \equiv \omega((\mathbf{T}|\mathbf{x})\mathbf{A}_1) \equiv \omega(\mathbf{A}_1) \equiv \overline{\omega}(\mathbf{A}_1).$$

Legyen $1 \leq k \leq n$ olyan szám, hogy minden $1 \leq i < k$ számra $\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_i) \equiv \overline{\omega}(\mathbf{A}_i)$. Az $\mathbf{A}_k$ formulára három eset teljesülhet.

1) $\mathbf{A}_k$ elemi formula. Ekkor $\mathbf{A}_k$ és $(\mathbf{T}|\mathbf{x})\mathbf{A}_k$ elemi formulák, így az ω helyettesítés-invarianciája folytán

$$\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_k) \equiv \omega((\mathbf{T}|\mathbf{x})\mathbf{A}_k) \equiv \omega(\mathbf{A}_k) \equiv \overline{\omega}(\mathbf{A}_k).$$

2) Van olyan $1 \leq i < k$ szám, hogy $\mathbf{A}_k \equiv \neg \mathbf{A}_i$. Ekkor az indukciós hipotézisből következik, hogy $\overline{\omega}(\mathbf{A}_i) \equiv \omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_i)$, tehát

$$\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_k) \equiv \omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}(\neg((\mathbf{T}|\mathbf{x})\mathbf{A}_i)) \equiv$$
$$\equiv \mathfrak{B}_\neg(\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_i)) \equiv \mathfrak{B}_\neg(\overline{\omega}(\mathbf{A}_i)) \equiv \overline{\omega}(\neg \mathbf{A}_i) \equiv \overline{\omega}(\mathbf{A}_k).$$

3) Léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_k \equiv \vee \mathbf{A}_i \mathbf{A}_j$. Ekkor az indukciós hipotézisből következik, hogy $\overline{\omega}(\mathbf{A}_i) \equiv \omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_i)$ és $\overline{\omega}(\mathbf{A}_j) \equiv \omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_j)$, tehát

$$\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_k) \equiv \omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}(\vee((\mathbf{T}|\mathbf{x})\mathbf{A}_i)((\mathbf{T}|\mathbf{x})\mathbf{A}_j)) \equiv$$
$$\equiv \mathfrak{B}_\vee(\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_i), \omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_j)) \equiv \mathfrak{B}_\vee(\overline{\omega}(\mathbf{A}_i), \overline{\omega}(\mathbf{A}_j)) \equiv$$
$$\equiv \overline{\omega}(\vee \mathbf{A}_i \mathbf{A}_j) \equiv \overline{\omega}(\mathbf{A}_k).$$

Ezért k-ra is teljesül az, hogy $\omega_{(\mathbf{T}|\mathbf{x})\mathfrak{a}}((\mathbf{T}|\mathbf{x})\mathbf{A}_k) \equiv \overline{\omega}(\mathbf{A}_k)$. ■

3.3.3. Következmény. *Ha ω helyettesítés-invariáns értékelése egy matematikai nyelvnek, akkor a nyelv minden $\mathbf{A}$ formulájára és minden $\mathbf{x}$ változójára*

$$\overline{\omega}((\exists \mathbf{x})\mathbf{A}) \equiv \overline{\omega}((\forall \mathbf{x})\mathbf{A}) \equiv \overline{\omega}(\mathbf{A}),$$

továbbá a nyelv minden n-változós $\mathfrak{f}$ logikai függvényére és minden $(\mathbf{T}_1, \dots \mathbf{T}_n)$ és $(\mathbf{S}_1, \dots, \mathbf{S}_n)$ objektum n-esre

$$\omega(\mathfrak{f}(\mathbf{T}_1, \dots \mathbf{T}_n)) \equiv \omega(\mathfrak{f}(\mathbf{S}_1, \dots, \mathbf{S}_n)).$$

Speciálisan, ha ω olyan helyettesítés-invariáns értékelése egy matematikai nyelvnek, hogy minden $\mathbf{x}$ és $\mathbf{y}$ változóra $\omega(\mathbf{x} = \mathbf{y}) \equiv \mathbf{i}$, akkor a nyelv bármely $\mathbf{T}$ és $\mathbf{S}$ objektumára $\omega(\mathbf{T} = \mathbf{S}) \equiv \mathbf{i}$.

Bizonyítás. Legyen ω helyettesítés-invariáns értékelése, $\mathbf{A}$ formulája és $\mathbf{x}$ változója egy matematikai nyelvnek. Az egzisztenciális kvantor definíciója és az előző állítás szerint

$$\overline{\omega}((\exists \mathbf{x})\mathbf{A}) \equiv \overline{\omega}((\varepsilon_{\mathbf{x}}(\mathbf{A})|\mathbf{x})\mathbf{A}) \equiv \overline{\omega}(\mathbf{A}).$$

Az univerzális kvantor értelmezése és az előzőek szerint

$$\overline{\omega}((\forall \mathbf{x})\mathbf{A}) \equiv \overline{\omega}(\neg(\exists \mathbf{x})(\neg \mathbf{A})) \equiv \mathfrak{B}_\neg(\overline{\omega}((\exists \mathbf{x})(\neg \mathbf{A}))) \equiv$$
$$\equiv \mathfrak{B}_\neg(\overline{\omega}(\neg \mathbf{A})) \equiv \mathfrak{B}_\neg(\mathfrak{B}_\neg(\overline{\omega}(\mathbf{A}))) \equiv \overline{\omega}(\mathbf{A}),$$

hiszen a $\mathfrak{B}_\neg$ definíciója szerint, ha $\mathbf{b}$ a $\mathbf{i}$ vagy $\mathbf{h}$ értékek bármelyikét jelöli, akkor nyilvánvalóan $\mathfrak{B}_\neg(\mathfrak{B}_\neg(\mathbf{b})) \equiv \mathbf{b}$.

Legyen $\mathfrak{f}$ tetszőleges n-változós logikai függvény, továbbá $(\mathbf{T}_1, \dots, \mathbf{T}_n)$ és $(\mathbf{S}_1, \dots, \mathbf{S}_n)$ objektum n-esek. Vegyünk olyan $\mathbf{x}_1, \dots, \mathbf{x}_n$ változókat, amelyek páronként különbözőek, és nem szerepelnek a $\mathbf{T}_1, \dots, \mathbf{T}_n, \mathbf{S}_1, \dots, \mathbf{S}_n$ objektumok egyikében sem. Az előző állítás szukcesszív alkalmazásával kapjuk, hogy

$$\omega(\mathfrak{f}(\mathbf{T}_1, \dots, \mathbf{T}_n)) \equiv \omega((\mathbf{T}_1|\mathbf{x}_1) \dots (\mathbf{T}_n|\mathbf{x}_n)\mathfrak{f}(\mathbf{x}_1, \dots, \mathbf{x}_n)) \equiv \omega(\mathfrak{f}(\mathbf{x}_1, \dots, \mathbf{x}_n)),$$

és teljesen hasonlóan kapjuk, hogy $\omega(\mathfrak{f}(\mathbf{S}_1, \dots, \mathbf{S}_n)) \equiv \omega(\mathfrak{f}(\mathbf{x}_1, \dots, \mathbf{x}_n))$, következésképpen $\omega(\mathfrak{f}(\mathbf{T}_1, \dots \mathbf{T}_n)) \equiv \omega(\mathfrak{f}(\mathbf{S}_1, \dots, \mathbf{S}_n))$. ■

Az előző állításból könnyen kapjuk, hogy ha egy matematikai nyelvnek n darab logikai függvénye van (beleértve az $=$ függvényt is), akkor a nyelvnek pontosan 2^n darab helyettesítés-invariáns értékelése van.

3.4. A predikátumkalkulus ellentmondásmentessége

3.4.1. Tétel. *Ha ω olyan értékelése a $\mathfrak{T}$ matematikai elmélet nyelvének, hogy $\overline{\omega}$ a $\mathfrak{T}$ elmélet minden axiómájához az* **i** *értéket rendeli, akkor $\overline{\omega}$ a $\mathfrak{T}$ elmélet minden tételéhez az* **i** *értéket rendeli, továbbá a $\mathfrak{T}$ matematikai elmélet ellentmondásmentes.*

Bizonyítás. Először megjegyezzük, hogy ha ω tetszőleges értékelése a $\mathfrak{T}$ matematikai elmélet nyelvének, és $\mathbf{A}$, $\mathbf{B}$ olyan formulák, hogy $\overline{\omega}(\mathbf{A}) \equiv \mathbf{i}$ és $\overline{\omega}(\mathbf{A} \Rightarrow \mathbf{B}) \equiv \mathbf{i}$, akkor $\overline{\omega}(\mathbf{B}) \equiv \mathbf{i}$, hiszen

$$\mathbf{i} \;\equiv\; \overline{\omega}(\mathbf{A} \Rightarrow \mathbf{B}) \;\equiv\; \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{B})) \;\equiv\; \mathfrak{B}_{\Rightarrow}(\mathbf{i}, \overline{\omega}(\mathbf{B})) \;\equiv\; \overline{\omega}(\mathbf{B}).$$

Legyen ω olyan értékelése a $\mathfrak{T}$ matematikai elmélet nyelvének, hogy $\overline{\omega}$ a $\mathfrak{T}$ minden axiómájához az $\mathbf{i}$ értéket rendeli. Legyen $\mathbf{A}$ tétel $\mathfrak{T}$-ben és $(\mathbf{A}_1, \dots, \mathbf{A}_n)$ az $\mathbf{A}$ formula bizonyítása $\mathfrak{T}$-ben. Megmutatjuk, hogy minden $1 \leq k \leq n$ számra $\overline{\omega}(\mathbf{A}_k) \equiv \mathbf{i}$ teljesül, tehát $\mathbf{A} \equiv \mathbf{A}_n$ miatt $\overline{\omega}(\mathbf{A}) \equiv \mathbf{i}$ is igaz.

Az $\mathbf{A}_1$ formula szükségképpen axiómája $\mathfrak{T}$-nek, ezért a hipotézis szerint $\overline{\omega}(\mathbf{A}_1) \equiv \mathbf{i}$.

Legyen $1 \leq k \leq n$ rögzített, és tegyük fel, hogy minden $1 \leq i < k$ számra $\overline{\omega}(\mathbf{A}_i) \equiv \mathbf{i}$. Ha $\mathbf{A}_k$ axiómája $\mathfrak{T}$-nek, akkor hipotézis szerint $\overline{\omega}(\mathbf{A}_k) \equiv \mathbf{i}$. Ha léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_j \equiv \mathbf{A}_i \Rightarrow \mathbf{A}_k$, akkor az indukciós hipotézis szerint $\overline{\omega}(\mathbf{A}_i \Rightarrow \mathbf{A}_k) \equiv \overline{\omega}(\mathbf{A}_j) \equiv \mathbf{i}$, továbbá $\overline{\omega}(\mathbf{A}_i) \equiv \mathbf{i}$, ezért $\overline{\omega}(\mathbf{A}_k) \equiv \mathbf{i}$.

Ha $\mathbf{A}$ tétel $\mathfrak{T}$-ben, akkor $\overline{\omega}(\neg\mathbf{A}) \equiv \mathfrak{B}_{\neg}(\overline{\omega}(\mathbf{A})) \equiv \mathfrak{B}_{\neg}(\mathbf{i}) \equiv \mathbf{h}$, tehát $\neg\mathbf{A}$ *nem tétel* $\mathfrak{T}$-ben, így a $\mathfrak{T}$ matematikai elmélet ellentmondásmentes. ■

3.4.2. Állítás. *Ha $\mathfrak{T}$ predikátumkalkulus, akkor a $\mathfrak{T}$ matematikai nyelvének minden* **A** *elemi formulájára* $\neg\mathbf{A}$ *nem tétel $\mathfrak{T}$-ben, vagyis* **A** *nem cáfolható a $\mathfrak{T}$ elméletben.*

Bizonyítás. (I) Megmutatjuk, hogy ha ω *tetszőleges* értékelése a $\mathfrak{T}$ matematikai nyelvének, akkor az $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$ és $\mathfrak{S}_4$ formula-sémák minden $\mathbf{A}$ elemére $\overline{\omega}(\mathbf{A}) \equiv \mathbf{i}$. Valóban, ha $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ formulák, akkor

$$\begin{gathered}
\overline{\omega}((\mathbf{A} \vee \mathbf{A}) \Rightarrow \mathbf{A}) \equiv \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{A})), \overline{\omega}(\mathbf{A})) \equiv \mathbf{i}, \\
\overline{\omega}(\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A}), \mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{B}))) \equiv \mathbf{i}, \\
\overline{\omega}((\mathbf{A} \vee \mathbf{B}) \Rightarrow (\mathbf{B} \vee \mathbf{A})) \equiv \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{B})), \mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{B}), \overline{\omega}(\mathbf{A}))) \equiv \mathbf{i}, \\
\overline{\omega}((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{C} \vee \mathbf{A}) \Rightarrow (\mathbf{C} \vee \mathbf{B}))) \equiv \\
\equiv \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{B})), \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{C}), \overline{\omega}(\mathbf{A})), \mathfrak{B}_{\vee}(\overline{\omega}(\mathbf{C}), \overline{\omega}(\mathbf{B})))) \equiv \mathbf{i},
\end{gathered}$$

mert egyszerű táblázatok elkészítésével ellenőrizhető, hogy ha $\mathbf{a}, \mathbf{b}, \mathbf{c}$ az $\mathbf{i}$ és $\mathbf{h}$ szimbólumok bármelyikét jelöli, akkor

$$\begin{gathered}
\mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\vee}(\mathbf{a}, \mathbf{a}), \mathbf{a}) \equiv \mathbf{i}, \\
\mathfrak{B}_{\Rightarrow}(\mathbf{a}, \mathfrak{B}_{\vee}(\mathbf{a}, \mathbf{b})) \equiv \mathbf{i}, \\
\mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\vee}(\mathbf{a}, \mathbf{b}), \mathfrak{B}_{\vee}(\mathbf{b}, \mathbf{a})) \equiv \mathbf{i}, \\
\mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\Rightarrow}(\mathbf{a}, \mathbf{b}), \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\vee}(\mathbf{c}, \mathbf{a}), \mathfrak{B}_{\vee}(\mathbf{c}, \mathbf{b}))) \equiv \mathbf{i}.
\end{gathered}$$

Ez azt jelenti, hogy az $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$ és $\mathfrak{S}_4$ axióma-sémák minden $\mathbf{B}$ elemére $\overline{\omega}(\mathbf{B}) \equiv \mathbf{i}$ teljesül.

(II) Megmutatjuk, hogy ha ω *helyettesítés-invariáns* értékelése a $\mathfrak{T}$ matematikai nyelvének, akkor az $\mathfrak{S}_5$ és $\mathfrak{S}_6$ formula-sémák minden $\mathbf{A}$ elemére $\overline{\omega}(\mathbf{A}) \equiv \mathbf{i}$.

Legyen $\mathbf{A}$ formula, $\mathbf{x}$ változó és $\mathbf{T}$ objektum. Ekkor

$$\overline{\omega}(((\mathbf{T}|\mathbf{x})\mathbf{A}) \Rightarrow (\exists\mathbf{x})\mathbf{A}) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}((\mathbf{T}|\mathbf{x})\mathbf{A}), \overline{\omega}((\exists\mathbf{x})\mathbf{A})) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{A})) \equiv \mathbf{i},$$

mert az ω helyettesítés-invarianciája folytán $\overline{\omega}((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv \overline{\omega}(\mathbf{A})$ és $\overline{\omega}((\exists\mathbf{x})\mathbf{A}) \equiv \overline{\omega}(\mathbf{A})$, valamint $\mathfrak{B}_{\Rightarrow}(\mathbf{i},\mathbf{i}) \equiv \mathfrak{B}_{\Rightarrow}(\mathbf{h},\mathbf{h}) \equiv \mathbf{i}$. Ezért az $\mathfrak{S}_5$ axióma-séma minden $\mathbf{B}$ elemére $\overline{\omega}(\mathbf{B}) \equiv \mathbf{i}$.

Legyenek $\mathbf{T}$, $\mathbf{S}$ objektumok, $\mathbf{x}$ változó és $\mathbf{A}$ formula. Ekkor

$$\begin{gathered}\overline{\omega}((\mathbf{T} = \mathbf{S}) \Rightarrow (((\mathbf{T}|\mathbf{x})\mathbf{A}) \Leftrightarrow ((\mathbf{S}|\mathbf{x})\mathbf{A})) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{T} = \mathbf{S}), \mathfrak{B}_{\Leftrightarrow}(\overline{\omega}((\mathbf{T}|\mathbf{x})\mathbf{A}), \overline{\omega}((\mathbf{S}|\mathbf{x})\mathbf{A}))) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{T} = \mathbf{S}), \mathfrak{B}_{\Leftrightarrow}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{A}))) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{T} = \mathbf{S}), \mathbf{i}) \equiv \mathbf{i},\end{gathered}$$

mert az ω helyettesítés-invarianciája folytán $\overline{\omega}((\mathbf{T}|\mathbf{x})\mathbf{A}) \equiv \overline{\omega}((\mathbf{S}|\mathbf{x})\mathbf{A}) \equiv \overline{\omega}(\mathbf{A})$ és $\mathfrak{B}_{\Leftrightarrow}(\mathbf{i},\mathbf{i}) \equiv \mathfrak{B}_{\Leftrightarrow}(\mathbf{h},\mathbf{h}) \equiv \mathbf{i}$, valamint $\mathfrak{B}_{\Rightarrow}(\mathbf{i},\mathbf{i}) \equiv \mathfrak{B}_{\Rightarrow}(\mathbf{h},\mathbf{i}) \equiv \mathbf{i}$.

(III) Megmutatjuk, hogy ha ω olyan helyettesítés-invariáns értékelése a $\mathfrak{T}$ matematikai nyelvének, hogy minden $\mathbf{T}$, $\mathbf{S}$ objektumra $\omega(\mathbf{T} = \mathbf{S}) \equiv \mathbf{i}$, akkor az $\mathfrak{S}_7$ formula-séma minden $\mathbf{C}$ elemére $\overline{\omega}(\mathbf{C}) \equiv \mathbf{i}$.

Legyenek $\mathbf{A}$, $\mathbf{B}$ formulák és $\mathbf{x}$ változó. Ekkor

$$\begin{gathered}\overline{\omega}((\forall\mathbf{x})(\mathbf{A} \Leftrightarrow \mathbf{B}) \Rightarrow (\varepsilon_{\mathbf{x}}(\mathbf{A}) = \varepsilon_{\mathbf{x}}(\mathbf{B}))) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}((\forall\mathbf{x})(\mathbf{A} \Leftrightarrow \mathbf{B})), \overline{\omega}(\varepsilon_{\mathbf{x}}(\mathbf{A}) = \varepsilon_{\mathbf{x}}(\mathbf{B}))) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}((\forall\mathbf{x})(\mathbf{A} \Leftrightarrow \mathbf{B})), \omega(\varepsilon_{\mathbf{x}}(\mathbf{A}) = \varepsilon_{\mathbf{x}}(\mathbf{B}))) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}((\forall\mathbf{x})(\mathbf{A} \Leftrightarrow \mathbf{B})), \mathbf{i}) \equiv \mathbf{i},\end{gathered}$$

mert $\mathfrak{B}_{\Rightarrow}(\mathbf{i},\mathbf{i}) \equiv \mathfrak{B}_{\Rightarrow}(\mathbf{h},\mathbf{i}) \equiv \mathbf{i}$, így az $\mathfrak{S}_7$ axióma-séma minden $\mathbf{C}$ elemére $\overline{\omega}(\mathbf{C}) \equiv \mathbf{i}$.

(IV) Legyen ω az a függvény, amely a $\mathfrak{T}$ matematikai nyelvének *minden* elemi formulájához az $\mathbf{i}$ értéket rendeli. Ekkor az (I), (II) és (III) szerint $\overline{\omega}$ a $\mathfrak{T}$ predikátumkalkulus minden axiómájához az $\mathbf{i}$ értéket rendeli. Ezért az előző tétel szerint $\overline{\omega}$ a $\mathfrak{T}$ minden tételéhez az $\mathbf{i}$ értéket rendeli. Ha $\mathbf{A}$ elemi formulája a $\mathfrak{T}$ matematikai nyelvének, akkor

$$\overline{\omega}(\neg\mathbf{A}) \equiv \mathfrak{B}_{\neg}(\overline{\omega}(\mathbf{A})) \equiv \mathfrak{B}_{\neg}(\mathbf{i}) \equiv \mathbf{h},$$

tehát $\neg\mathbf{A}$ *nem tétel* $\mathfrak{T}$-ben. ■

Vigyázzunk arra, hogy ha $\mathfrak{T}$ predikátumkalkulus, és $\mathbf{A}$ a $\mathfrak{T}$ matematikai nyelvének elemi formulája, akkor nem állítjuk azt, hogy $\mathbf{A}$ *tétel* $\mathfrak{T}$-ben, vagyis hogy $\mathbf{A}$ *bizonyítható* $\mathfrak{T}$-ben; csak annyit mondhatunk, hogy $\neg\mathbf{A}$ *nem tétel* $\mathfrak{T}$-ben, vagyis $\mathbf{A}$ *nem cáfolható* $\mathfrak{T}$-ben. Persze azért vannak olyan elemi formulák, amelyek tételek; ilyen például minden $\mathbf{T} = \mathbf{T}$ alakú egyenlőség, ahol $\mathbf{T}$ tetszőleges objektum.

3.4.3. Állítás. *Ha $\mathfrak{T}$ predikátumkalkulus, és $\mathbf{A}$ a $\mathfrak{T}$ matematikai nyelvének olyan elemi formulája, amely logikai sajátfüggvény-jellel kezdődik (vagyis az első karaktere az $=$ szimbólumtól különböző logikai függvényjel), akkor sem $\mathbf{A}$, sem $\neg\mathbf{A}$ nem tétel $\mathfrak{T}$-ben.*

Bizonyítás. Az előző tétel szerint $\neg\mathbf{A}$ nem tétel $\mathfrak{T}$-ben. Annak bizonyításához, hogy $\mathbf{A}$ sem tétel $\mathfrak{T}$-ben, jelölje ω azt a függvényt, amely az $\mathbf{i}$ értéket rendeli minden olyan elemi formulához, amely az $=$ jellel kezdődik, és a többi elemi formulához a $\mathbf{h}$ értéket rendeli. Ekkor ω nyilvánvalóan olyan értékelés, hogy bármely két $\mathbf{T}$ és $\mathbf{S}$ objektumra $\omega(\mathbf{T} = \mathbf{S}) \equiv \mathbf{i}$. Továbbá, ω helyettesítés-invariáns is, mert egy elemi formula bármely változója helyére objektumot helyettesítve a formula első karaktere nem változik, hiszen a logikai függvényjelek a változóktól különböznek. Ezért az előző állítás bizonyításának (I), (II) és (III) pontja szerint $\overline{\omega}$ a $\mathfrak{T}$ predikátumkalkulus minden axiómájához az $\mathbf{i}$ értéket rendeli, így a $\mathfrak{T}$ matematikai elmélet minden $\mathbf{B}$ tételére $\overline{\omega}(\mathbf{B}) \equiv \mathbf{i}$. Ebből következik, hogy $\mathbf{A}$ nem tétel $\mathfrak{T}$-ben, hiszen $\omega(\mathbf{A}) \equiv \mathbf{h}$. ■

3.4.4. Definíció. *Azt mondjuk, hogy a* $\mathfrak{T}$ *matematikai elmélet* **teljes**, *ha* $\mathfrak{T}$ *minden* **A** *zárt (vagyis változót nem tartalmazó) formulájára* **A** *tétel* $\mathfrak{T}$*-ben, vagy* ¬**A** *tétel* $\mathfrak{T}$*-ben.*

Az előző állításból következik, hogy ha a $\mathfrak{T}$ predikátumkalkulus nyelvében van logikai sajátfüggvény, akkor $\mathfrak{T}$ *nem teljes* matematikai elmélet, mert ekkor létezik olyan zárt elemi formula, amely logikai sajátfüggvény-jellel kezdődik. Valóban, ha **B** tetszőleges olyan elemi formula, amely logikai sajátfüggvény-jellel kezdődik, és $\mathbf{x}_1, \cdots, \mathbf{x}_n$ a **B**-ben szereplő változók, akkor az $\mathbf{A} \equiv (\exists \mathbf{x}_n)\,(\cdots((\exists \mathbf{x}_2)\,((\exists \mathbf{x}_1)\mathbf{B}))\cdots)$ formula zárt, és az első karaktere megegyezik **B** első karakterével, tehát **A** olyan zárt elemi formula, amely logikai sajátfüggvény-jellel kezdődik, így sem **A**, sem ¬**A** nem tétel $\mathfrak{T}$-ben.

3.4.5. Tétel. *Minden predikátumkalkulus ellentmondásmentes.*

Bizonyítás. A 3.4.2. állítás szerint minden predikátumkalkulusnak van olyan formulája, amely *nem tétel*, ezért az elmélet nem lehet ellentmondásos. ■

Ez a tétel azt mutatja, hogy egy matematikai elmélet esetleges ellentmondásosságának egyedüli oka az elmélet matematikai axióma-sémáiban és az explicit axiómáiban keresendő. Tehát ha egy matematikai elmélet ellentmondásosnak bizonyul, és ki akarjuk deríteni az ellentmondásosságának okát, akkor azt tehetjük, hogy egymás után töröljük az elmélet matematikai axióma-sémáit és explicit axiómáit, és minden lépésben ellenőrizzük, hogy a törlés után nyert *maradék matematikai axiómarendszer* ellentmondásmentes elméletet határoz-e meg? Az *összes* explicit axiómát és matematikai axióma-sémát törölve a matematikai elmélet alatt fekvő predikátumkalkulushoz jutunk, amely az előző tétel szerint biztosan ellentmondásmentes. Ha valamelyik törlés után már ellentmondásmentes az elmélet, akkor az ellentmondásosságot az addig törölt explicit axiómák vagy matematikai axióma-sémák valamelyike okozza.

4. fejezet

A halmazelmélet logikai alapjai

4.1. A halmazelmélet értelmezése

A *halmazelmélet* ($\mathfrak{Ens}$) egy speciális *formális axiomatikus matematikai elmélet*, amelynek pontos meghatározásához rögzíteni kell a matematikai függvényeit, a logikai sajátfüggvényeit, a matematikai axióma-sémáit, valamint az explicit axiómáit. Először a halmazelmélet formális matematikai nyelvét rögzítjük.

4.1.1. Definíció. *A* **halmazelmélet nyelvének** *nevezzük azt a formális matematikai nyelvet, amelynek az $=$ szimbólumon kívül az egyetlen logikai függvénye az $\in$ szimbólummal jelölt kétváltozós logikai függvény, és nincs matematikai függvénye, így konstansa sincs.*

Tehát, ha $\mathbf{T}$ és $\mathbf{S}$ objektumok a halmazelmélet nyelvében, akkor az $\in \mathbf{TS}$ (vagyis infix jelölést alkalmazva: $\mathbf{T} \in \mathbf{S}$) a halmazelméletnek formulája lesz; ezt a formulát úgy mondjuk ki, hogy "$\mathbf{T}$ *eleme* $\mathbf{S}$*-nek*". Ha $\mathbf{T}$ és $\mathbf{S}$ objektumok a halmazelmélet nyelvében, akkor rendszerint a $\mathbf{T} \notin \mathbf{S}$ infix jelölést alkalmazzuk a $\neg \in \mathbf{TS}$ formulára, és ezt úgy mondjuk ki, hogy "$\mathbf{T}$ *nem eleme* $\mathbf{S}$*-nek*".

Megjegyezzük, hogy a halmazelmélet nyelvének objektumait általában *halmazoknak* nevezzük: ez lehet a halmaz fogalmának *formális értelmezése*. Tehát amikor a halmazelméletben azt mondjuk, hogy "$\mathbf{T}$ *halmaz*", akkor ez azt jelenti, hogy "$\mathbf{T}$ *objektuma a halmazelmélet nyelvének*".

Figyeljük meg, hogy a halmazokat nem úgy értelmeztük, mint "matematikai objektumok összessége", hiszen ilyen definícióhoz szükség volna a "matematikai objektum" és az "összesség" fogalmának pontos (formális nyelvi) megfogalmazására, és ezek nem állnak a rendelkezésünkre. Azonban később (a $\{\cdot|\cdot\}$-objektumok értelmének vizsgálata után) világossá válik, hogy minden halmaz felfogható úgy, mint a saját elemeinek összessége.

A halmazelméletnek egyetlen matematikai axióma-sémája és hat explicit axiómája van. Itt az explicit axiómáknak csak rövid, de pontos felsorolását adjuk; azok részletezésére később, az **5.**, **6.** és **7.** fejezetekben kerül sor. Először csak két matematikai axiómát vizsgálunk közelebbről: a *meghatározottsági axiómát* és a *részhalmaz axióma-sémát.*

A halmazelmélet első explicit axiómája a *meghatározottsági axióma*, amely kapcsolatot teremt az $\in$ és $=$ logikai függvények között.

4.1.2. Definíció. Meghatározottsági axiómának *nevezzük a*

$$(\forall x)(\forall y)(\ (\forall z)((z \in x)\Leftrightarrow(z \in y))\ \Rightarrow\ x = y\ )$$

formulát.

A definíció alapján nyilvánvaló, hogy a meghatározottsági axióma egyetlen konkrét formula a halmazelmélet nyelvében, amelyben egyetlen változó sem szerepel.

4.1.3. Állítás. *Ha* $\mathbf{x}$*,* $\mathbf{y}$ *és* $\mathbf{z}$ *különböző változók, akkor a*

$$(\forall\mathbf{x})(\forall\mathbf{y})(\ (\forall\mathbf{z})((\mathbf{z}\in\mathbf{x})\Leftrightarrow(\mathbf{z}\in\mathbf{y}))\ \Rightarrow\ \mathbf{x}=\mathbf{y}\ )$$

formula azonos a meghatározottsági axiómával.

Bizonyítás. Válasszunk olyan $\mathbf{x}'$, $\mathbf{y}'$ és $\mathbf{z}'$ különböző változókat, amelyek az $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{z}$ változók mindegyikétől különböznek, és vezessük be a következő formulákat:

$$\mathbf{A} \overset{\text{def}}{\equiv} (\forall\mathbf{z})((\mathbf{z}\in\mathbf{x})\Leftrightarrow(\mathbf{z}\in\mathbf{y})) \Rightarrow (\mathbf{x}=\mathbf{y}),$$
$$\mathbf{A}' \overset{\text{def}}{\equiv} (\forall\mathbf{z}')((\mathbf{z}'\in\mathbf{x}')\Leftrightarrow(\mathbf{z}'\in\mathbf{y}')) \Rightarrow (\mathbf{x}'=\mathbf{y}').$$

Azt kell igazolni, hogy $(\forall\mathbf{x})(\forall\mathbf{y})\mathbf{A}\equiv(\forall\mathbf{x}')(\forall\mathbf{y}')\mathbf{A}'$. Az $\mathbf{x}'$ változó különbözik az $\mathbf{x}$ és $\mathbf{y}$ változóktól, így $\mathbf{x}'$ nem szerepel az $\mathbf{A}$ formulában, tehát a $(\forall\mathbf{y})\mathbf{A}$ formulában sem szerepel. Ebből a kvantoros kifejezésekre vonatkozó helyettesítések tranzitivitásának szabálya szerint következik, hogy $(\forall\mathbf{x})(\forall\mathbf{y})\mathbf{A}\equiv(\forall\mathbf{x}')((\mathbf{x}'|\mathbf{x})(\forall\mathbf{y})\mathbf{A})$. Ugyanakkor, $\mathbf{x}$ és $\mathbf{y}$ különbözőek, valamint $\mathbf{y}$ és $\mathbf{x}'$ is különbözőek, tehát $\mathbf{y}$ nem szerepel az $\mathbf{x}'$ kifejezésben, így a kvantoros kifejezésekre vonatkozó helyettesítés szabálya szerint $(\mathbf{x}'|\mathbf{x})(\forall\mathbf{y})\mathbf{A}\equiv(\forall\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})$. Az $\mathbf{y}'$ változó nem szerepel a $(\mathbf{x}'|\mathbf{x})\mathbf{A}$ formulában, így a kvantoros kifejezésekre vonatkozó helyettesítések tranzitivitásának szabályát alkalmazva kapjuk, hogy $(\forall\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})\equiv(\forall\mathbf{y}')((\mathbf{y}'|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A}))$. Ez azt jelenti, hogy

$$(\forall\mathbf{x})(\forall\mathbf{y})\mathbf{A}\equiv(\forall\mathbf{x}')(\forall\mathbf{y}')((\mathbf{y}'|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})),$$

így elegendő azt belátni, hogy $(\mathbf{y}'|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})\equiv\mathbf{A}'$. Az $\mathbf{A}$ formula definíciója szerint

$$(\mathbf{y}'|\mathbf{y})((\mathbf{x}'|\mathbf{x})\mathbf{A})\equiv(\mathbf{y}'|\mathbf{y})((\mathbf{x}'|\mathbf{x})(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x})\Leftrightarrow(\mathbf{z}\in\mathbf{y})))\Rightarrow(\mathbf{x}'=\mathbf{y}'),$$

ezért elegendő azt bizonyítani, hogy

$$(\mathbf{y}'|\mathbf{y})((\mathbf{x}'|\mathbf{x})(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x})\Leftrightarrow(\mathbf{z}\in\mathbf{y})))\equiv(\forall\mathbf{z}')((\mathbf{z}'\in\mathbf{x}')\Leftrightarrow(\mathbf{z}'\in\mathbf{y}')). \qquad (*)$$

Az $\mathbf{x}$ és $\mathbf{z}$ változók különbözőek, valamint $\mathbf{z}$ és $\mathbf{x}'$ is különbözőek, tehát $\mathbf{z}$ nwm szerepel az $\mathbf{x}'$ kifejezésben, így a kvantoros kifejezésekre vonatkozó helyettesítés szabálya szerint

$$(\mathbf{x}'|\mathbf{x})(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x})\Leftrightarrow(\mathbf{z}\in\mathbf{y}))\equiv(\forall\mathbf{z})((\mathbf{x}'|\mathbf{x})((\mathbf{z}\in\mathbf{x})\Leftrightarrow(\mathbf{z}\in\mathbf{y})))\equiv(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y})).$$

Ebből következik, hogy

$$(\mathbf{y}'|\mathbf{y})((\mathbf{x}'|\mathbf{x})(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x})\Leftrightarrow(\mathbf{z}\in\mathbf{y})))\equiv(\mathbf{y}'|\mathbf{y})(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y})).$$

Az $\mathbf{y}$ és $\mathbf{z}$ változók különbözőek, valamint $\mathbf{z}$ és $\mathbf{y}'$ is különbözőek, tehát $\mathbf{z}$ nem szerepel az $\mathbf{y}'$ kifejezésben, így a kvantoros kifejezésekre vonatkozó helyettesítés szabálya szerint

$$(\mathbf{y}'|\mathbf{y})(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y}))\equiv(\forall\mathbf{z})((\mathbf{y}'|\mathbf{y})((\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y})))\equiv(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y}')).$$

Végül, a $\mathbf{z}'$ változó nem szerepel a $(\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y}')$ formulában, hiszen $\mathbf{z}'$ a $\mathbf{z}$, $\mathbf{x}'$ és $\mathbf{y}'$ változóktól különbözik, ezért a kvantoros kifejezésekre vonatkozó helyettesítések tranzitivitásának szabályát alkalmazva kapjuk, hogy

$$(\forall\mathbf{z})((\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y}'))\equiv(\forall\mathbf{z}')((\mathbf{z}'|\mathbf{z})((\mathbf{z}\in\mathbf{x}')\Leftrightarrow(\mathbf{z}\in\mathbf{y}')))\equiv(\forall\mathbf{z}')((\mathbf{z}'\in\mathbf{x}')\Leftrightarrow(\mathbf{z}'\in\mathbf{y}')).$$

Ezzel az $(*)$ összefüggést igazoltuk. ■

4.1.4. Állítás. *Jelölje* $\mathfrak{T}$ *azt az elméletet, amelynek nyelve a halmazelmélet nyelve, és egyetlen explicit axiómája a meghatározottsági axióma. Ha* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumok a halmazelmélet nyelvében, és* $\mathbf{x}$ *olyan változó, amely nem szerepel sem* $\mathbf{T}$*-ben, sem* $\mathbf{S}$*-ben, akkor a*

$$(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{S})) \;\Rightarrow\; \mathbf{T} = \mathbf{S}$$

formula tétel $\mathfrak{T}$*-ben.*

Bizonyítás. Legyenek $\mathbf{x}'$ és $\mathbf{y}'$ olyan különböző változók a halmazelmélet nyelvében, amelyek $\mathbf{x}$-től is különböznek, és nem szerepelnek sem $\mathbf{T}$-ben, sem $\mathbf{S}$-ben. A

$$(\forall \mathbf{x}')(\forall \mathbf{y}')(\; (\forall \mathbf{x})((\mathbf{x} \in \mathbf{x}') \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\Rightarrow\; \mathbf{x}' = \mathbf{y}' \;)$$

formula azonos a meghatározottsági axiómával, így tétel $\mathfrak{T}$-ben. Az univerzális kvantor logikai alaptulajdonsága miatt ebből kapjuk, hogy a

$$(\mathbf{T}|\mathbf{x}')(\forall \mathbf{y}')(\; (\forall \mathbf{x})((\mathbf{x} \in \mathbf{x}') \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\Rightarrow\; \mathbf{x}' = \mathbf{y}' \;)$$

formula tétel $\mathfrak{T}$-ben. Mivel $\mathbf{x}'$ és $\mathbf{y}'$ különböző változók, és $\mathbf{y}'$ nem szerepel $\mathbf{T}$-ben így a kvantoros kifejezésekben alkalmazható helyettesítési szabály szerint ez a formula azonos a

$$(\forall \mathbf{y}')(\; (\mathbf{T}|\mathbf{x}')(\forall \mathbf{x})((\mathbf{x} \in \mathbf{x}') \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\Rightarrow\; (\mathbf{T}|\mathbf{x}')(\mathbf{x}' = \mathbf{y}') \;)$$

formulával. Mivel $\mathbf{x}'$ és $\mathbf{x}$ különböző változók és $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben, így a kvantoros kifejezésekben alkalmazható helyettesítési szabály szerint

$$(\mathbf{T}|\mathbf{x}')(\forall \mathbf{x})((\mathbf{x} \in \mathbf{x}') \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\equiv\; (\forall \mathbf{x})\,((\mathbf{T}|\mathbf{x}')((\mathbf{x} \in \mathbf{x}') \Leftrightarrow (\mathbf{x} \in \mathbf{y}')))\,.$$

Világos, hogy $(\mathbf{T}|\mathbf{x}')((\mathbf{x} \in \mathbf{x}') \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \equiv (\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{y}')$, ugyanakkor nyilvánvaló, hogy $(\mathbf{T}|\mathbf{x}')(\mathbf{x}' = \mathbf{y}') \equiv \mathbf{T} = \mathbf{y}'$. Mindez azt jelenti, hogy a

$$(\forall \mathbf{y}')(\; (\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\Rightarrow\; (\mathbf{T} = \mathbf{y}') \;)$$

formula tétel $\mathfrak{T}$-ben. Az univerzális kvantor logikai alaptulajdonsága miatt ebből kapjuk, hogy a

$$(\mathbf{S}|\mathbf{y}')(\; (\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\Rightarrow\; (\mathbf{T} = \mathbf{y}') \;)$$

formula tétel $\mathfrak{T}$-ben, vagyis

$$(\mathbf{S}|\mathbf{y}')(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\Rightarrow\; (\mathbf{S}|\mathbf{y}')(\mathbf{T} = \mathbf{y}')$$

tétel $\mathfrak{T}$-ben. Az $\mathbf{y}'$ és $\mathbf{x}$ változók különbözőek és $\mathbf{x}$ nem szerepel $\mathbf{S}$-ben, ezért a kvantoros kifejezésekben alkalmazható helyettesítési szabály szerint

$$(\mathbf{S}|\mathbf{y}')(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;\equiv\; (\forall \mathbf{x})(\; (\mathbf{S}|\mathbf{y}')((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \;).$$

Az $\mathbf{y}'$ változó nem szerepel $\mathbf{T}$-ben, így $(\mathbf{S}|\mathbf{y}')((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{y}')) \equiv (\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{S})$, és ugyanezen okból kifolyólag $(\mathbf{S}|\mathbf{y}')(\mathbf{T} = \mathbf{y}') \equiv (\mathbf{T} = \mathbf{S})$. Ez azt jelenti, hogy a $(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{S})) \Rightarrow (\mathbf{T} = \mathbf{S})$ formula tétel a $\mathfrak{T}$ elméletben. ■

4.1.5. Állítás. *Legyenek* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumok a halmazelmélet nyelvében. Ha* $\mathbf{x}$ *olyan változó a halmazelmélet nyelvében, amely nem szerepel sem* $\mathbf{T}$*-ben, sem* $\mathbf{S}$*-ben, akkor a*

$$(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S}))$$

formula független $\mathbf{x}$*-től, tehát ha* $\mathbf{x}'$ *szintén olyan változó a halmazelmélet nyelvében, amely nem szerepel sem* $\mathbf{T}$*-ben, sem* $\mathbf{S}$*-ben, akkor*

$$(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S})) \;\equiv (\forall \mathbf{x}')((\mathbf{x}' \in \mathbf{T}) \Rightarrow (\mathbf{x}' \in \mathbf{S})).$$

Bizonyítás. Ha $\mathbf{x}$ és $\mathbf{x}'$ olyan különböző változók, amelyek nem szerepelnek sem $\mathbf{T}$-ben, sem $\mathbf{S}$-ben, akkor $\mathbf{x}'$ nem szerepel az $(\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S})$ formulában, tehát alkalmazva a helyettesítés szabályát az univerzális kvantorra kapjuk, hogy

$$(\forall\mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S})) \;\equiv\; (\forall\mathbf{x}')\,((\mathbf{x}'|\mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S}))) \;\equiv$$
$$\equiv\; (\forall\mathbf{x}')((\mathbf{x}' \in \mathbf{T}) \Rightarrow (\mathbf{x}' \in \mathbf{S})). \;\blacksquare$$

4.1.6. Definíció. *Ha* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumok a halmazelmélet nyelvében, akkor*

$$\mathbf{T} \subseteq \mathbf{S}$$

jelöli a $(\forall\mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S}))$ *formulát, ahol* $\mathbf{x}$ *tetszőleges olyan változó a halmazelmélet nyelvében, amely nem szerepel sem* $\mathbf{T}$*-ben, sem* $\mathbf{S}$*-ben, továbbá a* $\mathbf{T} \subseteq \mathbf{S}$ *formulát úgy mondjuk ki, hogy "***$\mathbf{T}$ részhalmaza $\mathbf{S}$***-nek".*

4.1.7. Állítás. *Jelölje* $\mathfrak{T}$ *azt az elméletet, amelynek nyelve a halmazelmélet nyelve, és egyetlen explicit axiómája a meghatározottsági axióma. Ha* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumok a halmazelmélet nyelvében, akkor a*

$$((\mathbf{T} \subseteq \mathbf{S}) \wedge (\mathbf{S} \subseteq \mathbf{T})) \;\Rightarrow\; \mathbf{T} = \mathbf{S}$$

formula tétel $\mathfrak{T}$*-ben.*

Bizonyítás. A dedukció-tétel alapján elég azt bizonyítani, hogy ha $\mathfrak{T}'$ jelöli a $\mathfrak{T}[(\mathbf{T} \subseteq \mathbf{S}) \wedge (\mathbf{S} \subseteq \mathbf{T})]$ elméletet, akkor $\mathbf{T} = \mathbf{S}$ tétel $\mathfrak{T}'$-ben. A $(\mathbf{T} \subseteq \mathbf{S}) \wedge (\mathbf{S} \subseteq \mathbf{T})$ formula tétel (sőt explicit axióma) $\mathfrak{T}'$-ben, ugyanakkor, ha $\mathbf{x}$ olyan változó a halmazelmélet nyelvében, amely nem szerepel sem $\mathbf{T}$-ben, sem $\mathbf{S}$-ben, akkor

$$(\mathbf{T} \subseteq \mathbf{S}) \wedge (\mathbf{S} \subseteq \mathbf{T}) \;\equiv\; (\forall\mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S})) \wedge (\forall\mathbf{x})((\mathbf{x} \in \mathbf{S}) \Rightarrow (\mathbf{x} \in \mathbf{T})).$$

Tudjuk, hogy a

$$(\forall\mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S})) \wedge (\forall\mathbf{x})((\mathbf{x} \in \mathbf{S}) \Rightarrow (\mathbf{x} \in \mathbf{T})) \Leftrightarrow$$
$$\Leftrightarrow (\forall\mathbf{x})(((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S})) \wedge ((\mathbf{x} \in \mathbf{S}) \Rightarrow (\mathbf{x} \in \mathbf{T})))$$

formula logikai tétel $\mathfrak{T}'$-ben, és az ekvivalencia definíciója szerint

$$((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{S})) \wedge ((\mathbf{x} \in \mathbf{S}) \Rightarrow (\mathbf{x} \in \mathbf{T})) \;\equiv\; (\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{S}),$$

tehát $(\forall\mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{S}))$ tétel $\mathfrak{T}'$-ben. Mivel a megatározottsági axióma miatt $(\forall\mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathbf{S})) \Rightarrow (\mathbf{T} = \mathbf{S})$ tétel $\mathfrak{T}$-ben, tehát $\mathfrak{T}'$-ben is, így a leválasztás szabályának alkalmazásával nyerjük, hogy $\mathbf{T} = \mathbf{S}$ tétel a $\mathfrak{T}'$ elméletben. $\blacksquare$

Most részletesen megvizsgáljuk a halmazelmélet egyik alapvetően fontos formális nyelvi konstrukcióját.

4.1.8. Állítás. *Ha* $\mathbf{x}$ *változó és* $\mathbf{A}$ *formula a halmazelmélet nyelvében, valamint* $\mathbf{y}$ *tetszőleges* $\mathbf{x}$*-től különböző,* $\mathbf{A}$*-ban nem szereplő változó, akkor az*

$$\varepsilon_{\mathbf{y}}((\forall\mathbf{x})((\mathbf{x} \in \mathbf{y}) \Leftrightarrow \mathbf{A}))$$

objektum független $\mathbf{y}$*-tól, vagyis ha* $\mathbf{y}'$ *szintén* $\mathbf{x}$*-től különböző,* $\mathbf{A}$*-ban nem szereplő változó, akkor*

$$\varepsilon_{\mathbf{y}}((\forall\mathbf{x})((\mathbf{x} \in \mathbf{y}) \Leftrightarrow \mathbf{A})) \equiv \varepsilon_{\mathbf{y}'}((\forall\mathbf{x})((\mathbf{x} \in \mathbf{y}') \Leftrightarrow \mathbf{A})).$$

Bizonyítás. A helyettesítések szabályát, valamint a helyettesítések tranzitivitásának szabályát alkalmazva a kvantoros kifejezésekre

$$(\mathbf{y}'|\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A})\equiv(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y}')\Leftrightarrow\mathbf{A})$$

adódik, mert $\mathbf{y}$ és $\mathbf{y}'$ különböznek $\mathbf{x}$-től és nem szerepelnek az $\mathbf{A}$ formulában. Ezért a helyettesítések tranzitivitásának szabályát alkalmazva az ε-kifejezésekre kapjuk, hogy

$$\varepsilon_{\mathbf{y}}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}))\equiv\varepsilon_{\mathbf{y}'}((\mathbf{y}'|\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}))\equiv\varepsilon_{\mathbf{y}'}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{y}')\Leftrightarrow\mathbf{A})),$$

mert $\mathbf{y}'$ nem szerepel a $(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A})$ formulában. ■

4.1.9. Definíció. *Ha* $\mathbf{A}$ *formulája és* $\mathbf{x}$ *változója halmazelmélet nyelvének, valamint* $\mathbf{y}$ *tetszőleges* $\mathbf{x}$*-től különböző,* $\mathbf{A}$*-ben nem szereplő változó, akkor megállapodás szerint az* $\varepsilon_{\mathbf{y}}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A})))$ *objektumot az*

$$\{\mathbf{x}|\mathbf{A}\}$$

szimbólummal jelöljük. Az ilyen alakú objektumokat $\{\cdot|\cdot\}$**-objektumoknak** (*kiejtve:* **zárójel-objektumoknak**) *nevezzük.*

Vegyük észre, hogy egy $\{\mathbf{x}|\mathbf{A}\}$ alakú objektumban az $\mathbf{x}$ változó *nem szerepel*, de az $\mathbf{x}$-től lényegesen függ! Másként fogalmazva: ha veszünk egy $\mathbf{x}$-től különböző $\mathbf{x}'$ változót, akkor az $\{\mathbf{x}|\mathbf{A}\}$ és $\{\mathbf{x}'|\mathbf{A}\}$ objektumok teljesen különbözőek lehetnek. A definíció alapján nyilvánvaló, hogy ha $\mathbf{A}$ formula és $\mathbf{x}$ változó a halmazelmélet nyelvében, akkor az $\{\mathbf{x}|\mathbf{A}\}$ objektumban azok és csak azok a változók szerepelnek, amelyek $\mathbf{x}$-től különböznek és $\mathbf{A}$-ban szerepelnek.

Figyeljük meg, hogy az $\{\mathbf{x}|\mathbf{A}\}$ alakú kifejezéseket az előzőek mintájára értelmezhettük volna a halmazelmélet nyelvének tetszőleges $\mathbf{A}$ *kifejezésére* (tehát nem csak formulájára) és $\mathbf{x}$ változójára. Azonban ekkor az $\{\mathbf{x}|\mathbf{A}\}$ kifejezés nem szükségképpen *objektum*, és éppen az a célunk, hogy a halmazelmélet egy fontos objektum-típusát vezessük be.

Természetesen felvetődik a kérdés, hogy ha $\mathbf{A}$ formulája és $\mathbf{x}$ változója a halmazelmélet nyelvének, akkor mi az $\{\mathbf{x}|\mathbf{A}\}$ objektum *értelme*? Bármely matematikai elméletben az objektumoknak *jelentést* az elmélet igazság-fogalma (tehát axiomatikus elméletben az axiómarendszer) ad, ezért erre a kérdésre mindaddig nem adhatunk választ, amíg nem rögzítettük a halmazelmélet axiómarendszerét. Előrebocsátjuk, hogy a $\{\cdot|\cdot\}$-objektumok a legfontosabb halmazelméleti objektumok, mert a mindennapi matematikai gyakorlatban szinte mindig ilyeneket képezünk, és ilyenek tulajdonságai vizsgáljuk. Most megfogalmazunk néhány szintaktikus (vagyis formális nyelvi) szabályt a $\{\cdot|\cdot\}$-objektumokkal kapcsolatban.

4.1.10. Állítás. (**A helyettesítés szabálya** $\{\cdot|\cdot\}$**-objektumokban**.) *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$*,* $\mathbf{y}$ *különböző változók a halmazelmélet nyelvében. Ha* $\mathbf{T}$ *olyan objektum, amelyben* $\mathbf{x}$ *nem szerepel, akkor*

$$(\mathbf{T}|\mathbf{y})\{\mathbf{x}|\mathbf{A}\}\equiv\{\mathbf{x}|(\mathbf{T}|\mathbf{y})\mathbf{A}\}.$$

Bizonyítás. Legyen $\mathbf{z}$ olyan változó, amely különbözik $\mathbf{x}$-től és $\mathbf{y}$-tól, valamint nem szerepel $\mathbf{A}$-ban és $\mathbf{T}$-ben. Ekkor a helyettesítés szabályát alkalmazva az ε-kifejezésekre és a kvantoros kifejezésekre kapjuk, hogy

$$(\mathbf{T}|\mathbf{y})\{\mathbf{x}|\mathbf{A}\}\equiv(\mathbf{T}|\mathbf{y})\varepsilon_{\mathbf{z}}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{z})\Leftrightarrow\mathbf{A}))\equiv\varepsilon_{\mathbf{z}}((\mathbf{T}|\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{z})\Leftrightarrow\mathbf{A}))\equiv$$
$$\equiv\varepsilon_{\mathbf{z}}((\forall\mathbf{x})((\mathbf{T}|\mathbf{y})((\mathbf{x}\in\mathbf{z})\Leftrightarrow\mathbf{A})))\equiv\varepsilon_{\mathbf{z}}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{z})\Leftrightarrow(\mathbf{T}|\mathbf{y})\mathbf{A}))\equiv\{\mathbf{x}|(\mathbf{T}|\mathbf{y})\mathbf{A}\},$$

hiszen $\mathbf{z}$ nem szerepel a $(\mathbf{T}|\mathbf{y})\mathbf{A}$ formulában. ■

4.1.11. Állítás. (**A helyettesítések tranzitivitásának szabálya** $\{\cdot|\cdot\}$**-objektumokban**.) *Legyen* $\mathbf{A}$ *formula és* $\mathbf{x}$ *változó a halmazelmélet nyelvében. Ha az* $\mathbf{x}'$ *változó nem szerepel* $\mathbf{A}$*-ban, akkor*

$$\{\mathbf{x}|\mathbf{A}\} \equiv \{\mathbf{x}'|(\mathbf{x}'|\mathbf{x})\mathbf{A}\}.$$

Bizonyítás. Legyen $\mathbf{y}$ olyan változó, amely $\mathbf{x}$-től és $\mathbf{x}'$-től különbözik, valamint nem szerepel $\mathbf{A}$-ban. A helyettesítések tranzitivitásának szabályát alkalmazva a kvantoros kifejezésekre kapjuk, hogy

$$(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Rightarrow\mathbf{A}) \equiv (\forall\mathbf{x}')(\mathbf{x}'|\mathbf{x})((\mathbf{x}\in\mathbf{y})\Rightarrow\mathbf{A}) \equiv (\forall\mathbf{x}')((\mathbf{x}'\in\mathbf{y})\Rightarrow(\mathbf{x}'|\mathbf{x})\mathbf{A}),$$

mert $\mathbf{x}'$ nem szerepel az $(\mathbf{x}\in\mathbf{y})\Rightarrow\mathbf{A}$ formulában. Ebből a $\{\cdot|\cdot\}$-objektumok definíciója alapján következik, hogy

$$\{\mathbf{x}|\mathbf{A}\} \equiv \varepsilon_{\mathbf{y}}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Rightarrow\mathbf{A})) \equiv \varepsilon_{\mathbf{y}}((\forall\mathbf{x}')((\mathbf{x}'\in\mathbf{y})\Rightarrow(\mathbf{x}'|\mathbf{x})\mathbf{A})) \equiv \{\mathbf{x}'|(\mathbf{x}'|\mathbf{x})\mathbf{A}\},$$

amit bizonyítani kellett. ■

4.1.12. Állítás. *Legyen* $\mathbf{A}$ *formulája és* $\mathbf{x}$ *változója a halmazelmélet nyelvének. Ha* $\mathbf{y}$ *tetszőleges* $\mathbf{x}$*-től különböző,* $\mathbf{A}$*-ban nem szereplő változó, akkor a*

$$(\exists\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A})$$

formula független $\mathbf{y}$*-tól, vagyis ha* $\mathbf{y}'$ *szintén olyan változó, amely* $\mathbf{x}$*-től különbözik és nem szerepel* $\mathbf{A}$*-ban, akkor*

$$(\exists\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}) \equiv (\exists\mathbf{y}')(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y}')\Leftrightarrow\mathbf{A}).$$

Bizonyítás. A helyettesítések szabályát, valamint a helyettesítések tranzitivitásának szabályát alkalmazva a kvantoros kifejezésekre

$$(\exists\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A})\equiv(\exists\mathbf{y}')((\mathbf{y}'|\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}))\equiv(\exists\mathbf{y}')(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y}')\Leftrightarrow\mathbf{A}),$$

amit bizonyítani kellett. ■

Most bevezetjük azokat a formulákat, amelyek segítségével halmazelméleti értelmet lehet adni a $\{\cdot|\cdot\}$-objektumoknak.

4.1.13. Definíció. *Ha* $\mathbf{A}$ *formulája és* $\mathbf{x}$ *változója a halmazelmélet nyelvének, valamint* $\mathbf{y}$ *tetszőleges* $\mathbf{x}$*-től különböző,* $\mathbf{A}$*-ban nem szereplő változó, akkor megállapodás szerint a* $(\exists\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A})$ *formulát a*

$$\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$$

szimbólummal jelöljük.

Már most megjegyezzük, hogy ha $\mathbf{A}$ formulája és $\mathbf{x}$ változója a halmazelmélet nyelvének, akkor azt fogjuk mondani, hogy $\mathbf{A}$ *kollektivizáló az* $\mathbf{x}$ *változóban*, ha a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula *tétel a halmazelméletben.* A halmazelmélet kifejtésének jelenlegi szintjén ez az elnevezés még nem használható, mert nem mondtuk meg, hogy mik a halmazelmélet axiómái, tehát azt sem tudhatjuk, hogy mik a tételek a halmazelméletben. Azonban $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ egyszerű formális nyelvi konstrukcióval képezhető formula, vagyis az előállításához semmiféle axióma vagy igazság-fogalom ismerete nem szükséges.

4.1.14. Állítás. *Legyen* $\mathbf{A}$ *formulája és* $\mathbf{x}$ *változója a halmazelmélet nyelvének. Ha* $\mathbf{T}$ *objektuma és* $\mathbf{y}$ *olyan változója a halmazelmélet nyelvének, hogy* $\mathbf{x}$ *és* $\mathbf{y}$ *különbözőek, és* $\mathbf{x}$ *nem szerepel* $\mathbf{T}$*-ben, akkor*

$$(\mathbf{T}|\mathbf{y})\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}) \equiv \mathfrak{Coll}_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A}).$$

Ha $\mathbf{x}'$ *olyan változó, amely* $\mathbf{A}$*-ban nem szerepel, akkor*

$$\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}) \equiv \mathfrak{Coll}_{\mathbf{x}'}((\mathbf{x}'|\mathbf{x})\mathbf{A}).$$

Bizonyítás. Legyen $\mathbf{z}$ olyan változó, amely $\mathbf{x}$-től és $\mathbf{y}$-tól különbözik, valamint nem szerepel $\mathbf{A}$-ban és $\mathbf{T}$-ben. Ekkor a kvantoros kifejezésekre vonatkozó helyettesítés tételét kétszer alkalmazva, és felhasználva a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ és $\mathfrak{Coll}_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A})$ formulák értelmezését kapjuk, hogy

$$(\mathbf{T}|\mathbf{y})\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}) \equiv (\mathbf{T}|\mathbf{y})(\exists\mathbf{z})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{z})\Leftrightarrow\mathbf{A}) \equiv (\exists\mathbf{z})((\mathbf{T}|\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{z})\Leftrightarrow\mathbf{A})) \equiv$$
$$\equiv (\exists\mathbf{z})(\forall\mathbf{x})((\mathbf{T}|\mathbf{y})((\mathbf{x}\in\mathbf{z})\Leftrightarrow\mathbf{A})) \equiv (\exists\mathbf{z})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{z})\Leftrightarrow(\mathbf{T}|\mathbf{y})\mathbf{A}) \equiv \mathfrak{Coll}_{\mathbf{x}}((\mathbf{T}|\mathbf{y})\mathbf{A}),$$

hiszen $\mathbf{z}$ nem szerepel a $(\mathbf{T}|\mathbf{x})\mathbf{A}$ formulában sem.

Legyen $\mathbf{x}'$ olyan változó, amely $\mathbf{A}$-ban nem szerepel, és vegyünk olyan $\mathbf{y}$ változót, amely különbözik $\mathbf{x}$-től és $\mathbf{x}'$-től, valamint nem szerepel $\mathbf{A}$-ban. Ekkor a helyettesítések tranzitivitásának szabályát alkalmazva a kvantoros kifejezésekre, továbbá felhasználva a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ és $\mathfrak{Coll}_{\mathbf{x}'}((\mathbf{x}'|\mathbf{x})\mathbf{A})$ formulák definícióját kapjuk, hogy

$$\mathfrak{Coll}_{\mathbf{x}'}((\mathbf{x}'|\mathbf{x})\mathbf{A})\equiv(\exists\mathbf{y})(\forall\mathbf{x}')((\mathbf{x}'\in\mathbf{y})\Leftrightarrow(\mathbf{x}'|\mathbf{x})\mathbf{A})\equiv(\exists\mathbf{y})(\forall\mathbf{x}')((\mathbf{x}'|\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}))\equiv$$
$$\equiv (\exists\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}) \equiv \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}),$$

hiszen a feltevések szerint $\mathbf{x}'$ nem szerepel az $(\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}$ formulában. ■

4.1.15. Állítás. *Ha* $\mathbf{A}$ *formulája és* $\mathbf{x}$ *változója a halmazelmélet nyelvének, akkor*

$$\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}) \equiv (\forall\mathbf{x})((\mathbf{x}\in\{\mathbf{x}|\mathbf{A}\})\Leftrightarrow\mathbf{A}).$$

Bizonyítás. Legyen $\mathbf{y}$ olyan változó, amely $\mathbf{x}$-től különbözik és nem szerepel $\mathbf{A}$-ban. Ekkor a helyettesítések szabályát alkalmazva a kvantoros kifejezésekben, továbbá az $\{\mathbf{x}|\mathbf{A}\}$ objektum, valamint az univerzális és egzisztenciális kvantor definíciója alapján

$$(\forall\mathbf{x})((\mathbf{x}\in\{\mathbf{x}|\mathbf{A}\})\Leftrightarrow\mathbf{A}) \equiv (\forall\mathbf{x})((\{\mathbf{x}|\mathbf{A}\}|\mathbf{y})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A})) \equiv$$
$$\equiv (\{\mathbf{x}|\mathbf{A}\}|\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}) \equiv (\varepsilon_{\mathbf{y}}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}))|\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}) \equiv$$
$$\equiv (\exists\mathbf{y})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow\mathbf{A}) \equiv \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}). \blacksquare$$

Még nem adtuk meg a halmazelmélet axiómarendszerét, azonban a halmazelmélet nyelve rögzíti a halmazelmélet alatt fekvő *predikátumkalkulust*, amit $\mathfrak{Ens}_0$ jelöl. Ezzel együtt természetesen a halmazelmélet *logikai tételeiről* is beszélhetünk: ezek éppen az $\mathfrak{Ens}_0$ elmélet tételei.

4.1.16. Állítás. *Legyen* $\mathbf{A}$ *formula,* $\mathbf{T}$ *objektum és* $\mathbf{x}$ *változó a halmazelmélet nyelvében. Ha* $\mathbf{x}$ *nem szerepel* $\mathbf{T}$*-ben, akkor a*

$$(\ (\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Rightarrow\mathbf{A})\wedge(\forall\mathbf{x})(\mathbf{A}\Rightarrow(\mathbf{x}\in\mathbf{T}))\ )\ \Rightarrow\ \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$$

formula logikai tétel a halmazelméletben (vagyis tétel $\mathfrak{Ens}_0$*-ban).*

Bizonyítás. Legyen $\mathbf{y}$ olyan változó, amely $\mathbf{x}$-től különbözik és nem szerepel $\mathbf{A}$-ban. Az univerzális kvantor konjunkcióval való kapcsolata szerint a

$$(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow \mathbf{A}) \Leftrightarrow ((\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow \mathbf{A})) \wedge ((\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T}))),$$

formula logikai tétel a halmazelméletben, hiszen az $\Leftrightarrow$ definíciója alapján

$$(\mathbf{x} \in \mathbf{T}) \Leftrightarrow \mathbf{A} \;\equiv\; ((\mathbf{x} \in \mathbf{T}) \Rightarrow \mathbf{A})) \wedge (\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})).$$

Tehát azt kell igazolni, hogy $(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow \mathbf{A}) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ logikai tétel a halmazelméletben. A kvantorokra vonatkozó helyettesítési szabály szerint

$$(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Leftrightarrow \mathbf{A}) \;\equiv\; (\mathbf{T}|\mathbf{y})(\forall \mathbf{x})((\mathbf{x} \in \mathbf{y}) \Leftrightarrow \mathbf{A}),$$

ugyanakkor a

$$(\mathbf{T}|\mathbf{y})(\forall \mathbf{x})((\mathbf{x} \in \mathbf{y}) \Leftrightarrow \mathbf{A}) \;\Rightarrow\; (\exists \mathbf{y})(\forall \mathbf{x})((\mathbf{x} \in \mathbf{y}) \Leftrightarrow \mathbf{A})$$

formula eleme $\mathfrak{S}_5$-nek. Ez már az állítást igazolja, hiszen a definíció alapján $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}) \equiv (\exists \mathbf{y})(\forall \mathbf{x})((\mathbf{x} \in \mathbf{y}) \Leftrightarrow \mathbf{A})$. ■

Azonban rövidesen látni fogjuk, hogy ha $\mathbf{A}$ formula, $\mathbf{T}$ objektum és $\mathbf{x}$ olyan változó a halmazelmélet nyelvében, amely nem szerepel $\mathbf{T}$-ben, akkor lehetséges az, hogy a

$$(\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \;\Rightarrow\; \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$$

formula *nem logikai tétel* a halmazelméletben. Még ennél is több mondható: létezik a halmazelmélet alatt fekvő predikátumkalkulusnak olyan valódi bővítése, amelyben található ilyen alakú formula, amely *nem tétel.* Azonban a halmazelméletnek *matematikai axiómái* lesznek az ilyen alakú formulák. A pontos állítás megfogalmazásához értelmezünk egy nevezetes formula-sémát a halmazelmélet nyelvében.

4.1.17. Definíció. *Az $\mathfrak{S}_{\mathrm{sub}}$ szimbólummal jelöljük a*

$$(\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \;\Rightarrow\; \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$$

alakú formulák összességét, ahol $\mathbf{x}$ változó, $\mathbf{A}$ formula és $\mathbf{T}$ olyan objektum a halmazelmélet nyelvében, amelyben $\mathbf{x}$ nem szerepel.

4.1.18. Állítás. *$\mathfrak{S}_{\mathrm{sub}}$ formula-séma a halmazelmélet nyelvében.*

Bizonyítás. Legyen $\mathbf{x}$ változó, $\mathbf{A}$ formula és $\mathbf{T}$ olyan objektum a halmazelmélet nyelvében, amelyben $\mathbf{x}$ nem szerepel. Jelölje $\mathbf{B}$ a

$$(\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \;\Rightarrow\; \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$$

formulát, továbbá legyen $\mathbf{y}$ változó és $\mathbf{S}$ objektum a halmazelmélet nyelvében. Megmutatjuk, hogy $(\mathbf{S}|\mathbf{y})\mathbf{B}$ eleme $\mathfrak{S}_{\mathrm{sub}}$-nak.

Ehhez legyen $\mathbf{z}$ olyan változó, amely különbözik $\mathbf{x}$-től és $\mathbf{y}$-tól, valamint nem szerepel a $\mathbf{T}$ és $\mathbf{S}$ objektumokban és az $\mathbf{A}$ formulában. Ekkor

$$\begin{gathered}
(\mathbf{S}|\mathbf{y})\mathbf{B} \equiv (\mathbf{S}|\mathbf{y})((\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})) \equiv \\
\equiv (\mathbf{S}|\mathbf{y})((\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T}))) \Rightarrow (\mathbf{S}|\mathbf{y})\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}) \equiv \\
\equiv (\mathbf{S}|\mathbf{y})((\forall \mathbf{z})((\mathbf{z}|\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})))) \Rightarrow (\mathbf{S}|\mathbf{y})\mathfrak{Coll}_{\mathbf{z}}((\mathbf{z}|\mathbf{x})\mathbf{A}) \equiv \\
\equiv (\mathbf{S}|\mathbf{y})((\forall \mathbf{z})((\mathbf{z}|\mathbf{x})\mathbf{A} \Rightarrow (\mathbf{z} \in \mathbf{T}))) \Rightarrow (\mathbf{S}|\mathbf{y})\mathfrak{Coll}_{\mathbf{z}}((\mathbf{z}|\mathbf{x})\mathbf{A}) \equiv \\
\equiv (\forall \mathbf{z})((\mathbf{S}|\mathbf{y})((\mathbf{z}|\mathbf{x})\mathbf{A} \Rightarrow (\mathbf{z} \in \mathbf{T}))) \Rightarrow \mathfrak{Coll}_{\mathbf{z}}((\mathbf{S}|\mathbf{y})(\mathbf{z}|\mathbf{x})\mathbf{A}) \equiv \\
\equiv (\forall \mathbf{z})(\mathbf{A}' \Rightarrow (\mathbf{z} \in \mathbf{T}')) \Rightarrow \mathfrak{Coll}_{\mathbf{z}}(\mathbf{A}'),
\end{gathered}$$

ahol $\mathbf{A}'$ jelöli az $(\mathbf{S}|\mathbf{y})(\mathbf{z}|\mathbf{x})\mathbf{A}$ formulát, és $\mathbf{T}'$ jelöli az $(\mathbf{S}|\mathbf{y})\mathbf{T}$ objektumot. Világos, hogy a $\mathbf{z}$ változó nem szerepel $\mathbf{T}'$-ben, ezért $(\mathbf{S}|\mathbf{y})\mathbf{B}$ eleme $\mathfrak{S}_{\mathrm{sub}}$-nak. ■

4.1.19. Definíció. $\mathfrak{Ens}_*$ *jelöli azt a matematikai elméletet, amelynek*

- *matematikai nyelve a halmazelmélet nyelve;*
- *egyetlen matematikai axióma-sémája az* $\mathfrak{S}_{\text{sub}}$ *formula-séma;*
- *egyetlen explicit axiómája a meghatározottsági axióma.*

Ezzel még nem értelmeztük a halmazelméletet, amely az $\mathfrak{Ens}_*$ elméletnek olyan bővítése lesz, amelyet úgy nyerünk, hogy $\mathfrak{Ens}_*$ axiómarendszeréhez hozzáveszünk még öt explicit axiómát. Azonban minden olyan formula, amely tétel $\mathfrak{Ens}_*$-ban, a halmazelméletben is tétel lesz. Később azt is megmutatjuk, hogy az $\mathfrak{Ens}_*$ elmélet logikai szempontból kifogástalan, mert ellentmondásmentes.

Elnevezés. A $\mathfrak{S}_{\text{sub}}$ formula-sémát a halmazelmélet **részhalmaz axióma-sémájának** nevezzük. Az $\mathfrak{S}_{\text{sub}}$ formula-séma minden elemét a halmazelmélet **részhalmaz-axiómájának** nevezzük.

A definíció alapján világos, hogy ha $\mathbf{x}$ változó, $\mathbf{A}$ formula és $\mathbf{T}$ objektum a halmazelmélet nyelvében, valamint $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben, akkor a

$$(\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \;\Rightarrow\; \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$$

formula tétel $\mathfrak{Ens}_*$-ban, sőt matematikai axiómája az $\mathfrak{Ens}_*$ elméletnek. Tehát a részhalmaz axióma-séma *elégséges feltételt* ad ahhoz, hogy egy $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ alakú formula tétel legyen $\mathfrak{Ens}_*$-ban. Pontosabban: ha $\mathbf{x}$ változó és $\mathbf{A}$ formula a halmazelmélet nyelvében, akkor ahhoz, hogy a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula tétel legyen $\mathfrak{Ens}_*$-ban *elégséges* olyan $\mathbf{T}$ objektumot találni a halmazelmélet nyelvében, amelyben $\mathbf{x}$ nem szerepel és amelyre $(\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T}))$ tétel $\mathfrak{Ens}_*$-ban, hiszen ha $\mathbf{T}$ ilyen objektum, akkor a leválasztás szabályát alkalmazva a $(\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ részhalmaz-axiómára kapjuk, hogy a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula tétel $\mathfrak{Ens}_*$-ban.

4.1.20. Állítás. *Ha* $\mathbf{x}$ *változó,* $\mathbf{T}$ *objektum és* $\mathbf{A}$ *formula a halmazelmélet nyelvében, továbbá* $\mathbf{x}$ *nem szerepel* $\mathbf{T}$*-ben, akkor* $\mathfrak{Coll}_{\mathbf{x}}((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A})$ *tétel* $\mathfrak{Ens}_*$*-ban.*

Bizonyítás. Az $((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A}) \Rightarrow (\mathbf{x} \in \mathbf{T})$ formula logikai tétel, tehát az általánosítás szabályát alkalmazva $(\forall \mathbf{x})(((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A}) \Rightarrow (\mathbf{x} \in \mathbf{T}))$ is logikai tétel. Ugyanakkor a

$$(\forall \mathbf{x})(((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A}) \Rightarrow (\mathbf{x} \in \mathbf{T})) \;\Rightarrow\; \mathfrak{Coll}_{\mathbf{x}}((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A})$$

formula eleme $\mathfrak{S}_{\text{sub}}$-nak, mert $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben. Ebből a leválasztás szabályát alkalmazva kapjuk, hogy $\mathfrak{Coll}_{\mathbf{x}}((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A})$ tétel $\mathfrak{Ens}_*$-ban. ■

Jelölés. Ha $\mathbf{x}$ változó, $\mathbf{T}$ objektum és $\mathbf{A}$ formula a halmazelmélet nyelvében, továbbá $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben, akkor az $\{\mathbf{x} | (\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A}\}$ objektumot az $\{\mathbf{x} \in \mathbf{T} | \mathbf{A}\}$ szimbólummal rövidítjük.

Tehát az előző jelölés feltételeinek teljesülése mellett $\{\mathbf{x} \in \mathbf{T} | \mathbf{A}\}$ olyan objektum a halmazelmélet nyelvében, amelyre a $(\forall \mathbf{x})((\mathbf{x} \in \{\mathbf{x} \in \mathbf{T} | \mathbf{A}\}) \Leftrightarrow ((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A}))$ formula tétel $\mathfrak{Ens}_*$-ban.

4.1.21. Állítás. *Ha* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumok a halmazelmélet nyelvében, és* $\mathbf{x}$ *olyan változó, amely nem szerepel* $\mathbf{T}$*-ben és* $\mathbf{S}$*-ben, akkor a*

$$(\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{S}))\ \Rightarrow\ (\mathbf{T}=\mathbf{S})$$

formula tétel $\mathfrak{Ens}_*$*-ban.*

Bizonyítás. Legyenek $\mathbf{x}'$ és $\mathbf{y}'$ olyan különböző változók, amelyek $\mathbf{x}$-től is különböznek és nem szerepelnek a $\mathbf{T}$ és $\mathbf{S}$ objektumokban. Tudjuk, hogy a

$$(\forall\mathbf{x}')(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{x}')\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{x}'=\mathbf{y}'))$$

formula azonos a meghatározottsági axiómával, tehát tétel $\mathfrak{Ens}_*$-ban. Az univerzális kvantor logikai alaptulajdonsága szerint a

$$\begin{gathered}(\forall\mathbf{x}')(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{x}')\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{x}'=\mathbf{y}'))\ \Rightarrow\\ \Rightarrow\ (\mathbf{T}|\mathbf{x}')(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{x}')\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{x}'=\mathbf{y}'))\end{gathered}$$

formula logikai tétel, tehát a leválasztás szabályát alkalmazva kapjuk, hogy

$$(\mathbf{T}|\mathbf{x}')(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{x}')\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{x}'=\mathbf{y}'))$$

tétel $\mathfrak{Ens}_*$-ban. De $\mathbf{x}'$ és $\mathbf{y}'$ különbözőek, valamint $\mathbf{y}'$ nem szerepel $\mathbf{T}$-ben; ugyanakkor $\mathbf{x}'$ és $\mathbf{x}$ is különbözőek, valamint $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben, ezért kétszer alkalmazva a kvantoros kifejezésekre vonatkozó helyettesítés szabályát kapjuk, hogy

$$\begin{gathered}(\mathbf{T}|\mathbf{x}')(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{x}')\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{x}'=\mathbf{y}'))\equiv\\ \equiv(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{T}=\mathbf{y}')),\end{gathered}$$

tehát $(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{T}=\mathbf{y}'))$ tétel $\mathfrak{Ens}_*$-ban. Az univerzális kvantor logikai alaptulajdonsága szerint a

$$\begin{gathered}(\forall\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{T}=\mathbf{y}'))\ \Rightarrow\\ \Rightarrow\ (\mathbf{S}|\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{T}=\mathbf{y}'))\end{gathered}$$

formula logikai tétel, így a leválasztás szabályát alkalmazva kapjuk, hogy

$$(\mathbf{S}|\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{T}=\mathbf{y}'))$$

tétel $\mathfrak{Ens}_*$-ban. De $\mathbf{y}'$ és $\mathbf{x}$ különbözőek és nem szerepelnek $\mathbf{T}$-ben és $\mathbf{S}$-ben, így a kvantoros kifejezésekre vonatkozó helyettesítés szabályát alkalmazva kapjuk, hogy

$$(\mathbf{S}|\mathbf{y}')((\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{y}'))\Rightarrow(\mathbf{T}=\mathbf{y}'))\equiv(\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{S}))\Rightarrow(\mathbf{T}=\mathbf{S}),$$

vagyis $(\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow(\mathbf{x}\in\mathbf{S}))\Rightarrow(\mathbf{T}=\mathbf{S})$ tétel $\mathfrak{Ens}_*$-ban. ■

Világos, hogy az előző állításnak az a tartalma, hogy *ha két halmaznak ugyanazok az elemei, akkor a két halmaz egyenlő* az $\mathfrak{Ens}_*$ elméletben.

4.1.22. Állítás. *Ha* $\mathbf{T}$ *objektum és* $\mathbf{x}$ *olyan változó a halmazelmélet nyelvében, hogy* $\mathbf{x}$ *nem szerepel* $\mathbf{T}$*-ben, akkor* $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x}\in\mathbf{T})$ *és* $\{\mathbf{x}|\mathbf{x}\in\mathbf{T}\}=\mathbf{T}$ *tételek* $\mathfrak{Ens}_*$*-ban.*

Bizonyítás. A kizárt harmadik elve alapján $(\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{T})$ logikai tétel, tehát az általánosítás szabályát alkalmazva azt kapjuk, hogy $(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{T}))$ logikai tétel. Ugyanakkor világos, hogy a $(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \in \mathbf{T})$ formula eleme $\mathfrak{S}_{\mathrm{sub}}$-nak, tehát tétel $\mathfrak{Ens}_*$-ban. Ebből a leválasztás szabályát alkalmazva adódik, hogy $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \in \mathbf{T})$ tétel $\mathfrak{Ens}_*$-ban.

Tudjuk, hogy $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \in \mathbf{T}) \equiv (\forall \mathbf{x})((\mathbf{x} \in \{\mathbf{x}|\mathbf{x} \in \mathbf{T}\}) \Leftrightarrow (\mathbf{x} \in \mathbf{T}))$, következésképpen $(\forall \mathbf{x})((\mathbf{x} \in \{\mathbf{x}|\mathbf{x} \in \mathbf{T}\}) \Leftrightarrow (\mathbf{x} \in \mathbf{T}))$ tétel $\mathfrak{Ens}_*$-ban. Az $\mathbf{x}$ változó nem szerepel az $\{\mathbf{x}|\mathbf{x} \in \mathbf{T}\}$ és $\mathbf{T}$ objektumokban, így az előző állítás alapján kapjuk, hogy a

$$(\forall \mathbf{x})((\mathbf{x} \in \{\mathbf{x}|\mathbf{x} \in \mathbf{T}\}) \Leftrightarrow (\mathbf{x} \in \mathbf{T})) \;\Rightarrow\; (\{\mathbf{x}|\mathbf{x} \in \mathbf{T}\} = \mathbf{T})$$

formula tétel $\mathfrak{Ens}_*$-ban. Ebből a leválasztás szabályát alkalmazva következik, hogy az $\{\mathbf{x}|\mathbf{x} \in \mathbf{T}\} = \mathbf{T}$ formula tétel $\mathfrak{Ens}_*$-ban. ■

Ez az állítás azt mutatja, hogy ha az $\{\mathbf{x}|\mathbf{A}\}$ objektumokat úgy tekintenének, mint "azon $\mathbf{x}$-ek összessége, amelyekre $\mathbf{A}$ teljesül", akkor bármely $\mathbf{T}$ objektumra, és bármely $\mathbf{T}$-ben nem szereplő $\mathbf{x}$ változóra a $\mathbf{T}$ objektum egyenlő az $\mathfrak{Ens}_*$ elméletben "azon $\mathbf{x}$-ek összességével, amelyekre $\mathbf{x} \in \mathbf{T}$", vagyis *minden halmaz egyenlő az elemeinek halmazával.*

4.1.23. Állítás. (**Az üres halmaz létezése.**) *Ha $\mathbf{x}$ változó, akkor a $\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x} = \mathbf{x}))$ formula tétel $\mathfrak{Ens}_*$-ban, és az $\{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}$ objektum független az $\mathbf{x}$ változótól (vagyis minden $\mathbf{y}$ változóra $\{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\} \equiv \{\mathbf{y}|\neg(\mathbf{y} = \mathbf{y})\}$), és a $(\forall \mathbf{x})(\neg(\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}))$ formula tétel a $\mathfrak{Ens}_*$ elméletben.*

Bizonyítás. Legyen $\mathbf{T}$ olyan objektum, amelyben $\mathbf{x}$ nem szerepel; például $\mathbf{T}$ lehet bármelyik $\mathbf{x}$-től különböző változó. Az egyenlőség logikai tulajdonságai szerint az $\mathbf{x} = \mathbf{x}$ formula logikai tétel, ezért a $\neg(\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} = \mathbf{x})$ formula is logikai tétel (az igaz bármiből következik). A kontrapozíció elve és a kettős negáció szabálya szerint $\neg(\mathbf{x} = \mathbf{x}) \Rightarrow \neg\neg(\mathbf{x} \in \mathbf{T})$ és $\neg\neg(\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathbf{x} \in \mathbf{T})$ logikai tétel, így a láncszabályból következik, hogy $\neg(\mathbf{x} = \mathbf{x}) \Rightarrow (\mathbf{x} \in \mathbf{T})$ logikai tétel. Az általánosítás szabálya szerint $(\forall \mathbf{x})(\neg(\mathbf{x} = \mathbf{x}) \Rightarrow (\mathbf{x} \in \mathbf{T}))$ is logikai tétel. A $(\forall \mathbf{x})(\neg(\mathbf{x} = \mathbf{x}) \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x} = \mathbf{x}))$ formula eleme $\mathfrak{S}_{\mathrm{sub}}$-nak, tehát tétel $\mathfrak{Ens}_*$-ban. Ebből a leválasztás szabályát alkalmazva kapjuk, hogy $\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x} = \mathbf{x}))$ tétel $\mathfrak{Ens}_*$-ban.

Tudjuk, hogy $\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x} = \mathbf{x})) \equiv (\forall \mathbf{x})((\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}) \Leftrightarrow \neg(\mathbf{x} = \mathbf{x}))$, tehát a $(\forall \mathbf{x})((\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}) \Leftrightarrow \neg(\mathbf{x} = \mathbf{x})))$ formula formula tétel $\mathfrak{Ens}_*$-ban. Ebből az univerzális kvantor logikai alaptulajdonsága és a leválasztás szabálya szerint kapjuk, hogy $(\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}) \Leftrightarrow \neg(\mathbf{x} = \mathbf{x})$ tétel $\mathfrak{Ens}_*$-ban. Tehát 2.5.9. alapján a

$$\neg(\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}) \Leftrightarrow \neg\neg(\mathbf{x} = \mathbf{x})$$

formula tétel $\mathfrak{Ens}_*$-ban. Mivel $\neg\neg(\mathbf{x} = \mathbf{x}) \Leftrightarrow (\mathbf{x} = \mathbf{x})$ logikai tétel, ebből az ekvivalencia tranzitivitása szerint kapjuk, hogy a

$$\neg(\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}) \Leftrightarrow (\mathbf{x} = \mathbf{x})$$

formula tétel $\mathfrak{Ens}_*$-ban. Ugyanakkor $\mathbf{x} = \mathbf{x}$ logikai tétel, így $\neg(\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\})$ tétel $\mathfrak{Ens}_*$-ban. Az általánosítás szabályát alkalmazva kapjuk, hogy a

$$(\forall \mathbf{x})(\neg(\mathbf{x} \in \{\mathbf{x}|\neg(\mathbf{x} = \mathbf{x})\}))$$

formula tétel $\mathfrak{Ens}_*$-ban.

Ha $\mathbf{y}$ tetszőleges változó, akkor a helyettesítés szabályát alkalmazva az ε-objektumokra

$$\{\mathbf{x}|\neg(\mathbf{x}=\mathbf{x})\} \equiv \{\mathbf{y}|(\mathbf{y}|\mathbf{x})(\neg(\mathbf{x}=\mathbf{x}))\} \equiv \{\mathbf{y}|\neg(\mathbf{y}=\mathbf{y})\}$$

adódik, tehát az $\{\mathbf{x}|\neg(\mathbf{x}=\mathbf{x})\}$ objektum független az $\mathbf{x}$ változótól. ■

4.1.24. Definíció. *Az* $\{\mathbf{x}|\neg(\mathbf{x}=\mathbf{x})\}$ *halmazt az* **üres halmaznak** *nevezzük és a* $\emptyset$ *szimbólummal jelöljük, ahol* $\mathbf{x}$ *tetszőleges változó.*

Tehát az $\emptyset$ halmaz olyan objektum a halmazelmélet nyelvében, amelyben egyetlen változó sem szerepel (vagyis zárt objektum), és bármely $\mathbf{x}$ változóra

$$(\forall\mathbf{x})(\neg(\mathbf{x}\in\emptyset))$$

tétel $\mathfrak{Ens}_*$-ban, amit úgy is megfogalmazhatunk, hogy "*az üres halmaznak nincs eleme*"; ez indokolja az *üres halmaz* elnevezést. A definíció szerint nyilvánvaló, hogy

$$\emptyset \equiv \varepsilon_{\mathbf{y}}((\forall\mathbf{x})((\mathbf{x}\in\mathbf{y})\Leftrightarrow(\neg(\mathbf{x}=\mathbf{x})))),$$

ahol $\mathbf{x}$ és $\mathbf{y}$ tetszőleges különböző változók. Figyeljük meg, hogy a (megfelelő tulajdonságokkal rendelkező) üres halmaz bevezetéséhez csak a részhalmaz axióma-sémára volt szükségünk.

Most azt a problémát vizsgáljuk meg, hogy lehetséges-e az, hogy *minden* $\mathbf{A}$ formulára és $\mathbf{x}$ változóra a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula tétel $\mathfrak{Ens}_*$-ban? A következő állításból kiderül, hogy ez csakis akkor volna lehetséges, ha az $\mathfrak{Ens}_*$ matematikai elmélet ellentmondásos volna; ugyanakkor látni fogjuk, hogy még olyan bővítése is létezik az $\mathfrak{Ens}_*$ elméletnek (az $\mathfrak{Ens}_{**}$ elmélet), amely ellentmondásmentes (4.2.5.).

4.1.25. Állítás. (**Russel-tétel**.) *Ha* $\mathbf{x}$ *tetszőleges változó, akkor a* $\neg\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}\in\mathbf{x}))$ *formula logikai tétel a halmazelméletben, vagyis a* $\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}\in\mathbf{x}))$ *formula logikailag cáfolható a halmazelméletben.*

Bizonyítás. Jelölje $\mathfrak{T}$ az $\mathfrak{Ens}_0[\neg\neg\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}\in\mathbf{x}))]$ matematikai elméletet. Az indirekt bizonyítás elve alapján elegendő azt igazolni, hogy a $\mathfrak{T}$ elmélet ellentmondásos.

A $\neg\neg\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}\in\mathbf{x}))$ formula tétel, sőt explicit axióma $\mathfrak{T}$-ben, így a 2.5.3. állításból következik, hogy $\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}\in\mathbf{x}))$ is tétel $\mathfrak{T}$-ben. Tehát ha $\mathbf{T}$ jelöli az $\{\mathbf{x}|\neg(\mathbf{x}\in\mathbf{x})\}$ objektumot, akkor a $(\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow\neg(\mathbf{x}\in\mathbf{x}))$ formula tétel $\mathfrak{T}$-ben. Ugyanakkor az univerzális kvantor logikai alaptulajdonsága szerint

$$(\forall\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow\neg(\mathbf{x}\in\mathbf{x})) \Rightarrow (\mathbf{T}|\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow\neg(\mathbf{x}\in\mathbf{x}))$$

logikai tétel, és természetesen $(\mathbf{T}|\mathbf{x})((\mathbf{x}\in\mathbf{T})\Leftrightarrow\neg(\mathbf{x}\in\mathbf{x})) \equiv (\mathbf{T}\in\mathbf{T})\Leftrightarrow\neg(\mathbf{T}\in\mathbf{T})$, mert $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben. Ebből a leválasztás szabályát alkalmazva kapjuk, hogy $(\mathbf{T}\in\mathbf{T})\Leftrightarrow\neg(\mathbf{T}\in\mathbf{T})$ tétel $\mathfrak{T}$-ben. Ezért a konjunkció logikai alaptulajdonsága szerint a $(\mathbf{T}\in\mathbf{T})\Rightarrow\neg(\mathbf{T}\in\mathbf{T})$ és $\neg(\mathbf{T}\in\mathbf{T})\Rightarrow(\mathbf{T}\in\mathbf{T})$ formulák tételek $\mathfrak{T}$-ben. Ebből a leválasztás szabályának alkalmazásával következik, hogy a $\mathfrak{T}[\neg(\mathbf{T}\in\mathbf{T})]$ elméletben $\neg(\mathbf{T}\in\mathbf{T})$ és $\mathbf{T}\in\mathbf{T}$ tételek, vagyis ez az elmélet ellentmondásos. Tehát az indirekt bizonyítás elve alapján $\mathbf{T}\in\mathbf{T}$ tétel $\mathfrak{T}$-ben. De $(\mathbf{T}\in\mathbf{T})\Rightarrow\neg(\mathbf{T}\in\mathbf{T})$ tétel $\mathfrak{T}$-ben, amiből a leválasztás szabályát alkalmazva kapjuk, hogy $\neg(\mathbf{T}\in\mathbf{T})$ is tétel $\mathfrak{T}$-ben, így láthatóan a $\mathfrak{T}$ elmélet ellentmondásos. ■

4.1.26. Következmény. *Ha* $\mathbf{x}$ *és* $\mathbf{y}$ *különböző változók a halmazelméletben, akkor a* $\neg(\exists\mathbf{y})(\forall\mathbf{x})(\mathbf{x}\in\mathbf{y})$ *formula tétel* $\mathfrak{Ens}_*$*-ban.*

Bizonyítás. Jelölje $\mathfrak{T}$ az $\mathfrak{Ens}_*[\neg\neg(\exists\mathbf{y})(\forall\mathbf{x})(\mathbf{x}\in\mathbf{y})]$ matematikai elméletet, és $\mathbf{U}$ az $\varepsilon_{\mathbf{y}}((\forall\mathbf{x})(\mathbf{x}\in\mathbf{y}))$ objektumot. A 2.5.3. állítás szerint $(\exists\mathbf{y})(\forall\mathbf{x})(\mathbf{x}\in\mathbf{y})$ tétel $\mathfrak{T}$-ben, ami az egzisztenciális kvantor definíciója alapján azt jelenti, hogy $(\mathbf{U}|\mathbf{y})(\forall\mathbf{x})(\mathbf{x}\in\mathbf{y})$ tétel $\mathfrak{T}$-ben. De $\mathbf{x}$ és $\mathbf{y}$ különbözőek, valamint $\mathbf{x}$ nem szerepel $\mathbf{U}$-ban, így $(\mathbf{U}|\mathbf{y})(\forall\mathbf{x})(\mathbf{x}\in\mathbf{y})\equiv(\forall\mathbf{x})((\mathbf{U}|\mathbf{y})(\mathbf{x}\in\mathbf{y}))\equiv(\forall\mathbf{x})(\mathbf{x}\in\mathbf{U})$. A $(\forall\mathbf{x})(\mathbf{x}\in\mathbf{U})\Rightarrow(\mathbf{x}\in\mathbf{U})$ formula logikai tétel, így a leválasztás szabályát alkalmazva kapjuk, hogy $\mathbf{x}\in\mathbf{U}$ tétel $\mathfrak{T}$-ben. Ezért $\neg(\mathbf{x}\in\mathbf{x})\Rightarrow(\mathbf{x}\in\mathbf{U})$ is tétel $\mathfrak{T}$-ben (az igaz bármiből következik). Az $\mathbf{x}$ változó nem szerepel a $\mathfrak{T}$ egyetlen explicit axiómájában sem, így az általánosítás szabálya szerint $(\forall\mathbf{x})(\neg(\mathbf{x}\in\mathbf{x})\Rightarrow(\mathbf{x}\in\mathbf{U}))$ tétel $\mathfrak{T}$-ben. Világos, hogy a $(\forall\mathbf{x})(\neg(\mathbf{x}\in\mathbf{x})\Rightarrow(\mathbf{x}\in\mathbf{U}))\Rightarrow\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}\in\mathbf{x}))$ formula eleme $\mathfrak{S}_{\mathrm{sub}}$-nak, mert $\mathbf{x}$ nem szerepel $\mathbf{U}$-ban. Leválasztással kapjuk, hogy $\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}=\mathbf{x}))$ tétel $\mathfrak{T}$-ben. A Russel-tétel alapján $\neg\mathfrak{Coll}_{\mathbf{x}}(\neg(\mathbf{x}=\mathbf{x}))$ tétel $\mathfrak{Ens}_*$-ban, tehát $\mathfrak{T}$-ben is tétel, így a $\mathfrak{T}$ elmélet ellentmondásos. Az indirekt bizonyítás elve alapján $\neg(\exists\mathbf{y})(\forall\mathbf{x})(\mathbf{x}\in\mathbf{y})$ formula tétel $\mathfrak{Ens}_*$-ban. ■

Nyilvánvalóan az előző állítást úgy lehet értelmezni, hogy az $\mathfrak{Ens}_*$ elméletben (így annak minden bővítésében is) bizonyítható, hogy *nem létezik az összes halmazok halmaza.*

A következő állítást nagyon gyakran alkalmazzuk a $\{\cdot|\cdot\}$-objektumokat tartalmazó egyenlőségek bizonyításában.

4.1.27. Állítás. *Jelölje $\mathfrak{T}$ az $\mathfrak{Ens}_*$ matematikai elmélet tetszőleges bővítését, és legyenek $\mathbf{A}$, $\mathbf{B}$ formulák, valamint $\mathbf{x}$ olyan változó a halmazelmélet nyelvében, amely nem szerepel a $\mathfrak{T}$ elmélet egyetlen explicit axiómájában sem.*

a) *Ha az $\mathbf{A}\Rightarrow\mathbf{B}$ és $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})$ formulák tételek $\mathfrak{T}$-ben, akkor a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ és $\{\mathbf{x}|\mathbf{A}\}\subseteq\{\mathbf{x}|\mathbf{B}\}$ formulák is tételek $\mathfrak{T}$-ben.*

b) *Ha az $\mathbf{A}\Leftrightarrow\mathbf{B}$ formula tétel $\mathfrak{T}$-ben, akkor a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})\Leftrightarrow\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})$ formula tétel $\mathfrak{T}$-ben; továbbá, ha $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ tétel $\mathfrak{T}$-ben, akkor $\{\mathbf{x}|\mathbf{A}\}=\{\mathbf{x}|\mathbf{B}\}$ tétel $\mathfrak{T}$-ben.*

Bizonyítás. a) Tegyük fel, hogy az $\mathbf{A}\Rightarrow\mathbf{B}$ és $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})$ formulák tételek $\mathfrak{T}$-ben. Ekkor az $(\mathbf{x}\in\{\mathbf{x}|\mathbf{B}\})\Leftrightarrow\mathbf{B}$ formula tétel $\mathfrak{T}$-ben, így az ekvivalencia logikai alaptulajdonsága szerint $\mathbf{B}\Rightarrow(\mathbf{x}\in\{\mathbf{x}|\mathbf{B}\})$ tétel $\mathfrak{T}$-ben. A láncszabály alkalmazásával kapjuk, hogy $\mathbf{A}\Rightarrow(\mathbf{x}\in\{\mathbf{x}|\mathbf{B}\})$ tétel $\mathfrak{T}$-ben. Az $\mathbf{x}$ változó nem szerepel a $\mathfrak{T}$ elmélet egyetlen explicit axiómájában sem, így az általánosítás szabálya szerint $(\forall\mathbf{x})(\mathbf{A}\Rightarrow(\mathbf{x}\in\{\mathbf{x}|\mathbf{B}\}))$ tétel $\mathfrak{T}$-ben. Ugyanakkor a $(\forall\mathbf{x})(\mathbf{A}\Rightarrow(\mathbf{x}\in\{\mathbf{x}|\mathbf{B}\}))\Rightarrow\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula eleme $\mathfrak{S}_{\mathrm{sub}}$-nak, mert $\mathbf{x}$ nem szerepel az $\{\mathbf{x}|\mathbf{B}\}$ objektumban, tehát a leválasztás szabályát alkalmazva kapjuk, hogy $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ tétel $\mathfrak{T}$-ben, így az $\{\mathbf{x}|\mathbf{A}\}$ objektumra teljesül az, hogy az $(\mathbf{x}\in\{\mathbf{x}|\mathbf{A}\})\Leftrightarrow\mathbf{A}$ formula tétel $\mathfrak{T}$-ben. Ezért az ekvivalencia logikai alaptulajdonsága szerint $(\mathbf{x}\in\{\mathbf{x}|\mathbf{A}\})\Rightarrow\mathbf{A}$ tétel $\mathfrak{T}$-ben, tehát a láncszabály alkalmazásával kapjuk, hogy $(\mathbf{x}\in\{\mathbf{x}|\mathbf{A}\})\Rightarrow(\mathbf{x}\in\{\mathbf{x}|\mathbf{B}\})$ tétel $\mathfrak{T}$-ben. Az $\mathbf{x}$ változó nem szerepel a $\mathfrak{T}$ elmélet egyetlen explicit axiómájában sem, így az általánosítás szabálya szerint $(\forall\mathbf{x})((\mathbf{x}\in\{\mathbf{x}|\mathbf{A}\})\Rightarrow(\mathbf{x}\in\{\mathbf{x}|\mathbf{B}\}))$ tétel $\mathfrak{T}$-ben, ami éppen azt jelenti, hogy $\{\mathbf{x}|\mathbf{A}\}\subseteq\{\mathbf{x}|\mathbf{B}\}$ tétel $\mathfrak{T}$-ben, hiszen az $\mathbf{x}$ változó nem szerepel az $\{\mathbf{x}|\mathbf{A}\}$ és $\{\mathbf{x}|\mathbf{B}\}$ objektumokban.

b) Tegyük fel, hogy az $\mathbf{A}\Leftrightarrow\mathbf{B}$ formula tétel $\mathfrak{T}$-ben. Az ekvivalencia logikai alaptulajdonságából következik, hogy $\mathbf{A}\Rightarrow\mathbf{B}$ és $\mathbf{B}\Rightarrow\mathbf{A}$ tételek $\mathfrak{T}$-ben. Tehát az a) állítás alapján $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ tétel $\mathfrak{T}[\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})]$-ben és $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})$ tétel $\mathfrak{T}[\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})]$-ben, hiszen az $\mathbf{x}$ változó a $\mathfrak{T}[\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})]$ és $\mathfrak{T}[\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})]$ elméletek egyetlen explicit axiómájában sem szerepel. Kétszer alkalmazva a dedukció-tételt kapjuk, hogy $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})\Rightarrow\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ és $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})\Rightarrow\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})$ tétel $\mathfrak{T}$-ben, így a konjunkció logikai alaptulajdonsága szerint $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})\Leftrightarrow\mathfrak{Coll}_{\mathbf{x}}(\mathbf{B})$ tétel $\mathfrak{T}$-ben. Ugyanakkor az a) állítás szerint $\{\mathbf{x}|\mathbf{A}\}\subseteq\{\mathbf{x}|\mathbf{B}\}$ és $\{\mathbf{x}|\mathbf{B}\}\subseteq\{\mathbf{x}|\mathbf{A}\}$ tételek $\mathfrak{T}$-ben, ezért a meghatározottsági axióma szerint $\{\mathbf{x}|\mathbf{A}\}=\{\mathbf{x}|\mathbf{B}\}$ tétel $\mathfrak{T}$-ben. ■

A halmazelméletben leggyakrabban használt feltételes kvantorok feltételei $\mathbf{x} \in \mathbf{T}$ alakúak, ahol $\mathbf{x}$ olyan változó, amely nem szerepel a $\mathbf{T}$ objektumban. Az ilyen felépítésű feltételes kvantorokra speciális jelölést vezetünk be. Ha $\mathbf{x}$ változó és $\mathbf{T}$, $\mathbf{A}$ kifejezések a halmazelmélet nyelvében, akkor

- $(\forall \mathbf{x} \in \mathbf{T})\mathbf{A}$ jelöli a $(\forall_{\mathbf{x}\in\mathbf{T}}\mathbf{x})\mathbf{A}$ kifejezést;
- $(\exists \mathbf{x} \in \mathbf{T})\mathbf{A}$ jelöli a $(\exists_{\mathbf{x}\in\mathbf{T}}\mathbf{x})\mathbf{A}$ kifejezést.

Világos, hogy ha $\mathbf{T}$ objektum és $\mathbf{A}$ formula, akkor a

$$(\forall \mathbf{x} \in \mathbf{T})\mathbf{A} \Leftrightarrow (\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow \mathbf{A}),$$
$$(\exists \mathbf{x} \in \mathbf{T})\mathbf{A} \Leftrightarrow (\exists \mathbf{x})((\mathbf{x} \in \mathbf{T}) \wedge \mathbf{A})$$

formulák logikai tételek a halmazelméletben.

Most megfogalmazzuk a halmazelmélet összes explicit axiómáját. Ehhez néhány jelölést kell bevezetni az halmazelmélet nyelvével kapcsolatban. Az itt értelmezendő objektumok jelentésének és jelentőségének részletezésére majd a matematikai analízis halmazelméleti alapjaival foglalkozó fejezetben kerül sor.

Jelölés. Legyen $\mathbf{T}$ és $\mathbf{S}$ objektumok a halmazelmélet nyelvében. Ha $\mathbf{x}$ olyan változó, amely nem szerepel $\mathbf{T}$-ben és $\mathbf{S}$-ben, akkor az

$$\{\mathbf{x}|(\mathbf{x} = \mathbf{T}) \vee (\mathbf{x} = \mathbf{S})\}$$

objektum az $\mathbf{x}$ változótól független, vagyis ha $\mathbf{x}'$ szintén olyan változó, amely nem szerepel $\mathbf{T}$-ben és $\mathbf{S}$-ben, akkor

$$\{\mathbf{x}|(\mathbf{x} = \mathbf{T}) \vee (\mathbf{x} = \mathbf{S})\} \;\equiv\; \{\mathbf{x}'|(\mathbf{x}' = \mathbf{T}) \vee (\mathbf{x}' = \mathbf{S})\}.$$

Ezt az objektumot a $\{\mathbf{T}, \mathbf{S}\}$ szimbólummal jelöljük, továbbá a $\mathbf{T}$ és $\mathbf{S}$ ojektumokból álló *rendezetlen párnak* nevezzük. A $\{\mathbf{T}, \mathbf{T}\}$ objektumot a $\{\mathbf{T}\}$ szimbólummal rövidítjük. Továbbá, a $\{\mathbf{T}, \{\mathbf{T}, \mathbf{S}\}\}$ objektumot a $(\mathbf{T}, \mathbf{S})$ szimbólummal jelöljük, és a $\mathbf{T}$ és $\mathbf{S}$ objektumokból álló *rendezett párnak* (vagy egyszerűen *párnak*) nevezzük.

Jelölés. Legyen $\mathbf{T}$ és $\mathbf{S}$ objektumok a halmazelmélet nyelvében. Ha $\mathbf{x}$ olyan változó, amely nem szerepel $\mathbf{T}$-ben és $\mathbf{S}$-ben, akkor az

$$\{\mathbf{x}|(\mathbf{x} \in \mathbf{T}) \vee (\mathbf{x} \in \mathbf{S})\}$$

objektum az $\mathbf{x}$ változótól független, vagyis ha $\mathbf{x}'$ szintén olyan változó, amely nem szerepel $\mathbf{T}$-ben és $\mathbf{S}$-ben, akkor

$$\{\mathbf{x}|(\mathbf{x} \in \mathbf{T}) \vee (\mathbf{x} \in \mathbf{S})\} \;\equiv\; \{\mathbf{x}'|(\mathbf{x}' \in \mathbf{T}) \vee (\mathbf{x}' \in \mathbf{S})\}.$$

Ezt az objektumot a $\mathbf{T} \cup \mathbf{S}$ szimbólummal jelöljük, továbbá a $\mathbf{T}$ és $\mathbf{S}$ objektumok *uniójának* nevezzük.

Jelölés. Ha $\mathbf{T}$ objektum a halmazelmélet nyelvében, akkor a $\mathbf{T} \cup \{\mathbf{T}\}$ objektumot a $\mathbf{T}^+$ szimbólummal jelöljük, és a $\mathbf{T}$ objektum *szukcesszorának* nevezzük.

Jelölés. Legyen $\mathbf{T}$ objektum a halmazelmélet nyelvében. Ha $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{z}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor a

$$(\forall\mathbf{z})(\ (\mathbf{z}\in\mathbf{T})\ \Rightarrow\ (\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{z}=(\mathbf{x},\mathbf{y}))\ )$$

formula az $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{z}$ változóktól független, vagyis ha $\mathbf{x}'$, $\mathbf{y}'$ és $\mathbf{z}'$ szintén olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor

$$(\forall\mathbf{z})((\mathbf{z}\in\mathbf{T})\Rightarrow(\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{z}=(\mathbf{x},\mathbf{y})))\equiv(\forall\mathbf{z}')((\mathbf{z}'\in\mathbf{T})\Rightarrow(\exists\mathbf{x}')(\exists\mathbf{y}')(\mathbf{z}'=(\mathbf{x}',\mathbf{y}'))).$$

Ezt a formulát a $\mathfrak{Rel}(\mathbf{T})$ szimbólummal jelöljük, és úgy mondjuk ki, hogy $\mathbf{T}$ **reláció**.

Jelölés. Legyen $\mathbf{T}$ objektum a halmazelmélet nyelvében.

– Ha $\mathbf{x}$ és $\mathbf{y}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor az

$$\{\mathbf{x}|(\exists\mathbf{y})((\mathbf{x},\mathbf{y})\in\mathbf{T})\}$$

objektum az $\mathbf{x}$ és $\mathbf{y}$ változóktól független, tehát ha $\mathbf{x}'$ és $\mathbf{y}'$ szintén olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor

$$\{\mathbf{x}|(\exists\mathbf{y})((\mathbf{x},\mathbf{y})\in\mathbf{T})\}\equiv\{\mathbf{x}'|(\exists\mathbf{y}')((\mathbf{x}',\mathbf{y}')\in\mathbf{T})\}.$$

Ezt az objetumot a $\mathrm{pr}_1(\mathbf{T})$ szimbólummal jelöljük, és a $\mathbf{T}$ objektum *első projekciójának* nevezzük. A $\mathrm{pr}_1(\mathbf{T})$ szimbólum helyett a $\mathrm{Dom}(\mathbf{T})$ jelölést is alkalmazzuk, és ilyenkor ezt a $\mathbf{T}$ objektum *definíciós tartományának* nevezzük. (Ez utóbbi jelölést és elnevezést a későbbiekben bevezetésre kerülő *függvények* esetében szokás használni.)

– Ha $\mathbf{x}$ és $\mathbf{y}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor az

$$\{\mathbf{y}|(\exists\mathbf{x})((\mathbf{x},\mathbf{y})\in\mathbf{T})\}$$

objektum az $\mathbf{x}$ és $\mathbf{y}$ változóktól független, tehát ha $\mathbf{x}'$ és $\mathbf{y}'$ szintén olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor

$$\{\mathbf{y}|(\exists\mathbf{x})((\mathbf{x},\mathbf{y})\in\mathbf{T})\}\equiv\{\mathbf{y}'|(\exists\mathbf{x}')((\mathbf{x}',\mathbf{y}')\in\mathbf{T})\}.$$

Ezt az objetumot a $\mathrm{pr}_2(\mathbf{T})$ szimbólummal jelöljük, és a $\mathbf{T}$ objektum *második projekciójának* nevezzük. A $\mathrm{pr}_2(\mathbf{T})$ szimbólum helyett az $\mathrm{Im}(\mathbf{T})$ jelölést is alkalmazzuk, és ilyenkor ezt a $\mathbf{T}$ objektum *értékkészletének* nevezzük. (Ez utóbbi jelölést és elnevezést a későbbiekben bevezetésre kerülő *függvények* esetében szokás használni.)

Jelölés. Legyen $\mathbf{T}$ objektum a halmazelmélet nyelvében. Ha $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{z}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor a

$$\mathfrak{Rel}(\mathbf{T})\wedge(\forall\mathbf{x})(\forall\mathbf{y})(\forall\mathbf{z})((((\mathbf{x},\mathbf{y})\in\mathbf{T})\wedge((\mathbf{x},\mathbf{z})\in\mathbf{T}))\Rightarrow(\mathbf{y}=\mathbf{z}))$$

formula az $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{z}$ változóktól független, vagyis ha $\mathbf{x}'$, $\mathbf{y}'$ és $\mathbf{z}'$ szintén olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor

$$\mathfrak{Rel}(\mathbf{T})\wedge(\forall\mathbf{x})(\forall\mathbf{y})(\forall\mathbf{z})((((\mathbf{x},\mathbf{y})\in\mathbf{T})\wedge((\mathbf{x},\mathbf{z})\in\mathbf{T}))\Rightarrow(\mathbf{y}=\mathbf{z}))\ \equiv$$
$$\equiv\mathfrak{Rel}(\mathbf{T})\wedge(\forall\mathbf{x}')(\forall\mathbf{y}')(\forall\mathbf{z}')((((\mathbf{x}',\mathbf{y}')\in\mathbf{T})\wedge((\mathbf{x}',\mathbf{z}')\in\mathbf{T}))\Rightarrow(\mathbf{y}'=\mathbf{z}')).$$

Ezt a formulát az $\mathfrak{Fnc}(\mathbf{T})$ szimbólummal jelöljük, és úgy mondjuk ki, hogy $\mathbf{T}$ **függvény**.

Jelölés. Legyen $\mathbf{T}$ objektum és $\mathbf{x}$ változó a halmazelmélet nyelvében. Ha $\mathbf{y}$ olyan $\mathbf{x}$-től különböző változó, amely $\mathbf{T}$-ben nem szerepel, akkor az

$$\varepsilon_{\mathbf{y}}((\mathbf{x},\mathbf{y}) \in \mathbf{T})$$

objektum az $\mathbf{y}$ változótól független, vagyis ha $\mathbf{y}'$ szintén olyan $\mathbf{x}$-től különböző változó, amely $\mathbf{T}$-ben nem szerepel, akkor

$$\varepsilon_{\mathbf{y}}((\mathbf{x},\mathbf{y}) \in \mathbf{T}) \ \equiv\ \varepsilon_{\mathbf{y}'}((\mathbf{x},\mathbf{y}') \in \mathbf{T}).$$

Ezt az objektumot a $\mathbf{T}(\mathbf{x})$ szimbólummal jelöljük.

Megjegyezzük, hogy ha $\mathbf{T}$ objektum és $\mathbf{x}$ változó a halmazelmélet nyelvében, továbbá $\mathbf{y}$ olyan $\mathbf{x}$-től különböző változó, amely $\mathbf{T}$-ben nem szerepel, akkor a $\mathbf{T}(\mathbf{x})$ objektum és az egzisztenciális kvantor értelmezése alapján

$$\begin{aligned}(\mathbf{x},\mathbf{T}(\mathbf{x})) \in \mathbf{T} \ \equiv\ (\mathbf{T}(\mathbf{x})|\mathbf{y})((\mathbf{x},\mathbf{y}) \in \mathbf{T}) \ \equiv\ (\varepsilon_{\mathbf{y}}((\mathbf{x},\mathbf{y}) \in \mathbf{T})|\mathbf{y})((\mathbf{x},\mathbf{y}) \in \mathbf{T}) \ \equiv \\ \equiv\ (\exists\mathbf{y})((\mathbf{x},\mathbf{y}) \in \mathbf{T}),\end{aligned}$$

tehát ha $\mathfrak{Coll}_{\mathbf{x}}((\mathbf{x},\mathbf{y}) \in \mathbf{T})$ tétel $\mathfrak{Ens}_*$-ban (például ha $\mathfrak{Rel}(\mathbf{T})$ tétel $\mathfrak{Ens}_*$-ban), akkor

$$(\forall\mathbf{x})(\ ((\mathbf{x},\mathbf{T}(\mathbf{x})) \in \mathbf{T}) \Leftrightarrow (\mathbf{x} \in \mathrm{pr}_1(\mathbf{T}))\ )$$

is tétel $\mathfrak{Ens}_*$-ban.

Ezután könnyen megfogalmazható a halmazelmélet öt explicit axiómája.

Meghatározottsági axióma: $(\forall x)(\forall y)((\forall z)((z \in x)\Leftrightarrow(z \in y)) \Rightarrow (x = y))$.

Páraxióma: $(\forall x)(\forall y)(\exists u)(\forall z)((z \in u)\Leftrightarrow((z = x) \vee (z = y)))$, vagy ami ugyanaz $(\forall x)(\forall y)\mathfrak{Coll}_z((z = x) \vee (z = y))$.

Hatványhalmaz axióma: $(\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\forall u)((u \in z) \Rightarrow (u \in x)))$, vagy ami ugyanaz $(\forall x)\mathfrak{Coll}_z((\forall u)((u \in z) \Rightarrow (u \in x)))$, azaz $(\forall x)\mathfrak{Coll}_z(z \subseteq x)$.

Unió axióma: $(\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\exists u)((z \in u) \wedge (u \in x))))$, vagy ami ugyanaz $(\forall x)\mathfrak{Coll}_z((\exists u)((z \in u) \wedge (u \in x))))$.

Kiválasztási axióma: $(\forall F)(\ (\mathfrak{Fnc}(F) \wedge (\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset))) \Rightarrow (\exists f)((\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f) = \mathrm{Dom}(F)) \wedge (\forall x)((x \in \mathrm{Dom}(f)) \Rightarrow (f(x) \in F(x))))\ )$.

Végtelenségi axióma: $(\exists x)((\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^+ \in x)))$.

4.1.28. Definíció. Halmazelméletnek *nevezzük és az* $\mathfrak{Ens}$ *szimbólummal jelöljük azt a matematikai elméletet, amelynek*

- *matematikai nyelve a halmazelmélet nyelve;*
- $\mathfrak{S}_{\mathrm{sub}}$ *az egyetlen matematikai axióma-sémája;*
- *explicit axiómái a meghatározottsági axióma, páraxióma, hatványhalmaz axióma, unió axióma, kiválasztási axióma és a végtelenségi axióma.*

A halmazelmélet explicit axiómáinak szemantikus elemzésére a matematikai analízis halmazelméleti alapjainak kifejtése során nyílik lehetőség. Ott majd megvilágítjuk az axiómák halmazelméletben betöltött jelentőségét.

Természetesen $\mathfrak{Ens}_*$ részelmélete a halmazelméletnek, és $\mathfrak{Ens}_*$ úgy származtatható $\mathfrak{Ens}$-ből, hogy töröljük annak axiómarendszeréből a páraxiómát, a hatványhalmaz axiómát, az unió axiómát, a kiválasztási axiómát és a végtelenségi axiómát.

Elnevezés. Azt mondjuk, hogy a halmazelmélet $\mathbf{A}$ formulája **kollektivizáló** az $\mathbf{x}$ változóban, ha a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula tétel a halmazelméletben. Azt mondjuk, hogy a halmazelmélet $\mathbf{T}$ objektuma **reláció** (illetve **függvény**) a halmazelméletben, ha a $\mathfrak{Rel}(\mathbf{T})$ (illetve $\mathfrak{Fnc}(\mathbf{T})$) formula tétel a halmazelméletben.

Tehát az $\mathbf{A}$ formula pontosan akkor *nem kollektivizáló* az $\mathbf{x}$ változóban, ha a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula *nem tétel* a halmazelméletben. Ha a *nem kollektivizáló* kifejezést valóban így értjük, és be tudjuk bizonyítani valamely formulára, hogy az valamelyik változójában nem kollektivizáló, akkor ezzel beláttuk a halmazelmélet ellentmondásmentességét is, hiszen megmutattuk, hogy a halmazelméletnek van olyan formulája, amely nem tétel. Azonban a halmazelmélet ellentmondásmentességének problémája annyira nehéznek bizonyult, hogy azt eddig senki sem tudta megoldani. Ez azt is jelenti, hogy az iménti felfogás szerint egyetlen formulára sem sikerült igazolni azt, hogy valamelyik változóban nem kollektivizáló. Ez az oka annak, hogy a *nem kollektivizáló* kifejezést nem úgy értjük, ahogy azt a bekezdés elején megfogalmaztuk, holott az volna a természetes. E helyett azt mondjuk, hogy az $\mathbf{A}$ kifejezés *nem kollektivizáló* az $\mathbf{x}$ változóban, ha a $\neg\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula *tétel* a halmazelméletben, vagyis ha a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formula *cáfolható* a halmazelméletben.

A **2.10.** pontban bemutattunk két lényegesen nem triviális matematikai elméletet: a formális aritmetikát és a formális (sík)geometriát. Érdekességképpen megemlítjük, hogy mindkét elmélet bizonyos értelemben *előállítható* a halmazelméleten belül. Ennek az állításnak a pontos matematikai logikai megfogalmazásához határozottan túl kellene lépni azon az elemi szinten, amelyhez eddig tartottuk magunkat, ezért ezzel a problémával logikai szempontból nem foglalkozunk. Azonban a **7.** fejezetben megmutatjuk, hogy a *halmazelméleti aritmetika* miként jön létre a halmazelméletben, továbbá látni fogjuk, hogyan hajtható végre a többdimenziós valós *analitikus geometria* halmazelméletre alapozott konstrukciója (**GEA**).

Befejezésül még egy megjegyzést teszünk a halmazelmélet egy másik, valamivel *erősebb* formájával kapcsolatban. Ehhez szükségünk lesz a következő definícióra.

4.1.29. Definíció. *$\mathfrak{S}_{su}$ jelöli a*

$$(\forall\mathbf{y})(\exists\mathbf{X})(\mathbf{A}\Rightarrow(\mathbf{x}\in\mathbf{X}))\ \Rightarrow\ (\forall\mathbf{Y})(\exists\mathbf{X})(\forall\mathbf{x})((\mathbf{x}\in\mathbf{X})\Leftrightarrow(\exists\mathbf{y})((\mathbf{y}\in\mathbf{Y})\wedge\mathbf{A}))$$

alakú formulák összességét, ahol $\mathbf{A}$ formula és $\mathbf{x}$, $\mathbf{y}$, $\mathbf{X}$, $\mathbf{Y}$ olyan különböző változók halmazelmélet nyelvében, hogy $\mathbf{X}$ és $\mathbf{Y}$ nem szerepelnek $\mathbf{A}$-ban.

Világos, hogy $\mathfrak{S}_{su}$ azonos a

$$(\forall\mathbf{y})(\exists\mathbf{X})(\mathbf{A}\Rightarrow(\mathbf{x}\in\mathbf{X}))\ \Rightarrow\ (\forall\mathbf{Y})\mathfrak{Coll}_{\mathbf{x}}((\exists\mathbf{y})((\mathbf{y}\in\mathbf{Y})\wedge\mathbf{A}))$$

alakú formulák összességével, ahol $\mathbf{A}$ formula és $\mathbf{x}$, $\mathbf{y}$, $\mathbf{X}$, $\mathbf{Y}$ olyan különböző változók a halmazelmélet nyelvében, hogy $\mathbf{X}$ és $\mathbf{Y}$ nem szerepelnek $\mathbf{A}$-ban. Könnyen belátható, hogy $\mathfrak{S}_{su}$ formula-séma, és ha a halmazelmélet axiómarendszerét *úgy értelmezzük*, hogy az egyetlen matematikai axióma-sémája az $\mathfrak{S}_{su}$ formula-séma, valamint az explicit axiómái a meghatározottsági axióma, páraxióma, hatványhalmaz-axióma és a végtelenségi axióma, akkor ebben az elméletben az $\mathfrak{S}_{\mathrm{sub}}$ formula-séma minden eleme tétel, és bebizonyítható benne az unió axióma és a kiválasztási axióma, vagyis ebben az új halmazelméletben ezek az axiómák *feleslegesek*. A halmazelméletnek ezt a *Bourbaki-féle* felépítését részletezi a [**2**] könyv. Az általunk választott halmazelmélet valamivel jobban hasonlít a klasszikus *Zermelo-Fraenkel-Skolem* (ZFS) halmazelméletre, másfelől – legalábbis formálisan – *kevésbé erős* elmélet, vagyis "formálisan kevesebb" tétele van, mint a Bourbaki-féle halmazelméletnek, ezért az ellentmondásmentessége kevésbé kérdéses, mint a Bourbaki-féle halmazelméleté. Azonban eddig egyik igazán tartalmas halmazelmélet ellentmondásmentességét sem tudtuk bebizonyítani, habár senki nem tudott még olyan formulát adni ezekben az elméletekben, amelyet a negációjával együtt bizonyítani lehetett volna.

4.2. A halmazelmélet ellentmondásmentességéről

Nem tudjuk, hogy a halmazelmélet ellentmondásmentes-e vagy sem, ezért különös jelentősége van azoknak az eredményeknek, amelyek a halmazelmélet bizonyos részelméleteinek ellentmondásmentességéről szólnak. Ebben a pontban a korábban bemutatott (kétértékű) értékelések módszerének alkalmazásával bebizonyítjuk a halmazelmélet két nevezetes részelméletének ellentmondásmentességét.

A halmazelmélet nyelvének két logikai függvénye van, ezért a nyelvnek pontosan *négy* helyettesítés-invariáns értékelése van:

– az $\omega_{\mathbf{i},\mathbf{i}}$ függvény, amely minden elemi formulához az $\mathbf{i}$ értéket rendeli;

– az $\omega_{\mathbf{i},\mathbf{h}}$ függvény, amely minden $=$ jellel kezdődő (vagyis $\mathbf{T} = \mathbf{S}$ alakú) formulához az $\mathbf{i}$, és minden $\in$ jellel kezdődő (vagyis $\mathbf{T} \in \mathbf{S}$ alakú) formulához a $\mathbf{h}$ értéket rendeli;

– az $\omega_{\mathbf{h},\mathbf{i}}$ függvény, amely minden $=$ jellel kezdődő (vagyis $\mathbf{T} = \mathbf{S}$ alakú) formulához a $\mathbf{h}$, és minden $\in$ jellel kezdődő (vagyis $\mathbf{T} \in \mathbf{S}$ alakú) formulához az $\mathbf{i}$ értéket rendeli;

– az $\omega_{\mathbf{h},\mathbf{h}}$ függvény, amely minden elemi formulához a $\mathbf{h}$ értéket rendeli.

Jelölés. Ha ω a halmazelmélet nyelvének helyettesítés-invariáns értékelése, akkor $\omega[=]$ jelöli az $\omega(\mathbf{T} = \mathbf{S})$ értéket, és $\omega[\in]$ jelöli az $\omega(\mathbf{T} \in \mathbf{S})$ értéket, ahol $\mathbf{T}$ és $\mathbf{S}$ tetszőleges objektumok.

A definíció alapján nyilvánvaló, hogy fennállnak a következő összefüggések:

$$\omega_{\mathbf{i},\mathbf{i}}[=] \equiv \omega_{\mathbf{i},\mathbf{i}}[\in] \equiv \mathbf{i}, \quad \omega_{\mathbf{i},\mathbf{h}}[=] \equiv \mathbf{i}, \quad \omega_{\mathbf{i},\mathbf{h}}[\in] \equiv \mathbf{h},$$
$$\omega_{\mathbf{h},\mathbf{h}}[=] \equiv \omega_{\mathbf{h},\mathbf{h}}[\in] \equiv \mathbf{h}, \quad \omega_{\mathbf{h},\mathbf{i}}[=] \equiv \mathbf{h}, \quad \omega_{\mathbf{h},\mathbf{i}}[\in] \equiv \mathbf{i}.$$

4.2.1. Lemma. *Ha ω a halmazelmélet nyelvének helyettesítés-invariáns értékelése, akkor*

$$\overline{\omega}(\ (\forall x)(\forall y)((\forall z)((z \in x)\Leftrightarrow(z \in y)) \Rightarrow (x = y))\ ) \ \equiv\ \omega[=],$$
$$\overline{\omega}(\ (\forall x)(\forall y)(\exists u)(\forall z)((z \in u)\Leftrightarrow((z = x) \vee (z = y)))\ ) \ \equiv\ \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \omega[=]),$$
$$\overline{\omega}(\ (\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\forall u)((u \in z) \Rightarrow (u \in x)))\ ) \ \equiv\ \omega[\in],$$
$$\overline{\omega}(\ (\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\exists u)((z \in u) \wedge (u \in x)))\ ) \ \equiv\ \mathbf{i},$$
$$\overline{\omega}(\ (\exists x)((\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^+ \in x)))\ ) \ \equiv\ \omega[\in].$$

Ha $\mathbf{A}$ *formula,* $\mathbf{T}$ *objektum és* $\mathbf{x}$ *változó a halmazelméletben, akkor*

$$\overline{\omega}(\ (\forall\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})\ ) \ \equiv\ \mathfrak{B}_{\Rightarrow}(\omega[\in], \overline{\omega}(\mathbf{A})).$$

Továbbá, ha A_{ac} *jelöli a kiválasztási axiómát, akkor*

$$\overline{\omega}(A_{ac}) \ \equiv\ \mathfrak{B}_{\vee}(\omega[\in], \omega[=]).$$

Bizonyítás. A következő értékelésekben csak ω helyettesítés-invarianciáját alkalmazzuk.

$$\begin{gathered}\overline{\omega}((\forall x)(\forall y)((\forall z)((z \in x)\Leftrightarrow(z \in y)) \Rightarrow (x = y)))\equiv\overline{\omega}((\forall z)((z \in x)\Leftrightarrow(z \in y)) \Rightarrow (x = y)) \\ \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}((\forall z)((z \in x)\Leftrightarrow(z \in y))), \overline{\omega}(x = y)) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}((z \in x)\Leftrightarrow(z \in y)), \omega[=]) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\Leftrightarrow}(\overline{\omega}(z \in x), \overline{\omega}(z \in y)), \omega[=]) \equiv \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\Leftrightarrow}(\omega[\in], \omega[\in]), \omega[=]) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\mathbf{i}, \omega[=]) \equiv \omega[=].\end{gathered}$$

$$\begin{gathered}\overline{\omega}((\forall x)(\forall y)(\exists u)(\forall z)((z \in u)\Leftrightarrow((z = x) \vee (z = y))))\equiv\overline{\omega}((z \in u)\Leftrightarrow((z = x) \vee (z = y))) \\ \equiv \mathfrak{B}_{\Leftrightarrow}(\overline{\omega}(z \in u), \overline{\omega}((z = x) \vee (z = y))) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \mathfrak{B}_{\vee}(\overline{\omega}(z = x), \overline{\omega}(z = y))) \equiv \\ \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \mathfrak{B}_{\vee}(\omega[=], \omega[=])) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \omega[=]).\end{gathered}$$

$$\begin{gathered}\overline{\omega}((\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\forall u)((u \in z) \Rightarrow (u \in x)))) \equiv \\ \equiv \overline{\omega}((z \in y)\Leftrightarrow(\forall u)((u \in z) \Rightarrow (u \in x))) \equiv \mathfrak{B}_{\Leftrightarrow}(\overline{\omega}(z \in y), \overline{\omega}((\forall u)((u \in z) \Rightarrow (u \in x)))) \\ \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \overline{\omega}((u \in z) \Rightarrow (u \in x))) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \mathfrak{B}_{\Rightarrow}(\overline{\omega}(u \in z), \overline{\omega}(u \in x))) \equiv \\ \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \mathfrak{B}_{\Rightarrow}(\omega[\in], \omega[\in])) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \mathbf{i}) \equiv \omega[\in].\end{gathered}$$

$$\begin{gathered}\overline{\omega}((\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\exists u)((z \in u) \wedge (u \in x)))) \equiv \\ \overline{\omega}((z \in y)\Leftrightarrow(\exists u)((z \in u) \wedge (u \in x))) \equiv \mathfrak{B}_{\Leftrightarrow}(\overline{\omega}(z \in y), \overline{\omega}((\exists u)((z \in u) \wedge (u \in x)))) \equiv \\ \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \overline{\omega}((z \in u) \wedge (u \in x))) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \mathfrak{B}_{\wedge}(\overline{\omega}(z \in u), \overline{\omega}(u \in x))) \equiv \\ \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \mathfrak{B}_{\wedge}(\omega[\in], \omega[\in])) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \omega[\in]) \equiv \mathbf{i}.\end{gathered}$$

$$\begin{gathered}\overline{\omega}((\exists x)((\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^{+} \in x)))) \equiv \overline{\omega}((\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^{+} \in x))) \\ \equiv \mathfrak{B}_{\wedge}(\overline{\omega}(\emptyset \in x), \overline{\omega}((\forall y)((y \in x) \Rightarrow (y^{+} \in x)))) \equiv \mathfrak{B}_{\wedge}(\omega[\in], \overline{\omega}((y \in x) \Rightarrow (y^{+} \in x))) \equiv \\ \equiv \mathfrak{B}_{\wedge}(\omega[\in], \mathfrak{B}_{\Rightarrow}(\overline{\omega}(y \in x), \overline{\omega}(y^{+} \in x))) \equiv \mathfrak{B}_{\wedge}(\omega[\in], \mathfrak{B}_{\Rightarrow}(\omega[\in], \omega[\in])) \equiv \\ \equiv \mathfrak{B}_{\wedge}(\omega[\in], \mathbf{i}) \equiv \omega[\in].\end{gathered}$$

Ha $\mathbf{A}$ formula és $\mathbf{x}$, $\mathbf{y}$ olyan különböző változók, hogy $\mathbf{y}$ nem szerepel $\mathbf{A}$-ban, akkor

$$\begin{gathered}\overline{\omega}(\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})) \equiv \overline{\omega}((\exists\mathbf{y})(\forall\mathbf{x})((\mathbf{x} \in \mathbf{y})\Leftrightarrow\mathbf{A})) \equiv \overline{\omega}((\mathbf{x} \in \mathbf{y})\Leftrightarrow\mathbf{A}) \equiv \\ \equiv \mathfrak{B}_{\Leftrightarrow}(\overline{\omega}(x \in y), \overline{\omega}(\mathbf{A})) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \overline{\omega}(\mathbf{A})).\end{gathered}$$

Legyen most $\mathbf{A}$ formula, $\mathbf{T}$ objektum és $\mathbf{x}$ változó. Legyen $\mathbf{y}$ olyan $\mathbf{x}$-től különböző változó, amely nem szerepel $\mathbf{A}$-ban. Ekkor az előző bekezdés alapján

$$\begin{gathered}\overline{\omega}((\forall\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}((\forall\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T}))), \overline{\omega}(\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}))) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})), \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \overline{\omega}(\mathbf{A}))) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A}), \overline{\omega}(\mathbf{x} \in \mathbf{T})), \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \overline{\omega}(\mathbf{A}))) \equiv \\ \equiv \mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{A}), \omega[\in]), \mathfrak{B}_{\Leftrightarrow}(\omega[\in], \overline{\omega}(\mathbf{A}))) \equiv \mathfrak{B}_{\Rightarrow}(\omega[\in], \overline{\omega}(\mathbf{A})),\end{gathered}$$

mert könnyen ellenőrizhető (például megfelelő logikai táblázat felírásával), hogy ha **b** és **c** az **i** vagy **h** értékek bármelyikét jelölik, akkor

$$\mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\Rightarrow}(\mathbf{b},\mathbf{c}),\mathfrak{B}_{\Leftrightarrow}(\mathbf{c},\mathbf{b})) \equiv \mathfrak{B}_{\vee}(\mathbf{b},\mathfrak{B}_{\neg}(\mathbf{c})) \equiv \mathfrak{B}_{\Rightarrow}(\mathbf{c},\mathbf{b}).$$

Az $\overline{\omega}(A_{ac})$ értékének meghatározásához először kiszámítjuk az $\overline{\omega}(\mathfrak{Rel}(\mathbf{T}))$ és $\overline{\omega}(\mathfrak{Fnc}(\mathbf{T}))$ értékeket, ahol $\mathbf{T}$ tetszőleges objektum a halmazelmélet nyelvében.

Legyen tehát $\mathbf{T}$ objektum és $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben. Ekkor

$$\begin{aligned}\overline{\omega}(\mathfrak{Rel}(\mathbf{T})) &\equiv \overline{\omega}((\forall\mathbf{z})((\mathbf{z}\in\mathbf{T}) \Rightarrow (\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{z}=(\mathbf{x},\mathbf{y})))) \equiv \\ &\equiv \overline{\omega}((\mathbf{z}\in\mathbf{T}) \Rightarrow (\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{z}=(\mathbf{x},\mathbf{y}))) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{z}\in\mathbf{T}),\overline{\omega}((\exists\mathbf{x})(\exists\mathbf{y})(\mathbf{z}=(\mathbf{x},\mathbf{y})))) \\ &\equiv \mathfrak{B}_{\Rightarrow}(\omega[\in],\overline{\omega}(\mathbf{z}=(\mathbf{x},\mathbf{y}))) \equiv \mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]).\end{aligned}$$

Ebből következik, hogy ha $\mathbf{T}$ objektum és $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, akkor

$$\begin{aligned}\overline{\omega}(\mathfrak{Fnc}(\mathbf{T})) &\equiv \overline{\omega}(\mathfrak{Rel}(\mathbf{T}) \wedge (\forall\mathbf{x})(\forall\mathbf{y})(\forall\mathbf{z})((((\mathbf{x},\mathbf{y})\in\mathbf{T}) \wedge ((\mathbf{x},\mathbf{z})\in\mathbf{T})) \Rightarrow (\mathbf{y}=\mathbf{z}))) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\overline{\omega}(\mathfrak{Rel}(\mathbf{T})),\overline{\omega}((\forall\mathbf{x})(\forall\mathbf{y})(\forall\mathbf{z})((((\mathbf{x},\mathbf{y})\in\mathbf{T}) \wedge ((\mathbf{x},\mathbf{z})\in\mathbf{T})) \Rightarrow (\mathbf{y}=\mathbf{z})))) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\overline{\omega}((((\mathbf{x},\mathbf{y})\in\mathbf{T}) \wedge ((\mathbf{x},\mathbf{z})\in\mathbf{T})) \Rightarrow (\mathbf{y}=\mathbf{z}))) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\wedge}(\overline{\omega}((\mathbf{x},\mathbf{y})\in\mathbf{T}),\overline{\omega}((\mathbf{x},\mathbf{z})\in\mathbf{T})),\overline{\omega}(\mathbf{y}=\mathbf{z}))) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\mathfrak{B}_{\Rightarrow}(\mathfrak{B}_{\wedge}(\omega[\in],\omega[\in]),\omega[=])) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=])) \equiv \mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]).\end{aligned}$$

A definíció szerint nyilvánvaló, hogy $A_{ac} \equiv (\forall F)(\mathbf{B} \Rightarrow \mathbf{C})$, ahol

$$\begin{aligned}\mathbf{B} &\equiv \mathfrak{Fnc}(F) \wedge (\forall x)((x\in \mathrm{Dom}(F)) \Rightarrow (F(x)\neq\emptyset)), \\ \mathbf{C} &\equiv (\exists f)((\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f)=\mathrm{Dom}(F)) \wedge (\forall x)((x\in\mathrm{Dom}(f)) \Rightarrow (f(x)\in F(x)))),\end{aligned}$$

következésképpen

$$\overline{\omega}(A_{ac}) \equiv \overline{\omega}((\forall F)(\mathbf{B}\Rightarrow\mathbf{C})) \equiv \overline{\omega}(\mathbf{B}\Rightarrow\mathbf{C}) \equiv \mathfrak{B}_{\Rightarrow}(\overline{\omega}(\mathbf{B}),\overline{\omega}(\mathbf{C})).$$

Világos, hogy

$$\begin{aligned}\overline{\omega}(\mathbf{B}) &\equiv \mathfrak{B}_{\wedge}(\overline{\omega}(\mathfrak{Fnc}(F)),\overline{\omega}((\forall x)((x\in\mathrm{Dom}(F)) \Rightarrow (F(x)\neq\emptyset)))) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\overline{\omega}((x\in\mathrm{Dom}(F)) \Rightarrow (F(x)\neq\emptyset))) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\mathfrak{B}_{\Rightarrow}(\overline{\omega}(x\in\mathrm{Dom}(F)),\overline{\omega}(F(x)\neq\emptyset))) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\mathfrak{B}_{\Rightarrow}(\omega[\in],\mathfrak{B}_{\neg}(\omega[=]))) \equiv \mathfrak{B}_{\neg}(\omega[\in]),\end{aligned}$$

mert könnyen belátható, hogy ha **b** és **c** az **i** vagy **h** értékek bármelyikét jelölik, akkor

$$\mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\mathbf{b},\mathbf{c}),\mathfrak{B}_{\Rightarrow}(\mathbf{b},\mathfrak{B}_{\neg}(\mathbf{c}))) \equiv \mathfrak{B}_{\neg}(\mathbf{b}).$$

Ugyanakkor

$$\begin{aligned}\overline{\omega}(\mathbf{C}) &\equiv \overline{\omega}((\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f)=\mathrm{Dom}(F)) \wedge (\forall x)((x\in\mathrm{Dom}(f)) \Rightarrow (f(x)\in F(x)))) \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\wedge}(\overline{\omega}(\mathfrak{Fnc}(f)),\overline{\omega}(\mathrm{Dom}(f)=\mathrm{Dom}(F))),\overline{\omega}((x\in\mathrm{Dom}(f)) \Rightarrow (f(x)\in F(x)))) \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\omega[=]),\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[\in])) \equiv \\ &\equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\omega[=]),\mathbf{i}) \equiv \mathfrak{B}_{\wedge}(\mathfrak{B}_{\Rightarrow}(\omega[\in],\omega[=]),\omega[=]) \equiv \omega[=],\end{aligned}$$

mert könnyen belátható, hogy ha $\mathbf{b}$ és $\mathbf{c}$ az $\mathbf{i}$ vagy $\mathbf{h}$ értékek bármelyikét jelölik, akkor $\mathfrak{B}_\wedge(\mathfrak{B}_\Rightarrow(\mathbf{b},\mathbf{c}),\mathbf{c}) \equiv \mathbf{c}$. Ez azt jelenti, hogy

$$\overline{\omega}(A_{ac}) \equiv \mathfrak{B}_\Rightarrow(\overline{\omega}(\mathbf{B}),\overline{\omega}(\mathbf{C})) \equiv \mathfrak{B}_\Rightarrow(\mathfrak{B}_\neg(\omega[\in]),\omega[=]) \equiv \mathfrak{B}_\vee(\omega[\in],\omega[=]),$$

hiszen ha $\mathbf{b}$ és $\mathbf{c}$ az $\mathbf{i}$ vagy $\mathbf{h}$ értékek bármelyikét jelölik, akkor nyilvánvalóan teljesül az, hogy $\mathfrak{B}_\Rightarrow(\mathfrak{B}_\neg(\mathbf{b}),\mathbf{c}) \equiv \mathfrak{B}_\vee(\mathbf{b},\mathbf{c})$. ■

4.2.2. Definíció. $\mathfrak{Ens}^*$ *jelöli azt a matematikai elméletet, amelynek*

- *matematikai nyelve a halmazelmélet nyelve;*
- *nincs matematikai axióma-sémája;*
- *explicit axiómái a meghatározottsági axióma, páraxióma, hatványhalmaz axióma, unió axióma, kiválasztási axióma és a végtelenségi axióma.*

Nyilvánvaló, hogy $\mathfrak{Ens}^*$ a halmazelmélet *részelmélete*, és $\mathfrak{Ens}^*$ úgy származtatható $\mathfrak{Ens}$-ből, hogy töröljük annak axiómarendszeréből a részhalmaz axióma-sémát.

4.2.3. Tétel. *A halmazelmélet elemi formulái nem cáfolhatók* $\mathfrak{Ens}^*$*-ban. A* $\mathfrak{Ens}^*$ *matematikai elmélet ellentmondásmentes, és létezik* $\mathfrak{S}_{\mathrm{sub}}$*-nak olyan eleme, amely nem tétel* $\mathfrak{Ens}^*$*-ban.*

Bizonyítás. Megmutatjuk, hogy az $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ függvény az $\mathfrak{Ens}^*$ elmélet minden explicit axiómájához az $\mathbf{i}$ értéket rendeli.

(I) Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}((\forall x)(\forall y)((\forall z)((z \in x)\Leftrightarrow(z \in y)) \Rightarrow (x = y))) \equiv \omega_{\mathbf{i},\mathbf{i}}[\in] \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ a *meghatározottsági axiómához* az $\mathbf{i}$ értéket rendeli.

(II) Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}((\forall x)(\forall y)(\exists u)(\forall z)((z \in u)\Leftrightarrow((z = x)\vee(z = y)))) \equiv \mathfrak{B}_\Leftrightarrow(\omega_{\mathbf{i},\mathbf{i}}[\in],\omega_{\mathbf{i},\mathbf{i}}[=]) \equiv \mathfrak{B}_\Leftrightarrow(\mathbf{i},\mathbf{i}) \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ a *páraxiómához* az $\mathbf{i}$ értéket rendeli.

(III) Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}((\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\forall u)((u \in z) \Rightarrow (u \in x)))) \equiv \omega_{\mathbf{i},\mathbf{i}}[\in] \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ a *hatványhalmaz axiómához* az $\mathbf{i}$ értéket rendeli.

(IV) Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}((\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\exists u)((z \in u) \wedge (u \in x))))) \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ az *unió axiómához* az $\mathbf{i}$ értéket rendeli.

(V) Ha A_{ac} jelöli a kiválasztási axiómát, akkor az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}(A_{ac}) \equiv \mathfrak{B}_\vee(\omega_{\mathbf{i},\mathbf{i}}[\in],\omega_{\mathbf{i},\mathbf{i}}[=]) \equiv \mathfrak{B}_\vee(\mathbf{i},\mathbf{i}) \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ a *kiválasztási axiómához* az $\mathbf{i}$ értéket rendeli.

(VI) Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}((\exists x)((\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^+ \in x)))) \equiv \omega_{\mathbf{i},\mathbf{i}}[\in] \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ a *végtelenségi axiómához* az $\mathbf{i}$ értéket rendeli.

Ezzel megmutattuk, hogy $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ az $\mathfrak{Ens}^*$ elmélet minden explicit axiómájához az $\mathbf{i}$ értéket rendeli. A predikátumkalkulus ellentmondásmentességének bizonyítása szerint $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ minden logikai axiómához szintén az $\mathbf{i}$ értéket rendeli, mert $\omega_{\mathbf{i},\mathbf{i}}$ olyan helyettesítés-invariáns értékelés, hogy minden $\mathbf{T}$ és $\mathbf{S}$ objektumra $\omega_{\mathbf{i},\mathbf{i}}(\mathbf{T} = \mathbf{S}) \equiv \mathbf{i}$. Ebből következik, hogy az $\mathfrak{Ens}^*$ elmélet minden $\mathbf{A}$ tételére $\overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{A}) \equiv \mathbf{i}$. Ez maga után vonja azt, hogy ha $\mathbf{A}$ *elemi formula*, akkor $\neg\mathbf{A}$ *nem tétel* $\mathfrak{Ens}^*$-ban, mert

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}(\neg\mathbf{A}) \equiv \mathfrak{B}_{\neg}(\overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{A})) \equiv \mathfrak{B}_{\neg}(\mathbf{i}) \equiv \mathbf{h}.$$

Tehát elemi formula *nem cáfolható* $\mathfrak{Ens}^*$-ban, így $\mathfrak{Ens}^*$ szükségképpen ellentmondásmentes.

Megmutatjuk, hogy $\mathfrak{S}_{\mathrm{sub}}$-nak van olyan eleme, amelyhez $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ a $\mathbf{h}$ értéket rendeli. Az előző lemmában láttuk, hogy ha $\mathbf{A}$ formula, $\mathbf{T}$ objektum és $\mathbf{x}$ változó, akkor

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}((\forall\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})) \equiv \mathfrak{B}_{\Rightarrow}(\omega_{\mathbf{i},\mathbf{i}}[\in], \overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{A})) \equiv$$

$$\equiv \mathfrak{B}_{\Rightarrow}(\mathbf{i}, \overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{A})) \equiv \overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{A}).$$

Tehát ha $\overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{A}) \equiv \mathbf{h}$ (például $\mathbf{A}$ egy elemi formula negációja), akkor $\overline{\omega_{\mathbf{i},\mathbf{i}}}$ a $(\forall\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ formulához a $\mathbf{h}$ értéket rendeli, következésképpen $(\forall\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ *nem tétel* $\mathfrak{Ens}^*$-ban, ugyanakkor $(\forall\mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ eleme $\mathfrak{S}_{\mathrm{sub}}$-nak, ha $\mathbf{x}$ nem szerepel $\mathbf{T}$-ben. ■

Megjegyezzük, hogy az előző tétel *bizonyításából* látható, hogy bármely $\mathbf{x}$ változóra a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \notin \mathbf{x})$ formula *nem tétel* $\mathfrak{Ens}^*$-ban, hiszen

$$\overline{\omega_{\mathbf{i},\mathbf{i}}}(\ \mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \notin \mathbf{x})\ ) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega_{\mathbf{i},\mathbf{i}}[\in], \overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{x} \notin \mathbf{x})) \equiv \mathfrak{B}_{\Leftrightarrow}(\mathbf{i}, \overline{\omega_{\mathbf{i},\mathbf{i}}}(\mathbf{x} \notin \mathbf{x})) \equiv$$

$$\equiv \mathfrak{B}_{\neg}(\omega_{\mathbf{i},\mathbf{i}}(\mathbf{x} \in \mathbf{x})) \equiv \mathfrak{B}_{\neg}(\mathbf{i}) = \mathbf{h}.$$

A Russel-tétel alapján a $\neg\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \notin \mathbf{x})$ formula *tétel* $\mathfrak{Ens}^*$-ban, mert ez logikai tétel a halmazelméletben, vagyis tétel $\mathfrak{Ens}_0$-ban, és $\mathfrak{Ens}_0$ részelmélete $\mathfrak{Ens}^*$-nak (valójában $\mathfrak{Ens}_0$ azonos a $\mathfrak{Ens}^*$ elmélet alatt fekvő predikátumkalkulussal). Azonban az $\mathfrak{Ens}$ elméletben nem tudjuk bebizonyítani, hogy a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \notin \mathbf{x})$ formula *nem tétel*; ha ezt bizonyítani tudnánk, akkor máris igazolva lenne a halmazelmélet ellentmondásmentessége.

Szintén az előző tétel bizonyításából látható, hogy a halmazelmélet nyelvének helyettesítés-invariáns értékeléseinek alkalmazásával nem lehet bizonyítani a halmazelmélet ellentmondásmentességét. Ehhez ugyanis a halmazelmélet nyelvének olyan ω helyettesítés-invariáns értékelésére volna szükség, amely a halmazelmélet minden explicit axiómájához és a részhalmaz axióma-séma minden eleméhez, valamint minden logikai axiómához az $\mathbf{i}$ értéket rendeli. De látható, hogy ha ω a meghatározottsági axiómához és a hatványhalmaz axiómához az $\mathbf{i}$ értéket rendeli, akkor már szükségképpen teljesül az, hogy $\omega \equiv \omega_{\mathbf{i},\mathbf{i}}$, így az előző bizonyítás szerint ω a halmazelmélet minden explicit axiómájához és minden logikai axiómájához az $\mathbf{i}$ értéket rendeli, azonban van olyan részhalmaz axióma, amelyhez ω a $\mathbf{h}$ értéket rendeli.

4.2.4. Definíció. $\mathfrak{Ens}_{**}$ *jelöli azt a matematikai elméletet, amelynek*

- *matematikai nyelve a halmazelmélet nyelve;*
- $\mathfrak{S}_{\mathrm{sub}}$ *az egyetlen matematikai axióma-sémája;*
- *explicit axiómái a meghatározottsági axióma, az unió axióma és a kiválasztási axióma.*

Nyilvánvaló, hogy $\mathfrak{Ens}_{**}$ a halmazelmélet *részelmélete*, és $\mathfrak{Ens}_{**}$ úgy származtatható $\mathfrak{Ens}$-ből, hogy töröljük annak axiómarendszeréből a páraxiómát, a hatványhalmaz axiómát és a végtelenségi axiómát. Világos továbbá, hogy $\mathfrak{Ens}_{**}$ bővítése a korábban bevezetett $\mathfrak{Ens}_{*}$ elméletnek.

4.2.5. Tétel. *A* $\mathfrak{Ens}_{**}$ *matematikai elmélet ellentmondásmentes, továbbá a páraxióma, a hatványhalmaz axióma és a végtelenségi axióma nem tétel* $\mathfrak{Ens}_{**}$*-ban.*

Bizonyítás. Megmutatjuk, hogy az $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ az $\mathfrak{Ens}_{**}$ matematikai elmélet minden explicit axiómájához és matematikai axiómájához az $\mathbf{i}$ értéket rendeli.

(I) Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{h}}}((\forall x)(\forall y)((\forall z)((z \in x)\Leftrightarrow(z \in y)) \Rightarrow (x = y))) \equiv \omega_{\mathbf{i},\mathbf{h}}[\in] \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ a *meghatározottsági axiómához* az $\mathbf{i}$ értéket rendeli.

(II) Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{h}}}((\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\exists u)((z \in u) \wedge (u \in x))))) \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ az *unió axiómához* az $\mathbf{i}$ értéket rendeli.

(III) Ha A_{ac} jelöli a kiválasztási axiómát, akkor az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{h}}}(A_{ac}) \equiv \mathfrak{B}_{\vee}(\omega_{\mathbf{i},\mathbf{h}}[\in], \omega_{\mathbf{i},\mathbf{h}}[=]) \equiv \mathfrak{B}_{\vee}(\mathbf{i}, \mathbf{h}) \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ a *kiválasztási axiómához* az $\mathbf{i}$ értéket rendeli.

(IV) Legyen $\mathbf{A}$ formula, $\mathbf{T}$ objektum és $\mathbf{x}$ olyan változó, amely nem szerepel $\mathbf{T}$-ben. Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{h}}}((\forall \mathbf{x})(\mathbf{A} \Rightarrow (\mathbf{x} \in \mathbf{T})) \Rightarrow \mathfrak{Coll}_{\mathbf{x}}(\mathbf{A}))\equiv\mathfrak{B}_{\Rightarrow}(\omega_{\mathbf{i},\mathbf{h}}[\in], \overline{\omega_{\mathbf{i},\mathbf{h}}}(\mathbf{A}))\equiv\mathfrak{B}_{\Rightarrow}(\mathbf{h}, \overline{\omega_{\mathbf{i},\mathbf{h}}}(\mathbf{A})) \equiv \mathbf{i},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ minden *részhalmaz axiómához* az $\mathbf{i}$ értéket rendeli.

A predikátumkalkulus ellentmondásmentességének bizonyítása szerint $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ minden logikai axiómához szintén az $\mathbf{i}$ értéket rendeli, mert $\omega_{\mathbf{i},\mathbf{h}}$ olyan helyettesítés-invariáns értékelés, hogy minden $\mathbf{T}$ és $\mathbf{S}$ objektumra $\omega_{\mathbf{i},\mathbf{h}}(\mathbf{T} = \mathbf{S}) \equiv \mathbf{i}$. Ebből következik, hogy az $\mathfrak{Ens}_{**}$ elmélet minden $\mathbf{A}$ tételére $\overline{\omega_{\mathbf{i},\mathbf{h}}}(\mathbf{A}) \equiv \mathbf{i}$. Ezért a $\mathfrak{Ens}_{**}$ elméletben sem a $\mathbf{T} \neq \mathbf{S}$, sem a $\mathbf{T} \in \mathbf{S}$ alakú formulák *nem tételek* (ahol $\mathbf{T}$ és $\mathbf{S}$ objektumok), hiszen ezekhez $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ a $\mathbf{h}$ értéket rendeli. Ebből az is látható, hogy az $\mathfrak{Ens}_{**}$ matematikai elmélet ellentmondásmentes.

Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{h}}}((\forall x)(\forall y)(\exists u)(\forall z)((z \in u)\Leftrightarrow((z = x) \vee (z = y)))) \equiv \mathfrak{B}_{\Leftrightarrow}(\omega_{\mathbf{i},\mathbf{h}}[\in], \omega_{\mathbf{i},\mathbf{h}}[=]) \equiv$$

$$\equiv \mathfrak{B}_{\Leftrightarrow}(\mathbf{i}, \mathbf{h}) \equiv \mathbf{h},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ a *páraxiómához* a $\mathbf{h}$ értéket rendeli, következésképpen a páraxióma *nem tétel* $\mathfrak{Ens}_{**}$-ban.

Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{h}}}((\forall x)(\exists y)(\forall z)((z \in y)\Leftrightarrow(\forall u)((u \in z) \Rightarrow (u \in x)))) \equiv \omega_{\mathbf{i},\mathbf{h}}[\in] \equiv \mathbf{h},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ a *hatványhalmaz axiómához* a $\mathbf{h}$ értéket rendeli, következésképpen a hatványhalmaz axióma *nem tétel* $\mathfrak{Ens}_{**}$-ban.

Az előző lemma szerint

$$\overline{\omega_{\mathbf{i},\mathbf{h}}}((\exists x)((\emptyset \in x) \wedge (\forall y)((y \in x) \Rightarrow (y^+ \in x)))) \equiv \omega_{\mathbf{i},\mathbf{h}}[\in] \equiv \mathbf{h},$$

tehát $\overline{\omega_{\mathbf{i},\mathbf{h}}}$ a *végtelenségi axiómához* a $\mathbf{h}$ értéket rendeli, következésképpen a végtelenségi axióma *nem tétel* $\mathfrak{Ens}_{**}$-ban. ■

A Russel-tétel szerint, ha $\mathbf{x}$ változó, akkor a $\neg\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \notin \mathbf{x})$ formula *tétel* $\mathfrak{Ens}_{*}$-ban, ugyanakkor $\mathfrak{Ens}_{*}$ részelmélete $\mathfrak{Ens}_{**}$-nak, ezért ez a formula $\mathfrak{Ens}_{**}$-ban is tétel. Az előző tétel alapján $\mathfrak{Ens}_{**}$ ellentmondásmentes, ezért a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \notin \mathbf{x})$ formula *nem tétel* $\mathfrak{Ens}_{**}$-ban. Ez azt mutatja, hogy létezik a halmazelméletnek olyan $\mathbf{A}$ formulája és olyan $\mathbf{x}$ változó, hogy $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ nem tétel $\mathfrak{Ens}_{**}$-ban, vagyis $\mathbf{A}$ nem kollektivizáló az $\mathbf{x}$ változóban az $\mathfrak{Ens}_{**}$ elméletben.

Figyeljük meg a két utolsó tétel *komplementer* jellegét. A $\mathfrak{Ens}^{*}$ elmélet explicit axiómákban gazdag, hiszen a halmazelmélet mindegyik explicit axiómája $\mathfrak{Ens}^{*}$-nak is explicit axiómája; ugyanakkor $\mathfrak{Ens}^{*}$-nak nincs matematikai axióma-sémája. Ezzel szemben az $\mathfrak{Ens}_{**}$ elmélet explicit axiómákban jóval szegényebb, hiszen csak a meghatározottsági axióma, az unió axióma és a kiválasztási axióma az explicit axiómái; ugyanakkor a részhalmaz axióma-séma hozzátartozik az $\mathfrak{Ens}_{**}$ axiómarendszeréhez. Mindkét elmélet ellentmondásmentesnek bizonyult. A halmazelmélet ellentmondásmentességét azért nem tudtuk eddig bizonyítani, mert az explicit axiómákban gazdag *és* a részhalmaz axiómaséma is hozzártartozik az axióma-rendszeréhez. Az analízis halmazelméleti alapjait tárgyaló **5.**, **6.** és **7.** fejezetben nyilvánvalóvá válik az, hogy a matematika számára fontos matematikai objektumok akkor állíthatók elő és akkor rendelkeznek a velük kapcsolatban elvárható tulajdonságokkal, ha a részhalmaz axióma-sémát a halmazelmélet *összes* explicit axiómájával *együtt* alkalmazhatjuk. Ezért sem az $\mathfrak{Ens}^{*}$, sem az $\mathfrak{Ens}_{**}$ elmélet *nem elégséges* alap egy tartalmas matematika felépítéséhez.

4.3. A kiválasztási axióma bizonyításáról

Az elsőrendű nyelvekre alapozott halmazelméletelekben a kiválasztási axióma *konzisztens* abban az értelemben, hogy sem a kiválasztási axióma, sem annak tagadása nem tétel abban a "maradék" halmazelméletben, amelyben nem expicit axióma a kiválasztási axióma; feltéve, hogy e "maradék" halmazelmélet ellentmondásmentes. Azonban a Hilbert–Bourbaki-nyelvre alapozott halmazelméletben a kiválasztási axióma *bebizonyítható.* Most erről a bizonyításáról lesz szó.

4.3.1. Tétel. *Jelölje* $\mathfrak{Ens}_b$ *azt a matematikai elméletet amelynek*

• *matematikai nyelve a halmazelmélet nyelve;*

• $\mathfrak{S}_{sub}$ *az egyetlen axióma-sémája;*

• *explicit axiómái a meghatározottsági axióma, páraxióma, hatványhalmaz axióma, és az unió axióma.*

A kiválasztási axióma tétel $\mathfrak{Ens}_b$*-ben, vagyis a*

$$(\forall F)(\ (\mathfrak{Fnc}(F) \wedge (\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset)))\ \Rightarrow$$
$$(\exists f)((\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f) = \mathrm{Dom}(F)) \wedge (\forall x)((x \in \mathrm{Dom}(f)) \Rightarrow (f(x) \in F(x))))\ )$$

formula levezethető $\mathfrak{Ens}_b$*-ben.*

Bizonyítás. Jelölje $\mathfrak{T}$ az $\mathfrak{Ens}_b[\mathfrak{Fnc}(F) \wedge (\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset))]$ elméletet, tehát a $\mathfrak{T}$ elméletben explicit axióma a

$$\mathfrak{Fnc}(F) \wedge (\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset))$$

formula, így a konjunkció logikai alaptulajdonságából következik, hogy $\mathfrak{T}$-ben az $\mathfrak{Fnc}(F)$ és $(\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset))$ formulák tételek. Az univerzális kvantor logikai alaptulajdonsága szerint

$$(\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset)) \;\Rightarrow\; ((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset))$$

tétel $\mathfrak{T}$-ben, így a leválasztás szabályát alkalmazva kapjuk, hogy $(x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset)$ is tétel $\mathfrak{T}$-ben. Ugyanakkor, ha $\mathbf{T}$ tetszőleges olyan objektum a halmazelmélet nyelvében, amelyben nem szerepel az y változó, akkor

$$\mathbf{T} \neq \emptyset \;\Rightarrow\; (\exists y)(y \in \mathbf{T})$$

tétel $\mathfrak{T}$-ben. Itt $\mathbf{T}$ helyére az $F(x)$ objektumot helyettesítve kapjuk, hogy $(F(x) \neq \emptyset) \Rightarrow (\exists y)(y \in F(x))$ tétel $\mathfrak{T}$-ben, tehát a láncszabály alapján

$$(x \in \mathrm{Dom}(F)) \;\Rightarrow\; (\exists y)(y \in F(x))$$

tétel $\mathfrak{T}$-ben. Az egzisztenciális kvantor értelmezése szerint

$$(\exists y)(y \in F(x)) \equiv (\varepsilon_y(y \in F(x))|y)(y \in F(x)) \equiv \varepsilon_y(y \in F(x)) \in F(x)$$

teljesül, ami azt jelenti, hogy

$$(x \in \mathrm{Dom}(F)) \;\Rightarrow\; (\varepsilon_y(y \in F(x)) \in F(x))$$

tétel $\mathfrak{T}$-ben. Az x változó nem szerepel a $\mathfrak{T}$ elmélet egyetlen explicit axiómájában sem, ezért az általánosítás szabálya (GEN) alapján

$$(\forall x)((x \in \mathrm{Dom}(F)) \;\Rightarrow\; (\varepsilon_y(y \in F(x)) \in F(x)))$$

tétel $\mathfrak{T}$-ben.

Megmutatjuk, hogy a

$$\mathfrak{Coll}_z(\;(\exists x)(\;(x \in \mathrm{Dom}(F)) \wedge (z = (x, \varepsilon_y(y \in F(x))))\;)\;)$$

formula tétel $\mathfrak{T}$-ben. Jelölje $\mathfrak{T}'$ a $\mathfrak{T}[(\exists x)((x \in \mathrm{Dom}(F)) \wedge (z = (x, \varepsilon_y(y \in F(x)))))]$ elméletet, és jelölje $\mathbf{X}$ az $\varepsilon_x((x \in \mathrm{Dom}(F)) \wedge (z = (x, \varepsilon_y(y \in F(x)))))$ objektumot. Ekkor az egzisztenciális kvantor definíciója alapján az

$$(\mathbf{X} \in \mathrm{Dom}(F)) \wedge (z = (\mathbf{X}, \varepsilon_y(y \in F(\mathbf{X}))))$$

formula tétel $\mathfrak{T}'$-ben, ahol $F(\mathbf{X})$ jelöli az $(\mathbf{X}|x)F(x)$ objektumot. Itt felhasználtuk azt, hogy $(\mathbf{X}|x)\varepsilon_y(y \in F(x)) \equiv \varepsilon_y(y \in (\mathbf{X}|x)F(x))$, mert x és y különböző változók és y nem szerepel $\mathbf{X}$-ben. A konjunkció logikai alaptulajdonsága szerint az $\mathbf{X} \in \mathrm{Dom}(F)$ és $z = (\mathbf{X}, \varepsilon_y(y \in F(\mathbf{X})))$ formulák tételek $\mathfrak{T}'$-ben. Az univerzális kvantor logikai alaptulajdonsága szerint a

$$\begin{gathered}(\forall x)((x \in \mathrm{Dom}(F)) \;\Rightarrow\; (\varepsilon_y(y \in F(x)) \in F(x))) \;\Rightarrow\\ \Rightarrow\; ((\mathbf{X} \in \mathrm{Dom}(F)) \;\Rightarrow\; (\varepsilon_y(y \in F(\mathbf{X})) \in F(\mathbf{X})))\end{gathered}$$

formula logikai tétel, így a dedukció-tétel kétszeres alkalmazásával kapjuk, hogy $(\varepsilon_y(y \in F(\mathbf{X})) \in F(\mathbf{X})))$ tétel $\mathfrak{T}'$-ben. Ugyanakkor, $\mathbf{X} \in \mathrm{Dom}(F)$ miatt $F(\mathbf{X}) \in \mathrm{Im}(F)$, ezért $\varepsilon_y(y \in F(\mathbf{X})) \in \bigcup(\mathrm{Im}(F))$. Ez azt jelenti, hogy $(\mathbf{X}, \varepsilon_y(y \in F(\mathbf{X}))) \in \mathrm{Dom}(F) \times \bigcup(\mathrm{Im}(F))$. Mivel pedig $z = (\mathbf{X}, \varepsilon_y(y \in F(\mathbf{X})))$ tétel $\mathfrak{T}'$-ben, így azt kapjuk, hogy $z \in \mathrm{Dom}(F) \times \bigcup(\mathrm{Im}(F))$ is tétel $\mathfrak{T}'$-ben. Ezért a dedukció-tétel szerint a

$$(\exists x)((x \in \mathrm{Dom}(F)) \wedge (z = (x, \varepsilon_y(y \in F(x))))) \;\Rightarrow\; (z \in \mathrm{Dom}(F) \times \bigcup(\mathrm{Im}(F)))$$

formula tétel $\mathfrak{T}$-ben. A (GEN) szabály alkalmazásával ebből kapjuk, hogy

$$(\forall z)(\ (\exists x)((x \in \mathrm{Dom}(F)) \wedge (z = (x, \varepsilon_y(y \in F(x))))) \;\Rightarrow\; (z \in \mathrm{Dom}(F) \times \bigcup(\mathrm{Im}(F)))\ )$$

tétel $\mathfrak{T}$-ben. Mivel a $\mathrm{Dom}(F) \times \bigcup(\mathrm{Im}(F))$ objektumban nem szerepel a z változó, így a részhalmaz axiómaséma alapján a $(\exists x)((x \in \mathrm{Dom}(F)) \wedge (z = (x, \varepsilon_y(y \in F(x)))))$ formula kollektivizáló a z változóban a $\mathfrak{T}$ elméletben.

Legyen

$$\Phi := \{\ z \mid (\exists x)(\ (x \in \mathrm{Dom}(F)) \wedge (\ z = (x, \varepsilon_y(y \in F(x)))\ )\ )\}.$$

Könnyen belátható, hogy a

$$(\mathfrak{Fnc}(\Phi)) \wedge (\mathrm{Dom}(\Phi) = \mathrm{Dom}(F)) \wedge (\forall x)((x \in \mathrm{Dom}(\Phi)) \Rightarrow (\Phi(x) \in F(x)))$$

formula tétel $\mathfrak{T}$-ben, tehát a

$$(\Phi|f)(\ (\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f) = \mathrm{Dom}(F)) \wedge (\forall x)((x \in \mathrm{Dom}(f)) \Rightarrow (f(x) \in F(x)))\ )$$

formula tétel $\mathfrak{T}$-ben, így a $\mathfrak{S}_5$ axiómasémát és a leválasztás szabályát alkalmazva nyerjük, hogy

$$(\exists f)((\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f) = \mathrm{Dom}(F)) \wedge (\forall x)((x \in \mathrm{Dom}(f)) \Rightarrow (f(x) \in F(x))))\ )$$

tétel $\mathfrak{T}$-ben. A dedukció-tétel alapján ez azt jelenti, hogy a

$$(\mathfrak{Fnc}(F) \wedge (\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset))) \;\Rightarrow$$
$$(\exists f)((\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f) = \mathrm{Dom}(F)) \wedge (\forall x)((x \in \mathrm{Dom}(f)) \Rightarrow (f(x) \in F(x))))$$

formula levezethető $\mathfrak{Ens}_b$-ben. Az F változó nem szerepel az $\mathfrak{Ens}_b$ elmélet egyetlen explicit axiómájában sem, így az általánosítás szabályát alkalmazva kapjuk, hogy a

$$(\forall F)(\ (\mathfrak{Fnc}(F) \wedge (\forall x)((x \in \mathrm{Dom}(F)) \Rightarrow (F(x) \neq \emptyset))) \;\Rightarrow$$
$$(\exists f)((\mathfrak{Fnc}(f)) \wedge (\mathrm{Dom}(f) = \mathrm{Dom}(F)) \wedge (\forall x)((x \in \mathrm{Dom}(f)) \Rightarrow (f(x) \in F(x))))\ )$$

formula levezethető $\mathfrak{Ens}_b$-ben. ■

4.4. Számosságok és számosság-operációk

Egy formális axiomatikus halmazelmélet feletti *számosság-operációnak* nevezünk minden olyan hozzárendelést, amely az elmélet minden objektumához egy vele ekvipotens objektumot rendel úgy, hogy bármely két objektum *ekvipotenciája* ekvivalens a hozzájuk számosság-operáció által rendelt objektumok *egyenlőségével*. Az elsőrendű nyelvekre alapozott halmazelméletelekben csak lényegesen nem triviális módszerekkel lehet számosság-operációt értelmezni. Azonban a Hilbert–Bourbaki-nyelvre alapozott halmazelméletben bevezethető egy kitüntetett számosság-operáció. Itt ennek az előállításáról lesz szó.

4.4.1. Definíció. *Ha* **T** *és* **S** *objektumok a halmazelmélet nyelvében, akkor* $\mathfrak{Eq}(\mathbf{T}, \mathbf{S})$ *a következő formula rövidítése*

$$(\exists \mathbf{f})\ (\ \mathfrak{Fnc}(\mathbf{f}) \wedge (\mathrm{Dom}(\mathbf{f}) = \mathbf{T}) \wedge (\mathrm{Im}(\mathbf{f}) = \mathbf{S}) \wedge \\ \wedge (\forall \mathbf{z})(\forall \mathbf{z}')(((\mathbf{z} \in \mathrm{Dom}(\mathbf{f})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{f})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathbf{f}(\mathbf{z}) \neq \mathbf{f}(\mathbf{z}'))\ ),$$

ahol a $\mathbf{z}$, $\mathbf{z}'$, $\mathbf{f}$ *változók különbözőek és nem szerepelnek sem* **T***-ben, sem* **S***-ben. Ha az* $\mathfrak{Eq}(\mathbf{T}, \mathbf{S})$ *formula tétel a halmazelméletben, akkor azt mondjuk, hogy a* **T** *és* **S** *halmazok* **ekvipotensek**.

Könnyen belátható, hogy az előző definícióban felírt formula nem függ a $\mathbf{z}$, $\mathbf{z}'$, $\mathbf{f}$ változók választásától (feltéve, hogy azok különbözőek és nem szerepelnek sem **T**-ben, sem **S**-ben), ezért helyes a formula *jelölésében* csak a **T** és **S** objektumokat szerepeltetni.

4.4.2. Állítás. *Ha* **T***,* **S** *és* **R** *a halmazelmélet nyelvének objektumai, akkor az*

$$\mathfrak{Eq}(\mathbf{T}, \mathbf{T}), \\ \mathfrak{Eq}(\mathbf{T}, \mathbf{S}) \ \Rightarrow\ \mathfrak{Eq}(\mathbf{S}, \mathbf{T}), \\ (\ \mathfrak{Eq}(\mathbf{T}, \mathbf{S}) \wedge \mathfrak{Eq}(\mathbf{S}, \mathbf{R})\ ) \ \Rightarrow\ \mathfrak{Eq}(\mathbf{T}, \mathbf{R})$$

kijelentések tételek a halmazelméletben.

Bizonyítás. (I) Jelölje $\mathrm{id}_{\mathbf{T}}$ az

$$\{\ \mathbf{u} \mid (\exists \mathbf{x})((\mathbf{x} \in \mathbf{T}) \wedge (\mathbf{u} = (\mathbf{x}, \mathbf{x})))\ \}$$

objektumot, ahol **x** és **u** olyan különböző változók, amelyek nem szerepelnek **T**-ben. Könnyen ellenőrizhető, hogy az $\mathfrak{Fnc}(\mathrm{id}_{\mathbf{T}})$, a $\mathrm{Dom}(\mathrm{id}_{\mathbf{T}}) = \mathbf{T}$, és az $\mathrm{Im}(\mathrm{id}_{\mathbf{T}}) = \mathbf{T}$ formulák tételek a halmazelméletben. Továbbá, a

$$(\forall \mathbf{x})((\mathbf{x} \in \mathbf{T}) \Rightarrow (\mathrm{id}_{\mathbf{T}}(\mathbf{x}) = \mathbf{x}))$$

formula is tétel a halmazelméletben, amiből következik, hogy a

$$(\forall \mathbf{z})(\forall \mathbf{z}')(\ ((\mathbf{z} \in \mathrm{Dom}(\mathrm{id}_{\mathbf{T}})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathrm{id}_{\mathbf{T}})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathrm{id}_{\mathbf{T}}(\mathbf{z}) \neq \mathrm{id}_{\mathbf{T}}(\mathbf{z}')\ )$$

formula tétel a halmazelméletben, ahol $\mathbf{z}$ és $\mathbf{z}'$ olyan különböző változók, amelyek nem szerepelnek **T**-ben. Ezért a konjunkció logikai alaptulajdonsága szerint az

$$\mathfrak{Fnc}(\mathrm{id}_{\mathbf{T}}) \ \wedge\ (\mathrm{Dom}(\mathrm{id}_{\mathbf{T}}) = \mathbf{T}) \ \wedge\ (\mathrm{Im}(\mathrm{id}_{\mathbf{T}}) = \mathbf{T}) \wedge \\ \wedge\ (\forall \mathbf{z})(\forall \mathbf{z}')(\ ((\mathbf{z} \in \mathrm{Dom}(\mathrm{id}_{\mathbf{T}})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathrm{id}_{\mathbf{T}})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathrm{id}_{\mathbf{T}}(\mathbf{z}) \neq \mathrm{id}_{\mathbf{T}}(\mathbf{z}')\ )$$

formula tétel a halmazelméletben, és ez a formula azonos a következővel:

$$(\mathrm{id}_{\mathbf{T}}|\mathbf{f})\ \ (\ \mathfrak{Fnc}(\mathbf{f}) \ \wedge\ (\mathrm{Dom}(\mathbf{f}) = \mathbf{T}) \ \wedge\ (\mathrm{Im}(\mathbf{f}) = \mathbf{T}) \wedge \\ \wedge\ (\forall \mathbf{z})(\forall \mathbf{z}')(\ ((\mathbf{z} \in \mathrm{Dom}(\mathbf{f})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{f})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathbf{f}(\mathbf{z}) \neq \mathbf{f}(\mathbf{z}')\ )\ ),$$

ahol **f** olyan változó, amely különbözik $\mathbf{z}$-től és $\mathbf{z}'$-től, és nem szerepel **T**-ben. Ebből a $\mathfrak{S}_5$ axiómaséma alapján leválasztással kapjuk, hogy $\mathfrak{Eq}(\mathbf{T}, \mathbf{T})$ tétel a halmazelméletben.

(II) Tegyük fel, hogy $\mathfrak{Eq}(\mathbf{T}, \mathbf{S})$ tétel a halmazelméletben, és jelöljön **F** egy olyan objektumot, amelyre

$$\mathfrak{Fnc}(\mathbf{F}) \wedge (\mathrm{Dom}(\mathbf{F}) = \mathbf{T}) \wedge (\mathrm{Im}(\mathbf{F}) = \mathbf{S}) \wedge \\ \wedge (\forall \mathbf{z})(\forall \mathbf{z}')(((\mathbf{z} \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathbf{F}(\mathbf{z}) \neq \mathbf{F}(\mathbf{z}'))$$

tétel a halmazelméletben, ahol $\mathbf{z}$ és $\mathbf{z}'$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, $\mathbf{S}$-ben és $\mathbf{F}$-ben. A konjunkció logikai alaptulajdonsága szerint az $\mathfrak{Fnc}(\mathbf{F})$, a $\mathrm{Dom}(\mathbf{F}) = \mathbf{T}$, az $\mathrm{Im}(\mathbf{F}) = \mathbf{S}$, valamint a

$$(\forall\mathbf{z})(\forall\mathbf{z}')(\ ((\mathbf{z} \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathbf{F}(\mathbf{z}) \neq \mathbf{F}(\mathbf{z}')\ )$$

formulák tételek a halmazelméletben. Jelölje $\mathbf{F}^{-1}$ az

$$\{\ \mathbf{u} \mid (\exists\mathbf{x})(\exists\mathbf{y})((\mathbf{x},\mathbf{y}) \in \mathbf{F}) \wedge (\mathbf{u} = (\mathbf{y},\mathbf{x})))\ \}$$

objektumot, ahol $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{u}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{F}$-ben. Könnyen ellenőrizhető, hogy az $\mathfrak{Fnc}(\mathbf{F}^{-1})$, a $\mathrm{Dom}(\mathbf{F}^{-1}) = \mathbf{S}$, valamint az $\mathrm{Im}(\mathbf{F}^{-1}) = \mathbf{T}$ formulák tételek a halmazelméletben. Továbbá, a

$$(\forall\mathbf{z})(\forall\mathbf{z}')\big(\big((\mathbf{z} \in \mathrm{Dom}(\mathbf{F}^{-1})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{F}^{-1})) \wedge (\mathbf{z} \neq \mathbf{z}')\big) \Rightarrow \mathbf{F}^{-1}(\mathbf{z}) \neq \mathbf{F}^{-1}(\mathbf{z}')\big)$$

tétel a halmazelméletben, ahol $\mathbf{z}$ és $\mathbf{z}'$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{F}^{-1}$-ben. Ezért a konjunkció logikai alaptulajdonsága szerint az

$$\begin{gathered}\mathfrak{Fnc}(\mathbf{F}^{-1})\ \wedge\ (\mathrm{Dom}(\mathbf{F}^{-1}) = \mathbf{S})\ \wedge\ (\mathrm{Im}(\mathbf{F}^{-1}) = \mathbf{T})\ \wedge \\ \wedge\ (\forall\mathbf{z})(\forall\mathbf{z}')\big(\big((\mathbf{z} \in \mathrm{Dom}(\mathbf{F}^{-1})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{F}^{-1})) \wedge (\mathbf{z} \neq \mathbf{z}')\big) \Rightarrow \mathbf{F}^{-1}(\mathbf{z}) \neq \mathbf{F}^{-1}(\mathbf{z}')\big)\end{gathered}$$

formula tétel a halmazelméletben, amiből a $\mathfrak{S}_5$ axiómaséma alapján leválasztással kapjuk, hogy $\mathfrak{Eq}(\mathbf{S},\mathbf{T})$ tétel a halmazelméletben.

(III) Tegyük fel, hogy $\mathfrak{Eq}(\mathbf{T},\mathbf{S}) \wedge \mathfrak{Eq}(\mathbf{S},\mathbf{R})$ tétel a halmazelméletben. Ekkor a konjunkció logikai alaptulajdonsága szerint a $\mathfrak{Eq}(\mathbf{T},\mathbf{S})$ és $\mathfrak{Eq}(\mathbf{S},\mathbf{R})$ formulák tételek a halmazelméletben. Jelöljön $\mathbf{F}$ egy olyan objektumot, amelyre

$$\begin{gathered}\mathfrak{Fnc}(\mathbf{F}) \wedge (\mathrm{Dom}(\mathbf{F}) = \mathbf{T}) \wedge (\mathrm{Im}(\mathbf{F}) = \mathbf{S}) \wedge \\ \wedge\ (\forall\mathbf{z})(\forall\mathbf{z}')(((\mathbf{z} \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathbf{F}(\mathbf{z}) \neq \mathbf{F}(\mathbf{z}'))\end{gathered}$$

tétel a halmazelméletben, ahol $\mathbf{z}$ és $\mathbf{z}'$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, $\mathbf{S}$-ben és $\mathbf{R}$-ben. Továbbá, jelöljön $\mathbf{G}$ egy olyan objektumot, amelyre

$$\begin{gathered}\mathfrak{Fnc}(\mathbf{G}) \wedge (\mathrm{Dom}(\mathbf{G}) = \mathbf{S}) \wedge (\mathrm{Im}(\mathbf{G}) = \mathbf{R}) \wedge \\ \wedge\ (\forall\mathbf{v})(\forall\mathbf{v}')(((\mathbf{v} \in \mathrm{Dom}(\mathbf{G})) \wedge (\mathbf{v}' \in \mathrm{Dom}(\mathbf{G})) \wedge (\mathbf{v} \neq \mathbf{v}')) \Rightarrow \mathbf{G}(\mathbf{v}) \neq \mathbf{G}(\mathbf{v}'))\end{gathered}$$

tétel a halmazelméletben, ahol $\mathbf{v}$ és $\mathbf{v}'$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, $\mathbf{S}$-ben és $\mathbf{R}$-ben. Jelölje $\mathbf{H}$ az

$$\{\ \mathbf{u} \mid (\exists\mathbf{x})(\exists\mathbf{y})(\exists\mathbf{z})\ ((\mathbf{x},\mathbf{y}) \in \mathbf{F}) \wedge ((\mathbf{y},\mathbf{z}) \in \mathbf{G})) \wedge (\mathbf{u} = (\mathbf{x},\mathbf{z}))\ \}$$

objektumot, ahol $\mathbf{u}$, $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{z}$ olyan különböző változók, amelyek nem szerepelnek $\mathbf{T}$-ben, $\mathbf{S}$-ben, $\mathbf{R}$-ben, $\mathbf{F}$-ben és $\mathbf{G}$-ben. A konjunkció logikai alaptulajdonsága szerint az $\mathfrak{Fnc}(\mathbf{F})$ és $\mathfrak{Fnc}(\mathbf{G})$ formulák tételek a halmazelméletben, amiből könnyen következik, hogy $\mathfrak{Fnc}(\mathbf{H})$ is tétel a halmazelméletben. Szintén a konjunkció logikai alaptulajdonsága szerint $\mathrm{Dom}(\mathbf{F}) = \mathbf{T}$, $\mathrm{Im}(\mathbf{F}) = \mathbf{S}$, $\mathrm{Dom}(\mathbf{G}) = \mathbf{S}$ és $\mathrm{Im}(\mathbf{G}) = \mathbf{R}$ tételek a halmazelméletben, ezért $\mathrm{Dom}(\mathbf{H}) = \mathbf{T}$ és $\mathrm{Im}(\mathbf{H}) = \mathbf{R}$ tétel a halmazelméletben. Végül, ismét a konjunkció logikai alaptulajdonsága szerint

$$(\forall\mathbf{z})(\forall\mathbf{z}')(((\mathbf{z} \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z}' \in \mathrm{Dom}(\mathbf{F})) \wedge (\mathbf{z} \neq \mathbf{z}')) \Rightarrow \mathbf{F}(\mathbf{z}) \neq \mathbf{F}(\mathbf{z}'))$$

és
$$(\forall \mathbf{v})(\forall \mathbf{v}')(((\mathbf{v} \in \mathrm{Dom}(\mathbf{G})) \wedge (\mathbf{v}' \in \mathrm{Dom}(\mathbf{G})) \wedge (\mathbf{v} \neq \mathbf{v}')) \Rightarrow \mathbf{G}(\mathbf{v}) \neq \mathbf{G}(\mathbf{v}'))$$
tételek a halmazelméletben, amiből könnyen belátható, hogy
$$(\forall \mathbf{z})(\forall \mathbf{v}')(((\mathbf{z} \in \mathrm{Dom}(\mathbf{H})) \wedge (\mathbf{v}' \in \mathrm{Dom}(\mathbf{H})) \wedge (\mathbf{z} \neq \mathbf{v}')) \Rightarrow (\mathbf{H}(\mathbf{z}) \neq \mathbf{H}(\mathbf{v}'))$$
tétel a halmazelméletben. Ezért a konjunkció logikai alaptulajdonsága szerint
$$\begin{gathered}\mathfrak{Fnc}(\mathbf{H}) \ \wedge \ (\mathrm{Dom}(\mathbf{H}) = \mathbf{T}) \ \wedge \ (\mathrm{Im}(\mathbf{H}) = \mathbf{R}) \wedge \\ \wedge \ (\forall \mathbf{z})(\forall \mathbf{v}')(((\mathbf{z} \in \mathrm{Dom}(\mathbf{H})) \wedge (\mathbf{v}' \in \mathrm{Dom}(\mathbf{H})) \wedge (\mathbf{z} \neq \mathbf{v}')) \Rightarrow (\mathbf{H}(\mathbf{z}) \neq \mathbf{H}(\mathbf{v}'))\end{gathered}$$
tétel a halmazelméletben, így a $\mathfrak{S}_5$ axiómaséma alapján leválasztással kapjuk, hogy $\mathfrak{Eq}(\mathbf{T}, \mathbf{R})$ tétel a halmazelméletben. ■

4.4.3. Definíció. *Ha* $\mathbf{T}$ *objektum a halmazelmélet nyelvében és az* $\mathbf{x}$ *változó nem szerepel* $\mathbf{T}$*-ben, akkor*
$$\mathrm{Card}(\mathbf{T}) \ := \ \varepsilon_{\mathbf{x}} (\mathfrak{Eq}(\mathbf{T}, \mathbf{x})),$$
és a $\mathrm{Card}(\mathbf{T})$ *objektumot a* $\mathbf{T}$ *halmaz* **számosságának** *nevezzük.*

Természetesen a definíció jó, mert ha az $\mathbf{x}$ és $\mathbf{x}'$ változók nem szerepelnek a halmazelmélet nyelvének $\mathbf{T}$ objektumában, akkor a helyettesítések tranzitivitásának szabályát alkalmazva ε-kifejezésekre kapjuk, hogy $\varepsilon_{\mathbf{x}} (\mathfrak{Eq}(\mathbf{T}, \mathbf{x})) \equiv \varepsilon_{\mathbf{x}'} (\mathfrak{Eq}(\mathbf{T}, \mathbf{x}'))$.

4.4.4. Tétel. *Ha* $\mathbf{T}$ *és* $\mathbf{S}$ *objektumok a halmazelmélet nyelvében, akkor az*
$$\begin{gathered}\mathfrak{Eq}(\mathbf{T}, \mathrm{Card}(\mathbf{T})), \\ \mathfrak{Eq}(\mathbf{T}, \mathbf{S}) \Leftrightarrow \mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S})\end{gathered}$$
formulák tételek a halmazelméletben. (*Tehát minden halmaz ekvipotens a számosságával, és két halmaz pontosan akkor ekvipotens, ha a számosságaik egyenlőek.*)

Bizonyítás. Legyen $\mathbf{x}$ olyan változó, amely nem szerepel a $\mathbf{T}$ objektumban. Ekkor $\mathfrak{Eq}(\mathbf{T}, \mathbf{T}) \equiv (\mathbf{T}|\mathbf{x})\mathfrak{Eq}(\mathbf{T}, \mathbf{x})$, tehát az előző állítás szerint $(\mathbf{T}|\mathbf{x})\mathfrak{Eq}(\mathbf{T}, \mathbf{x})$ tétel a halmazelméletben. Ugyanakkor a
$$(\mathbf{T}|\mathbf{x})\mathfrak{Eq}(\mathbf{T}, \mathbf{x}) \ \Rightarrow \ (\exists \mathbf{x}) \ \mathfrak{Eq}(\mathbf{T}, \mathbf{x})$$
formula eleme $\mathfrak{S}_5$-nek, tehát axióma, így a leválasztás szabálya szerint $(\exists \mathbf{x}) \ \mathfrak{Eq}(\mathbf{T}, \mathbf{x})$ tétel a halmazelméletben. Az egzisztenciális kvantor és a $\mathrm{Card}(\mathbf{T})$ objektum értelmezése alapján
$$\begin{gathered}(\exists \mathbf{x}) \ \mathfrak{Eq}(\mathbf{T}, \mathbf{x}) \ \equiv \ (\varepsilon_{\mathbf{x}} (\mathfrak{Eq}(\mathbf{T}, \mathbf{x})) \,|\mathbf{x})\mathfrak{Eq}(\mathbf{T}, \mathbf{x}) \ \equiv \\ \equiv (\mathrm{Card}(\mathbf{T})|\mathbf{x})\mathfrak{Eq}(\mathbf{T}, \mathbf{x}) \ \equiv \ \mathfrak{Eq}(\mathbf{T}, \mathrm{Card}(\mathbf{T})),\end{gathered}$$
így az $\mathfrak{Eq}(\mathbf{T}, \mathrm{Card}(\mathbf{T}))$ formula tétel a halmazelméletben.

Jelölje $\mathfrak{T}$ a halmazelméletet és jelölje $\mathfrak{T}'$ a $\mathfrak{T}[\mathfrak{Eq}(\mathbf{T}, \mathbf{S})]$ matematikai elméletet. Legyen $\mathbf{x}$ olyan változó, amely nem szerepel sem $\mathbf{T}$-ben, sem $\mathbf{S}$-ben. Ekkor $\mathfrak{Eq}(\mathbf{T}, \mathbf{x}) \Rightarrow \mathfrak{Eq}(\mathbf{S}, \mathbf{x})$ tétel $\mathfrak{T}'$-ben. Valóban, az $\mathfrak{Eq}(\mathbf{T}, \mathbf{S})$ és $\mathfrak{Eq}(\mathbf{T}, \mathbf{x})$ formulák tételek a $\mathfrak{T}'[\mathfrak{Eq}(\mathbf{T}, \mathbf{x})]$ elméletben, így az előző állítás szerint $\mathfrak{Eq}(\mathbf{S}, \mathbf{x})$ is tétel ebben az elméletben, vagyis a dedukció-tétel alapján $\mathfrak{Eq}(\mathbf{T}, \mathbf{x}) \Rightarrow \mathfrak{Eq}(\mathbf{S}, \mathbf{x})$ tétel $\mathfrak{T}'$-ben. Hasonlóan látható be, hogy $\mathfrak{Eq}(\mathbf{S}, \mathbf{x}) \Rightarrow \mathfrak{Eq}(\mathbf{T}, \mathbf{x})$ is tétel $\mathfrak{T}'$-ben. Ezért a konjunkció logikai alaptulajdonsága szerint

$\mathfrak{Eq}(\mathbf{T},\mathbf{x}) \Leftrightarrow \mathfrak{Eq}(\mathbf{S},\mathbf{x})$ tétel $\mathfrak{T}'$-ben. A halmazelmélet nyelvében egyáltalán nincs konstans, és a $\mathfrak{T}'$ elmélet nyelvében csak a $\mathbf{T}$-ben vagy $\mathbf{S}$-ben szereplő változók konstansok, hiszen $\mathfrak{T}'$-nek $\mathfrak{Eq}(\mathbf{T},\mathbf{S})$ az egyetlen explicit axiómája. Mivel $\mathbf{x}$ sem $\mathbf{T}$-ben, sem $\mathbf{S}$-ben nem szerepel, így $\mathbf{x}$ nem konstans a $\mathfrak{T}'$ elmélet nyelvében. Ezért a (GEN) szabály alapján $(\forall\mathbf{x})(\mathfrak{Eq}(\mathbf{T},\mathbf{x}) \Leftrightarrow \mathfrak{Eq}(\mathbf{S},\mathbf{x}))$ tétel $\mathfrak{T}'$-ben. Ugyanakkor, a

$$(\forall\mathbf{x})(\mathfrak{Eq}(\mathbf{T},\mathbf{x}) \Leftrightarrow \mathfrak{Eq}(\mathbf{S},\mathbf{x})) \;\Rightarrow\; \varepsilon_{\mathbf{x}}(\mathfrak{Eq}(\mathbf{T},\mathbf{x})) = \varepsilon_{\mathbf{x}}(\mathfrak{Eq}(\mathbf{S},\mathbf{x}))$$

formula eleme $\mathfrak{S}_7$-nek, tehát tétel $\mathfrak{T}'$-ben. Ebből a leválasztás szabálya és a számosság definíciója alapján következik, hogy $\mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S})$ tétel $\mathfrak{T}'$-ben. Még egyszer alkalmazva a dedukció tételt kapjuk, hogy $\mathfrak{Eq}(\mathbf{T},\mathbf{S}) \Rightarrow \mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S})$ tétel $\mathfrak{T}$-ben, vagyis a halmazelméletben.

Megfordítva, jelölje $\mathfrak{T}''$ a $\mathfrak{T}[\mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S})]$ elméletet. Legyen ismét $\mathbf{x}$ olyan változó, amely nem szerepel sem $\mathbf{T}$-ben, sem $\mathbf{S}$-ben. Nyilvánvaló, hogy a

$$\mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S}) \;\Rightarrow\; (\mathrm{Card}(\mathbf{T})|\mathbf{x})\mathfrak{Eq}(\mathbf{T},\mathbf{x}) \Leftrightarrow (\mathrm{Card}(\mathbf{S})|\mathbf{x})\mathfrak{Eq}(\mathbf{T},\mathbf{x})$$

formula eleme $\mathfrak{S}_6$-nak, tehát tétel $\mathfrak{T}''$-ben. Ugyanakkor $\mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S})$ is tétel a $\mathfrak{T}''$ elméletben, így a leválasztás szabályát alkalmazva kapjuk, hogy

$$(\mathrm{Card}(\mathbf{T})|\mathbf{x})\mathfrak{Eq}(\mathbf{T},\mathbf{x}) \Leftrightarrow (\mathrm{Card}(\mathbf{S})|\mathbf{x})\mathfrak{Eq}(\mathbf{T},\mathbf{x})$$

tétel $\mathfrak{T}''$-ben. Mivel $(\mathrm{Card}(\mathbf{T})|\mathbf{x})\mathfrak{Eq}(\mathbf{T},\mathbf{x}) \equiv \mathfrak{Eq}(\mathbf{T},\mathbf{T})$ és $(\mathrm{Card}(\mathbf{S})|\mathbf{x})\mathfrak{Eq}(\mathbf{T},\mathbf{x}) \equiv \mathfrak{Eq}(\mathbf{T},\mathbf{S})$, így $\mathfrak{Eq}(\mathbf{T},\mathbf{T}) \Leftrightarrow \mathfrak{Eq}(\mathbf{T},\mathbf{S})$ tétel $\mathfrak{T}''$-ben. Az ekvivalencia definíciója és a konjunkció logikai alaptulajdonsága szerint ebből következik, hogy $\mathfrak{Eq}(\mathbf{T},\mathbf{T}) \Rightarrow \mathfrak{Eq}(\mathbf{T},\mathbf{S})$ tétel $\mathfrak{T}''$-ben. Az előző állítás szerint $\mathfrak{Eq}(\mathbf{T},\mathbf{T})$ tétel a halmazelméletben, így $\mathfrak{T}''$-ben is tétel, tehát a leválasztás szabályát alkalmazva kapjuk, hogy $\mathfrak{Eq}(\mathbf{T},\mathbf{S})$ tétel $\mathfrak{T}''$-ben. Végül, a dedukció tételre hivatkozva, ebből adódik, hogy $\mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S}) \Rightarrow \mathfrak{Eq}(\mathbf{T},\mathbf{S})$ tétel a halmazelméletben.

A két előző bekezdés eredménye, a konjunkció logikai alaptulajdonsága, és az ekvivalencia definíciója alapján arra jutunk, hogy a $\mathfrak{Eq}(\mathbf{T},\mathbf{S}) \Leftrightarrow \mathrm{Card}(\mathbf{T}) = \mathrm{Card}(\mathbf{S})$ formula tétel a halmazelméletben. ■

Az előző tétel alapján érthető, hogy a "két halmaz ekvipotens" kifejezés helyett miért használjuk a "két halmaz egyenlő számosságú" kifejezést.

Az előző állítás szerint az 4.4.3. definícióban bevezetett $\mathbf{T} \mapsto \mathrm{Card}(\mathbf{T})$ hozzárendelés számosság-operáció az $\mathfrak{Ens}$ halmazelmélet felett. Nem ez az egyetlen számosság-operáció $\mathfrak{Ens}$ felett. Később, a jólrendezett halmazok és a rendszámok elméletében látni fogjuk, hogy a Hilbert-Bourbaki–nyelvre alapozott $\mathfrak{Ens}$ elméletben értelmezhetőek az ún. *kezdeti rendszámok*, és az $\mathfrak{Ens}$ elméletben tétel az, hogy minden halmaz ekvipotens egyetlen kezdeti rendszámmal. Kiderül, hogy az a hozzárendelés, amely minden halmazhoz a vele ekvipotens kezdeti rendszámot rendeli, szintén számosság-operáció $\mathfrak{Ens}$ felett.

Befejezés

Más matematikai nyelvek és elméletek

Az ítéletkalkulusnak és a matematikai elméleteknek más alakjaival is találkozunk a szakirodalomban. Most rövid áttekintést adunk ezekről.

Az ítéletkalkulus nyelvében alapvető szerepet játszottak a $\vee$ és $\neg$ logikai operátorok; a $\Rightarrow$, $\wedge$ és $\Leftrightarrow$ szimbólumokat ezekből származtattuk. Választhattuk volna logikai operátoroknak a $\Rightarrow$ és $\neg$ szimbólumokat is; ekkor a következő definíciót adhattuk volna: ha $\mathbf{A}$ és $\mathbf{B}$ kifejezések az ítéletkalkulus nyelvében, akkor

- $\mathbf{A} \vee \mathbf{B}$ jelöli a $\Rightarrow \neg\mathbf{A}\mathbf{B}$ kifejezést, vagyis $\mathbf{A} \vee \mathbf{B} \equiv (\neg\mathbf{A}) \Rightarrow \mathbf{B}$;
- $\mathbf{A} \wedge \mathbf{B}$ jelöli a $\neg \Rightarrow \mathbf{A}\neg\mathbf{B}$ kifejezést, vagyis $\mathbf{A} \wedge \mathbf{B} \equiv \neg(\mathbf{A} \Rightarrow (\neg\mathbf{B}))$;
- $\mathbf{A}\Leftrightarrow\mathbf{B}$ jelöli a $\neg \Rightarrow\Rightarrow \mathbf{A}\mathbf{B}\neg \Rightarrow \mathbf{B}\mathbf{A}$ kifejezést, vagyis $\mathbf{A}\Leftrightarrow\mathbf{B} \equiv (\mathbf{A} \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow \mathbf{A})$.

Ezután a nyelv *ítélet-konstrukcióinak* és *ítéleteinek* fogalmát hasonlóan vezethettük volna be, mint ahogy az 1. pontban tettük, csak a $\vee$ szimbólum helyett a $\Rightarrow$ jelet kell használni. Természetesen az így nyert formális nyelv *nem azonos* az 1. pontban értelmezett nyelvvel, azonban az ítéleteik között létezik egy kölcsönösen egyértelmű megfeleltetés; ilyen értelemben a két nyelv ítéletei *azonosíthatók*. Csupán érdekességként említjük meg, hogy elegendő volna egyetlen logikai operátor is, például a $|$ szimbólummal jelölt *Sheffer-vonás*. Ennek segítségével az ítéletkalkulus bármely $\mathbf{A}$ és $\mathbf{B}$ kifejezésére a $\neg\mathbf{A} \equiv \mathbf{A}|\mathbf{A}$ és $\mathbf{A} \vee \mathbf{B} \equiv (\mathbf{A}|\mathbf{A})|(\mathbf{B}|\mathbf{B})$ jelöléseket alkalmazhatnánk, és ezután a $\Rightarrow$, $\wedge$ és $\Leftrightarrow$ szimbólumok ugyanúgy vezethetők be, mint az általunk vizsgált ítéletkalkulusban. Az így kapott nyelv ítéletei szintén azonosíthatók az 1. pontban értelmezett nyelv ítéleteivel.

Más nyelvi alapra építve is ugyanúgy értelmezhető az *axiomatikus ítéletkalkulus*, mint a 2. pontban. Eltérés lehet az axiómarendszer választásában. Minden axiómarendszertől elvárjuk azt, hogy a belőle származtatható tételek megegyezzenek a tautológiákkal. Könnyen belátható például, hogy ha a Hilbert–Ackermann-féle axiómák helyett az

$$\begin{gathered}\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})\\ (\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}))\\ ((\neg\mathbf{A}) \Rightarrow (\neg\mathbf{B})) \Rightarrow (((\neg\mathbf{A}) \Rightarrow \mathbf{B}) \Rightarrow \mathbf{A})\end{gathered}$$

alakú ítéleteket neveztük volna axiómáknak, ahol $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ az ítéletkalkulus ítéletei, akkor ugyanazokhoz a tételekhez jutnánk, vagyis a tautológiákhoz.

Most röviden vázoljuk az *elsőrendű nyelvek*, valamint az ezekre alapozott *elsőrendű elméletek* felépítését. Egy elsőrendű nyelv szimbólum-készlete csak a logikai operátorokban különbözik a matematikai nyelvek szimbólum-készletétől. Az elsőrendű nyelvekben logikai operátorok a $\neg$, $\Rightarrow$ és $\forall$ szimbólumok, de az ε és $\square$ jelek nem tartoznak hozzá a jelkészlethez. *Kifejezéseknek* nevezzük a nyelv szimbólumaiból álló karakterláncokat, tehát itt a kifejezések fogalma határozottan egyszerűbb, mint a matematikai nyelvekben, amennyiben hiányoznak belőle a karakterpárokat összekötő vonalak. Ezután a *termek* és *formulák* értelmezése következik. *Termeknek* nevezzük a változókat és konstansokat, továbbá, ha $\mathfrak{m}$ n-változós matematikai függvény és $(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ term n-est, akkor az $\mathfrak{m}\mathbf{T}_1 \ldots \mathbf{T}_n$ kifejezés szintén term. Ezzel megadtuk a termek formuláktól teljesen független rekurzív definícióját. *Elemi formuláknak* nevezzük az $\mathfrak{f}\mathbf{T}_1 \ldots \mathbf{T}_n$ alakú kifejezéseket, ahol $\mathfrak{f}$ tetszőleges n-változós logikai függvény és $(\mathbf{T}_1, \ldots, \mathbf{T}_n)$ tetszőleges term n-es. Az elsőrendű nyelv $\mathbf{A}$ kifejezését *formulának* nevezzük, ha létezik kifejezéseinek olyan

$(\mathbf{A}_1, \dots, \mathbf{A}_n)$ n-ese, hogy $\mathbf{A}_n \equiv \mathbf{A}$ és minden $1 \leq k \leq n$ számra a következő feltételek valamelyike teljesül:

– $\mathbf{A}_k$ elemi formula;

– létezik olyan $1 \leq i < k$ szám, hogy $\mathbf{A}_k \equiv \neg\mathbf{A}_i$;

– léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_k \equiv\Rightarrow \mathbf{A}_i\mathbf{A}_j$;

– létezik olyan $1 \leq i < k$ szám és olyan $\mathbf{x}$ változó, hogy $\mathbf{A}_k \equiv \forall\mathbf{x}\mathbf{A}_i$.

Megállapodunk abban, hogy ha $\mathbf{x}$ változó és $\mathbf{A}$ kifejezés egy elsőrendű nyelvben, akkor $\exists\mathbf{x}\mathbf{A}$ *jelöli* a $\neg\forall\mathbf{x}\neg\mathbf{A}$ kifejezést. A $\vee$, $\wedge$ és $\Leftrightarrow$ szimbólumokat ugyanúgy vezetjük be, mint az előzőekben. A világosabb tagoltság kedvéért a logikai operátorokkal kapcsolatban az infix jelölést, valamint a logikai és matematikai függvényekkel kapcsolatban a funkcionális jelölést alkalmazzuk. Továbbá, ha $\mathbf{x}$ változó és $\mathbf{A}$ kifejezés, akkor a $\forall\mathbf{x}\mathbf{A}$ (illetve $\exists\mathbf{x}\mathbf{A}$) kifejezés helyett a $(\forall\mathbf{x})\mathbf{A}$ (illetve $(\exists\mathbf{x})\mathbf{A}$) jelölést alkalmazzuk.

Világos, hogy az elsőrendű nyelvek esetében bevezetett term-fogalom a 4. pontban tárgyalt matematikai nyelvek objektum fogalmának felel meg. Az elsőrendű nyelvek logikai függvényeit néha *predikátumoknak* nevezik.

Az elsőrendű nyelv $\mathbf{B}$ formuláját az $\mathbf{A}$ formula *részformulájának* nevezzük, ha léteznek a nyelvnek olyan $\mathbf{C}$ és $\mathbf{D}$ (esetleg üres) kifejezései, hogy $\mathbf{A} = \mathbf{CBD}$. Az $\mathbf{x}$ változó valamely előfordulását az $\mathbf{A}$ formulában *szabadnak* nevezzük, ha $\mathbf{x}$ előtt nem a $\forall$ szimbólum áll, és $\mathbf{x}$ nem szerepel olyan $\mathbf{B}$ formulában, hogy $\forall\mathbf{x}\mathbf{B}$ részformulája $\mathbf{A}$-nak. Azt mondjuk, hogy $\mathbf{x}$ *szabad változója* az $\mathbf{A}$ formulának, ha létezik $\mathbf{x}$-nek szabad szereplése $\mathbf{A}$-ban; ellenkező esetben azt mondjuk, hogy $\mathbf{x}$ *kötött változója* $\mathbf{A}$-nak. Azt mondjuk, hogy a $\mathbf{T}$ term az $\mathbf{x}$ változóra nézve *szabad* az $\mathbf{A}$ formulában, ha az $\mathbf{x}$ minden $\mathbf{A}$-beli szabad előfordulására teljesül a következő: nem létezik olyan $\mathbf{T}$-ben szereplő $\mathbf{y}$ változó és olyan $\mathbf{B}$ formula, hogy $\mathbf{x}$ szerepel $\mathbf{B}$-ben és $\forall\mathbf{y}\mathbf{B}$ részformulája $\mathbf{A}$-nak.

Az *axiomatikus elsőrendű elméletek* értelmezése hasonló módon történik, mint az axiomatikus formális matematikai elméleteké; tehát rögzítünk egy elsőrendű nyelvet, majd kijelölünk egy axiómarendszert, végül megadjuk a levezetések és tételek fogalmát. Vezessük be a következő jelöléseket:

• $\mathfrak{S}'_1$ jelöli az $\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})$ alakú formulák összességét, ahol $\mathbf{A}$ és $\mathbf{B}$ formulák;

• $\mathfrak{S}'_2$ jelöli az $(\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}))$ alakú formulák összességét, ahol $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ formulák;

• $\mathfrak{S}'_3$ jelöli az $((\neg\mathbf{A}) \Rightarrow (\neg\mathbf{B})) \Rightarrow (((\neg\mathbf{A}) \Rightarrow \mathbf{B}) \Rightarrow \mathbf{A})$ alakú formulák összességét, ahol $\mathbf{A}$ és $\mathbf{B}$;

• $\mathfrak{S}'_4$ jelöli a $((\forall\mathbf{x})\mathbf{A}) \Rightarrow (\mathbf{T}|\mathbf{x})\mathbf{A}$ alakú formulák összességét, ahol $\mathbf{x}$ változó, $\mathbf{A}$ formula és $\mathbf{T}$ olyan term, amely az $\mathbf{x}$ változóra nézve szabad $\mathbf{A}$-ban;

• $\mathfrak{S}'_5$ jelöli a $((\forall\mathbf{x})(\mathbf{A} \Rightarrow \mathbf{B})) \Rightarrow (\mathbf{A} \Rightarrow ((\forall\mathbf{x})\mathbf{B}))$ alakú formulák összességét, ahol $\mathbf{A}$ és $\mathbf{B}$ formulák, valamint $\mathbf{x}$ olyan változó, amely nem szabad változója $\mathbf{A}$-nak.

Egy elsőrendű nyelv $\mathbf{A}$ formuláját *logikai axiómának* nevezzük, ha $\mathbf{A}$ eleme az $\mathfrak{S}'_1$, $\mathfrak{S}'_2$, $\mathfrak{S}'_3$, $\mathfrak{S}'_4$, vagy $\mathfrak{S}'_5$ formula-összességek valamelyikének. Látszik, hogy ez tisztán nyelvi fogalom.

Ezután következhet az *elsőrendű elméletek* definíciója. Egy *elsőrendű elmélet* két részből áll:

• egy elsőrendű nyelvből, amit az elmélet nyelvének nevezünk;

• az elmélet nyelvében megfogalmazható formulák valamilyen (esetleg üres) összességéből, amelynek az elemeit az elmélet *sajátaxiómáinak* nevezzük.

Az elsőrendű elméletekhez még hozzátartozik a *tételek* fogalma. A $\mathfrak{T}$ elsőrendű elmélet $\mathbf{A}$ formulája *levezetésének* (vagy *bizonyításának*) nevezzük a $\mathfrak{T}$ formuláinak bármely olyan $(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ n-esét, amelyre $\mathbf{A} \equiv \mathbf{A}_n$, és minden $1 \leq k \leq n$ számra a következő feltételek valamelyike teljesül:

– $\mathbf{A}_k$ logikai axióma a $\mathfrak{T}$ elsőrendű nyelvben vagy sajátaxiómája $\mathfrak{T}$ -nek;

– léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_j \equiv \mathbf{A}_i \Rightarrow \mathbf{A}_k$;

– létezik olyan $1 \leq i < k$ szám és $\mathbf{x}$ változó, hogy $\mathbf{A}_k \equiv (\forall \mathbf{x})\mathbf{A}_i$.

A $\mathfrak{T}$ elsőrendű elmélet $\mathbf{A}$ formuláját *tételnek* (vagy *bizonyíthatónak*, vagy *levezethetőnek*) nevezzük $\mathfrak{T}$-ben, ha létezik $\mathbf{A}$-nak bizonyítása $\mathfrak{T}$-ben.

Most az elsőrendű nyelvekkel és elsőrendű elméletekkel kapcsolatban néhány összehasonlító kritikai észrevételt teszünk.

1) Láthatóan az elsőrendű nyelvekben az objektumok (vagyis a termek) abban az értelemben *elsődlegesek* a formulákhoz képest, hogy a formulák fogalma nélkül értelmezhetők. Ez nincs összhangban azzal a mindennapi matematikai gyakorlatban tapasztalható ténynyel, hogy az objektumokat és a kijelentéseket csak egymással összefüggésben tudjuk értelmezni. Ugyanakkor kétségtelen, hogy az elsőrendű nyelvek felépítése egyszerűbb, mint a matematikai nyelveké. A továbbiakban látni fogjuk, hogy milyen árat kell fizetni ezért az egyszerűségért.

2) Elsőrendű nyelvben az univerzális kvantor logikai operátorként szerepel, nem pedig jelölésként, mint a matematikai nyelvekben. Ezért a $(\forall \mathbf{x})\mathbf{A}$ és $(\exists \mathbf{x})\mathbf{A}$ formulákban *szintaktikusan szerepel az* $\mathbf{x}$ *változó*, ugyanakkor világos, hogy $\mathbf{x}$ *szemantikusan nem szerepel bennük*, vagyis e formulák "jelentése" $\mathbf{x}$-től független. Ennek pontos értelmezéséhez és magyarázatához az elsőrendű elméletekben szükség van olyan tételek bizonyítására, amelyek éppen ezt fejezik ki. Például, ha $\mathbf{A}$ formula és $\mathbf{x}$, $\mathbf{y}$ olyan különböző változók, hogy $\mathbf{y}$ nem szabad változó $\mathbf{A}$-ban, akkor a

$$((\forall \mathbf{x})\mathbf{A}) \Leftrightarrow (\forall \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}), \quad ((\exists \mathbf{x})\mathbf{A}) \Leftrightarrow (\exists \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A})$$

formulák tételek az elsőrendű elméletekben. Ugyanakkor a matematikai nyelvekkel kapcsolatban igazoltuk a változók helyettesítésének szabályát kvantoros kifejezésekre, és ott látható volt, hogy a $(\forall \mathbf{x})\mathbf{A}$ (illetve $(\exists \mathbf{x})\mathbf{A}$) kifejezés *azonos* a $(\forall \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A})$ (illetve $(\exists \mathbf{y})((\mathbf{y}|\mathbf{x})\mathbf{A}))$ kifejezéssel, ha $\mathbf{x}$ és $\mathbf{y}$ különböző változók, valamint $\mathbf{y}$ nem szerepel $\mathbf{A}$-ban. Vagyis a matematikai nyelvekbe *bele van írva* ez a természetes tulajdonság, ugyanakkor az elsőrendű nyelvek esetében ez már nem is nyelvi, hanem egyenesen logikai problémaként jelentkezik.

3) Az elsőrendű nyelvek változóival kapcsolatban feltétlenül értelmezni kell azok szabad, illetve kötött szereplését egy formulában, mert e fogalmak alkalmazása nélkül az elsőrendű elméletek logikai axiómái nem azt fejezik ki, amit elvárunk tőlük. Ugyanakkor a matematikai nyelvekben semmi ilyesmire nincs szükség. Ennek az az oka, hogy a matematikai nyelvek változó-fogalma teljes összhangban van a változók intuitív fogalmával, míg az elsőrendű nyelvek esetében nem ez a helyzet.

4) A matematikai elméletekben bebizonyítottuk az egzisztenciális kvantor logikai alaptulajdonságát, amely szerint a $(\exists \mathbf{x})\mathbf{A}$ formula pontosan akkor tétel, ha van olyan $\mathbf{T}$ objektum, amelyre $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel. Ezzel szemben, ha egy elsőrendű elmélet $(\exists \mathbf{x})\mathbf{A}$ alakú formulája tétel, akkor egyáltalán nem biztos olyan $\mathbf{T}$ term létezése, amelyre $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel, holott ez nagyon is természetes elvárás a $\exists$ kvantorral kapcsolatban. Ismét arról van szó, hogy az elsőrendű nyelvek egzisztenciális formulái inadekvát módon fejezik ki azok tartalmát. Ezért szükséges az elsőrendű nyelvek konstansokkal való bővítésének

fogalmát bevezetni és bebizonyítani, hogy minden elsőrendű elmélet nyelve bővíthető konstansokkal úgy, hogy abban minden $(\exists \mathbf{x})\mathbf{A}$ alakú tételhez létezzen olyan $\mathbf{T}$ term, amelyre $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel (*Gentzen-tétel*).

5) Az elsőrendű nyelvek esetleges "term-szegénységével" kapcsolatos a *C(hoice)-szabály* szükségessége az elsőrendű elméletekben. A mindennapi matematikai bizonyításokban sokszor a következőképpen járunk el. Tegyük fel, hogy bebizonyítottuk a $(\exists \mathbf{x})\mathbf{A}$ formuláról, hogy tétel. Ekkor azt mondjuk, hogy "legyen $\mathbf{T}$ olyan objektum, amelyre $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel", majd tovább folytatjuk a bizonyítást. Végül eljutunk egy $\mathbf{B}$ formulához, amelyben $\mathbf{T}$ nem szerepel, és akkor azt állítjuk, hogy "ha létezik olyan $\mathbf{x}$, hogy $\mathbf{A}$, akkor $\mathbf{B}$ igaz". Ez az érvelés teljesen helyénvaló a matematikai elméletek esetében, hiszen $\mathbf{T}$ lehet az $\varepsilon_{\mathbf{x}}(\mathbf{A})$ objektum. Ugyanakkor elsőrendű elmélet esetén ilyenkor előfordulhat, hogy bővíteni kell az elmélet nyelvét egy $\mathbf{T}$ konstanssal úgy, hogy a bővebb elméletben $(\mathbf{T}|\mathbf{x})\mathbf{A}$ tétel legyen. Ekkor viszont a bizonyítás további része ebben a bővebb elméletben folyik, és végeredményül csak az adódik, hogy $\mathbf{B}$ tétel a bővebb elméletben. Honnan tudjuk, hogy ekkor $\mathbf{B}$ az eredeti elsőrendű elméletben is tétel? Erre a kérdésre ad egy viszonylag egyszerű választ a C-szabály, amelynek részletes tárgyalása megtalálható [**3**]-ban. A gyakorlati probléma viszont az, hogy a C-szabály feltételeinek teljesülését már egy átlagosan bonyolult matematikai bizonyítás esetében is nehéz lehet ellenőrizni.

6) Ahhoz hogy az elsőrendű nyelvek változóknak nevezett szimbólumai értelmi szempontból is változókként működjenek, az elsőrendű elméletek bizonyítás-fogalmában *két* levezetési szabályra van szükség, míg a matematikai elméletek esetében elegendő egy. Látható, hogy az elsőrendű elméletek bizonyítás-fogalmába bele van foglalva az *általánosítás szabálya* (Gen), amit a matematikai elméletekben egyszerűen bizonyítani tudtunk. Ennek az az oka, hogy az univerzális kvantor logikai alaptulajdonsága következtében a $(\forall \mathbf{x})\mathbf{A}$ alakú univerzális formulák pontosan azt fejezik ki a matematikai elméletekben, amit elvárunk tőlük, míg az elsőrendű elméletekben ezt csak egy újabb levezetési szabály és az $\mathfrak{S}_5'$ logikai axióma-séma előírásával lehet biztosítani.

7) Természetesen az elsőrendű elméletekben is igazolhatók azok az egyszerű bizonyítási módszerek, amelyeket az 5. pontban bemutattunk (láncszabály, esetszétválasztás, indirekt bizonyítás). Ott láttuk, hogy a dedukció-tétel nagyon fontos bizonyítási módszert fogalmaz meg, amit állandóan használunk. Ezért fontos, hogy a dedukció-tétel feltételei egyszerűek, könnyen ellenőrizhetőek legyenek. Azonban az elsőrendű elméletek dedukció-tétele csak egy olyan mellékfeltétel teljesülése esetén bizonyítható, amelynek az ellenőrzése a gyakorlati bizonyításokban nem szükségképpen triviális feladat. Az elsőrendű elméletek dedukció-tételének feltételeit megtaláljuk a [**3**] könyvben.

8) Az elsőrendű nyelvek logikai függvényei (vagyis predikátumai) között nem szerepel az $=$ szimbólum. Ha olyan elsőrendű elméletet akarunk értelmezni, amelyben van egyenlőség-jel, és az rendelkezik a tőle elvárható tulajdonságokkal (ezek a *normális elsőrendű elméletek*), akkor további axiómákra van szükség. Tehát csak *látszólagos* az, hogy az elsőrendű elméleteknek kevesebb logikai axióma-sémája van, mint a matematikai elméleteknek, hiszen ez utóbbiak esetében az $\mathfrak{S}_6$ és $\mathfrak{S}_7$ logikai axióma-sémák éppen az egyenlőség logikai tulajdonságait rögzítik. A normális elsőrendű elméletek egyenlőség-predikátummal kapcsolatos logikai axióma-sémáinak részletes vizsgálata megtalálható például [**3**]-ban.

9) Létezik egy nagyon mély eredmény (Hilbert két *ε-tétele*), amely azt mutatja, hogy a normális elsőrendű elméletek *bizonyos értelemben* egyenértékűek a matematikai elméletekkel. Ezen a helyen nem áll módunkban részletezni sem a pontos állítást, sem a pontos eredményt. Az érdeklődő olvasó minden ezzel kapcsolatos részletet megtalál az [**1**] logikai

alapműben.

Az előző észrevételek fényében mondható, hogy az elsőrendű elméletek kevésbé alkalmasak a matematika megalapozására, mint az 5. pontban tárgyalt matematikai elméletek. De az elsőrendű nyelveket és elméleteket eredetileg sem erre, hanem logikai vizsgálatok céljára fejlesztették ki.

Nem klasszikus matematikai elméletek

Mindeddig a *klasszikus* ítéletkalkulusról és *klasszikus* matematikai elméletekről volt szó. Régebben, amikor a logika és a halmazelmélet paradoxonainak feloldása még kevésbé volt nyilvánvaló, néhányan arra gyanakodtak, hogy a logikai ellentmondások kiküszöbölése csak akkor lehetséges, ha a *kizárt harmadik elvét* eltávolítják a logikából. Ezért komoly erőfeszítéseket tettek olyan *nemklasszikus logikai elméletek* kidolgozására, amelyek ellentmondásmentesek, ugyanakkor nem bizonyítható bennük a kizárt harmadik elve. E kísérletek közül egyet mutatunk be részletesebben: az *intuicionista ítéletkalkulust*.

Az intuicionista ítéletkalkulus formális nyelvében az elemi ítéleteket ugyanúgy értelmezzük, mint a klasszikus ítéletkalkulus esetében, azonban a $\neg$, $\vee$, $\wedge$, $\Rightarrow$ szimbólumok mindannyian logikai operátorok (tehát egyik sincs a többiből származtatva). A nyelv *kifejezésének* nevezünk minden olyan karakterláncot, amelynek karakterei az inuicionista ítéletkalkulus nyelvének szimbóluma. Ennek megfelelően, az intuicionista ítéletkalkulus *ítélet-konstrukciójának* nevezzük az intuicionista ítéletkalkulus kifejezéseinek bármely olyan $(\mathbf{A}_1, \dots \mathbf{A}_n)$ n-esét, amelyre minden $1 \leq k \leq n$ számra a következő feltételek valamelyike teljesül:

- $\mathbf{A}_k$ elemi ítélet;
- létezik olyan $1 \leq i < k$ szám, hogy $\mathbf{A}_k \equiv \neg \mathbf{A}_i$;
- léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_k \equiv \vee \mathbf{A}_i \mathbf{A}_j$;
- léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_k \equiv \wedge \mathbf{A}_i \mathbf{A}_j$;
- léteznek olyan $1 \leq i, j < k$ számok, hogy $\mathbf{A}_k \equiv\Rightarrow \mathbf{A}_i \mathbf{A}_j$.

Az intuicionista ítéletkalkulus $\mathbf{A}$ kifejezését *ítéletnek* nevezzük, ha van olyan $(\mathbf{A}_1, \dots \mathbf{A}_n)$ ítélet-konstrukció, hogy $\mathbf{A} \equiv \mathbf{A}_n$. A $\vee$, $\wedge$ és $\Rightarrow$ logikai operátorokkal kapcsolatban itt is az infix jelölést alkalmazzuk, és ha $\mathbf{A}$, $\mathbf{B}$ kifejezések, akkor $\mathbf{A} \Leftrightarrow \mathbf{B}$ jelöli az $(\mathbf{A} \Rightarrow \mathbf{B}) \wedge (\mathbf{B} \Rightarrow \mathbf{A})$ kifejezést (tehát $\Leftrightarrow$ már származtatott jel, nem pedig logikai operátor).

Az *axiomatikus intuicionista ítéletkalkulus* igazság-fogalmát pontosan ugyanúgy vezetjük be, mint a klasszikus ítéletkalkulus esetében, csak az axiómák összessége különbözik. Azt mondjuk, hogy az intuicionista ítéletkalkulus egy ítélete *intuicionista axióma*, ha azonos az alábbi ítéletek valamelyikével:

$$\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})$$
$$(\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}))$$
$$(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{A}$$
$$(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \mathbf{B}$$
$$\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow (\mathbf{A} \wedge \mathbf{B}))$$
$$\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})$$
$$\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})$$
$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{A} \vee \mathbf{B}) \Rightarrow \mathbf{C}))$$

$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{A} \Rightarrow (\neg\mathbf{B})) \Rightarrow (\neg\mathbf{A}))$$
$$\neg\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$$

ahol $\mathbf{A}$, $\mathbf{B}$ és $\mathbf{C}$ az intuicionista ítéletkalkulus ítéletei. Ezután az *intuicionista tételek* fogalmát pontosan úgy értelmezhetjük, mint a klasszikus ítéletkalkulusban.

Láthatóan az intuicionista ítéletkalkulus formális nyelve határozottan különbözik a klasszikus ítéletkalkulusétól, ugyanakkor az intuicionista és a klasszikus ítéletek összessége között létezik egy kitüntetett kölcsönösen egyértelmű megfeleltetés. A klasszikus ítéletkalkulus formális nyelvébe *bele van írva* egy lényegesen klasszikus összefüggés a negáció, diszjunkció és implikáció között, ti. az, hogy ha $\mathbf{A}$ és $\mathbf{B}$ ítéletek akkor $\mathbf{A} \Rightarrow \mathbf{B}$ *azonos* a $(\neg\mathbf{A}) \vee \mathbf{B}$ kifejezéssel. Ugyanakkor az intuicionista ítéletkalkulusban még az sem teljesül, hogy az

$$(\mathbf{A} \Rightarrow \mathbf{B}) \Leftrightarrow ((\neg\mathbf{A}) \vee \mathbf{B})$$

ítélet tétel, ahol $\mathbf{A}$ és $\mathbf{B}$ ítéletek. Mindazonáltal belátható, hogy az intuicionista ítéletkalkulus (bizonyos jól meghatározható értelemben) a klasszikus ítéletkalkulusnak *részelmélete*.

Az intuicionista ítéletkalkulusban nem érvényes a 2.5.3. állítás. (Figyeljük meg, a logikai tételek bizonyításában milyen gyakran alkalmaztuk ezt az állítást!) Pontosabban, ha $\mathbf{A}$ elemi ítélet az intuicionista ítéletkalkulusban, akkor $(\neg\neg\mathbf{A}) \Rightarrow \mathbf{A}$ nem intuicionista tétel. Nem érvényes benne a kizárt harmadik elve sem. Pontosabban, ha $\mathbf{A}$ elemi ítélet az intuicionista ítéletkalkulusban, akkor $(\neg\mathbf{A}) \vee \mathbf{A}$ nem intuicionista tétel. A Kalmár-féle teljességi tétel is csak korlátozott formában érvényes az intuicionista ítéletkalkulusban: az $\mathbf{A}$ ítélet pontosan akkor tautológia, ha $\neg\neg\mathbf{A}$ intuicionista tétel. Ezzel szemben a dedukció-tétel ugyanolyan formában évényes az intuicionista ítéletkalkulusban, mint a klasszikus ítéletkalkulusban.

Természetesen az ítéletkalkulushoz hasonlóan a klasszikus matematikai elméleteknek is létezik intuicionista változata. Ennek a matematikai nyelvében a $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\exists$ és $\forall$ szimbólumok mindannyian logikai operátorok. Az intuicionista függvénykalkulus logikai axiómarendszere sokkal bonyolultabb annál, amit az 5. pontban tekintettünk. Az intuicionista elsőrendű elméletek nevezetes sajátossága, hogy ha $\mathbf{x}$ változó és $\mathbf{A}$ formula, akkor a $((\exists\mathbf{x})\mathbf{A}) \Rightarrow \neg(\forall\mathbf{x})(\neg\mathbf{A})$ formula intuicionista logikai tétel, ugyanakkor az $\neg(\forall\mathbf{x})(\neg\mathbf{A}) \Rightarrow (\exists\mathbf{x})\mathbf{A}$ formula nem az, vagyis a kvantoros kifejezések negációjának klasszikus szabálya nem érvényes az intuicionista elméletekben. Az intuicionista logikák szerkezetéről bővebben olvashatunk a [**4**] és [**5**] könyvben.

A matematikai (illetve elsőrendű) elméletek klasszikus alakjának léteznek másféle nemklasszikus változatai is. A *pozitív logikák* nyelvében nincs negáció, míg a *modális logikák* nyelvében az egzisztenciális és univerzális kvantor mellett ezek gyengítései, a *lehetségesség* és *szükségesség kvantorok* is szerepelnek, természetesen olyan axiómákkal együtt, amelyek megfelelő értelmet adnak az ilyen kvantorokat tartalmazó formuláknak. A pozitív és modális elméletek szintaxisával és szemantikájával megismerkedhetünk például a [**4**] könyvből.

A halmazelmélet paradoxonai

Ezen a szinten már nem kerülhető meg az a kérdés, hogy *mit értünk* (*halmazelméleti*) *halmazon*? A nem formális (naiv) halmazelmélet egyszerű választ ad: a matematikai objektumok összességeit nevezzük halmazoknak. Ez a válasz csak akkor volna elfogadható, ha pontosan tudnánk, hogy mit értsünk matematikai objektumon, továbbá határozott elképzelésünk lenne az összességek fogalmáról. De még a pontos fogalmi ismeretek birtokában is fenyeget a nem formális logika ellentmondásosságának veszélye a halmazelmélettel kapcsolatban is. Semmi meglepő nincs abban, hogy a nem formális halmazelmélet ugyanúgy szemantikus ellentmondásokat tartalmaz, mint annak a szülő-elmélete (a nem formális logika) is. Az axiomatikus formális halmazelmélet (például az $\mathfrak{Ens}$ elmélet) létrehozása után feleslegesnek tűnik a naiv halmazelmélet azon paradoxonaival foglalkozni, amelyek éppen a nem formális jellegből adódnak. E helyett inkább az axiomatikus formális halmazelmélet ellentmondásmentességét kellene alaposabb vizsgálat alá vetni. Azonban a naiv halmazelmélettel kapcsolatban is van két olyan probléma, amelyekkel (a halmazfogalom tisztázása érdekében) érdemes foglalkozni. Megállapodunk abban, hogy a továbbiakban a *halmazelmélet* névvel az axiomatikus formális halmazelméletet illetjük (például az $\mathfrak{Ens}$ elméletet).

Az egyik olyan halmazelméleti probléma, amely döntő módon befolyásolja a halmazelmélet jelenlegi alakját a 7. pontban érelmezett *kollektivizálhatósággal* kapcsolatos. Láttuk, hogy ha $\mathbf{x}$ változó és $\mathbf{A}$ formula a halmazelméletben, akkor képezhető az $\{\mathbf{x}|\mathbf{A}\}$ objektum, amelynek jelentését és tulajdonságait illetően helyénvaló bizonyos óvatosság. A naiv halmazelmélet felfogása szerint ez az objektum nem más, mint "azon $\mathbf{x}$ halmazok halmaza, amelyekre $\mathbf{A}$ teljesül". Vagyis a naiv halmazelmélet ezt az objektumot hallgatólagosan felruházza azzal a tulajdonsággal, hogy teljesül rá a $(\forall\mathbf{x})((\mathbf{x} \in \{\mathbf{x}|\mathbf{A}\})\Leftrightarrow\mathbf{A})$ állítás. Ugyanakkor a 7. pontban láttuk, hogy ez az állítás *azonos* a $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ állítással. Vagyis a naiv halmazelmélet szerint minden $\mathbf{A}$ kijelentésre és $\mathbf{x}$ változóra $\mathfrak{Coll}_{\mathbf{x}}(\mathbf{A})$ igaz. Azonban a Russel-tételből következik, hogy a $\neg\mathfrak{Coll}_{\mathbf{x}}(\mathbf{x} \notin \mathbf{x})$ formula tétel a halmazelméletben, tehát ha elfogadjuk a naiv halmazelmélet hipotézisét, akkor a halmazelmélet biztosan ellentmondásos. Korábban *Russel-paradoxonnak* nevezték ezt a látszólagos ellentmondást.

Világosan látható, hogy a Russel-paradoxon azonnal eltűnik, ha nem tesszük fel eleve, hogy minden halmazelméleti kijelentés minden változóban kollektivizáló. Ekkor viszont meg kell mondani, hogy melyek (vagy milyenek) azok a kijelentések, amelyek valamelyik változójukban kollektivizálók. Ezért szükségszerű, hogy a halmazelmélet bizonyos axiómái éppen a kollektivizálhatóság tulajdonságait írják elő. A páraxióma, a hatványhalmaz axióma és az unió axióma teljesen konkrétan megfogalmaz egy kijelentést, amely valamelyik változóban kollektivizáló. Ugyanakkor a részhalmaz axiómák elégséges feltételeket fogalmaznak meg a kollektivizálhatóságra. *Remélhető*, de ma még nem ismeretes, hogy ez az axiómarendszer ellentmondásmentes. Ha így van, akkor egy $\{\mathbf{x}|\mathbf{A}\}$ alakú objektum nem tekinthető automatikusan "azon $\mathbf{x}$ halmazok halmazának, amelyekre $\mathbf{A}$ teljesül".

A másik érdekes halmazelméleti probléma a *Skolem-paradoxon*. Ennek ismertetéséhez tekintsük a halmazelmélet nyelvében megadható objektumok összességét. Ez *végtelen*, hiszen minden változó is objektum, és már a változók összessége is végtelen. A naiv halmazelmélet nem éppen elemi meggondolásai oda vezetnek, hogy ez *megszámlálhatóan végtelen* összesség, abban az értelemben, hogy minden eleme megindexelhető természetes számmal úgy, hogy különböző indexekhez különböző objektumok tartozzanak. Ha tehát megállapodás szerint a halmazelmélet objektumait tekintjük halmazoknak, akkor *a halmazok összessége megszámlálható*. Ugyanakkor a Cantor-tétel szerint létezik nem megszámlálhatóan végelen halmaz (I. fejezet, 2. és 3. pont), például a természetes számok halmazának hatványhalmaza. Ezért a *halmazok összessége nem megszámlálható*, így logikai ellentmondásra jutunk.

A Skolem-paradoxonra vezető gondolatmenetben összekeveredik két teljesen különböző elmélet objektum-, illetve igazság-fogalma. A halmazelmélet objektumairól és azok összességéről csak a halmazelméletet definiáló és vizsgáló *metanyelvben*, vagyis a szűkebb értelemben vett matematikai logikában beszélhetünk. Ezek a fogalmak *nem formalizálhatók* a halmazelméletben, vagyis a halmazelmélet formális nyelvén nem értelmezhetők a saját objektumai, illetve a saját objektumainak összessége. Ezért a halmazelmélet fogalmait és tételeit (például a megszámlálhatóság fogalmát és a Cantor-tételt) *nem alkalmazhatjuk* ezekre az "objektumokra", vagyis a halmazelmélet igazság-fogalma szerint semmilyen, ezekre vonatkozó állítás nem értékelhető. Figyeljük meg a Skolem-paradoxonhoz vezető "indexező függvény" definíciós tartományát! Ez a "függvény" a halmazelmélet bizonyos objektumainak összességén (vagyis nem halmazon) értelmezett, tehát nyilvánvalóan nem tekinthető halmazelméleti függvénynek, hiszen azok definíciós tartománya halmaz. Ezért egyáltalán nem meglepő, hogy logikai ellentmondásra jutunk, ha erre a *metafüggvényre* alkalmazzuk a *halmazelméleti függvényekre* vonatkozó Cantor-tételt.

Láthatóan meglehetősen durva gondolati hiba vezet a Skolem-paradoxonra, mégis érdemes róla beszélni, mert van egy fontos tanulsága. A 7. pontban a halmazelmélet (tehát az $\mathfrak{Ens}$ matematikai elmélet) definíciójában megállapodtunk abban, hogy a halmazelmélet objektumait nevezzük halmazoknak. Ugyanakkor a halmazelméletben bizonyítható, hogy nem létezik olyan halmaz, amelynek minden halmaz eleme volna (I. fejezet, 1. pont). Semmi akadálya sincs annak, hogy gondoljunk a halmazelmélet objektumainak *összességére*, azonban az előzőek alapján komoly okunk van azt állítani, hogy ez nem lehet az összes halmazok halmaza. Ennek lényegi oka az, hogy ezt az összességet nem lehet előállítani a halmazelmélet formális nyelvében egy alkalmas objektum-formula-konstrukcióval. Ezért azt kell gondolnuk, hogy a halmazelmélet objektumai a *formálisan megfogalmazható halmazok*, vagyis azok, amelyek a formális nyelvben előállíthatók.

A matematika fogalmáról

Az utolsó kérdésünk így hangzik: *mi a matematika*? Árnyaltabban fogalmazva: módunkban áll-e konkrét, nem filozófiai szintű választ adni arra a kérdésre, hogy mi a matematika? A válasz: teljesen határozott *igen*. Az alábbiakban megadjuk e válasz pontos indoklását, amelyből világosan ki fog derülni, hogy a válasz elégséges mélységű megértése rendkívüli szellemi erőfeszítést igényel.

Cantor első halmazelméleti munkáitól kezdve sejthető volt, hogy az *egész matematika* felépíthető halmazelméleti alapon. Kezdetben nem állt rendelkezésre az axiomatikus formális halmazelmélet, de már a naiv halmazelmélet fogalmaival is elő lehetett állítani az aritmetikát, vagyis a természetes számok elméletét (Peano), majd később (Dedekind munkássága folytán) a valós számok elméletét. A valós számok halmazelméleti bevezethetőségéből következett a (többdimenziós) geometriák előállíthatósága a halmazelméleten belül. Az euklidészi geometriákkal kapcsolatban halmazelméleti módon értelmezni lehetett a környezetek fogalmát. Ennek általánosításaként született meg (Fréchet kezdeményezésére) a halmazelméleti topológia. Könnyen látható volt, hogy az algebrai műveletek a halmazelméleti függvényfogalom speciális esetei, ezáltal a legkülönfélébb algebrai objektumok (csoportok, gyűrűk, hálók, vektorterek, stb.) egyszerűen értelmezhető halmazelméleti objektumokká váltak. Könnyen össze lehetett illeszteni az algebrai objektumok műveleteit a topologikus terek környezet-fogalmával; így nyertük a topologikus algebrai objektumokat (topologikus csoportokat, topologikus testeket, topologikus vektortereket, normált algebrákat, stb.). Ettől kezdve pedig nyilvánvalóvá vált, hogy a számelmélet, az algebra, a geometria, a valószínűségszámítás, a lineáris analízis és a lokálisan lineáris analízis (vagyis a sokaságelmélet) egyszerűen a halmazelmélet részének tekinhető.

Tehát a matematika mibenlétre vonatkozó kérdésre adható lehetséges konkrét válasz így hangzik: a matematika *azonosítható* azzal a formális axiomatikus halmazelmélettel (például a $\mathfrak{Ens}$ elmélettel), amely alapként szolgál számára. Ezt az állítást egyetlen módon lehet bizonyítani: végre kell hajtani a matematikai felépítését a halmazelméletből kiindulva. Az analízis elemei biztosan megfogalmazhatók az $\mathfrak{Ens}$ elméleten belül; ennek pár ezer oldalas "bizonyítását" tartalmazza az ezután következő tizenhét fejezet. Az egész matematika elemei biztosan előállíthatók a Bourbaki-féle halmazelméletben; ennek több ezer oldalas "bizonyítása" megtalálható a Bourbaki-sorozatban. Tehát a matematika konkrét lényegének kérdésére adott válaszunkat csak az értheti meg maradéktalanul, aki maga is átéli a halmazelméletre alapozott matematika felépítésének élményét.

Természetesen kissé leegyszerűsítettük a választ, hiszen nem egyetlen (formális axiomatikus) halmazelmélet létezik. Továbbá kétségtelenül léteznek a matematikának olyan területei, amelyekben megjelennek az $\mathfrak{Ens}$ elméletben biztosan nem formalizálható "nagy összességek". Például a *kategóriaelméletben*, *algebrai topológiában* és *homologikus algebrában* gondolnunk kell az összes halmazok, az összes topologikus terek, az összes Abel-csoportok és modulusok *osztályára*; ugyanakkor ezek *halmaza* nem képezhető az $\mathfrak{Ens}$ elmélet formális nyelvében. Azonban kellő találékonysággal ezeknek az elméleteknek a lényeges állításai is átfogalmazhatók úgy, hogy azok formalizálható (és bizonyítható) kijelentésekké váljanak az $\mathfrak{Ens}$ elméletben.

A matematika konkrét lényegét az imént *formalista-konvencionalista-logicista* nézőpontból magyaráztuk. *Formalista*, mert formális nyelvre alapozott halmazelméletről van szó. *Konvencionalista*, mert a matematikai kijelentések értelmességének és igazságának fogalmát egy megállapodáson alapuló szabály-rendszertől (formális nyelvi konstrukciók létezésétől, önkényesen választott axiómáktól és bizonyítási szabályoktól) tesszük függővé. Végül *logicista* is, amennyiben a matematikát azonosítjuk egy speciális logikai elmélettel, ezáltal a matematikát a logika részének tekintjük. Egyáltalán nem állítjuk kategorikusan, hogy ez a matematika egyedül helyes felfogása. Azt viszont határozottan mondhatjuk, hogy ez a felfogás *alkalmas* a matematika egyfajta konkrét értelmezésére.

II. rész

A matematikai analízis halmazelméleti alapjai

BEVEZETÉS

Ebben a részben azokról a halmazelméleti alapfogalmakról lesz szó, amelyek nemcsak az analízis, hanem a matematika bármely területének komoly vizsgálatához nélkülözhetetlenek.

A matematika legfontosabb fogalma a *halmaz* és a *halmaz eleme*. Ezeket nem lehet egyszerűbb fogalmakból származtatni; csak annyit tehetünk, hogy leírjuk azokat a tulajdonságokat, amelyeket érvényeseknek fogunk gondolni rájuk. Ezek a tulajdonságok a halmazelmélet axiómái. Az első pontban megfogalmazzuk a halmazelmélet öt legelemibb axiómáját, amelyek – a meghatározottsági axióma kivételével – olyan természetűek, hogy bizonyos tulajdonságú halmazok egzisztenciáját írják elő.

A matematikai objektumok közötti kapcsolatok leírására szolgálnak a *relációk* és a *függvények*; a második pontban ezek szisztematikus vizsgálatára kerül sor. Különös hangsúlyt kap három nevezetes reláció-típus; a *függvények*, az *ekvivalenciák* és a *rendezések* típusa, mivel ezeket az analízisben (is) állandóan használjuk. Ugyanez érvényes a *műveletekre*, amelyek speciális típusú függvények, és amelyek lehetővé teszik az algebrai objektumok konstrukcióját. Ebben a pontban vezetjük be a halmazelmélet legsokoldalúbb vizsgálatnak alávetett axiómáját: a *kiválasztási axiómát*, amelynek jelentősége csak a halmazelméletre alapozott matematika felépítése során derül ki.

A harmadik pontban azt az axiómát mutatjuk be, amelynek alkalmazásával lehetővé válik a természetes számok halmazának bevezetése a matematikába; ez a *végtelenségi axióma*. Látni fogjuk, hogy a természetes számok halmazából kiindulva egyszerű halmazelméleti és algebrai meggondolásokkal előállíthatók az egész számok.

A végtelenségi axiómával teljessé válik a matematika axiómarendszere. A kiválasztási és végtelenségi axiómával bővített halmazelméletre alapozott matematika (és azon belül az analízis) a mai felfogásunk szerint nagymértékben alkalmas természeti (különösen fizikai) jelenségkörök matematikai modellezésére. Ennek a kijelentésnek "bizonyítása" természetesen csak a szóban forgó matematika felépítése *után* lehetséges.

A negyedik pontban a véges halmazok fogalmának és a véges halmazok számosságának bevezetésével foglalkozunk. A véges halmazok alkalmazásával igazoljuk a prímszámok halmazának végtelenségét, valamint a számelmélet alaptételét. Bemutatunk néhány elemi kombinatorikai tényt is.

Az utolsó pontban a halmazok végtelenségének kétféle fogalmáról lesz szó, és igazoljuk a végtelen halmazokkal kapcsolatos legfontosabb tételt: a számosságaritmetika alaptételét. Szó lesz a megszámlálható végtelenségről, valamint a rendszámokról, amelyek a jólrendezett halmazok prototípusai. Végül érintjük a számosságok és a számosságaritmetika alapfogalmait és legegyszerűbb állításait.

Az itt vázolt halmazelmélet az ZFC (kiválasztási axiómával bővített *Zermelo-Fraenkel*) halmazelmélet egyfajta variánsa. Léteznek olyan matematikai elméletek, amelyek felépítéséhez ez a halmazelmélet túlságosan szűk. A tágabb értelemben vett (például a kategóriaelméletet is tartalmazó) matematika felépítése céljából megfelelő lehet a ZFC elmélet olyan bővítése, amelynek nem a halmaz, hanem az *osztály* az alapfogalma. Ilyen elmélet az NBG (*Neumann-Bernays-Gödel*) osztályelmélet, amellyel rendszerint a kiválasztási axiómával bővített formában találkozunk. Léteznek még ennél is radikálisabb általánosítások, amelyek formális nyelvi és logikai szempontból is kategóriaelméleti alapokra helyezik a matematikát: a *toposzelméletek*. E modernebb matematikai logikai és halmazelméleti vizsgálatok mind feltételezik annak a standard (szűkebb értelemben vett) halmazelméletnek az ismeretét, amelynek alapjaival ez a fejezet foglalkozik.

Hangsúlyozzuk, hogy ebben a fejezetben nem az a célunk, hogy egy halmazelmélet szisztematikus felépítését adjuk. A halmazelméletet vizsgáló metaelméletek legfontosabb problémája az axiómarendszerek ellentmondásmentessége, konzisztenciája és függetlensége; ezek képezik egy valóban teljesség igényével fellépő halmazelmélet tárgyát. Továbbá minden halmazelmélet centrális jelentőségű problémája a halmazok számosságának fogalma (*kardinális aritmetika*) és a rendtípusok, illetve rendszámok fogalma (*ordinális aritmetika*). Ezekből néhány részlet megtalálható az anyagban, de ezek rendszeres vizsgálatára itt nem kerülhet sor. E helyett azokra a halmazelméleti fogalmakra és állításokra helyezzük a hangsúlyt, amelyek az analízis speciális területein alkalmazhatóak.

Végül megemlítjük, hogy a halmazelmélet a matematikának nem a legelső fejezete. Ahhoz, hogy a halmazelmélet minden tétele a legteljesebb mértékben érthető legyen szükséges a halmazelméletet megelőző matematikai logikai alapozás. Komoly matematikai logika pedig elképzelhetetlen a matematika formális nyelvének konstrukciója híján. Ezeket a halmazelméletet előkészítő elméleteket itt nem tárgyalhatjuk, csak utalhatunk a jelentőségükre és az ide vonatkozó szakirodalomra.

Irodalomjegyzék

[1] N. Bourbaki, **Éleménts de mathématique. Théorie des ensembles.** Hermann, Paris, 1966.

[2] K. Kuratowski-A. Mostowski, **Set Theory**, North-Holland Pub. Co., Amsterdam-Warsaw, 1967.

[3] J. Barwise (editor), **Handbook of Mathematical Logic**, North-Holland Pub. Co., Amsterdam-New York-Oxford, 1977.

[4] P. J. Cohen, **Set Theory and the Continuum Hypothesis**, W.A.Benjamin, Inc., New York-Amsterdam, 1966.

[5] A. Mostowski, **Constructible sets with Applications**, North-Holland Pub. Co., 1969.

5. fejezet

A halmazelmélet elemi axiómái

5.1. Meghatározottsági axióma

A halmazelmélet alapvető szimbóluma az $\in$ (*elem*) jel. Ha E és F halmazok, akkor $E \in F$ kijelentés, amit úgy olvasunk, hogy "E *eleme* F*-nek*". A halmazelmélet axiómái azok a mélyebb okokra vissza nem vezethető, igaznak tekintett kijelentések, amelyek értelmet adnak az $\in$ szimbólumnak.

A halmazelmélet első axiómája kapcsolatot teremt a logikai egyenlőség és az $\in$ szimbólum között.

Meghatározottsági axióma – $(\forall x)(\forall y)(\,(\forall z)((z \in x)\Leftrightarrow(z \in y)) \Rightarrow (x = y)\,)$

A meghatározottsági axiómának az a tartalma, hogy két halmaz egyenlő, ha az elemeik ugyanazok.

5.1.1. Definíció. *Ha E és F halmazok, akkor $E \subseteq F$ a $(\forall x)((x \in E) \Rightarrow (x \in F))$ kijelentés rövidítése, ahol az x változó nem szerepel sem E-ben, sem F-ben. Ha $E \subseteq F$ igaz, akkor azt mondjuk, hogy E* **részhalmaza** *F-nek.*

5.1.2. Állítás. *A meghatározottsági axióma ekvivalens azzal, hogy minden E és F halmazra, ha $E \subseteq F$ és $F \subseteq E$, akkor $E = F$.*

Bizonyítás. Ha E és F halmazok, akkor az $(E \subseteq F) \wedge (F \subseteq E)$ kijelentés (a definíció szerint) azzal ekvivalens, hogy

$$((\forall x)((x \in E) \Rightarrow (x \in F))) \wedge ((\forall x)((x \in F) \Rightarrow (x \in E)))\,,$$

ami ekvivalens azzal, hogy $(\forall x)((x \in E) \Leftrightarrow (x \in F))$. Az, hogy bármely két E és F halmazra ez maga után vonja az E és F (logikai) egyenlőségét egyenértékű a meghatározottsági axiómával. (Itt azt a logikai tételt alkalmaztuk, hogy bármely két $\mathscr{A}$ és $\mathscr{B}$ kijelentésre a $(((\forall x)\mathscr{A}) \wedge ((\forall x)\mathscr{B})) \Leftrightarrow (\forall x)(\mathscr{A} \wedge \mathscr{B})$ kijelentés tétel). ■

5.2. Részhalmaz axióma

Ha $\mathscr{A}$ kijelentés, akkor szeretnénk gondolni arra a halmazra, amelynek elemei pontosan azok az x-ek, amelyekre $\mathscr{A}$ teljesül. Pontosabban; azt az E halmazt szeretnénk (gondolatilag) előállítani, amelyre $x \in E$ ugyanazt jelenti, mint $\mathscr{A}$ (itt $\mathscr{A}$ az x változóra vonatkozó *tulajdonságként* szerepel), vagyis amelyre a $(\forall x)\,((x \in E) \Leftrightarrow \mathscr{A})$ kijelentés tétel. Elképzelhető volna, hogy minden $\mathscr{A}$ kijelentéshez van ilyen halmaz, azonban nem ez a helyzet.

5.2.1. Állítás. (Russel-tétel.) *Nem létezik olyan R halmaz, hogy minden x-re $x \in R$ ekvivalens azzal, hogy $x \notin x$.*

Bizonyítás. Ha R ilyen halmaz volna, akkor x helyére az R halmazt helyettesítve kapjuk, hogy $(R \in R) \Leftrightarrow (R \notin R)$, ami a logikai ekvivalencia definíciója alapján azt jelenti, hogy $((R \in R) \Rightarrow (R \notin R)) \wedge ((R \notin R) \Rightarrow (R \in R))$ logikai tétel. A konjunkció logikai alaptulajdonsága szerint ez azt jelenti, hogy az $(R \in R) \Rightarrow (R \notin R)$ és $(R \notin R) \Rightarrow (R \in R)$ kijelentések tételek. Ha $R \in R$ igaz (vagyis tétel) volna, akkor az első kijelentésből leválasztással kapjuk, hogy $R \notin R$, tehát ellentmondásra jutunk. Ebből az indirekt bizonyítás elvét alkalmazva következik, hogy $R \notin R$ tétel, amiből viszont a második kijelentés alapján leválasztással kapjuk, hogy $R \in R$. Ez azt jelenti, hogy az adott tulajdonságú R halmaz létezését feltevő elmélet ellentmondásos, így az indirekt bizonyítás elve alapján az állítást igazoltuk. ■

5.2.2. Definíció. *Azt mondjuk, hogy az $\mathscr{A}$ kijelentés* **kollektivizáló az x változóban***, ha a*

$$(\exists y)(\forall x)((x \in y) \Leftrightarrow \mathscr{A})$$

kijelentés tétel, ahol az y változó nem szerepel $\mathscr{A}$-ban.

Az előző állítás szerint ez nem triviális követelmény az $\mathscr{A}$ kijelentésre vonatkozóan, mert például az $x \notin x$ kijelentés nem kollektivizáló az x változóban. Sok egyéb, egészen egyszerű szerkezetű kijelentés is megadható, amely nem kollektivizáló valamelyik változójában (**5**., **6**. és **8**. gyakorlatok).

5.2.3. Állítás. *Ha $\mathscr{A}$ kijelentés, akkor legfeljebb egy olyan E halmaz létezik, amelyben az x változó nem szerepel és a $(\forall x)((x \in E) \Leftrightarrow \mathscr{A})$ kijelentés tétel.*

Bizonyítás. Ha E és F ilyen halmazok, akkor világos, hogy $(\forall x)((x \in E) \Leftrightarrow \mathscr{A})$ és $(\forall x)((x \in F) \Leftrightarrow \mathscr{A})$ tétel, amiből kapjuk, hogy $(\forall x)((x \in E) \Leftrightarrow (x \in F))$ is tétel, tehát a meghatározottsági axióma szerint $E = F$. ■

Jelölés. Ha az $\mathscr{A}$ kijelentés kollektivizáló az x változóban, akkor $\{x|\mathscr{A}\}$ jelöli azt a halmazt, amelyre teljesül a

$$(\forall x)\,((x \in \{x|\mathscr{A}\}) \Leftrightarrow \mathscr{A})$$

kijelentés.

Ha az $\mathscr{A}$ kijelentés kollektivizáló az x változóban, akkor az $\{x|\mathscr{A}\}$ halmaz formális nyelvi konstrukciója olyan, hogy abban az x változó nem szerepel. Ezért ahhoz, hogy egy $\mathscr{A}$ kijelentés kollektivizáló legyen az x változóban *szükséges* olyan E halmaz létezése, amelyben nem szerepel az x változó és amelyre a $(\forall x)(\mathscr{A} \Rightarrow (x \in E))$ kijelentés tétel. A második axióma azt követeli meg, hogy ez a feltétel *elégséges* is legyen.

Részhalmaz axióma – *Ha $\mathscr{A}$ olyan kijelentés, hogy létezik olyan E halmaz, amelyben az x változó nem szerepel és amelyre a $(\forall x)(\mathscr{A} \Rightarrow (x \in E))$ kijelentés tétel, akkor $\mathscr{A}$ az x változóban kollektivizáló.*

A részhalmaz axióma nagyon erős feltétel, amely rendkívül sokféle halmaz létezését biztosítja.

5.2.4. Állítás. *Ha $\mathscr{A}$ és $\mathscr{B}$ kijelentések és $(\forall x)(\mathscr{A} \Rightarrow \mathscr{B})$ tétel, továbbá $\mathscr{B}$ kollektivizáló az x változóban, akkor $\mathscr{A}$ is kollektivizáló x-ben és $\{x|\mathscr{A}\} \subseteq \{x|\mathscr{B}\}$.*

Bizonyítás. A $\mathscr{B}$ kollektivizáló az x változóban, ezért az $E := \{x|\mathscr{B}\}$ halmazban x nem szerepel. Ugyanakkor $(\forall x)(\mathscr{B} \Rightarrow x \in E)$ tétel, ezért az implikáció tranzitivitása folytán $(\forall x)(\mathscr{A} \Rightarrow (x \in E))$ is tétel, vagyis a részhalmaz axióma alapján $\mathscr{A}$ is kollektivizáló x-ben. Ezért az $x \in \{x|\mathscr{A}\}$ kijelentés ekvivalens $\mathscr{A}$-val és $\mathscr{A} \Rightarrow \mathscr{B}$ tétel, így $x \in \{x|\mathscr{B}\}$ is teljesül, vagyis

$$(\forall x)((x \in \{x|\mathscr{A}\}) \Rightarrow (x \in \{x|\mathscr{B}\}))$$

tétel, és ez azt jelenti, hogy $\{x|\mathscr{A}\} \subseteq \{x|\mathscr{B}\}$. ■

5.2.5. Állítás. *Ha E halmaz és az x változó nem szerepel E-ben, akkor az $x \in E$ kijelentés kollektivizáló az x változóban és $E = \{x|x \in E\}$.*

Bizonyítás. Nyilvánvaló, hogy ha $\mathscr{A}$ jelöli az $x \in E$ kijelentést, akkor a

$$(\forall x)(\mathscr{A} \Rightarrow (x \in E))$$

kijelentés tétel, tehát a részhalmaz axióma szerint az $x \in E$ kijelentés kollektivizáló az x változóban és az $\{x|x \in E\}$ halmaz definíciója szerint a

$$(\forall x)((x \in \{x|x \in E\}) \Leftrightarrow (x \in E))$$

kijelentés tétel. Ezért a meghatározottsági axióma alapján $E = \{x|x \in E\}$. ■

Tehát minden halmaz egyenlő az elemeinek halmazával. Itt kezd értelmet nyerni az $\in$ szimbólum, amit eddig akárhogy is jelölhettünk volna és akárhogy is nevezhettünk volna.

5.2.6. Állítás. *Az $x \neq x$ kijelentés kollektivizáló az x változóban. Az $\{x|x \neq x\}$ halmaz az egyetlen olyan halmaz, amelynek nincs eleme.*

Bizonyítás. Legyen E tetszőleges olyan halmaz, amelyben az x változó nem szerepel (például E lehet bármilyen x-től különböző változó). Az $x = x$ kijelentés tétel, ezért $(x \notin E) \Rightarrow (x = x)$ is tétel, így az $(x \neq x) \Rightarrow (x \in E)$ kijelentés tétel. Ezért a részhalmaz axióma alapján az $x \neq x$ kijelentés kollektivizáló az x változóban. Ekkor az $\{x|x \neq x\}$ halmaz definíciója szerint $(\forall x)((x \in \{x|x \neq x\}) \Leftrightarrow x \neq x)$ teljesül, ezért az $\{x|x \neq x\}$ halmaz minden eleme nem egyenlő önmagával, vagyis ennek nincs eleme. ■

5.2.7. Definíció. *Az $\{x|x \neq x\}$ halmazt üres halmaznak nevezzük és az $\emptyset$ szimbólummal jelöljük.*

A következő állítás megmutatja, hogy mi indokolja a részhalmaz axióma elnevezést.

5.2.8. Állítás. *Ha $\mathscr{A}$ kijelentés és E olyan halmaz, amelyben az x változó nem szerepel, akkor az $\mathscr{A} \wedge (x \in E)$ kijelentés kollektivizáló az x változóban, és $\{x|\mathscr{A} \wedge (x \in E)\}$ részhalmaza az E halmaznak.*

Bizonyítás. Világos, hogy a $(\forall x)(((\mathscr{A} \wedge (x \in E)) \Rightarrow (x \in E))$ kijelentés tétel, ezért a részhalmaz axióma szerint az $\mathscr{A} \wedge (x \in E)$ kijelentés x-ben kollektivizáló és az $\{x|\mathscr{A} \wedge (x \in E)\}$ halmaz definíciója alapján

$$(\forall x)((x \in \{x|\mathscr{A} \wedge (x \in E)\}) \Rightarrow (x \in E))$$

teljesül, azaz $\{x|\mathscr{A} \wedge (x \in E)\} \subseteq (x \in E)$. ■

5.2.9. Következmény. *Ha E és F halmazok és az x változó nem szerepel sem E-ben, sem F-ben, akkor az $(x \in E) \wedge (x \in F)$ és $(x \in E) \wedge (x \notin F)$ kijelentések kollektivizálók x-ben.*

5.2.10. Definíció. *Ha E és F halmazok és az x változó nem szerepel sem E-ben, sem F-ben, akkor*

$$\begin{aligned} E \cap F &:= \{x | (x \in E) \wedge (x \in F)\} \\ E \setminus F &:= \{x | (x \in E) \wedge (x \notin F)\}, \end{aligned}$$

és $E \cap F$-t az E és F halmazok **metszetének**, *míg $E \setminus F$-t az E és F halmazok* **különbségének** *nevezzük.*

A részhalmaz axióma alkalmazhatóságához szükség van néhány egészen elemi módon előállítható halmaztípus létezésére.

5.3. Hatványhalmaz axióma

Természetesnek tűnik az, hogy ha E halmaz, akkor gondolhatunk az E összes részhalmazainak halmazára. Kiderül, hogy ennek létezése nem következik az eddigi axiomatikából (ha az ellentmondásmentes elméletet határoz meg), ezért vezetjük be a következő axiómát.

Hatványhalmaz axióma – *Ha E halmaz és az x változó nem szerepel E-ben, akkor az $x \subseteq E$ kijelentés kollektivizáló az x változóban. Ekkor*

$$\mathscr{P}(E) := \{x | x \subseteq E\},$$

és ezt a halmazt az E **hatványhalmazának** *nevezzük.*

A hatványhalmaz axiómából következik, hogy minden halmaz eleme valamelyik halmaznak, hiszen ha E halmaz, akkor $E \subseteq E$ miatt $E \in \mathscr{P}(E)$.

Ha E halmaz és az x változó nem szerepel E-ben, akkor az $x = E$ kijelentés kollektivizáló x-ben, mert a hatványhalmaz axióma szerint képezhető a $\mathscr{P}(E)$ halmaz, amelyben x nem szerepel, és nyilvánvaló, hogy $(\forall x)((x = E) \Rightarrow (x \in \mathscr{P}(E)))$ tétel, tehát a részhalmaz axióma alapján $x = E$ kollektivizáló x-ben. Az $\{x | x = E\}$ halmazt az E-t tartalmazó *egy elemű* halmaznak nevezzük és $\{E\}$-vel jelöljük.

5.4. Páraxióma

Felvetődik két elemű halmaz létezésének bizonyíthatósága, vagyis az, hogy ha E és F halmazok és az x változó nem szerepel E-ben és F-ben, akkor kollektivizáló-e x-ben az $(x = E) \vee (x = F)$ kijelentés? Kiderül, hogy ez nem következik az eddigi axiomatikából (ha az ellentmondásmentes elméletet határoz meg), ezért van szükség a következő axiómára.

Páraxióma – *Ha E és F halmazok és az x változó nem szerepel E-ben és F-ben, akkor az $(x = E) \vee (x = F)$ kijelentés kollektivizáló x-ben. Ekkor*

$$\{E, F\} := \{x | (x = E) \vee (x = F)\},$$

és ezt a halmazt az E és F halmazokból álló (**rendezetlen**) **párnak** *nevezzük.*

A "rendezetlen" jelzőt az indokolja, hogy ha E és F halmazok, akkor az $(x = E) \vee (x = F)$ és $(x = F) \vee (x = E)$ kijelentések ekvivalenciája miatt $\{E, F\} = \{F, E\}$ teljesül, így az $\{E, F\}$ jelölésben az E és F elemek sorrendisége csak *látszólagos.* Könnyen látható, hogy ha E halmaz, akkor $\{E\} = \{E, E\}$.

A halmazok közötti kapcsolatok (relációk) és függvények értelmezhetősége tekintetében döntő jelentőségű lesz a rendezett párok létezése. Bármely két E és F halmazhoz olyan (E, F) halmazt szeretnénk előállítani, amelyre teljesül az, hogy ha E' és F' szintén halmazok, akkor $(E, F) = (E', F')$ ekvivalens legyen azzal, hogy $(E = E') \wedge (F = F')$. Ilyen tulajdonságú "rendezett" párok konstrukciójához nincs szükség új axiómára.

5.4.1. Definíció. *Ha E és F halmazok, akkor*

$$(E, F) := \{\{E\}, \{E, F\}\},$$

és ezt a halmazt az E és F halmazokból álló (**rendezett**) **párnak** *nevezzük.*

5.4.2. Állítás. *Ha E, F, E' és F' halmazok, akkor az $(E, F) = (E', F')$ kijelentés ekvivalens az $(E = E') \wedge (F = F')$ kijelentéssel.*

Bizonyítás. Nyilvánvaló, hogy $(E = E') \wedge (F = F') \Rightarrow (E, F) = (E', F')$ teljesül, ezért csak a fordított következtetést kell igazolni. Tegyük fel, hogy $(E, F) = (E', F')$. Ekkor a definíció szerint $\{\{E\}, \{E, F\}\} = \{\{E'\}, \{E', F'\}\}$, ezért $\{E\} \in \{\{E'\}, \{E', F'\}\}$, így $\{E\} = \{E'\}$ vagy $\{E\} = \{E', F'\}$. Ha $\{E\} = \{E'\}$, akkor $E = E'$; ha pedig $\{E\} = \{E', F'\}$, akkor $E' \in \{E', F'\} = \{E\}$ miatt ismét $E = E'$ adódik, tehát $E = E'$. Ezért az $(E, F) = (E', F')$ egyenlőség ekvivalens azzal, hogy $\{\{E\}, \{E, F\}\} = \{\{E\}, \{E, F'\}\}$. Az $\{E, F'\}$ halmaz eleme a jobb oldalon álló halmaznak, ezért $\{E\} = \{E, F'\}$ vagy $\{E, F\} = \{E, F'\}$ teljesül. Az első esetben $E = F'$, míg a második esetben $F' \in \{E, F'\}$ miatt $E = F'$ vagy $F = F'$. Ezért az $F = F'$ egyenlőség bizonyításához elég azt megmutatni, hogy $E = F'$ esetén is fennáll az $F = F'$ egyenlőség. Ha $E = F'$, akkor az $(E, F) = (E', F')$ egyenlőség a következőképpen néz ki:

$$\{\{E\}, \{E, F\}\} = \{\{E\}, \{E, F'\}\} = \{\{E\}, \{E\}\} = \{\{E\}\}.$$

Ezért $\{E, F\} = \{E\}$, így $F = E$. A feltevés szerint $E = F'$, ezért $F = F'$. ■

Később látni fogjuk, hogy létezik olyan eljárás, amelynek segítségével kijelölhető egy (E, F) pár első, illetve második "komponense", tehát az (E, F) jelölésben az E és F "komponensek" sorrendisége *valóságos.*

5.5. Unió axióma

A részhalmaz axiómából következett, hogy minden halmaz egyenlő az elemeinek halmazával. Felmerül a kérdés, hogy egy halmaz elemeinek az elemei is halmazt alkotnak-e, vagyis ha E halmaz és az x és y változók nem szerepelnek E-ben, akkor a

$$(\exists y)((x \in y) \wedge (y \in E))$$

kijelentés kollektivizáló-e az x változóban? Ha az eddigi axiomatika ellentmondásmentes elméletet határoz meg, akkor ez a kijelentés nem bizonyítható. Ezért vezetjük be a következő axiómát.

Unió axióma - *Ha E halmaz és az x és y változók nem szerepelnek E-ben, akkor a $(\exists y)((x \in y) \wedge (y \in E))$ kijelentés kollektivizáló x-ben. Ekkor*

$$\bigcup E := \{x|(\exists y)((x \in y) \wedge (y \in E))\},$$

és ezt a halmazt az E halmaz **uniójának** *nevezzük.*

Tehát ha E halmaz, és az x változó nem szerepel E-ben, akkor az

$$x \in \bigcup E \;\Leftrightarrow\; (\exists y)((x \in y) \wedge (y \in E))$$

kijelentés tétel, ami pontosan azt fejezi ki, hogy x eleme az E halmaz valamelyik elemének.

5.5.1. Állítás. *Ha E és F halmazok és x olyan változó, amely nem szerepel E-ben és F-ben, akkor az $(x \in E) \vee (x \in F)$ kijelentés kollektivizáló x-ben, és az $\{x|(x \in E) \vee (x \in F)\}$ halmaz egyenlő az $\bigcup\{E, F\}$ halmazzal.*

Bizonyítás. A páraxióma és az unió axióma szerint képezhető az $\bigcup\{E, F\}$ halmaz, és az unió definíciója alapján az $x \in \bigcup\{E, F\}$ és $(\exists y)((x \in y) \wedge (y \in \{E, F\}))$ kijelentések ekvivalensek. Viszont a rendezetlen párok definíciója szerint $y \in \{E, F\}$ ekvivalens azzal, hogy $(y = E) \vee (y = F)$. Ezért az $(x \in E) \vee (x \in F)$ és $(\exists y)((x \in y) \wedge (y \in \{E, F\}))$ kijelentések ekvivalensek. ■

5.5.2. Definíció. *Ha E és F halmazok és x olyan változó, amely nem szerepel E-ben és F-ben, akkor*

$$E \cup F := \{x|(x \in E) \vee (x \in F)\},$$

és ezt a halmazt az E és F halmazok **uniójának** *nevezzük.*

5.5.3. Állítás. *Ha E és F halmazok, továbbá x, y és z olyan változók, amelyek nem szerepelnek E-ben és F-ben, akkor a $(\exists x)(\exists y)((z = (x, y)) \wedge (x \in E) \wedge (y \in F))$ kijelentés kollektivizáló a z változóban.*

Bizonyítás. Jelölje $\mathscr{A}$ a $(\exists x)(\exists y)((z = (x, y)) \wedge (x \in E) \wedge (y \in F))$ kijelentést. Ha $\mathscr{A}$ teljesül, akkor vannak olyan X és Y halmazok, hogy $z = (X, Y)$ és $X \in E$ és $Y \in F$. Ekkor $z = \{\{X\}, \{X, Y\}\}$ és $X \in E \cup F$ és $Y \in E \cup F$, ezért $\{X\} \in \mathscr{P}(E \cup F)$, így $z \subseteq \mathscr{P}(E \cup F)$, vagyis $z \in \mathscr{P}(\mathscr{P}(E \cup F))$. A $\mathscr{P}(\mathscr{P}(E \cup F))$ halmazban nem szerepel a z változó, és az imént láttuk, hogy az $\mathscr{A} \Rightarrow z \in \mathscr{P}(\mathscr{P}(E \cup F))$ kijelentés tétel, tehát $(\forall z)(\mathscr{A} \Rightarrow z \in \mathscr{P}(\mathscr{P}(E \cup F)))$ is tétel. Ezért a részhalmaz axióma alkalmazásával kapjuk, hogy az $\mathscr{A}$ kijelentés kollektivizáló a z változóban. ■

5.5.4. Definíció. *Ha E és F halmazok, továbbá x, y és z olyan változók, amelyek nem szerepelnek E-ben és F-ben, akkor*

$$E \times F := \{z|(\exists x)(\exists y)((z = (x, y)) \wedge (x \in E) \wedge (y \in F))\},$$

és ezt a halmazt az E és F halmazok (**Descartes-**) **szorzatának** *nevezzük.*

Eddig öt halmazelméleti axiómát vezettünk be. Ezek alkalmazásával nagyon sok nemtriviális halmaz létezése igazolható. Azonban még két egzisztencia-axiómára szükségünk lesz ahhoz, hogy az analízis legfontosabb objektumait létrehozhassuk.

5.6. Gyakorlatok

1. A matematika formális nyelve. Nem axiomatikus és axiomatikus ítéletkalkulus. Axiomatikus predikátumkalkulus. Matematikai elméletek. Az igazság (tétel) fogalma. (A matematikai analízis logikai alapjai.)

2. Gyűjtsük össze azokat a logikai tételeket, amelyeket az eddigi bizonyításokban felhasználtunk!

3. Mit jelent az, hogy egy kijelentés *nem igaz* (a kétféle értelmezés)? Mit értünk azon, hogy egy kijelentés *nem kollektivizáló* valamely változójában (a kétféle értelmezés)?

4. Ha $\mathscr{A}$ és $\mathscr{B}$ olyan kijelentések és x olyan változó, hogy $(\forall x)(\mathscr{A} \Leftrightarrow \mathscr{B})$ tétel, akkor az $\mathscr{A}$ és $\mathscr{B}$ kijelentések egyszerre kollektivizálók az x változóban, vagy egyikük sem kollektivizáló az x változóban, továbbá, ha $\mathscr{A}$ kollektivizáló az x változóban, akkor $\{x|\mathscr{A}\} = \{x|\mathscr{B}\}$.

5. Nem létezik olyan halmaz, amelynek minden halmaz az eleme. Az $x = x$ és $x \subseteq x$ kijelentések nem kollektivizálók az x változóban.

6. Ha az $\mathscr{A}$ kijelentés tétel, akkor $\mathscr{A}$ nem kollektivizáló az x változóban. Ha az $\mathscr{A}$ kijelentésben nem szerepel az x változó, akkor $\mathscr{A}$ nem kollektivizáló az x változóban.

7. Ha $\mathscr{A}$ kijelentés és $\mathscr{B}$ tétel, akkor a $(\forall x)(\mathscr{A} \Rightarrow \mathscr{B})$ kijelentés tétel.

8. Ha E halmaz és az x változó nem szerepel E-ben, akkor az $x \notin E$ és $x \neq E$ kijelentések nem kollektivizálók az x változóban.

9. Az $\cup$, $\cap$ és $\setminus$ halmazműveletekre vonatkozó azonosságok és azok logikai okai. Az üres halmaz szerepe a halmazalgebrákban.

10. Halmazszorzással kapcsolatos egyenlőségek és azok logikai okai. A halmazszorzás kapcsolatai a többi halmazművelettel.

11. A *szimmetrikus halmazkülönbség* ($\triangle$) bevezetése és annak műveleti tulajdonságai.

12. Ha E és F halmazok, akkor $\mathscr{P}(E) \subseteq \mathscr{P}(F)$ *ekvivalens* azzal, hogy $E \subseteq F$.

13. Az E halmazt *tranzitívnak* nevezzük, ha az E minden eleme részhalmaza E-nek. Egy E halmaz tranzitivitása azzal ekvivalens, hogy $\bigcup E \subseteq E$. Két tranzitív halmaz metszete és uniója szintén tranzitív.

14. A matematikában sok esetben képezünk "adott alakú" halmazok halmazát. Pontosabban arról van szó, hogy ha x változó és T az x változó segítségével előállított halmaz (pl. $\{x\}$), továbbá $\mathscr{A}$ kijelentés, akkor előfordulhat az, hogy a $(\exists x)((y = T) \wedge \mathscr{A})$ kijelentés kollektivizáló az y változóban, ahol y nem szerepel sem T-ben, sem $\mathscr{A}$-ban. Ekkor az $\{y|(\exists x)((y = T) \wedge \mathscr{A})\}$ halmaz azon T "alakú" halmazok halmaza, amelyekre $\mathscr{A}$ teljesül. Ilyenkor az

$$\{T|\mathscr{A}\} := \{y|(\exists x)((y = T) \wedge \mathscr{A})\}$$

jelölést alkalmazzuk. Ha például E halmaz, amelyben az x és y változók nem szerepelnek, akkor a részhalmaz axióma alapján képezhető az $\{y|(\exists x)((y = \{x\}) \wedge (x \in E))\}$ halmaz, amit az előzőek alapján $\{\{x\}|x \in E\}$-vel jelölünk.

15. Legyen x változó, valamint $\mathscr{A}$ és $\mathscr{B}$ kijelentések. Ekkor a következő definíciókat alkalmazzuk:

$$(\forall_{\mathscr{B}} x)\mathscr{A} := (\forall x)(\mathscr{B} \Rightarrow \mathscr{A})$$
$$(\exists_{\mathscr{B}} x)\mathscr{A} := (\exists x)(\mathscr{B} \wedge \mathscr{A}),$$

és $\forall_{\mathscr{B}} x$ (illetve $\exists_{\mathscr{B}} x$) kifejezéseket *$\mathscr{B}$-feltételű univerzális* (illetve *egzisztenciális*) *kvantoroknak* nevezzük az x változó szerint. A leggyakoribb feltétel $x \in E$ alakú, ahol az x változó nem szerepel az E halmazban, tehát a legsűrűbben előforduló, feltételes kvantorokat tartalmazó kijelentések

$$(\forall_{x \in E} x)\mathscr{A} := (\forall x)((x \in E) \Rightarrow \mathscr{A})$$
$$(\exists_{x \in E} x)\mathscr{A} := (\exists x)((x \in E) \wedge \mathscr{A}),$$

alakúak. A $\forall_{x \in E} x$ (illetve $\exists_{x \in E} x$) feltételes kvantort rendszerint a $\forall x \in E$ (illetve $\exists x \in E$) szimbólummal is jelöljük.

6. fejezet

Relációk és függvények

6.1. Relációk

6.1.1. Definíció. *Az R halmazt* **relációnak** *nevezzük, ha R minden eleme pár, tehát ha a*

$$(\forall z)((z \in R) \Rightarrow (\exists x)(\exists y)(z = (x, y)))$$

kijelentés tétel, ahol az x, y és z változók nem szerepelnek R-ben.

6.1.2. Állítás. *Ha R reláció és az x, y változók nem szerepelnek R-ben, akkor a $(\exists y)((x, y) \in R)$ kijelentés kollektivizáló x-ben, és a $(\exists x)((x, y) \in R)$ kijelentés kollektivizáló y-ban.*

Bizonyítás. Könnyen látható, hogy ha $(\exists y)((x, y) \in R)$ teljesül, akkor létezik olyan Y halmaz, hogy $(x, Y) \in R$. Ekkor $\{x\} \in (x, Y) \in R$, tehát $x \in \{x\}$ miatt $x \in \bigcup\left(\bigcup R\right)$. De $\bigcup\left(\bigcup R\right)$ olyan halmaz, amelyben az x változó nem szerepel, ezért a részhalmaz axióma szerint a $(\exists y)((x, y) \in R)$ kijelentés kollektivizáló x-ben. Hasonlóan kapjuk, hogy ha $(\exists x)((x, y) \in R)$ teljesül, akkor $y \in \bigcup\left(\bigcup R\right)$, tehát a $(\exists x)((x, y) \in R)$ kijelentés kollektivizáló y-ban. ■

6.1.3. Definíció. *Ha R reláció, akkor*

$$\begin{aligned} \mathrm{pr}_1\langle R\rangle &:= \{\ x \mid (\exists y)((x, y) \in R)\ \}, \\ \mathrm{pr}_2\langle R\rangle &:= \{\ y \mid (\exists x)((x, y) \in R)\ \}, \end{aligned}$$

és a $\mathrm{pr}_1\langle R\rangle$ (illetve $\mathrm{pr}_2\langle R\rangle$) halmazt az R reláció **első** *(illetve* **második***)* **projekciójának** *nevezzük.*

Ha R reláció, akkor $R \subseteq (\mathrm{pr}_1\langle R\rangle \times (\mathrm{pr}_2\langle R\rangle)$, és ha E és F olyan halmazok, hogy $R \subseteq E \times F$, akkor $\mathrm{pr}_1\langle R\rangle \subseteq E$ és $\mathrm{pr}_2\langle R\rangle \subseteq F$.

6.1.4. Állítás. *Ha E és F halmazok, akkor $E = \bigcup\left(\mathrm{pr}_1\langle\{(E, F)\}\rangle\right)$ valamint $F = \bigcup\left(\mathrm{pr}_2\langle\{(E, F)\}\rangle\right)$. Ha E halmaz, akkor $E = \bigcup\{E\}$.*

Bizonyítás. A relációk projekciójának definíciója alapján világos, hogy $\mathrm{pr}_1\langle\{(E, F)\}\rangle = \{E\}$ és $\mathrm{pr}_2\langle\{(E, F)\}\rangle = \{F\}$, ezért elég a második állítást igazolni. Az $E \in \{E\}$ összefüggés miatt, $x \in E$ esetén, az unió definíciója szerint $x \in \bigcup\{E\}$, tehát $E \subseteq \bigcup\{E\}$.

Megfordítva, ha $x \in \bigcup\{E\}$, akkor létezik olyan $y \in \{E\}$, hogy $x \in y$; ekkor $y = E$ és $x \in y$, azaz $x \in E$, tehát $\bigcup\{E\} \subseteq E$. Ezért a meghatározottsági axiómából kapjuk, hogy $E = \bigcup\{E\}$. ∎

Ez az állítás egyszerű eljárást szolgáltat, amelynek alkalmazásával megadható egy elemű halmaz eleme, illetve egy pár első és második komponense.

6.1.5. Állítás. *Ha R reláció, X halmaz, és az x, y változók nem szerepelnek sem R-ben, sem X-ben, akkor a $(\exists x)((x \in X) \wedge (x, y) \in R)$ kijelentés kollektivizáló y-ban.*

Bizonyítás. A $(\exists x)((x \in X) \wedge (x, y) \in R)$ kijelentésből adódik, hogy $y \in \mathrm{pr}_2\langle R\rangle$, így a részhalmaz axióma szerint a $(\exists x)((x \in X) \wedge (x, y) \in R)$ kijelentés kollektivizáló az y változóban. ∎

6.1.6. Definíció. *Ha R reláció, X halmaz, és az x, y változók nem szerepelnek sem R-ben, sem X-ben, akkor*

$$R\langle X\rangle := \{\ y \mid (\exists x)((x \in X) \wedge (x, y) \in R)\ \},$$

és ezt a halmazt **az X halmaz R reláció által létesített képének** *nevezzük.*

Ha R reláció, akkor az $R\langle\{x\}\rangle = \{y|(x, y) \in R\}$ halmazt az R reláció x-szel vett **szeletének** is nevezzük, és olykor az $R(x)$ szimbólummal is jelöljük.

6.2. Függvények

6.2.1. Definíció. *Az f relációt* **függvényrelációnak** (*vagy* **függvénynek**) *nevezzük, ha*

$$(\forall x)(\forall y)(\forall y')(\ (((x, y) \in f) \wedge ((x, y') \in f)) \Rightarrow y = y'\ ),$$

ahol az x, y és y' változók nem szerepelnek f-ben.

Tehát az f reláció pontosan akkor függvény, ha minden x halmazra az $f\langle\{x\}\rangle$ szelet *legfeljebb* egy elemű halmaz. Ha f függvény, akkor minden x halmazra $x \in \mathrm{pr}_1\langle f\rangle$ ekvivalens azzal, hogy az $f\langle\{x\}\rangle$ szelet *pontosan* egy elemű halmaz.

6.2.2. Definíció. *Legyen f függvény.*

– *A $\mathrm{pr}_1\langle f\rangle$ halmazt az f* **értelmezési** (*vagy* **definíciós**) **tartományának** *nevezzük és $\mathrm{Dom}(f)$-fel jelöljük.*

– *A $\mathrm{pr}_2\langle f\rangle$ halmazt az f* **értékkészletének** (*vagy* **képének**) *nevezzük és $\mathrm{Im}(f)$-fel jelöljük.*

– *Ha $x \in \mathrm{Dom}(f)$ akkor az $f\langle\{x\}\rangle$ halmaz egyetlen elemét $f(x)$ jelöli, tehát $f\langle\{x\}\rangle = \{f(x)\}$, vagyis írható, hogy $f(x) := \bigcup f\langle\{x\}\rangle$. Az $f(x)$ halmazt* **az f függvény x helyen felvett értékének** *nevezzük.*

Ha f függvény, akkor $f = \{(x, f(x))|x \in \mathrm{Dom}(f)\}$, továbbá, ha X halmaz, akkor

$$f\langle X\rangle = \{f(x)|x \in (X \cap \mathrm{Dom}(f))\},$$

és $\mathrm{Dom}(f) \subseteq X$ esetén $f\langle X\rangle = \mathrm{Im}(f)$.

Ha f és g függvények, akkor $f = g$ ekvivalens azzal, hogy $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ és minden $x \in \mathrm{Dom}(f)$ elemre $f(x) = g(x)$. Ha f és g függvények és $E \subseteq \mathrm{Dom}(f) \cap \mathrm{Dom}(g)$, akkor azt mondjuk, hogy *$f = g$ az E halmazon*, ha minden $x \in E$ pontra $f(x) = g(x)$.

6.2.3. Definíció. *Legyenek E, F halmazok és f függvény.*

– *Azt mondjuk, hogy f E-**ben értelmezett** (illetve E-**n értelmezett**) függvény, ha* $\mathrm{Dom}(f) \subseteq E$ *(illetve* $\mathrm{Dom}(f) = E$*).*

– *Azt mondjuk, hogy az f függvény az F **halmazba érkezik**, ha* $\mathrm{Im}(f) \subseteq F$*.*

Jelölés. Legyenek E, F halmazok és f függvény. Azt, hogy az f függvény az E halmazban (illetve E halmazon) értelmezett és F-be érkezik az $f : E \rightarrowtail F$ (illetve $f : E \to F$) szimbólummal jelöljük.

Tehát az $f : E \rightarrowtail F$ és $f : E \to F$ jelölések olyan kijelentések rövidítései, amelyek az f függvény definíciós tartományának E-vel és az értékkészletének F-fel való *kapcsolatát* fejezik ki.

6.2.4. Definíció. *Az R relációt* **injektívnek** *nevezzük, ha*

$$(\forall x)(\forall x')(\forall y)(\forall y')\,((((x, y) \in R) \wedge ((x', y') \in R) \wedge (x \neq x')) \Rightarrow y \neq y')$$

teljesül, ahol az x, x', y és y' változók nem szerepelnek R-ben. Az injektív függvényeket **injekcióknak** *is nevezzük.*

Tehát egy f függvény injektivitása azzal ekvivalens, hogy $x, x' \in \mathrm{Dom}(f)$ és $x \neq x'$ esetén $f(x) \neq f(x')$ teljesül.

6.2.5. Definíció. *Legyenek E, F halmazok és f függvény.*

– *Azt mondjuk, hogy f **ráképez** az F halmazra, ha* $F \subseteq \mathrm{Im}(f)$*. Ilyenkor azt is mondjuk, hogy f **szürjektív** F-re. Ha $f : E \rightarrowtail F$ függvény és f ráképez F-re, tehát* $\mathrm{Im}(f) = F$*, akkor azt mondjuk, hogy f **szürjekció** E és F között.*

– *Azt mondjuk, hogy f **bijekció** az E és F halmazok között, ha f injektív és* $\mathrm{Dom}(f) = E$ *és* $\mathrm{Im}(f) = F$*.*

Minden injekció bijekció a definíciós tartománya és az értékkészlete között. Míg az injektivitás egy függvény "belső" tulajdonsága, addig a szürjektivitás és a bijektivitás a függvény más halmazokkal való kapcsolatát fejezi ki.

Példák. 1) Az $\emptyset$ halmaz injektív függvény (ez az *üres függvény*).

2) Ha E halmaz, akkor az $\mathrm{id}_E := \{(x, x) | x \in E\}$ halmaz bijektív függvény az E és E halmazok között (ez az E halmaz *identikus függvénye*).

3) Ha E és F halmazok, és $c \in F$ rögzített pont, akkor az $\{(x, c) | x \in E\}$ halmaz E-n értelmezett, F-be érkező függvény (ez az E halmazon értelmezett, c-értékű *konstansfüggvény*).

4) Ha E halmaz, akkor az $\{(x, \{x\}) | x \in E\}$ halmaz E-n értelmezett, $\mathscr{P}(E)$-be érkező injekció. Azonban látni fogjuk, hogy nem létezik $E \to \mathscr{P}(E)$ szürjekció (6.5.4.).

6.2.6. Állítás. *Legyenek E és F halmazok. Az $f : E \to F$ függvény pontosan akkor bijekció E és F között, ha minden $y \in F$ esetén létezik egyetlen olyan $x \in E$, hogy $f(x) = y$.*

Bizonyítás. Ha f bijekció, akkor f szürjekció E és F között, így $\mathrm{Im}(f) = F$, tehát minden $y \in F$ esetén létezik olyan $x \in E$, hogy $f(x) = y$, és ez az $x \in E$ elem f injektivitása miatt egyértelműen van meghatározva.

Tegyük fel, hogy f-re teljesül az, hogy minden $y \in F$ esetén létezik egyetlen olyan $x \in E$, hogy $f(x) = y$. Ekkor $F \subseteq \mathrm{Im}(f)$, így $\mathrm{Im}(f) = F$, és ha $x, x' \in E$ olyanok, hogy $f(x) = f(x')$, akkor a feltétel szerint $x = x'$, vagyis f injekció. Ez azt jelenti, hogy f bijekció E és F között. ■

6.2.7. Állítás. *Ha f függvény és $E \subseteq \mathrm{Dom}(f)$, akkor az $\{(x, f(x)) | x \in E\}$ halmaz függvény.*

Bizonyítás. Nyilvánvalóan következik abból, hogy f függvényreláció. ■

6.2.8. Definíció. *Ha f függvény és $E \subseteq \mathrm{Dom}(f)$, akkor az $\{(x, f(x)) | x \in E\}$ halmazt az f függvény E halmazra vett* **leszűkítésének** *nevezzük és az $f|_E$ szimbólummal jelöljük. A g függvényt az f függvény* **kiterjesztésének** *nevezzük, ha f egyenlő a g valamelyik leszűkítésével.*

Tehát, ha f függvény és $E \subseteq \mathrm{Dom}(f)$, akkor $\mathrm{Dom}(f|_E) = E$, $\mathrm{Im}(f|_E) = f\langle E\rangle$, és minden $x \in E$ pontra $f|_E(x) = f(x)$. A g függvény pontosan akkor kiterjesztése f-nek, ha $f \subseteq g$.

6.2.9. Állítás. *Ha E és F halmazok, és $f : E \rightarrowtail F$ függvény, akkor $F \neq \emptyset$ esetén létezik olyan $\tilde{f} : E \to F$ függvény, amely f-nek kiterjesztése.*

Bizonyítás. Rögzítve egy $c \in F$ elemet, könnyen látható, hogy az

$$\tilde{f} := f \cup ((E \setminus \mathrm{Dom}(f)) \times \{c\})$$

halmaz olyan $E \to F$ függvény, amelyre $f \subseteq \tilde{f}$. ■

Függvények előállításának gyakori módja a "függvények összeragasztása". Erről szól a következő állítás.

6.2.10. Állítás. (**Függvények összeragasztása**) *Legyen H olyan halmaz, amelynek minden eleme függvény, és teljesül rá az, hogy minden $h, h' \in H$ esetén*

$$h|_{\mathrm{Dom}(h) \cap \mathrm{Dom}(h')} = h'|_{\mathrm{Dom}(h) \cap \mathrm{Dom}(h')}.$$

Ekkor az $f := \bigcup H$ halmaz függvény, és $\mathrm{Dom}(f) = \bigcup\{\mathrm{Dom}(h) | h \in H\}$, és $\mathrm{Im}(f) = \bigcup\{\mathrm{Im}(h) | h \in H\}$, továbbá minden $h \in H$ esetén

$$h = f|_{\mathrm{Dom}(h)}.$$

Bizonyítás. Ha $z \in f$, akkor van olyan $h \in H$, hogy $z \in h$, ezért z pár, hiszen h függvény. Ez azt jelenti, hogy f reláció.

Legyenek $(x, y), (x, y') \in f$. Ekkor vehetünk olyan $h, h' \in H$ elemeket, hogy $(x, y) \in h$ és $(x, y') \in h'$, tehát $x \in \mathrm{Dom}(h)$ és $h(x) = y$, valamint $x \in \mathrm{Dom}(h')$ és $h'(x) = y'$. Ebből következik, hogy $x \in \mathrm{Dom}(h) \cap \mathrm{Dom}(h')$, és $y = h(x) = h'(x) = y'$, mert a H-ra előírt feltétel szerint $h|_{\mathrm{Dom}(h) \cap \mathrm{Dom}(h')} = h'|_{\mathrm{Dom}(h) \cap \mathrm{Dom}(h')}$. Ez azt jelenti, hogy f függvény.

Nyilvánvaló, hogy

$$x \in \mathrm{Dom}(f) \Leftrightarrow (\exists y)((x,y) \in \bigcup H) \Leftrightarrow (\exists y)(\exists h)((h \in H) \wedge ((x,y) \in h)) \Leftrightarrow$$
$$\Leftrightarrow (\exists h)(\exists y)((h \in H) \wedge ((x,y) \in h)) \Leftrightarrow (\exists h)((h \in H) \wedge (\exists y)((x,y) \in h)) \Leftrightarrow$$
$$\Leftrightarrow (\exists h)((h \in H) \wedge (x \in \mathrm{Dom}(h))) \Leftrightarrow x \in \bigcup\{\mathrm{Dom}(h) | h \in H\},$$

tehát fennáll a $\mathrm{Dom}(f) = \bigcup\{\mathrm{Dom}(h)|h \in H\}$ egyenlőség.

Az előzőekhez hasonlóan kapjuk, hogy

$$y \in \mathrm{Im}(f) \Leftrightarrow (\exists x)((x,y) \in \bigcup H) \Leftrightarrow (\exists x)(\exists h)((h \in H) \wedge ((x,y) \in h)) \Leftrightarrow$$
$$\Leftrightarrow (\exists h)(\exists x)((h \in H) \wedge ((x,y) \in h)) \Leftrightarrow (\exists h)((h \in H) \wedge (\exists x)((x,y) \in h)) \Leftrightarrow$$
$$\Leftrightarrow (\exists h)((h \in H) \wedge (y \in \mathrm{Im}(h))) \Leftrightarrow y \in \bigcup\{\mathrm{Im}(h) | h \in H\},$$

tehát fennáll a $\mathrm{Im}(f) = \bigcup\{\mathrm{Im}(h)|h \in H\}$ egyenlőség.

Ha $h \in H$, akkor az f függvény definíciója szerint $h \subseteq f$, vagyis $h = f|_{\mathrm{Dom}(h)}$. ■

6.2.11. Definíció. *Ha H olyan halmaz, amelynek minden eleme függvény, és teljesül rá az, hogy minden $h, h' \in H$ esetén*

$$h|_{\mathrm{Dom}(h)\cap\mathrm{Dom}(h')} = h'|_{\mathrm{Dom}(h)\cap\mathrm{Dom}(h')},$$

akkor az $\bigcup H$ függvényt a H-beli függvények **összeragasztásával** *létrehozott függvénynek nevezzük.*

A függvények összeragasztásának gyakran előforduló speciális esete az, amikor a H függvényhalmaz olyan, hogy minden $h, h' \in H$ esetén $h \subseteq h'$ vagy $h' \subseteq h$. Ekkor még az is teljesül, hogy ha minden $h \in H$ esetén a h függvény injekció, akkor a H-beli függvények összeragasztásával létrehozott f függvény is injekció. Valóban, ha $x, x' \in \mathrm{Dom}(f)$, akkor léteznek olyan $h \in H$ és $h' \in H$ függvények, hogy $x \in \mathrm{Dom}(h)$ és $x' \in \mathrm{Dom}(h')$; ekkor $h \subseteq h'$ esetén $x, x' \in \mathrm{Dom}(h)$, míg $h' \subseteq h$ esetén $x, x' \in \mathrm{Dom}(h')$, így a h és h' függvények injektivitásából, valamint a $h \subseteq f$ és $h' \subseteq f$ összefüggésekből következik, hogy ha $x \neq x'$, akkor $f(x) \neq f(x')$.

6.2.12. Tétel. *Ha E és F halmazok, akkor az "$f : E \to F$ függvény" és az "$f : E \rightarrowtail F$ függvény" kijelentések kollektivizálók az f változóban.*

Bizonyítás. Ha $f : E \rightarrowtail F$ függvény, akkor $f \subseteq \mathrm{Dom}(f) \times \mathrm{Im}(f) \subseteq E \times F$, következésképpen $f \in \mathscr{P}(E \times F)$, ezért a részhalmaz axióma szerint az "$f : E \rightarrowtail F$ *függvény*" kijelentés kollektivizáló az f változóban, így létezik az E-ben értelmezett, F-be érkező függvények H halmaza. Ha $f : E \to F$ függvény, akkor $f \in H$, tehát ismét a részhalmaz axióma alkalmazásával kapjuk, hogy az "$f : E \to F$ *függvény*" kijelentés kollektivizáló az f változóban. ■

6.2.13. Definíció. *Ha E és F halmazok, akkor az*

$$\mathscr{F}(E; F) := \{\ f \mid f : E \to F \text{ függvény}\ \}$$

halmazt az E**-n értelmezett** F**-be érkező függvények halmazának** *nevezzük. Az $\mathscr{F}(E; F)$ halmazt néha az F^E szimbólummal is jelöljük.*

6.3. Relációk és függvények inverze

6.3.1. Állítás. *Ha R reláció és az x, y és z változók nem szerepelnek R-ben, akkor a*

$$(\exists x)(\exists y)\,((z = (y,x)) \wedge ((x,y) \in R))$$

kijlentés kollektivizáló z-ben.

Bizonyítás. Ha $(\exists x)(\exists y)\,((z = (y,x)) \wedge ((x,y) \in R))$ teljesül, akkor vehetünk olyan X és Y halmazokat, hogy $z = (Y,X)$ és $(X,Y) \in R$. Ekkor $X \in \mathrm{pr}_1\langle R\rangle$ és $Y \in \mathrm{pr}_2\langle R\rangle$, így $z = (Y,X) \in (\mathrm{pr}_2\langle R\rangle) \times (\mathrm{pr}_1\langle R\rangle)$, ezért elég a részhalmaz axiómát alkalmazni. ■

6.3.2. Definíció. *Ha R reláció, és az x, y és z változók nem szerepelnek R-ben, akkor*

$$\overset{-1}{R} := \{\ z \mid (\exists x)(\exists y)\,((z = (y,x)) \wedge ((x,y) \in R))\ \},$$

és ezt a halmazt **az R reláció inverzének** *nevezzük.*

6.3.3. Állítás. *Ha R reláció, akkor $\overset{-1}{\overset{-1}{R}} = R$, $\mathrm{pr}_1\langle \overset{-1}{R}\rangle = \mathrm{pr}_2\langle R\rangle$ és $\mathrm{pr}_2\langle \overset{-1}{R}\rangle = \mathrm{pr}_1\langle R\rangle$.*

Bizonyítás. Az $\overset{-1}{\overset{-1}{R}} = R$ egyenlőség triviálisan következik a definícióból. Az $y \in \mathrm{pr}_1\langle \overset{-1}{R}\rangle$ kijelentés ekvivalens azzal, hogy létezik olyan x, amelyre $(y,x) \in \overset{-1}{R}$, vagyis $(x,y) \in R$, azaz $y \in \mathrm{pr}_2\langle R\rangle$. Ezért $\mathrm{pr}_1\langle \overset{-1}{R}\rangle = \mathrm{pr}_2\langle R\rangle$ teljesül. Ezt az egyenlőséget felírva az $\overset{-1}{R}$ relációra és alkalmazva az $\overset{-1}{\overset{-1}{R}} = R$ egyenlőséget kapjuk, hogy $\mathrm{pr}_2\langle \overset{-1}{R}\rangle = \mathrm{pr}_1\langle R\rangle$. ■

6.3.4. Állítás. *Ha f függvény, akkor az $\overset{-1}{f}$ reláció pontosan akkor függvény, ha f injektív.*

Bizonyítás. Ha f injektív függvény, akkor $(y,x) \in \overset{-1}{f}$ és $(y,x') \in \overset{-1}{f}$ esetén $(x,y) \in f$ és $(x',y) \in f$, tehát $x = x'$, vagyis az $\overset{-1}{f}$ reláció függvény. Megfordítva, ha az $\overset{-1}{f}$ reláció függvény, akkor $(x,y) \in f$ és $(x',y) \in f$ esetén $(y,x) \in \overset{-1}{f}$ és $(y,x') \in \overset{-1}{f}$, így $x = x'$, ami azt jelenti, hogy f injekció. ■

Jelölés. Ha f injektív függvény, akkor az $\overset{-1}{f}$ függvényt az f^{-1} szimbólummal jelöljük.

Tehát, ha f injektív függvény, akkor

$$\mathrm{Dom}(f^{-1}) = \mathrm{Im}(f); \quad \mathrm{Im}(f^{-1}) = \mathrm{Dom}(f),$$

és minden $y \in \mathrm{Dom}(f^{-1})$ pontra $f^{-1}(y)$ az az egyértelműen meghatározott eleme $\mathrm{Dom}(f)$-nek, amelyre $f(f^{-1}(y)) = y$ teljesül. Továbbá, ekkor minden $x \in \mathrm{Dom}(f)$ pontra $f^{-1}(f(x)) = x$ is teljesül, mert az előzek szerint az $y := f(x)$ pontra $f^{-1}(y)$ az az eleme $\mathrm{Dom}(f)$-nek, amelyre $f(f^{-1}(y)) = y$, vagyis $f(f^{-1}(f(x))) = f(x)$, így f injektivitása folytán $f^{-1}(f(x)) = x$. Nyilvánvaló, hogy minden injekció inverze bijekció az eredeti függvény értékkészlete és definíciós tartománya között.

6.4. Relációk és függvények kompozíciója

6.4.1. Állítás. *Ha R és S relációk, akkor a*

$$(\exists x)(\exists y)\,((u = (x, y)) \wedge (\exists z)(((x, z) \in R) \wedge ((z, y) \in S)))$$

kijelentés kollektivizáló az u változóban, ha az x, y, z és u változók nem szerepelnek R-ben és S-ben.

Bizonyítás. Jelölje $\mathscr{A}$ az $(\exists x)(\exists y)\,((u = (x, y)) \wedge (\exists z)(((x, z) \in R) \wedge ((z, y) \in S)))$ kijelentést. Ha $\mathscr{A}$ igaz, akkor léteznek olyan X és Y halmazok, hogy $u = (X, Y)$ és $(\exists z)(((X, z) \in R) \wedge ((z, Y) \in S))$ igaz, tehát van olyan Z halmaz, hogy $(X, Z) \in R$ és $(Z, Y) \in S$. Ekkor $X \in \mathrm{pr}_1\langle R\rangle$ és $Y \in \mathrm{pr}_2\langle S\rangle$, tehát $u \in (\mathrm{pr}_1\langle R\rangle \times (\mathrm{pr}_2\langle S\rangle)$. Az u változó nem szerepel $(\mathrm{pr}_1\langle R\rangle) \times (\mathrm{pr}_2\langle S\rangle)$-ben, ezért a részhalmaz axióma szerint $\mathscr{A}$ kollektivizáló az u változóban. ■

6.4.2. Definíció. *Ha R és S relációk, akkor az*

$$S \circ R := \{\ u \mid (\exists x)(\exists y)\,((u = (x, y)) \wedge (\exists z)(((x, z) \in R) \wedge ((z, y) \in S)))\ \}$$

halmazt **az S és R relációk kompozíciójának** *vagy* **összetételének** *nevezzük, ahol az x, y, z és u változók nem szerepelnek R-ben és S-ben.*

6.4.3. Állítás. *Injektív relációk kompozíciója injektív reláció.*

Bizonyítás. Legyenek R és S injektív relációk, és x, x', y és y' olyan változók, amelyek nem szerepelnek R-ben és S-ben. Tegyük fel, hogy $(x, y) \in S \circ R$, $(x', y') \in S \circ R$ és $x \neq x'$. Léteznek olyan u és v halmazok, hogy $(x, u) \in R$, $(u, y) \in S$, $(x', v) \in R$ és $(v, y') \in S$. Az R injektivitása és $x \neq x'$ folytán $u \neq v$, továbbá S injektivitása miatt $y \neq y'$, amiből következik, hogy az $S \circ R$ reláció injektív. ■

6.4.4. Állítás. *Legyenek R és S relációk. Ekkor teljesülnek a következő egyenlőségek:*

$$\overset{-1}{(S \circ R)} = \overset{-1}{R} \circ \overset{-1}{S}, \qquad \mathrm{pr}_1\langle S \circ R\rangle = \overset{-1}{R}\langle \mathrm{pr}_1\langle S\rangle\rangle, \qquad \mathrm{pr}_2\langle S \circ R\rangle = S\langle \mathrm{pr}_2\langle R\rangle\rangle.$$

Bizonyítás. 1) Az $(x, y) \in \overset{-1}{(S \circ R)}$ kijelentés ekvivalens azzal, hogy $(y, x) \in S \circ R$, vagyis létezik olyan z, amelyre $(y, z) \in R$ és $(z, x) \in S$. Ez viszont éppen azt jelenti, hogy létezik olyan z, amelyre $(x, z) \in \overset{-1}{S}$ és $(z, y) \in \overset{-1}{R}$, vagyis $(x, y) \in \overset{-1}{R} \circ \overset{-1}{S}$.
2) Ha $x \in \mathrm{pr}_1\langle S \circ R\rangle$, akkor létezik olyan y, hogy $(x, y) \in S \circ R$. Ekkor létezik olyan z, hogy $(x, z) \in R$ és $(z, y) \in S$, ezért $(z, x) \in \overset{-1}{R}$ és $z \in \mathrm{pr}_1\langle S\rangle$, így $x \in \overset{-1}{R}\langle \mathrm{pr}_1\langle S\rangle\rangle$. Megfordítva, ha $x \in \overset{-1}{R}\langle \mathrm{pr}_1\langle S\rangle\rangle$, akkor van olyan z, hogy $(z, x) \in \overset{-1}{R}$ és $z \in \mathrm{pr}_1\langle S\rangle$. Ekkor $(x, z) \in R$ és létezik olyan y, hogy $(z, y) \in S$. Ebből kapjuk, hogy $(x, y) \in S \circ R$, ezért $x \in \mathrm{pr}_1\langle S \circ R\rangle$.
3) Ha $y \in \mathrm{pr}_2\langle S \circ R\rangle$, akkor van olyan x, hogy $(x, y) \in S \circ R$, vagyis létezik olyan z, amelyre $(x, z) \in R$ és $(z, y) \in S$. Ekkor $z \in \mathrm{pr}_2\langle R\rangle$, tehát $y \in S\langle \mathrm{pr}_2\langle R\rangle\rangle$. Megfordítva, ha $y \in S\langle \mathrm{pr}_2\langle R\rangle\rangle$, akkor van olyan z, hogy $z \in \mathrm{pr}_2\langle R\rangle$ és $(z, y) \in S$. Ekkor van olyan x, hogy $(x, z) \in R$, így $(x, y) \in S \circ R$, tehát $y \in \mathrm{pr}_2\langle S \circ R\rangle$. ■

6.4.5. Állítás. *Függvények kompozíciója függvény.*

Bizonyítás. Legyenek f és g függvények, és x, y, y' olyanok, hogy $(x,y) \in g \circ f$ és $(x,y') \in g \circ f$. Ekkor van olyan z és z', hogy $(x,z) \in f$, $(z,y) \in g$, $(x,z') \in f$ és $(z',y') \in g$. Az f reláció függvény, ezért $z = z'$, következésképpen $(z,y') \in g$. De az g reláció is függvény, így $y = y'$, amiből kapjuk, hogy a $g \circ f$ reláció is függvény. ■

Tehát, ha f és g függvények, akkor $g \circ f$ az a függvény, amelyre

$$\mathrm{Dom}(g \circ f) = \overset{-1}{f}\langle \mathrm{Dom}(g) \rangle,$$
$$\mathrm{Im}(g \circ f) = g\langle \mathrm{Im}(f) \rangle,$$

és minden $x \in \mathrm{Dom}(g \circ f)$ pontra $(g \circ f)(x) = g(f(x))$ teljesül.

6.4.6. Állítás. *Ha R, S és T relációk, akkor*

$$(T \circ S) \circ R = T \circ (S \circ R).$$

Bizonyítás. Legyen $(x,y) \in (T \circ S) \circ R$. Ekkor van olyan z, hogy $(x,z) \in R$ és $(z,y) \in (T \circ S)$. Ez utóbbi állításból kapjuk olyan u létezését, amelyre $(z,u) \in S$ és $(u,y) \in T$. Ekkor $(x,z) \in R$ és $(z,u) \in S$ miatt $(x,u) \in S \circ R$, ugyanakkor $(u,y) \in T$ is igaz, így $(x,y) \in T \circ (S \circ R)$. Ez azt jelenti, hogy $(T \circ S) \circ R \subseteq T \circ (S \circ R)$.
Megfordítva, tegyük fel, hogy $(x,y) \in T \circ (S \circ R)$. Létezik olyan u, hogy $(x,u) \in (S \circ R)$ és $(u,y) \in T$. Ekkor van olyan z, hogy $(x,z) \in R$ és $(z,u) \in S$. Ebből következik, hogy $(z,y) \in (T \circ S)$ így $(x,z) \in R$ miatt $(x,y) \in (T \circ S) \circ R$. Ez azt jelenti, hogy $T \circ (S \circ R) \subseteq (T \circ S) \circ R$.
Ezekből a meghatározottsági axióma alapján kapjuk a bizonyítandó állítást. ■

6.4.7. Definíció. *Ha R reláció és Y halmaz, akkor az $\overset{-1}{R}\langle Y \rangle$ halmazt* **az Y halmaz R által létesített inverz képének** (*vagy* **ősképének**) *nevezzük.*

Ha f függvény és Y halmaz, akkor $\overset{-1}{f}\langle Y \rangle = \{x | (x \in \mathrm{Dom}(f)) \wedge (f(x) \in Y)\}$, tehát minden $x \in \mathrm{Dom}(f)$ elemre az $x \in \overset{-1}{f}\langle Y \rangle$ és $f(x) \in Y$ kijelentések ekvivalensek. Ha f injektív függvény és X halmaz, akkor $f^{-1}\langle X \rangle = \overset{-1}{f}\langle X \rangle$.

6.4.8. Állítás. *Ha f függvény és X, Y halmazok, akkor*

a) $f\langle \overset{-1}{f}\langle Y \rangle \rangle = Y \cap \mathrm{Im}(f)$,

b) $X \cap \mathrm{Dom}(f) \subseteq \overset{-1}{f}\langle f\langle X \rangle \rangle$ *és ha f injekció, akkor* $X \cap \mathrm{Dom}(f) = \overset{-1}{f}\langle f\langle X \rangle \rangle$.

Bizonyítás. a) Ha $y \in f\langle \overset{-1}{f}\langle Y \rangle \rangle$, akkor van olyan $x \in \overset{-1}{f}\langle Y \rangle$, hogy $y = f(x)$; ekkor $f(x) \in Y$, tehát $y \in Y$, amiből következik, hogy $f\langle \overset{-1}{f}\langle Y \rangle \rangle \subseteq Y \cap \mathrm{Im}(f)$. Megfordítva, ha $y \in Y \cap \mathrm{Im}(f)$, akkor $y \in \mathrm{Im}(f)$ miatt van olyan $x \in \mathrm{Dom}(f)$, hogy $y = f(x)$; ekkor $y \in Y$ miatt $x \in \overset{-1}{f}\langle Y \rangle$ is teljesül, tehát $y \in f\langle \overset{-1}{f}\langle Y \rangle \rangle$, vagyis $Y \cap \mathrm{Im}(f) \subseteq f\langle \overset{-1}{f}\langle Y \rangle \rangle$.

b) Ha $x \in X \cap \mathrm{Dom}(f)$, akkor $f(x) \in f\langle X \rangle$, tehát $x \in \overset{-1}{f}\langle f\langle X \rangle \rangle$. Megfordítva, tegyük fel, hogy $x \in \overset{-1}{f}\langle f\langle X \rangle \rangle$. Ekkor $x \in \mathrm{Dom}(f)$ és $f(x) \in f\langle X \rangle$, tehát létezik olyan $x' \in X \cap \mathrm{Dom}(f)$, hogy $f(x) = f(x')$. Ha f injektív, akkor ebből az adódik, hogy $x = x'$, tehát $x \in X \cap \mathrm{Dom}(f)$, így fennáll az $X \cap \mathrm{Dom}(f) = \overset{-1}{f}\langle f\langle X \rangle \rangle$ egyenlőség. ■

Tehát, ha f függvény, akkor

– minden Y halmazra $f\langle \overset{-1}{f}\langle Y\rangle\rangle \subseteq Y$ és ha $Y \subseteq \mathrm{Im}(f)$, akkor $f\langle \overset{-1}{f}\langle Y\rangle\rangle = Y$;

– minden $X \subseteq \mathrm{Dom}(f)$ halmazra $X \subseteq \overset{-1}{f}\langle f\langle X\rangle\rangle$, és ha f injektív, akkor $X = \overset{-1}{f}\langle f\langle X\rangle\rangle$.

6.4.9. Állítás. *Legyenek f és g függvények.*

a) *Ha f és g injekciók, akkor $g \circ f$ is injekció és $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

b) *Ha f ráképez a* $\mathrm{Dom}(g)$ *halmazra és g ráképez az F halmazra, akkor $g \circ f$ ráképez az F halmazra.*

c) *Ha f bijekció az E és F halmazok között, és g bijekció az F és G halmazok között, akkor $g \circ f$ bijekció az E és G halmazok között.*

Bizonyítás. a) Tudjuk, hogy injektív relációk kompozíciója injektív és függvények kompozíciója függvény. Ha R és S relációk, akkor $\overset{-1}{(S \circ R)} = \overset{-1}{R} \circ \overset{-1}{S}$. Ezekből az állításokból és az inverzfüggvények értelmezéséből következik az állítás.

b) Ha $z \in F$, akkor van olyan $y \in \mathrm{Dom}(g)$, hogy $z = g(y)$, mivel g ráképez F-re. Az f ráképez $\mathrm{Dom}(g)$-re, ezért van olyan $x \in \mathrm{Dom}(f)$, hogy $y = f(x)$. Ekkor $x \in \mathrm{Dom}(g \circ f)$ és $z = (g \circ f)(x)$, tehát $g \circ f$ ráképez F-re.

c) Az a) alapján $g \circ f$ injekció, és a b) alapján $g \circ f$ ráképez G-re. ■

6.4.10. Állítás. *Legyen $f : E \to F$ függvény.*

a) *Ha van olyan $g : F \to E$ függvény, hogy $f \circ g = \mathrm{id}_F$, akkor* $\mathrm{Im}(f) = F$. (*Az ilyen tulajdonságú g függvényeket az f* **jobbinverzeinek** *nevezzük.*) *Az f minden jobbinverze injekció.*

b) *Akkor és csak akkor létezik olyan $g : F \to E$ függvény, hogy $g \circ f = \mathrm{id}_E$, ha f injekció.* (*Az ilyen tulajdonságú g függvényeket az f* **balinverezeinek** *nevezzük.*) *Az f minden balinverze ráképez E-re.*

Bizonyítás. a) Ha a $g : F \to E$ függvény jobbinverze f-nek, akkor $y \in F$ esetén $y = f(g(y))$, tehát $y \in \mathrm{Im}(f)$. Továbbá, $y, y' \in \mathrm{Dom}(g)$ és $g(y) = g(y')$ esetén $y = f(g(y)) = f(g(y')) = y'$, tehát g injekció.

b) Ha a $g : F \to E$ függvény balinverze f-nek, akkor $x, x' \in \mathrm{Dom}(f)$ és $f(x) = f(x')$ esetén $x = g(f(x)) = g(f(x')) = x'$, tehát f injekció. Továbbá, ha $x \in E$, akkor $f(x) \in F$ olyan, hogy $x = g(f(x))$, tehát g ráképez E-re.

Megfordítva, ha f injekció és $\mathrm{Dom}(f) \neq \emptyset$, akkor rögzítve tetszőleges $c \in \mathrm{Dom}(f)$ pontot, a $g := \overset{-1}{f} \cup ((F \setminus \mathrm{Im}(f)) \times \{c\})$ halmaz olyan függvény, amely balinverze f-nek. Ha $\mathrm{Dom}(f) = \emptyset$, akkor az üres függvény balinverze f-nek. ■

6.4.11. Állítás. *Minden $f : E \to F$ függvényre a következő állítások ekvivalensek:*

a) *f bijekció az E és F halmazok között.*

b) *Létezik olyan $g : F \to E$ függvény, hogy $f \circ g = \mathrm{id}_F$ és $g \circ f = \mathrm{id}_E$ (vagyis létezik olyan függvény, amely az f-nek egyszerre jobbinverze és balinverze).*

c) *Léteznek olyan $g, h : E \to F$ függvények, hogy $f \circ g = \mathrm{id}_F$ és $h \circ f = \mathrm{id}_E$ (vagyis f-nek létezik jobbinverze és létezik balinverze).*

Bizonyítás. *a)* $\Rightarrow$ *b)* Ha f bijekció E és F között, akkor f injekció, tehát van olyan $g : F \to E$ függvény, amely balinverze f-nek, vagyis $g \circ f = \mathrm{id}_E$. Ekkor f a g-nek jobbinverze, tehát $\mathrm{Im}(g) = E$. Megmutatjuk, hogy g injekció. Valóban, ha $y, y' \in F$ és $g(y) = g(y')$, akkor léteznek olyan $x, x' \in E$, hogy $y = f(x)$ és $y' = f(x')$, mivel f ráképez F-re. Ekkor $x = g(f(x)) = g(y) = g(y') = g(f(x')) = x'$, tehát g injekció. Ez azt jelenti, hogy g bijekció F és E között, így $g^{-1} = g^{-1} \circ \mathrm{id}_E = g^{-1} \circ (g \circ f) = (g^{-1} \circ g) \circ f = \mathrm{id}_F \circ f = f$, amiből nyilvánvalóan következik, hogy g jobbinverze is f-nek, mert $f \circ g = f \circ (g^{-1})^{-1} = f \circ f^{-1} = \mathrm{id}_F$.

b) $\Rightarrow$ *c)* Triviális.

c) $\Rightarrow$ *a)* Ha a c) állítás feltétele teljesül, akkor az előző állítás szerint f injekció, mert van balinverze, és ráképez F-re, mert létezik jobbinverze. ∎

6.4.12. Tétel. *Legyenek E, F és G halmazok, valamint $f : E \to F$ és $g : E \to G$ függvények. Akkor és csak akkor létezik olyan $h : F \to G$ függvény, hogy $h \circ f = g$, vagyis az*

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[dr, "g"'] & F \arrow[d, "h"] \\ & G \end{tikzcd}$$

diagram kommutatív, ha minden $(x, x') \in E \times E$ párra teljesül az, hogy $f(x) = f(x')$ esetén $g(x) = g(x')$. Bármely $h : F \to G$ függvény a $h \circ f = g$ feltétellel az $\mathrm{Im}(f)$ halmazon egyértelműen van meghatározva.

Bizonyítás. A feltétel nyilvánvalóan szükséges, mert ha $h : F \to G$ olyan függvény, hogy $h \circ f = g$, akkor minden $(x, x') \in E \times E$ párra, $f(x) = f(x')$ esetén $g(x) = h(f(x)) = h(f(x')) = f(x')$.

Az elégségesség bizonyításához tekintsük a

$$h_* := \{\ (f(x), g(x)) \mid x \in E\ \}$$

halmazt, amely jól értelmezett mert a definíció szerint $h_* := \{u | (\exists x)((x \in E) \wedge (u = (f(x), g(x)))\}$, és a $(\exists x)((x \in E) \wedge (u = (f(x), g(x)))$ kijelentés kollektivizáló az u változóban, hiszen ebből a kijelentésből következik, hogy $u \in F \times G$, így elég a részhalmaz axiómára hivatkozni. Világos, hogy h_* olyan reláció, amelyre $h_* \subseteq F \times G$. Ha $(z, y) \in h_*$ és $(z, y') \in h_*$, akkor h_* definíciója szerint vehetünk olyan $x, x' \in E$ elemeket, amelyekre $(z, y) = (f(x), g(x))$ és $(z, y') = (f(x'), g(x'))$, tehát $f(x) = z = f(x')$, valamint $y = g(x)$ és $y' = g(x')$. Ekkor a hipotézis szerint $g(x) = g(x')$, tehát $y = y'$. Ez azt jelenti, hogy a h_* reláció függvény, továbbá nyilvánvaló, hogy $\mathrm{Dom}(h_*) \subseteq \mathrm{Im}(f) \subseteq F$ és $\mathrm{Im}(h_*) \subseteq G$. Ha $x \in E$, akkor $(f(x), g(x)) \in h_*$, tehát $f(x) \in \mathrm{Dom}(h_*)$ és $h_*(f(x)) = g(x)$, amiből következik, hogy $\mathrm{Im}(f) \subseteq \mathrm{Dom}(h_*)$ és $h_* \circ f = g$. Tehát ha $\mathrm{Dom}(h_*) = F$, akkor $h := h_* : F \to G$ olyan függvény, amelyre $h \circ f = g$. Ha $\mathrm{Dom}(h_*) \neq F$, vagyis $\mathrm{Dom}(h_*)$ valódi részhalmaza F-nek, akkor vegyük h_*-nak tetszőleges $h : F \to G$ függvény-kiterjesztését (6.2.9.). Világos, hogy $h \circ f = g$ ekkor is teljesül, hiszen minden $x \in E$ esetén $f(x) \in \mathrm{Dom}(h_*)$, tehát $h_* \subseteq h$ miatt $h(f(x)) = h_*(f(x)) = g(x)$.

Ha $h : F \to G$ tetszőleges olyan függvény, amelyre $h \circ f = g$, akkor $h_* \circ f = g = h \circ f$, ezért $\mathrm{Im}(f) \subseteq \{y \in F | h_*(y) = h(y)\}$, vagyis $h|_{\mathrm{Im}(f)} = h_*$. Ez azt jelenti, hogy a $h : F \to G$ függvény a $h \circ f = g$ a feltétellel az $\mathrm{Im}(f)$ halmazon egyértelműen van meghatározva. ∎

6.5. Halmazok számosságának összehasonlítása

Halmazok *méretének* összehasonlítása céljából vezetjük be a következő fogalmakat.

6.5.1. Definíció. *Legyenek E és F halmazok.*

– *Az E és F halmazok* **ekvipotensek**, *ha létezik bijekció E és F között.*

– *Az E halmaz* **kisebb-egyenlő számosságú** *F-nél, ha létezik F-nek olyan részhalmaza, amely ekvipotens E-vel.*

– *Az E halmaz* **kisebb számosságú** *F-nél, ha E kisebb-egyenlő számosságú F-nél és E nem ekvipotens F-fel.*

– *Az E és F halmazok* **számosság tekintetében összehasonlíthatóak**, *ha E kisebb-egyenlő számosságú F-nél, vagy F kisebb-egyenlő számosságú E-nél.*

6.5.2. Állítás. (**Halmazok ekvipotenciájának tulajdonságai**.)

a) *Minden halmaz ekvipotens önmagával.* (*Halmazok ekvipotenciája* **reflexív**.)

b) *Ha E és F halmazok ekvipotensek, akkor az F és E halmazok is ekvipotensek.* (*Halmazok ekvipotenciája* **szimmetrikus**.)

c) *Ha az E és F halmazok ekvipotensek, és az F és G halmazok ekvipotensek, akkor az E és G halmazok ekvipotensek.* (*Halmazok ekvipotenciája* **tranzitív**.)

Bizonyítás. a) Ha E halmaz, akkor az id_E függvény bijekció E és E között.

b) Ha E és F halmazok, és $f : E \to F$ bijekció, akkor $f^{-1} : F \to E$ bijekció.

c) Ha E, F és G halmazok, valamint $f : E \to F$ bijekció és $g : F \to G$ bijekció, akkor $g \circ f : E \to G$ bijekció. ■

Az ekvipotencia reflexivitásából nyilvánvalóan következik, hogy ha F halmaz és $E \subseteq F$, akkor E kisebb-egyenlő számosságú F-nél.

6.5.3. Állítás. *Az E halmaz pontosan akkor kisebb-egyenlő számosságú az F halmaznál, ha létezik $E \to F$ injekció.*

Bizonyítás. Tegyük fel, hogy az E halmaz kisebb-egyenlő számosságú az F halmaznál. Legyen $F' \subseteq F$ olyan halmaz, hogy E és F' ekvipotensek, és vegyünk egy $f : E \to F'$ bijekciót. Ekkor az $f : E \to F$ függvény injekció.

Megfordítva, legyen $f : E \to F$ injekció. Ekkor $\mathrm{Im}(f) \subseteq F$ és f bijekció az E és $\mathrm{Im}(f)$ halmazok között, vagyis E ekvipotens $\mathrm{Im}(f)$-fel. Ezért E kisebb-egyenlő számosságú F-nél. ■

6.5.4. Tétel. (Cantor-tétel) *Ha E halmaz, akkor nem létezik olyan E-n értelmezett függvény, amely ráképez $\mathscr{P}(E)$-re. Minden halmaz kisebb számosságú a saját hatványhalmazánál.*

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük olyan E halmaz létezését, amelyhez létezik $f : E \to \mathscr{P}(E)$ szürjekció. Értelmezzük az

$$F := \{x | (x \in E) \wedge (x \notin f(x))\}$$

halmazt. Ekkor $F \in \mathscr{P}(E)$, tehát van olyan $x \in E$, hogy $F = f(x)$, mivel f ráképez $\mathscr{P}(E)$-re. Ha $x \in F$ igaz volna, akkor az F definíciója szerint $x \notin f(x)$, ami lehetetlen.

Ebből következik, hogy $x \notin F$. Ez viszont az F értelmezése alapján azt jelenti, hogy $x \in f(x)$, vagyis $x \in F$, ami ellentmondás.

Ha E halmaz, akkor nyilvánvaló, hogy az

$$E \to \mathscr{P}(E); \quad x \mapsto \{x\}$$

függvény injekció, ezért E kisebb-egyenlő számosságú a $\mathscr{P}(E)$ halmaznál, és az előzőek szerint nem ekvipotensek, tehát E kisebb számosságú a $\mathscr{P}(E)$ hatványhalmaznál. ■

A Cantor-tételből (is) látszik, hogy nem létezik az összes halmazok halmaza, hiszen ha $\mathbf{U}$ az összes halmazok halmaza volna, akkor $\mathscr{P}(\mathbf{U}) \subseteq \mathbf{U}$ teljesülne, így $\mathscr{P}(\mathbf{U})$ kisebb-egyenlő számosságú volna $\mathbf{U}$-nál.

Megjegyezzük, hogy a *halmazok számosságának* fogalmát nem vezettük be. A *számosságoperáció* pontos definíciója megtalálható az I. fejezet 3. pontjának **40**. gyakorlatában.

Az eddigi axiomatikából nem következik, hogy bármely két halmaz összehasonlítható volna számosság tekintetében (feltéve, hogy az elmélet ellentmondásmentes). Azonban bebizonyítható, hogy ha két halmaz mindegyike kisebb-egyenlő számosságú a másiknál, akkor ekvipotensek egymással. Erről szól a következő tétel.

6.5.5. Tétel. (Schröder–Bernstein-tétel) *Ha az E halmaz kisebb-egyenlő számosságú az F halmaznál és az F halmaz kisebb-egyenlő számosságú az E halmaznál, akkor E és F ekvipotensek.*

Bizonyítás. Legyenek $f : E \to F$ és $g : F \to E$ injekciók.

Először azt mutatjuk meg, hogy ha $H \subseteq E$ olyan halmaz, hogy $g\langle F \setminus f\langle H\rangle\rangle = E \setminus H$, és $h : E \to F$ az a függvény, amelyre $x \in E$ esetén

$$h(x) := \begin{cases} f(x) & \text{, ha } x \in H \\ g^{-1}(x) & \text{, ha } x \in E \setminus H, \end{cases}$$

akkor h bijekció E és F között.

A h függvény *injektív*. Legyenek ugyanis $x, x' \in E$ és tegyük fel, hogy $h(x) = h(x')$. Ekkor lehetetlen az, hogy $x \in H$ és $x' \in E \setminus H$, különben $h(x) = f(x) \in f\langle H\rangle$ és $h(x') = g^{-1}(x') \in F \setminus f\langle H\rangle$, vagyis $h(x) \neq h(x')$. Az is lehetetlen, hogy $x \in E \setminus H$ és $x' \in H$ teljesüljön, különben $h(x) = g^{-1}(x) \in F \setminus f\langle H\rangle$ és $h(x') = f(x') \in f\langle H\rangle$, vagyis $h(x) \neq h(x')$. Ezért vagy $x, x' \in H$, vagy $x, x' \in E \setminus H$ teljesül. Az első esetben $f(x) = f(x')$, tehát f injektivitása miatt $x = x'$. A második esetben $g^{-1}(x) = g^{-1}(x')$, tehát g^{-1} injektivitása miatt $x = x'$.

A h függvény ráképez F-re. Legyen ugyanis $y \in F$ tetszőleges. Ha $y \in F \setminus f\langle H\rangle$, akkor $g(y) \in E \setminus H$, így $h(g(y)) = g^{-1}(g(y)) = y$. Ha $y \in f\langle H\rangle$, akkor létezik olyan $x \in H$, hogy $y = f(x)$, tehát $h(x) = f(x) = y$.

Tehát elegendő olyan $H \subseteq E$ halmazt előállítani, amelyre $g\langle F \setminus f\langle H\rangle\rangle = E \setminus H$. Ehhez legyen $\mathscr{H} := \{X | (X \subseteq E) \wedge (g\langle F \setminus f\langle X\rangle\rangle \subseteq E \setminus X)\}$, és $H := \bigcup \mathscr{H}$. Megmutatjuk, hogy H olyan halmaz, amely rendelkezik a megkövetelt tulajdonsággal. Valóban, ha $X \in \mathscr{H}$, akkor $X \subseteq H$, tehát $g\langle F \setminus f\langle H\rangle\rangle \subseteq g\langle F \setminus f\langle X\rangle\rangle \subseteq E \setminus X$, így $X \subseteq E \setminus g\langle F \setminus f\langle H\rangle\rangle$. Ebből következik, hogy $H \subseteq E \setminus g\langle F \setminus f\langle H\rangle\rangle$. Legyen most $X := E \setminus g\langle F \setminus f\langle H\rangle\rangle$. Az imént láttuk, hogy $H \subseteq X$, ezért $g\langle F \setminus f\langle X\rangle\rangle \subseteq g\langle F \setminus f\langle H\rangle\rangle = E \setminus X$, vagyis $X \in \mathscr{H}$, így $X \subseteq H$, azaz $X = H$. Ebből azonnal következik, hogy $E \setminus g\langle F \setminus f\langle H\rangle\rangle = H$, azaz $g\langle F \setminus f\langle H\rangle\rangle = E \setminus H$. ■

A Schröder–Bernstein-tételnek különösen fontos jelentősége van halmazok ekvipotenciájának eldöntésében.

6.5.6. Definíció. *Vezessük be a* $0 := \emptyset$ *és* $1 := \{\emptyset\}$ *jelöléseket. Ha* E *halmaz, akkor minden* $H \subseteq E$ *halmazra* $\chi_{H,E}$ *jelöli a következő függvényt:*

$$\chi_{H,E} : E \to \{0,1\}; \quad x \mapsto \chi_{H,E}(x) := \begin{cases} 1 & , \text{ha } x \in H; \\ 0 & , \text{ha } x \in E \setminus H. \end{cases}$$

Ha $H \subseteq E$*, akkor a* $\chi_{H,E} \in \mathscr{F}(E;\{0,1\})$ *függvényt a* H *halmaz (*E*-re vonatkozó)* **karakterisztikus függvényének** *nevezzük. Ha világos, hogy a* H *melyik (rögzített)* E *halmaz részhalmaza, akkor a* $\chi_{H,E}$ *szimbólum helyett az egyszerűbb* χ_H *jelet használjuk.*

Nyilvánvaló, hogy minden E halmazra a $\mathscr{P}(E) \to \mathscr{F}(E;\{0,1\})$; $H \mapsto \chi_H$ leképezés *bijekció*, tehát az E halmaz hatványhalmaza és az $\mathscr{F}(E;\{0,1\})$ függvényhalmaz között nagyon szoros kapcsolat van (ti. kitüntetett módon azonosíthatóak).

6.5.7. Állítás. *Legyenek* E*,* F*,* G *halmazok és minden* $f : E \times F \to G$ *függvényre, valamint* $x \in E$ *pontra legyen* $f(x,\cdot) : F \to G$ *az a függvény, amely minden* $y \in F$ *ponthoz az* $f(x,y)$ *értéket rendeli, vagyis* $f(x,\cdot)(y) := f(x,y)$*. Ekkor az*

$$\mathscr{F}(E \times F; G) \to \mathscr{F}(E;\mathscr{F}(F;G)) \quad ; \quad f \mapsto (x \mapsto f(x,\cdot))$$

függvény bijekció. (Ezt nevezzük az $\mathscr{F}(E \times F;G)$ *és* $\mathscr{F}(E;\mathscr{F}(F;G))$ *függvényhalmazok közötti* **kanonikus bijekciónak***.)*

Bizonyítás. Jelölje Φ a vizsgálandó függvényt.

Legyenek $f, f' \in \mathscr{F}(E\times F;G)$ olyanok, hogy $f \neq f'$. Ekkor vehetünk olyan $(x,y) \in E\times F$ párt, amelyre $f(x,y) \neq f'(x,y)$. Ebből következik, hogy $(\Phi(f))(x) = f(x,\cdot) \neq f'(x,\cdot) = (\Phi(f'))(x)$, hiszen az y pontban ezek a függvények különböző értéket vesznek fel. Tehát $\Phi(f) \neq \Phi(f')$, hiszen az x pontban ezek a függvények különböző értéket vesznek fel. Ez azt jelenti, hogy a Φ függvény injektív.

Legyen $h \in \mathscr{F}(E;\mathscr{F}(F;G))$, és értelmezzük az

$$f : E \times F \to G; \quad (x,y) \mapsto (h(x))(y)$$

függvényt. Ekkor minden $x \in E$ esetén $f(x,\cdot) = h(x)$, vagyis $\Phi(f) = h$. Ezért a Φ függvény szürjektív. ■

6.5.8. Definíció. *Azt mondjuk, hogy az* E *halmaz* **legalább két elemű***, ha* E *nagyobb-egyenlő számosságú a* $\{0,1\}$ *halmaznál, ahol* $0 := \emptyset$ *és* $1 := \{\emptyset\}$*.*

Könnyen látható, hogy az E halmaz pontosan akkor legalább két elemű, ha léteznek olyan $a \in E$ és $b \in E$ elemek, hogy $a \neq b$. Valóban, ha a és b ilyen elemek, akkor az

$$\{0,1\} \to E; \quad x \mapsto \begin{cases} a, & \text{ha } x = 0 \\ b, & \text{ha } x = 1 \end{cases}$$

leképezés injekció, tehát az E halmaz legalább két elemű. Megfordítva, ha az E halmaz legalább két elemű, akkor létezik $f : \{0,1\} \to E$ injekció, és ekkor $a := f(0)$ és $b := f(1)$ olyanok, hogy $a \in E$, $b \in E$ és $a \neq b$.

6.5.9. Állítás. *Legyenek E, E', F és F' olyan halmazok, hogy E kisebb-egyenlő számosságú F-nél és E' kisebb-egyenlő számosságú F'-nél.*

a) *Ha $F \cap F' = \emptyset$, akkor $E \cup E'$ kisebb-egyenlő számosságú az $F \cup F'$ halmaznál.*

b) *Az $E \times E'$ halmaz kisebb-egyenlő számosságú az $F \times F'$ halmaznál.*

c) *Ha F és F' mindketten legalább két elemű halmazok, akkor $E \cup E'$ kisebb-egyenlő számosságú az $F \times F'$ halmaznál.*

Bizonyítás. a) Ha $f : E \to F$ és $f' : E' \to F'$ injekciók, akkor nyilvánvaló, hogy az $f \cup (f'|_{E' \setminus E}) : E \cup E' \to F \cup F'$ függvény injekció, tehát az $E \cup E'$ halmaz kisebb-egyenlő számosságú az $F \cup F'$ halmaznál.

b) Ha $f : E \to F$ és $f' : E' \to F'$ intekciók, akkor nyilvánvaló, hogy az

$$E \times E' \to F \times F'; \quad (x, x') \mapsto (f(x), f'(x'))$$

leképezés injekció, tehát az $E \times E'$ halmaz kisebb-egyenlő számosságú az $F \times F'$ halmaznál.

c) Először megmutatjuk, hogy ha F és F' mindketten legalább két elemű *diszjunkt* halmazok, akkor $F \cup F'$ kisebb-egyenlő számosságú az $F \times F'$ halmaznál.

Ehhez legyenek $a, b \in F$, illetve $a', b' \in F'$ olyanok, hogy $a \neq b$ és $a' \neq b'$, és értelmezzük azt a $g : F \cup F' \to F \times F'$ függvényt, amelyre $y \in F$ esetén

$$g(y) = \begin{cases} (y, a'), & \text{ha } y \neq a \\ (a, b'), & \text{ha } y = a, \end{cases}$$

továbbá $y' \in F'$ esetén

$$g(y') = \begin{cases} (a, y'), & \text{ha } y' \neq b' \\ (b, b'), & \text{ha } y' = b'. \end{cases}$$

Nyilvánvaló, hogy g az F és az F' halmazon injektív, továbbá

$$g\langle F\rangle = ((F \setminus \{a\}) \times \{a'\}) \cup \{(a, b')\},$$
$$g\langle F'\rangle = (\{a\} \cup (F' \setminus \{b'\})) \cup \{(b, b')\},$$

amiből látható, hogy $g\langle F\rangle \cap g\langle F'\rangle = \emptyset$, tehát $g : F \cup F' \to F \times F'$ injekció.

Most könnyen belátható, hogy ha E kisebb-egyenlő számosságú F-nél, és E' kisebb-egyenlő számosságú F'-nél, valamint az F és F' halmazok legalább két elemű *diszjunkt* halmazok, akkor $E \cup E'$ kisebb-egyenlő számosságú az $F \times F'$ halmaznál. Valóban, az a) állítás szerint $E \cup E'$ kisebb-egyenlő számosságú az $F \cup F'$ halmaznál, amely az előző bekezdés alapján kisebb-egyenlő számosságú az $F \times F'$ halmaznál.

Végül, áttérve az általános esetre: $\{0\} \times F$ ekvipotens F-fel, tehát E kisebb-egyenlő számosságú a $\{0\} \times F$ halmaznál, továbbá $\{1\} \times F'$ ekvipotens F'-vel, tehát E' kisebb-egyenlő számosságú a $\{1\} \times F'$ halmaznál. Világos, hogy $(\{0\} \times F) \cap (\{1\} \times F') = \emptyset$, ezért az előző bekezdés alapján $E \cup E'$ kisebb-egyenlő számosságú a $(\{0\} \times F) \times (\{1\} \times F')$ halmaznál. Ez utóbbi halmaz a b) állítás alapján kisebb-egyenlő számosságú az $F \times F'$ halmaznál (sőt azzal ekvipotens). Ezért $E \cup E'$ kisebb-egyenlő számosságú az $F \times F'$ halmaznál. ■

6.6. Műveletek

6.6.1. Definíció. *Az E halmaz feletti (belső, kétváltozós)* **műveletnek** *nevezünk minden $E \times E \to E$ típusú függvényt.*

A műveletek adott helyen felvett értékének jelölésére háromféle konvenciót alkalmaznak. Ha E halmaz és $\top : E \times E \to E$ művelet, akkor $(x, y) \in E \times E$ esetén a $\top((x, y)) \in E$ értéket a következőképpen jelölhetjük:

– *prefix* jelöléssel $\top\, x\, y$,

– *infix* jelöléssel $x \top y$,

– *postfix* jelöléssel $x\, y \top$.

Mi a továbbiakban az infix jelölési konvenciót alkalmazzuk.

6.6.2. Definíció. *Legyen E halmaz és $\top : E \times E \to E$ művelet.*

– *A $\top$ műveletet* **asszociatívnak** *nevezzük, ha minden $x, y, z \in E$ elemre*

$$x \top (y \top z) = (x \top y) \top z.$$

– *A $\top$ műveletet* **kommutatívnak** *nevezzük, ha minden $x, y \in E$ elemre*

$$x \top y = y \top x.$$

– *A $\top$ műveletetet* **neutrális-elemesnek** *nevezzük, ha létezik olyan $e \in E$, hogy minden $x \in E$ elemre*

$$x \top e = e \top x = x.$$

Minden ilyen tulajdonságú $e \in E$ elemet a $\top$ művelet **neutrális elemének** *nevezünk. (Megjegyezzük, hogy legfeljebb egy neutrális elem létezhet, mert ha $e, e' \in E$ neutrális elemek, akkor $e = e \top e' = e'$.)*

– *Ha $\top$ neutrális-elemes és $e \in E$ a $\top$ neutrális eleme, akkor az $x \in E$ elem* **inverzének** *nevezünk minden olyan $x' \in E$ elemet, amelyre*

$$x \top x' = x' \top x = e.$$

(Megjegyezzük, hogy ha $\top$ asszociatív és neutrális-elemes művelet, akkor minden $x \in E$ elemnek legfeljebb egy inverze létezik, mert ha $x', x'' \in E$ inverzei x-nek, akkor $x' = e \top x' = (x'' \top x) \top x' = x'' \top (x \top x') = x'' \top e = x''$.)

– *A neutrális-elemes $\top$ műveletet* **inverzelemesnek** *nevezzük, ha az E minden elemének létezik inverze.*

– *A $\top$ műveletetet* **zérus-elemesnek** *nevezzük, ha létezik olyan $z \in E$, hogy minden $x \in E$ elemre*

$$x \top z = z \top x = z.$$

Minden ilyen tulajdonságú $z \in E$ elemet a $\top$ művelet **zéruselemének** *nevezünk. (Megjegyezzük, hogy legfeljebb egy zéruselem létezhet, mert ha $z, z' \in E$ zéruselemek, akkor $z = z \top z' = z'$.)*

6.6.3. Definíció. *Legyenek $\top$ és $\perp$ műveletek az E halmaz felett. Azt mondjuk, hogy a $\top$ művelet* **disztributív** *a $\perp$ műveletre nézve, ha minden $x, y, z \in E$ esetén*

$$x \top (y \perp z) = (x \top y) \perp (x \top z)$$
$$(y \perp z) \top x = (y \top x) \perp (z \top x).$$

6.6.4. Definíció. *Legyenek $\top$ és $\perp$ műveletek az E halmaz felett. Azt mondjuk, hogy a $\top$ művelet* **abszorptív**, *vagy* **elnyelő** *a $\perp$ műveletre nézve, ha minden $x, y \in E$ esetén*

$$\begin{aligned} x \top (x \perp y) &= x, \\ (y \perp x) \top x &= x. \end{aligned}$$

6.6.5. Definíció. *Egy halmaz feletti műveletet* **csoportműveletnek** *nevezünk, ha asszociatív, neutrális-elemes és inverzelemes. A $(G, \top)$ párt* **csoportnak** *nevezzük, ha $\top$ csoportművelet a G halmaz felett.*

6.6.6. Definíció. *Ha $\top$ művelet az E halmaz felett, akkor minden $X, Y \subseteq E$ halmazra*

$$X \top Y := \{\ x \top y \mid (x \in X) \wedge (y \in Y)\ \},$$

továbbá, a

$$\mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E); \quad (X, Y) \mapsto X \top Y$$

$\mathscr{P}(E)$ feletti műveletet a $\top$ művelet által meghatározott **komplexusműveletnek** *nevezzük.*

6.7. Halmazrendszerek

6.7.1. Definíció. *Azt mondjuk, hogy $(E_i)_{i \in I}$* **halmazrendszer**, *ha ez olyan függvény, amely az I halmazon értelmezett és minden $i \in I$ elemhez az E_i értéket rendeli. Ekkor az I halmazt (tehát a függvény definíciós tartományát) a halmazrendszer* **indexhalmazának** *és az I elemeit* **indexeknek** *nevezzük. Azt mondjuk, hogy az $(E_i)_{i \in I}$ halmazrendszer* **diszjunkt**, *ha minden $i, j \in I$ indexre, $i \neq j$ esetén $E_i \cap E_j = \emptyset$ teljesül.*

6.7.2. Állítás. *Legyen $(E_i)_{i \in I}$ halmazrendszer.*

a) *A $(\exists i)((i \in I) \wedge (x \in E_i))$ kijelentés kollektivizáló az x változóban.*

b) *Ha $I \neq \emptyset$, akkor a $(\forall i)((i \in I) \Rightarrow (x \in E_i))$ kijelentés kollektivizáló az x változóban.*

c) *Az "$(f$ függvény$) \wedge (\mathrm{Dom}(f) = I) \wedge ((\forall i)((i \in I) \Rightarrow (f(i) \in E_i)))$" kijelentés kollektivizáló az f változóban.*

Bizonyítás. Jelölje F az $(E_i)_{i \in I}$ halmazrendszert.

a) Ha $(\exists i)((i \in I) \wedge (x \in E_i))$ teljesül, akkor van olyan $i \in I$, hogy $x \in E_i = F(i) \in \mathrm{Im}(F)$, tehát $x \in \bigcup \mathrm{Im}(F)$, így a részhalmaz axióma alapján a) teljesül.

b) Legyen $i_* \in I$ rögzített index. Ha $(\forall i)((i \in I) \Rightarrow (x \in E_i))$ teljesül, akkor $x \in E_{i_*}$, ezért a részhalmaz axióma alapján b) teljesül.

c) Az a) szerint képezhető a $H := \{x \mid (\exists i)((i \in I) \wedge (x \in E_i))\}$ halmaz. Ha "$(f$ *függvény*$) \wedge (\mathrm{Dom}(f) = I) \wedge ((\forall i)((i \in I) \Rightarrow (f(i) \in E_i)))$" teljesül, akkor $f \subseteq I \times H$, tehát $f \in \mathscr{P}(I \times H)$, ezért a részhalmaz axióma alapján c) teljesül. ■

6.7.3. Definíció. *Legyen $(E_i)_{i \in I}$ halmazrendszer.*

– $\bigcup\limits_{i \in I} E_i := \{x \mid (\exists i)((i \in I) \wedge (x \in E_i))\}$ *és ezt a halmazt az $(E_i)_{i \in I}$* **halmazrendszer uniójának** *nevezzük.*

– *Ha $I \neq \emptyset$, akkor $\bigcap\limits_{i \in I} E_i := \{x \mid (\forall i)((i \in I) \Rightarrow (x \in E_i))\}$ és ezt a halmazt az $(E_i)_{i \in I}$*

halmazrendszer metszetének *nevezzük.*

– $\prod\limits_{i\in I} E_i := \{f|(f \text{ függvény}) \wedge (\mathrm{Dom}(f) = I) \wedge ((\forall i)((i \in I) \Rightarrow (f(i) \in E_i)))\}$ *és ezt a halmazt az* $(E_i)_{i\in I}$ **halmazrendszer szorzatának** *nevezzük.*

Vigyázzunk arra, hogy halmazrendszer metszetének értelmezhetőségéhez szükséges az, hogy az indexhalmaz ne legyen üres! Ugyanis az $(E_i)_{i\in\emptyset}$ *üres halmazrendszerre* a $(\forall i)((i \in \emptyset) \Rightarrow (x \in E_i))$ kijelentés *tétel* minden x változóra (ex falso sequitur quodlibet 2.4.8.), tehát ha ez a kijelentés kollektivizáló volna az x változóban, akkor az $\{x|(\forall i)((i \in I) \Rightarrow (x \in E_i))\}$ halmaz egyenlő volna az összes halmazok halmazával, amely nem létezik.

Ugyanakkor az $(E_i)_{i\in\emptyset}$ üres halmazrendszer uniója és szorzata jól értelmezett, és könnyen látható, hogy $\bigcup\limits_{i\in\emptyset} E_i = \emptyset$, valamint $\prod\limits_{i\in\emptyset} E_i = \{\emptyset\}$ teljesül.

6.7.4. Állítás. *Legyen* $(E_i)_{i\in I}$ *halmazrendszer. Ekkor jól értelmezett az* $(\{i\} \times E_i)_{i\in I}$ *diszjunkt halmazrendszer, és jól értelmezettek az*

$$\iota : \bigcup_{i\in I}(\{i\} \times E_i) \to I; \quad (i, x) \mapsto i,$$

$$f : \bigcup_{i\in I}(\{i\} \times E_i) \to \bigcup_{i\in I} E_i; \quad (i, x) \mapsto x$$

függvények. A ι *függvényre* $\mathrm{Im}(\iota) = \{i \in I|E_i \neq \emptyset\}$ *teljesül. Az* f *függvény szürjekció és pontosan akkor injektív, ha az* $(E_i)_{i\in I}$ *halmazrendszer diszjunkt.*

Bizonyítás. Legyen $E := (E_i)_{i\in I}$, vagyis E az a függvény, amelyre $\mathrm{Dom}(E) = I$ és minden $i \in I$ esetén $E(i) = E_i$. Ha $i \in I$, akkor $\{i\} \times E_i \in \mathscr{P}(I) \times \mathrm{Im}(E)$. Ez azt jelenti, hogy ha $\mathscr{A}(z)$ jelöli a $(\exists i)\,((i \in I) \wedge (z = (i, \{i\} \times E_i)))$ kijelentést, akkor $z \in I \times (\mathscr{P}(I) \times \mathrm{Im}(E))$, így a részhalmaz axióma szerint a $(\exists i)\,((i \in I) \wedge (z = (i, \{i\} \times E_i)))$ kijelentés kollektivizáló a z változóban, így képezhető az $F := \{z|\mathscr{A}(z)\}$ halmaz.

Ha $z \in F$, akkor vehetünk olyan $i_* \in I$ indexet, hogy $z = (i_*, \{i_*\} \times E_{i_*})$, tehát z pár, vagyis az f halmaz reláció. Ha $(x, y') \in F$ és $(x, y'') \in F$, akkor F definíciója szerint vehetünk olyan $i' \in I$ és $i'' \in I$ indexeket, hogy $(x, y') = (i', \{i'\} \times E_{i'})$ és $(x, y'') = (i'', \{i''\} \times E_{i''})$, tehát $i' = x = i''$ és $y' = \{i'\} \times E_{i'}$ és $y'' = \{i''\} \times E_{i''}$. Ekkor $i' = i''$ miatt $\{i''\} = \{i'\}$ és $E_{i''} = E_{i'}$, így $y'' = \{i''\} \times E_{i''} = \{i'\} \times E_{i'} = y'$. Ez azt jelenti, hogy F függvény.

Ha $x \in \mathrm{Dom}(F)$, vagyis $(\exists y)((x, y) \in F)$ tétel, akkor rögzíthetünk olyan y_* halmazt, hogy $(x, y_*) \in F$, tehát F definíciója szerint vehetünk olyan $i_* \in I$ indexet, hogy $(x, y_*) = (i_*, \{i_*\} \times E_{i_*})$, így $x = i_* \in I$, ami azt jelenti, hogy $\mathrm{Dom}(F) \subseteq I$. Megfordítva, ha $i \in I$, akkor $y_* := \{i\} \times E_i$ olyan halmaz, hogy $(i, y_*) \in F$, tehát $(\exists y)((i, y) \in F)$ tétel, ami azt jelenti, hogy $i \in \mathrm{Dom}(F)$, ezért $I \subseteq \mathrm{Dom}(F)$. Ezzel beláttuk, hogy $\mathrm{Dom}(F) = I$.

Ha $i \in I$, akkor $(i, F(i)) \in F$, tehát vehetünk olyan $i_* \in I$ indexet, hogy $(i.F(i)) = (i_*, \{i_*\} \times E_{i_*})$, tehát $i_* = i$ és $F(i) = \{i_*\} \times E_{i_*} = \{i\} \times E_i$. Ez azt jelenti, hogy az F függvény definíciós tartománya I és minden $i \in I$ esetén $F(i) = \{i\} \times E_i$, vagyis F azonos az $(\{i\} \times E_i)_{i\in I}$ halmazrendszerrel.

Az $(\{i\} \times E_i)_{i\in I}$ halmazrendszer diszjunkt, mert $i', i'' \in I$ és $i' \neq i''$ esetén $\{i'\} \neq \{i''\}$, következésképpen $(\{i'\} \times E_{i'}) \cap (\{i''\} \times E_{i''}) = \emptyset$, hiszen ha z eleme volna a metszetnek, akkor léteznének olyan $y' \in E_{i'}$ és $y'' \in E_{i''}$ elemek, hogy $(i', y') = z = (i'', y'')$, ezért $i' = i''$ teljesülne, holott $i' \neq i''$.

Vezessük be a $D := \bigcup_{i \in I}(\{i\} \times E_i)$ és $E := \bigcup_{i \in I} E_i$ halmazokat.

A $\iota := \{(z, i) \in D \times I | z \in \{i\} \times E_i\}$ reláció függvény, mert $(z, i'), (z, i'') \in \iota$ esetén $z \in (\{i'\} \times E_{i'}) \cap (\{i''\} \times E_{i''})$, tehát az $(\{i\} \times E_i)_{i \in I}$ halmazrendszer diszjunktsága folytán $i' = i''$. Továbbá nyilvánvaló, hogy $\{z \in D | (\exists i \in I)(z, i) \in \iota\} = D$, tehát $\mathrm{Dom}(\iota) = D$, és $z \in D$ esetén $\iota(z) \in I$ az az index, amelyre $z \in \{i\} \times E_i$, vagyis minden $(i, x) \in D$ esetén $\iota(x, i) = i$. Ha $i \in \mathrm{Im}(\iota)$, akkor van olyan $x \in E_i$, hogy $\iota(x, i) = i$, tehát $E_i \neq \emptyset$. Megfordítva, ha $i \in I$ olyan, hogy $E_i \neq \emptyset$, és $x \in E_i$, akkor $i = \iota(x, i) \in \mathrm{Im}(\iota)$. Ez azt jelenti, hogy $\mathrm{Im}(\iota) = \{i \in I | E_i \neq \emptyset\}$.

Az $f := \{(z, x) \in D \times E | (\exists i)((i \in I) \wedge (x \in E_i) \wedge (z = (i, x))\}$ reláció függvény, mert $(z, x'), (z, x'') \in f$ esetén vehetünk olyan $i', i'' \in I$ indexeket, hogy $x' \in E_{i'}$ és $x'' \in E_{i''}$ és $(i', x') = z = (i'', x'')$, tehát $x' = x''$. Világos, hogy $\mathrm{Dom}(f) \subseteq D$, és ha $z \in D$, akkor D definíciója szerint van olyan $i \in I$, hogy $z \in \{i\} \times E_i$, tehát van olyan $x \in E_i$, hogy $z = (i, x)$, vagyis $z \in \mathrm{Dom}(f)$. Ezért $\mathrm{Dom}(f) = D$, továbbá $x \in E$ esetén E definíciója szerint van olyan $i \in I$, hogy $x \in E_i$, tehát $(i, x) \in D$ és $x = f(i, x) \in \mathrm{Im}(f)$, vagyis $f : D \to E$ szürjekció.

Ha f injekció, és $i', i'' \in I$ olyan indexek, hogy $E_{i'} \cap E_{i''} \neq \emptyset$, akkor vehetünk egy $x \in E_{i'} \cap E_{i''}$ elemet, és ekkor $f(i', x) = x = f(i'', x)$, tehát $i' = i''$, ami azt jelenti, hogy az $(E_i)_{i \in I}$ halmazrendszer diszjunkt. Megfordítva, ha az $(E_i)_{i \in I}$ halmazrendszer diszjunkt, és $(i', x'), (i'', x'') \in D$ olyanok, hogy $f(i', x') = f(i'', x'')$, akkor f definíciója szerint $x' = x'' \in E_{i'} \cap E_{i''}$, tehát $i' = i''$, vagyis $(i', x') = (i'', x'')$, azaz f injekció. ■

6.7.5. Definíció. *Az $(E_i)_{i \in I}$ halmazrendszer* **diszjunkt uniójának** *nevezzük az*

$$(\{i\} \times E_i)_{i \in I}$$

diszjunkt halmazrendszer unióját, és ezt a $\bigsqcup_{i \in I} E_i$ szimbólummal jelöljük, tehát

$$\bigsqcup_{i \in I} E_i \ := \ \bigcup_{i \in I}(\{i\} \times E_i).$$

Továbbá, ha $(E_i)_{i \in I}$ halmazrendszer, akkor a

$$\bigsqcup_{i \in I} E_i \to \bigcup_{i \in I} E_i; \quad (i, x) \mapsto x$$

leképezést a $\bigsqcup_{i \in I} E_i$ diszjunkt unió és a $\bigcup_{i \in I} E_i$ unió közötti **kanonikus szürjekciónak** *nevezzük.*

Halmazrendszer uniójának (illetve metszetének) fogalma a halmazok uniójának (illetve metszetének) általánosítása. Erről szól a következő állítás.

6.7.6. Állítás. *Legyenek A és B halmazok. Legyen I tetszőleges két elemű halmaz, vagyis léteznek olyan α és β halmazok, amelyekre $\alpha \neq \beta$ és $I = \{\alpha, \beta\}$. Ha $E_\alpha := A$ és $E_\beta := B$, akkor*

$$\bigcup_{i \in I} E_i \ = \ A \cup B; \quad \bigcap_{i \in I} E_i \ = \ A \cap B.$$

Bizonyítás. Ha $x \in \bigcup_{i \in I} E_i$, akkor van olyan $i \in I = \{\alpha, \beta\}$, hogy $x \in E_i$, ezért $i = \alpha$ esetén $x \in E_\alpha = A$, míg $i = \beta$ esetén $x \in E_\beta = B$, amiből következik, hogy $x \in A \cup B$. Megfordítva, ha $x \in A \cup B$, akkor $x \in A = E_\alpha$ vagy $x \in B = E_\beta$, ezért van olyan $i \in \{\alpha, \beta\} = I$, hogy $x \in E_i$, ami azt jelenti, hogy $x \in \bigcup_{i \in I} E_i$.

Ha $x \in \bigcap_{i \in I} E_i$, akkor minden $i \in I = \{\alpha, \beta\}$ esetén $x \in E_i$, ezért $x \in E_\alpha = A$ és $x \in E_\beta = B$, vagyis $x \in A \cap B$. Megfordítva, ha $x \in A \cap B$, akkor $x \in A = E_\alpha$ és $x \in B = E_\beta$, ezért minden $i \in \{\alpha, \beta\} = I$ esetén $x \in E_i$, vagyis $x \in \bigcap_{i \in I} E_i$. ■

Halmazrendszer szorzatának fogalma a Descartes-szorzat fogalmának általánosítása. Erről szól a következő állítás.

6.7.7. Állítás. *Legyenek A és B halmazok. Vezessük be a $0 := \emptyset$ és $1 := \{\emptyset\}$ objektumokat, és legyen $I := \{0, 1\}$. Ha $(E_i)_{i \in I}$ jelöli azt a halmazrendszert, amelyre $E_0 := A$ és $E_1 := B$, akkor a*

$$\Phi : \prod_{i \in I} E_i \to A \times B; \quad f \mapsto (f(0), f(1)),$$

függvény bijekció.

Bizonyítás. Legyenek $f, f' \in \prod_{i \in I} E_i$ olyanok, hogy $\Phi(f) = \Phi(f')$. Ekkor $(f(0), f(1)) = (f'(0), f'(1))$, tehát $f(0) = f'(0)$ és $f(1) = f'(1)$, így $f = f'$. Ezért Φ injekció.
Legyen $(a, b) \in A \times B$, és tekintsük az $f := \{(0, a), (1, b)\}$ halmazt. Nyilvánvaló, hogy f olyan függvény, amelyre $\mathrm{Dom}(f) = \{0, 1\} = I$ és $f(0) = a \in A = E_0$, valamint $f(1) = b \in B = E_1$, tehát $f \in \prod_{i \in I} E_i$. Továbbá, $\Phi(f) := (f(0), f(1)) = (a, b)$, amiből következik, hogy Φ szürjekció. ■

A halmazrendszerek szorzatával kapcsolatban a következő függvényeket értelmezzük.

6.7.8. Definíció. – *Legyen $(E_i)_{i \in I}$ halmazrendszer és $E := \prod_{i \in I} E_i$. Ekkor minden $i \in I$ indexre a*

$$\mathrm{pr}_i : E \to E_i \ ; \ f \mapsto f(i)$$

függvényt az E szorzathalmaz i-edik **projekció-függvényének** *nevezzük.*
– *Legyen $(E_i)_{i \in I}$ halmazrendszer. Minden $k \in I$ és $\mathbf{x} = (x_i)_{i \in I} \in \prod_{i \in I} E_i$ esetén*

$$\mathrm{in}_{k,\mathbf{x}} : E_k \to \prod_{i \in I} E_i$$

az a függvény, amelyre minden $x \in E_k$ és $i \in I$ esetén

$$(\mathrm{in}_{k,\mathbf{x}}(x))\,(i) := \begin{cases} x_i & , \textit{ha } i \neq k; \\ x & , \textit{ha } i = k, \end{cases}$$

és az $\mathrm{in}_{k,\mathbf{x}}$ *függvényt az* E_k *halmaz* $\mathbf{x}$ *ponthoz tartozó* **injekció-függvényének** *nevezzük.*

– *Legyen* $(E_i)_{i\in I}$ *halmazrendszer,* F *halmaz, és* $f : \prod_{i\in I} E_i \rightarrowtail F$ *függvény. Ekkor minden* $k \in I$ *és* $\mathbf{x} = (x_i)_{i\in I} \in \prod_{i\in I} E_i$ *esetén az*

$$f \circ \mathrm{in}_{k,\mathbf{x}} : E_k \rightarrowtail F$$

függvényt az f *függvény* $\mathbf{x}$ *ponthoz tartozó* k*-adik* **parciális függvényének** *nevezzük.*

– *Legyen* E *halmaz,* $(E_i)_{i\in I}$ *halmazrendszer és* $(f_i)_{i\in I} \in \prod_{i\in I} \mathscr{F}(E; E_i)$*. Ekkor az*

$$E \to \prod_{i\in I} E_i \quad ; \quad x \mapsto (f_i(x))_{i\in I}$$

függvényt az $(f_i)_{i\in I}$ **függvényrendszer együttesének** *nevezzük.*

– *Legyenek* $(E_i)_{i\in I}$ *és* $(F_i)_{i\in I}$ *(egyenlő indexhalmazú) halmazrendszerek és legyen* $(f_i)_{i\in I} \in \prod_{i\in I} \mathscr{F}(E_i; F_i)$*. Ekkor a*

$$\mathop{\times}_{i\in I} f_i : \prod_{i\in I} E_i \to \prod_{i\in I} F_i \quad ; \quad (x_i)_{i\in I} \mapsto (f_i(x_i))_{i\in I}$$

függvényt az $(f_i)_{i\in I}$ **függvényrendszer szorzatának** *nevezzük.*

Érdemes itt megfogalmazni a függvények összeragasztásának tételét (6.2.10.) függvényhalmaz helyett függvényrendszert véve.

6.7.9. Állítás. (**Függvényrendszer összeragasztása**) *Legyen* $(f_i)_{i\in I}$ *olyan rendszer, amelynek minden tagja függvény, és teljesül az, hogy minden* $i, j \in I$ *indexre*

$$f_i|_{\mathrm{Dom}(f_i)\cap\mathrm{Dom}(f_j)} = f_j|_{\mathrm{Dom}(f_i)\cap\mathrm{Dom}(f_j)}.$$

Ekkor az $f := \bigcup_{i\in I} f_i$ *halmaz függvény, és* $\mathrm{Dom}(f) = \bigcup_{i\in I} \mathrm{Dom}(f_i)$*, és* $\mathrm{Im}(f) = \bigcup_{i\in I} \mathrm{Im}(f_i)$*, valamint minden* $i \in I$ *esetén* $f_i = f|_{\mathrm{Dom}(f_i)}$*.*

Bizonyítás. Elegendő az 6.2.10. állítást alkalmazni az $\{f_i | i \in I\}$ függvényhalmazra. ■

6.7.10. Következmény. *Legyen* $(f_i)_{i\in I}$ *olyan rendszer, amelynek minden tagja függvény, és teljesül az, hogy minden* $i, j \in I$ *indexre, ha* $i \neq j$*, akkor* $\mathrm{Dom}(f_i)\cap\mathrm{Dom}(f_j) = \emptyset$*. Ekkor az* $f := \bigcup_{i\in I} f_i$ *halmaz függvény, és* $\mathrm{Dom}(f) = \bigcup_{i\in I} \mathrm{Dom}(f_i)$*, és* $\mathrm{Im}(f) = \bigcup_{i\in I} \mathrm{Im}(f_i)$*, valamint minden* $i \in I$ *esetén* $f_i = f|_{\mathrm{Dom}(f_i)}$*.*

Bizonyítás. Az előző állítás alapján nyilvánvaló, mert ekkor minden $i, j \in I$ esetén, ha $i \neq j$, akkor $f_i|_{\mathrm{Dom}(f_i)\cap\mathrm{Dom}(f_j)} = \emptyset = f_j|_{\mathrm{Dom}(f_i)\cap\mathrm{Dom}(f_j)}$. ■

6.7.11. Állítás. (**Függvényhalmaz-rendszerek értelmezése**) *Ha* $(E_i)_{i\in I}$ *és* $(F_j)_{j\in J}$ *halmazrendszerek, akkor jól értelmezett az*

$$(\mathscr{F}_0(E_i; F_j))_{(i,j)\in I\times J}$$

halmazrendszer, ahol $(i, j) \in I \times J$ *esetén* $\mathscr{F}_0(E_i; F_j)$ *jelöli az* $E_i \rightarrowtail F_j$ *függvények halmazát.*

Bizonyítás. Először azt igazoljuk, hogy az

$$(\exists i)(\exists j)(\ (i \in I) \wedge (j \in J) \wedge (x = ((i,j), \mathscr{F}_0(E_i;F_j)))\ )$$

kijelentés kollektivizáló az x változóban, ahol x nem szerepel az $(E_i)_{i\in I}$ és $(F_j)_{j\in J}$ halmazrendszerekben. Jelölje ezt a kijelentést $\mathscr{A}(x)$.

Legyen $E := \bigcup_{i\in I} E_i$ és $F := \bigcup_{j\in J} F_j$, továbbá jelölje $\mathscr{F}_0(E;F)$ az $E \rightarrowtail F$ függvények halmazát. Világos, hogy x nem szerepel E-ben és F-ben, így $\mathscr{F}_0(E;F)$-ben sem. Tegyük fel, hogy $\mathscr{A}(x)$ igaz. Ekkor vehetünk olyan $i \in I$ és $j \in J$ elemeket, hogy $x = ((i,j), \mathscr{F}_0(E_i;F_j))$. Ekkor $E_i \subseteq E$ és $F_j \subseteq F$ miatt $\mathscr{F}_0(E_i;F_j) \subseteq \mathscr{F}_0(E;F)$, tehát $\mathscr{F}_0(E_i;F_j) \in \mathscr{P}(\mathscr{F}_0(E;F))$. Ez azt jelenti, hogy $x \in (I \times J) \times \mathscr{P}(\mathscr{F}_0(E;F))$, és természetesen x nem szerepel az $(I \times J) \times \mathscr{P}(\mathscr{F}_0(E;F))$ halmazban. Ezért a részhalmaz axióma-sémából következik, hogy az $\mathscr{A}(x)$ kijelentés kollektivizáló x-ben, tehát a

$$G := \{x|\mathscr{A}(x)\}$$

halmaz rendelkezik azzal a tulajdonsággal, hogy $(\forall x)(\ (x \in G) \Leftrightarrow \mathscr{A}(x)\ )$ tétel.

A bizonyítást azzal fejezzük be, hogy megmutatjuk, hogy G függvény, és $\mathrm{Dom}(G) = I \times J$, és minden $(i,j) \in I \times J$ esetén $G(i,j) = \mathscr{F}_0(E_i;F_j)$, ami pontosan azt jelenti, hogy G egyenlő az $(\mathscr{F}_0(E_i;F_j))_{(i,j)\in I\times J}$ függvényhalmaz-rendszerrel. ∎

6.8. Kiválasztási axióma

Kiválasztási axióma. *Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ indexre $E_i \neq \emptyset$, akkor $\prod_{i\in I} E_i \neq \emptyset$.*

Megjegyezzük, hogy ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ indexre $E_i \neq \emptyset$, akkor a $\prod_{i\in I} E_i \neq \emptyset$ szorzathalmaz elemeit **kiválasztó függvényeknek** nevezik, mert ezek minden $i \in I$ indexhez hozzárendelik az E_i valamelyik elemét, vagyis az E_i nem üres halmazból kiválasztanak egy elemet.

A kiválasztási axióma olyan egzisztencia-axióma, amely abban az értelemben *nem konstruktív*, hogy semmiféle utalást nem tartalmaz arra vonatkozóan, hogy milyen módon lehet kiválasztó függvényt előállítani; csak kiválasztó függvény *létezését* állítja. Ebből következik, hogy a kiválasztási axiómára hivatkozó bizonyítások szintén nem konstruktívak.

Habár a kiválasztási axiómának kigondolható olyan "természetes bizonyítása", amely első ránézésre elfogadhatónak tűnik (**46**. gyakorlat); alaposabb vizsgálatok után kiderül, hogy minden ilyen bizonyítás rossz az elsőrendű nyelvekre alapozott halmazelméletben, ha a kiválasztási axióma nélküli halmazelmélet ellentmondásmentes. Ma már ismeretes az, hogy a kiválasztási axióma *nem bizonyítható* az elsőrendű nyelvekre alapozott halmazelmélet többi axiómájából (*Cohen tétele*, 1963.), és *nem cáfolható*, vagyis a negációja sem bizonyítható (*Gödel tétele*, 1939.), feltéve, hogy a többi axióma ellentmondásmentes elméletet határoz meg. Ebből az is következik, hogy ha az elsőrendű nyelvekre alapozott halmazelmélet a kiválasztási axióma nélkül ellentmondásmentes, akkor az axiómarendszert akár a kiválasztási axiómával, akár annak negációjával bővítve szintén ellentmondásmentes elméletet kapunk.

A kiválasztási axiómát rendkívül gyakran alkalmazzuk a matematikában. A segítségével sok olyan matematikai objektum létezése igazolható, amelyek létezését eleve elvárjuk. Azonban a kiválasztási axiómára hivatkozva olyan megdöbbentő tulajdonságokkal rendelkező ún. *paradox* halmazok létezése is igazolható, amelyek előállíthatósága elképzelhetetlennek tűnik. E paradox halmazok közül az egyik leghíresebbet a *Banach-Tarski paradoxon* szolgáltatja, amely szerint bármely egységsugarú térbeli gömb szétdarabolható *véges sok* részhalmazra úgy, hogy e darabokból összeállíthatunk *két*, ugyancsak egységsugarú gömböt. Ebben nincs semmi *logikai* ellentmondás; csak *szemléleti* paradoxonról van szó.

6.8.1. Állítás. *A kiválasztási axióma ekvivalens azzal, hogy minden f függvényhez létezik olyan $g : \operatorname{Im}(f) \to \operatorname{Dom}(f)$ függvény, amely jobbinverze f-nek, vagyis $f \circ g = \operatorname{id}_{\operatorname{Im}(f)}$.*

Bizonyítás. Tegyük fel a kiválasztási axiómát és legyen f tetszőleges függvény. Az $\operatorname{Im}(f)$ halmaz definíciója szerint az $(\overset{-1}{f}\langle\{y\}\rangle)_{y\in\operatorname{Im}(f)}$ halmazrendszerre teljesül az, hogy minden $y \in \operatorname{Im}(f)$ elemre $\overset{-1}{f}\langle\{y\}\rangle \neq \emptyset$, tehát $\prod\limits_{y\in\operatorname{Im}(f)} \overset{-1}{f}\langle\{y\}\rangle \neq \emptyset$. Ha g eleme ennek a szorzathalmaznak, akkor g függvény és $\operatorname{Dom}(g) = \operatorname{Im}(f)$, továbbá $f \circ g = \operatorname{id}_{\operatorname{Im}(f)}$.

Megfordítva; tegyük fel, hogy minden f függvényhez létezik olyan $g : \operatorname{Im}(f) \to \operatorname{Dom}(f)$ függvény, amely jobbinverze f-nek, vagyis $f \circ g = \operatorname{id}_{\operatorname{Im}(f)}$. Legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ indexre $E_i \neq \emptyset$. Értelmezzük az $E := \bigcup\limits_{i\in I} E_i$ halmazt, és tekintsük az $(\{i\} \times E_i)_{i\in I}$ halmazrendszert. Legyen $E' := \bigcup\limits_{i\in I}(\{i\} \times E_i)$ és jelölje p_1 (illetve p_2) az $I \times E \to I$ (illetve $I \times E \to E$) projekció-függvényt. Ekkor $E' \subseteq I \times E$ és az $f := p_1|_{E'} : E' \to I$ függvény *ráképez* I-re, mert minden $i \in I$ indexre $E_i \neq \emptyset$. Ezért $\operatorname{Im}(f) = I$ és $\operatorname{Dom}(f) = E'$. Ha $g : I \to E'$ olyan függvény, hogy $f \circ g = \operatorname{id}_{\operatorname{Im}(f)} = \operatorname{id}_I$, akkor az $s := p_2 \circ g : I \to E$ függvény olyan, hogy $\operatorname{Dom}(s) = I$ és minden $i \in I$ elemre $s(i) \in E_i$, vagyis $s \in \prod\limits_{i\in I} E_i$. ■

Ennek fontos következménye, hogy ha E és F halmazok és létezik $E \to F$ szürjekció, akkor F kisebb-egyenlő számosságú E-nél.

A következő – kombinatorikus meggondolásokban gyakran alkalmazott – tétel bizonyításából jól látható, hogyan alkalmazhatjuk a kiválasztási axiómát.

6.8.2. Tétel. *Legyenek E, F halmazok, $f : E \to F$ olyan függvény, és G olyan halmaz, hogy minden $y \in F$ esetén G és $\overset{-1}{f}\langle\{y\}\rangle$ ekvipotensek. Ekkor az E és $F \times G$ halmazok ekvipotensek.*

Bizonyítás. Minden $y \in F$ esetén jelölje $\mathbb{B}(G; \overset{-1}{f}\langle\{y\}\rangle)$ az $G \to \overset{-1}{f}\langle\{y\}\rangle$ bijekciók halmazát. A hipotézis szerint minden $y \in F$ esetén $\mathbb{B}(G; \overset{-1}{f}\langle\{y\}\rangle) \neq \emptyset$, ezért a kiválasztási axióma alkalmazásával vehetünk egy $g \in \prod\limits_{y\in F} \mathbb{B}(G; \overset{-1}{f}\langle\{y\}\rangle)$ elemet. Tehát g olyan függvény, hogy $\operatorname{Dom}(g) = F$ és minden $y \in F$ elemere $g(y) : G \to \overset{-1}{f}\langle\{y\}\rangle$ bijekció. Értelmezzük a

$$\Phi : F \times G \to E; \quad (y, z) \mapsto (g(y))(z)$$

leképezést. Megmutatjuk, hogy Φ bijekció $F \times G$ és E között.

Legyenek $(y, z), (y', z') \in F \times G$ olyan párok, hogy $\Phi(y, z) = \Phi(y', z')$, vagyis $(g(y))(z) = (g(y'))(z')$. A definíció szerint $(g(y))(z) \in \overset{-1}{f}\langle\{y\}\rangle$, tehát $f((g(y))(z)) = y$, és hasonlóan kapjuk, hogy $f((g(y'))(z')) = y'$. Ebből adódik, hogy $y = y'$, tehát $(g(y))(z) = (g(y))(z')$. A $g(y) : G \to \overset{-1}{f}\langle\{y\}\rangle$ függvény injektív, ezért $z = z'$. Ebből kapjuk, hogy $(y, z) = (y', z')$, tehát a Φ függvény injektív.

Legyen $x \in E$ tetszőleges. Ekkor $y := f(x) \in F$ olyan, hogy $x \in \overset{-1}{f}\langle\{y\}\rangle$, vagyis a $g(y) : G \to \overset{-1}{f}\langle\{y\}\rangle$ függvény szürjektivitása miatt vehetünk olyan $z \in G$ elemet, hogy $\Phi(y, z) = (g(y))(z) = x$. Ez azt jelenti, hogy a $\Phi : F \times G \to E$ függvény szürjektív. ■

6.8.3. Következmény. *Legyen $(E_i)_{i\in I}$ olyan diszjukt halmazrendszer és G olyan halmaz, hogy minden $i \in I$ esetén E_i ekvipotens G-vel. Ekkor az $\bigcup_{i\in I} E_i$ halmaz ekvipotens $I \times G$-vel.*

Bizonyítás. Ha $G = \emptyset$, akkor $\bigcup_{i\in I} E_i = \emptyset = I \times G$, tehát az állítás igaz, így feltehető, hogy $G \neq \emptyset$. Ekkor legyen $E := \bigcup_{i\in I} E_i$ és $f : E \to I$ az a függvény, amely minden $x \in E$ elemhez hozzárendeli azt az $f(x) \in I$ elemet, amelyre $x \in E_{f(x)}$. Minden $i \in I$ esetén $\overset{-1}{f}\langle\{i\}\rangle = E_i$, tehát ez a halmaz ekvipotens G-vel. A 6.8.2. tételt alkalmazva azonnal kapjuk, hogy E és $I \times G$ ekvipotensek. ■

6.8.4. Állítás. *Legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ indexre $E_i \neq \emptyset$. Ha f olyan függvény, hogy $\mathrm{Dom}(f) \subseteq I$ és minden $i \in \mathrm{Dom}(f)$ esetén $f(i) \in E_i$, akkor létezik olyan $\bar{f} \in \prod_{i\in I} E_i$ függvény, hogy $\bar{f}$ az f kiterjesztése.*

Bizonyítás. A hipotézis szerint minden $i \in I \setminus \mathrm{Dom}(f)$ esetén $E_i \neq \emptyset$, ezért a kiválasztási axióma alkalmazásával vehetünk egy $g \in \prod_{i\in I\setminus \mathrm{Dom}(f)} E_i$ függvényt. Ekkor $\bar{f} := f \cup g$ olyan függvény, hogy $f \subseteq \bar{f}$ és $\bar{f} \in \prod_{i\in I} E_i$. ■

6.8.5. Állítás. *Legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ indexre $E_i \neq \emptyset$. Ekkor minden $k \in I$ indexre a*

$$\mathrm{pr}_k : \prod_{i\in I} E_i \to E_k \quad ; \quad f \mapsto f(k)$$

projekció-függvény szürjektív, és minden $J \subseteq I$ halmazra a

$$\mathrm{pr}_J : \prod_{i\in I} E_i \to \prod_{i\in J} E_i \quad ; \quad f \mapsto f|_J$$

leképezés is szürjektív.

Bizonyítás. Legyen $k \in I$ és $y \in E_k$. A kiválasztási aióma alapján vehetünk egy $g \in \prod_{i\in I\setminus\{k\}} E_i$ elemet. Ekkor $f := g \cup \{(k, y)\}$ olyan függvény, amely I-n van értelmezve és minden $i \in I \setminus \{k\}$ esetén $f(i) := g(i) \in E_i$, és $f(k) := y \in E_k$, tehát f a g függvénynek az a kiterjesztése $I \setminus \{k\}$-ról I-re, amely k-hoz az y értéket rendeli. Ez azt jelenti, hogy $f \in \prod_{i \in I} E_i$ és $\mathrm{pr}_k(f) := f(k) = y$, ezért a $\mathrm{pr}_k : \prod_{i \in I} E_i \to E_k$ függvény szürjektív.

Legyen $J \subseteq I$ és $h \in \prod_{i \in J} E_i$. A kiválasztási axióma alapján vehetünk egy $g \in \prod_{i \in I \setminus J} E_i$ elemet. Ekkor $f := g \cup h$ olyan függyvény, amely I-n van értelmezve, és minden $i \in I \setminus J$ esetén $f(i) := g(i) \in E_i$, és minden $i \in J$ esetén $f(i) := h(i) \in E_i$, tehát f a g és h függvényeknek kiterjesztése. Ez azt jelenti, hogy $f \in \prod_{i \in I} E_i$ és $\mathrm{pr}_J(f) := f|_J = h$, ezért a $\mathrm{pr}_J : \prod_{i \in I} E_i \to \prod_{i \in J} E_i$ függvény szürjektív. ■

6.8.6. Állítás. *Legyenek $(E_i)_{i \in I}$ és $(F_i)_{i \in I}$ (egyenlő indexhalmazú) halmazrendszerek és legyen $(f_i)_{i \in I} \in \prod_{i \in I} \mathscr{F}(E_i; F_i)$. Ha minden $i \in I$ esetén az $f_i : E_i \to F_i$ függvény injekció (illetve szürjekció, illetve bijekció), akkor a $\times_{i \in I} f_i : \prod_{i \in I} E_i \to \prod_{i \in I} F_i$ függvény is injekció (illetve szürjekció, illetve bijekció).*

Bizonyítás. Tegyük fel, hogy minden $i \in I$ esetén az $f_i : E_i \to F_i$ függvény injekció. Ha $x := (x_i)_{i \in I}$, $x' := (x'_i)_{i \in I} \in \prod_{i \in I} E_i$, és $\left(\times_{i \in I} f_i\right)(x) = \left(\times_{i \in I} f_i\right)(x')$, akkor $(f_i(x_i))_{i \in I} = (f_i(x'_i))_{i \in I}$, tehát minden $i \in I$ indexre $f_i(x_i) = f_i(x'_i)$, így f_i injektivitásából következik, hogy $x_i = x'_i$, tehát $x = (x_i)_{i \in I} = (x'_i)_{i \in I} = x'$. Ez azt jelenti, hogy a $\times_{i \in I} f_i : \prod_{i \in I} E_i \to \prod_{i \in I} F_i$ függvény injekció.

Tegyük fel, hogy minden $i \in I$ esetén az $f_i : E_i \to F_i$ függvény szürjekció. Legyen $y := (y_i)_{i \in I} \in \prod_{i \in I} F_i$ rögzített. Ekkor minden $i \in I$ esetén $y_i \in \mathrm{Im}(f_i)$ miatt van olyan $x_i \in E_i$, hogy $f_i(x_i) = y_i$, vagyis $\overset{-1}{f_i}\langle\{y_i\}\rangle \neq \emptyset$. A kiválasztási axióma szerint

$$\prod_{i \in I} \overset{-1}{f_i}\langle\{y_i\}\rangle \neq \emptyset.$$

Legyen $x := (x_i)_{i \in I}$ eleme ennek a szorzathalmaznak. Ekkor $x \in \prod_{i \in I} E_i$ és minden $i \in I$ esetén $f_i(x_i) = y_i$, vagyis

$$\left(\times_{i \in I} f_i\right)(x) = (f_i(x_i))_{i \in I} = (y_i)_{i \in I} = y,$$

tehát a $\times_{i \in I} f_i : \prod_{i \in I} E_i \to \prod_{i \in I} F_i$ függvény szürjekció.

Ha minden $i \in I$ esetén az $f_i : E_i \to F_i$ függvény bijekció, akkor injekció is és szürjekció is, ezért az előző bekezdések alapján a $\times_{i \in I} f_i : \prod_{i \in I} E_i \to \prod_{i \in I} F_i$ függvény injekció és szürjekció, tehát bijekció. ■

Vannak olyan esetek, amikor szükségünk van szorzathalmaz elemének létezésére, de ehhez nem kell a kiválasztási axiómára hivatkozni. Ilyen eset az, amikor nem üres halmazok *véges* indexhalmazú rendszerének szorzatáról van szó (8.1.19.), és ebben az esetben a halmazrendszer tagjai bármilyen méretű (nem üres) halmazok lehetnek. Ha az indexhalmaz számosságára nincs korlátozás, akkor is van ilyen eset, ami a következő állításból látható.

6.8.7. Állítás. *Legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ indexre E_i egy elemű halmaz. Ekkor $\prod_{i\in I} E_i$ is egy elemű halmaz.*

Bizonyítás. Jelölje E az $(E_i)_{i\in I}$ rendszert, így E az a függvény, amelyre $\mathrm{Dom}(E)=I$ és minden $i \in I$ esetén $E(i) = E_i$. Jelölje $\mathscr{A}$ a következő kijelentést:

$$(\exists x)(\exists y)((z = (x, y)) \wedge (x \in \mathrm{Dom}(E)) \wedge (y \in E(x))),$$

ami az E definíciója alapján ekvivalens a

$$(\exists i)(\exists y)((z = (i, y)) \wedge (i \in I) \wedge (y \in E_i))$$

kijelentéssel (természetesen az x, y és z változókat úgy választjuk, hogy E-ben ne szerepeljenek). Az $\mathscr{A}$ kijelentés kollektivizáló a z változóban, mert ha $z = (x, y)$, $x \in \mathrm{Dom}(E)$ és $y \in E(x)$, akkor $z \in \mathrm{Dom}(E) \times \left(\bigcup \mathrm{Im}(E)\right)$, ezért elég a részhalmaz axiómára hivatkozni. Megmutatjuk, hogy az $f := \{z|\mathscr{A}\}$ halmazra $f \in \prod_{i\in I} E_i$ teljesül. Valóban, f minden eleme pár, vagyis f reláció, továbbá f függvényreláció, mert ha $(x, y), (x, y') \in f$, akkor $x \in \mathrm{Dom}(E)$ és $y, y' \in E(x)$, így $y = y'$, mivel $E(x)$ egy elemű halmaz. Azonkívül $\mathrm{Dom}(f) \subseteq \mathrm{Dom}(E) = I$ nyilvánvaló, és ha $i \in I$, akkor $E(i) = E_i \neq \emptyset$, tehát ha $y \in E(i)$ tetszőleges elem, akkor $(i, y) \in f$, így $\mathrm{Dom}(f) = I$. Az f definíciója szerint minden $i \in I$ elemre $f(i) \in E_i$, tehát $f \in \prod_{i\in I} E_i$. Ez azt mutatja, hogy $\prod_{i\in I} E_i \neq \emptyset$. Ha $f' \in \prod_{i\in I} E_i$ tetszőleges, akkor minden $i \in I$ indexre $f'(i) \in E_i$ és $f(i) \in E_i$, így $f'(i) = f(i)$, mivel E_i egy elemű halmaz. Ezért $f' = f$, vagyis $\prod_{i\in I} E_i$ egy elemű halmaz. ■

6.8.8. Állítás. *Legyenek E, F, E' és F' halmazok.*

a) *Ha $u : E' \to E$ szürjekció és $v : F \to F'$ injekció, akkor az*

$$\mathscr{F}(E; F) \to \mathscr{F}(E'; F') \quad ; \quad f \mapsto v \circ f \circ u$$

függvény injekció.

b) *Ha $u : E' \to E$ injekció és $v : F \to F'$ szürjekció, akkor az*

$$\mathscr{F}(E; F) \to \mathscr{F}(E'; F') \quad ; \quad f \mapsto v \circ f \circ u$$

függvény szürjekció, feltéve, hogy $F \neq \emptyset$, vagy $E = \emptyset = F$.

c) *Ha $u : E' \to E$ bijekció és $v : F \to F'$ bijekció, akkor az*

$$\mathscr{F}(E; F) \to \mathscr{F}(E'; F') \quad ; \quad f \mapsto v \circ f \circ u$$

függvény bijekció.

Bizonyítás. a) Legyenek $f, g \in \mathscr{F}(E; F)$ olyanok, hogy $v \circ f \circ u = v \circ g \circ u$. Ha $x \in E$, akkor az $u : E' \to E$ függvény szürjektivitása miatt van olyan $x' \in E'$, hogy $x = u(x')$, tehát $v(f(x)) = (v \circ f \circ u)(x') = (v \circ g \circ u)(x') = v(g(x))$, következésképpen $f(x) = g(x)$, hiszen v injekció. Ez azt jelenti, hogy $f = g$, tehát a

$$\mathscr{F}(E; F) \ \to \ \mathscr{F}(E'; F') \quad ; \quad f \mapsto v \circ f \circ u$$

függvény injekció.

b) Ha $F = \emptyset$, akkor a $v : F \to F'$ függvény szürjektivitása miatt $F' = \mathrm{Im}(v) = \emptyset$, ezért $\mathscr{F}(E'; F') = \{\emptyset\}$. Ugyanakkor, ha $E \neq \emptyset$, akkor $\mathscr{F}(E; F) = \emptyset$ tehát egyáltalán nem létezik $\mathscr{F}(E; F) \to \mathscr{F}(E'; F')$ szürjekció. Ezért kötjük ki, hogy $F \neq \emptyset$, vagy $E = \emptyset = F$.

Ha $E = \emptyset = F$, akkor $\mathscr{F}(E; F) = \{\emptyset\} = \mathscr{F}(E'; F')$, és ekkor az

$$\mathscr{F}(E; F) \ \to \ \mathscr{F}(E'; F') \quad ; \quad f \mapsto v \circ f \circ u$$

függvény egyenlő az egyetlen $\mathscr{F}(E; F) \to \mathscr{F}(E'; F')$ függvénnyel, tehát az állítás igaz.

Legyen $F \neq \emptyset$ és $f' \in \mathscr{F}(E'; F')$ tetszőleges. Az

$$\mathscr{F}(E; F) \ \to \ \mathscr{F}(E'; F') \quad ; \quad f \mapsto v \circ f \circ u$$

függvény szürjektivitásának bizonyításához olyan $f \in \mathscr{F}(E; F)$ függvényt keresünk, amelyre $v \circ f \circ u = f'$. Ha f ilyen függvény volna, akkor

$$(v \circ f)|_{\mathrm{Im}(u)} = (v \circ f \circ u) \circ u^{-1} = f' \circ u^{-1}$$

teljesülne, vagyis minden $x \in \mathrm{Im}(u)$ esetén $v(f(x)) = f'(u^{-1}(x))$ lenne, vagyis fennállna az $f(x) \in \overset{-1}{v}\langle\{f'(u^{-1}(x))\}\rangle$ összefüggés. Ez azt jelenti, hogy a keresett $f \in \mathscr{F}(E; F)$ függvényre

$$f|_{\mathrm{Im}(u)} \in \prod_{x \in \mathrm{Im}(u)} \overset{-1}{v}\langle\{f'(u^{-1}(x))\}\rangle$$

szükségképpen teljesül. Az itt látható szorzathalmaz a kiválasztási axióma miatt nem üres, mert $v : F \to F'$ szürjekció és minden $x \in \mathrm{Im}(u)$ esetén $f'(u^{-1}(x)) \in F'$, tehát $\overset{-1}{v}\langle\{f'(u^{-1}(x))\}\rangle \neq \emptyset$. Legyen

$$f_0 \in \prod_{x \in \mathrm{Im}(u)} \overset{-1}{v}\langle\{f'(u^{-1}(x))\}\rangle$$

rögzített. Ekkor f_0 olyan függvény, hogy $\mathrm{Dom}(f_0) = \mathrm{Im}(u) \subseteq E$ és $\mathrm{Im}(f_0) \subseteq F$. Legyen $f : E \to F$ az $f_0 : E \rightarrowtail F$ függvény tetszőleges kiterjesztése $\mathrm{Im}(u)$-ról E-re (6.2.9.). Ekkor $x' \in E'$ esetén $u(x') \in \mathrm{Im}(u)$, ezért $(v \circ f \circ u)(x') = v(f(u(x')) = v(f_0(u(x'))) = f'(u^{-1}(u(x'))) = f'(x')$, vagyis $v \circ f \circ u = f'$.

c) Az a) és b) kijelentések konjunkciójából következik. ■

6.8.9. Következmény. *Legyenek E, F, E' és F' halmazok. Ha E ekvipotens E'-vel és F ekvipotens F'-vel, akkor az $\mathscr{F}(E; F)$ függvényhalmaz ekvipotens az $\mathscr{F}(E'; F')$ függvényhalmazzal.*

Bizonyítás. Nyilvánvalóan következik az előző állítás c) pontjából. ■

6.9. Az unió, a metszet és a szorzat tulajdonságai

6.9.1. Állítás. (**de Morgan egyenlőségek**) *Ha E halmaz és $(E_i)_{i\in I}$ olyan halmazrendszer, hogy $I \neq \emptyset$, akkor*

$$E \setminus \bigcap_{i\in I} E_i = \bigcup_{i\in I} (E \setminus E_i),$$
$$E \setminus \bigcup_{i\in I} E_i = \bigcap_{i\in I} (E \setminus E_i).$$

Bizonyítás. (I) Legyen $x \in E \setminus \bigcap_{i\in I} E_i$. Ekkor $x \in E$ és $x \notin \bigcap_{i\in I} E_i$, tehát vehetünk olyan $i_* \in I$ indexet, hogy $x \notin E_{i_*}$. Nyilvánvaló, hogy $x \in E \setminus E_{i_*} \subseteq \bigcup_{i\in I}(E \setminus E_i)$, vagyis $x \in \bigcup_{i\in I}(E \setminus E_i)$. Megfordítva, tegyük fel, hogy $x \in \bigcup_{i\in I}(E \setminus E_i)$, és rögzítsünk olyan $i_* \in I$ indexet, hogy $x \in E \setminus E_{i_*}$. Ekkor $x \in E$ és $x \notin E_{i_*}$, tehát $x \notin \bigcap_{i\in I} E_i$, vagyis $x \in E \setminus \bigcap_{i\in I} E_i$.

(II) Legyen $x \in E \setminus \bigcup_{i\in I} E_i$. Ekkor $x \in E$ és $x \notin \bigcup_{i\in I} E_i$, tehát minden $i \in I$ esetén $x \notin E_i$. Ez azt jelenti, hogy minden $i \in I$ indexre $x \in E \setminus E_i$, vagyis $x \in \bigcap_{i\in I}(E \setminus E_i)$. Megfordítva, tegyük fel, hogy $x \in \bigcap_{i\in I}(E \setminus E_i)$. Az I halmaz nem üres, tehát vehetünk egy $i_* \in I$ indexet. Ekkor $x \in E \setminus E_{i_*}$, következésképpen $x \in E$. Ugyanakkor minden $I \ni i$-re $x \in E \setminus E_i$, tehát $x \notin E_i$, így $x \notin \bigcup_{i\in I} E_i$. Ez azt jelenti, hogy $x \in E \setminus \bigcup_{i\in I} E_i$. ■

6.9.2. Állítás. (Az unió és metszet kommutativitása.) *Ha $(E_i)_{i\in I}$ halmazrendszer, K halmaz és $\sigma : K \to I$ szürjekció, akkor*

$$\bigcup_{i\in I} E_i = \bigcup_{k\in K} E_{\sigma(k)},$$

és ha $I \neq \emptyset$, akkor

$$\bigcap_{i\in I} E_i = \bigcap_{k\in K} E_{\sigma(k)}.$$

Bizonyítás. (I) Ha $x \in \bigcup_{i\in I} E_i$, akkor vehetünk olyan $i_* \in I$ elemet, hogy $x \in E_{i_*}$. A $\sigma : K \to I$ függvény szürjektivitása miatt van olyan $k_* \in K$, hogy $i_* = \sigma(k_*)$. Ekkor $x \in E_{\sigma(k_*)}$, tehát van olyan $k \in K$, amelyre $x \in E_{\sigma(k)}$, így $x \in \bigcup_{k\in K} E_{\sigma(k)}$. Ez azt jelenti, hogy $\bigcup_{i\in I} E_i \subseteq \bigcup_{k\in K} E_{\sigma(k)}$. Megfordítva, ha $k \in K$, akkor $\sigma(k) \in I$, ezért $E_{\sigma(k)} \subseteq \bigcup_{i\in I} E_i$, következésképpen $\bigcup_{k\in K} E_{\sigma(k)} \subseteq \bigcup_{i\in I} E_i$ (még akkor is, ha a $\sigma : K \to I$ függvény nem szürjektív).

(II) Tegyük fel, hogy $I \neq \emptyset$. Ekkor a $\sigma : K \to I$ függvény szürjektivitása miatt $K \neq \emptyset$, ezért a $\bigcap_{i\in I} E_i$ és $\bigcap_{k\in K} E_{\sigma(k)}$ metszetek mindketten jól értelmezettek.

Ha $k \in K$, akkor $\sigma(k) \in I$, ezért $\bigcap_{i\in I} E_i \subseteq E_{\sigma(k)}$, következésképpen $\bigcap_{i\in I} E_i \subseteq \bigcap_{k\in K} E_{\sigma(k)}$ (még akkor is, ha a $\sigma : K \to I$ függvény nem szürjektív). Megfordítva, legyen $i \in I$. A $\sigma : K \to I$ függvény szürjektivitása miatt vehetünk olyan $k_* \in K$ elemet, hogy $\sigma(k_*) = i$. Ekkor $\bigcap_{k\in K} E_{\sigma(k)} \subseteq E_{\sigma(k_*)} = E_i$. Ebből következik, hogy $\bigcap_{k\in K} E_{\sigma(k)} \subseteq \bigcap_{i\in I} E_i$. ■

6.9.3. Állítás. (**A halmazszorzás kommutativitása.**) *Legyen $(E_i)_{i\in I}$ halmazrendszer, K halmaz és $\sigma : K \to I$ bijekció. Ekkor minden $f \in \prod_{i\in I} E_i$ elemre $f\circ\sigma \in \prod_{k\in K} E_{\sigma(k)}$, és az*

$$F : \prod_{i\in I} E_i \to \prod_{k\in K} E_{\sigma(k)} \quad ; \quad f \mapsto f\circ\sigma$$

leképezés bijekció.

Bizonyítás. Ha $f \in \prod_{i\in I} E_i$, akkor minden $k \in K$ esetén $f(\sigma(k)) \in E_{\sigma(k)}$, ami azt jelenti, hogy $f\circ\sigma \in \prod_{k\in K} E_{\sigma(k)}$.

Ha $f, f' \in \prod_{i\in I} E_i$ és $f\circ\sigma = f'\circ\sigma$, akkor a $\sigma : K \to I$ függvény szürjektivitása miatt $f = f'$, ezért az F leképezés injektív.

Ha $g \in \prod_{k\in K} E_{\sigma(k)}$, akkor $g\circ\sigma^{-1}$ olyan I-n értelmezett függvény, hogy minden $i \in I$ esetén $g(\sigma^{-1}(i)) \in E_{\sigma(\sigma^{-1}(i))} = E_i$, vagyis $g\circ\sigma^{-1} \in \prod_{i\in I} E_i$ és természetesen $(g\circ\sigma^{-1})\circ\sigma = g$, ezért az F leképezés szürjektív. ■

6.9.4. Állítás. (**Az unió és metszet asszociativitása.**) *Legyen $(E_i)_{i\in I}$ halmazrendszer és $(I_j)_{j\in J}$ olyan halmazrendszer, amelyre $I = \bigcup_{j\in J} I_j$. Ekkor*

$$\bigcup_{i\in I} E_i = \bigcup_{j\in J}\bigcup_{i\in I_j} E_i,$$

és ha $J \neq \emptyset$, valamint minden $j \in J$ indexre $I_j \neq \emptyset$, akkor

$$\bigcap_{i\in I} E_i = \bigcap_{j\in J}\bigcap_{i\in I_j} E_i.$$

Bizonyítás. (I) Legyen $x \in \bigcup_{i\in I} E_i$, és vegyünk olyan $i_* \in I$ elemet, amelyre $x \in E_{i_*}$. Az $I = \bigcup_{j\in J} I_j$ feltétel alapján vehetünk olyan $j_* \in J$ elemet, amelyre $i_* \in I_{j_*}$. Ekkor van olyan $i \in I$, hogy $i \in I_{j_*}$ és $x \in E_i$ (ti. $i := i_*$ ilyen), tehát $x \in \bigcup_{i\in I_{j_*}} E_i$. Ez azt jelenti, hogy létezik $j \in J$, amelyre $x \in \bigcup_{i\in I_j} E_i$ (ti. $j := j_*$ ilyen), tehát $x \in \bigcup_{j\in J}\bigcup_{i\in I_j} E_i$. Ezzel megmutattuk, hogy $\bigcup_{i\in I} E_i \subseteq \bigcup_{j\in J}\bigcup_{i\in I_j} E_i$.

Megfordítva, tegyük fel, hogy $x \in \bigcup_{j\in J}\bigcup_{i\in I_j} E_i$, és vegyünk olyan $j_* \in J$ elemet, amelyre $x \in \bigcup_{i\in I_{j_*}} E_i$. Ekkor rögzíthetünk olyan $i_* \in I_{j_*}$ elemet, hogy $x \in E_{i_*}$. Mivel $I_{j_*} \subseteq I$, így $i_* \in I$, következésképpen van olyan $i \in I$, hogy $x \in E_i$ (ti. $i := i_*$ ilyen). Ez azt jelenti, hogy $x \in \bigcup_{i\in I} E_i$, tehát igazoltuk, hogy $\bigcup_{j\in J}\bigcup_{i\in I_j} E_i \subseteq \bigcup_{i\in I} E_i$.

(II) Tegyük fel, hogy $I \neq \emptyset$, és legyen $x \in \bigcap_{i\in I} E_i$. Ekkor minden $i \in I$ esetén $x \in E_i$. Ha $j \in J$ tetszőleges, akkor $I_j \subseteq I$ miatt minden $i \in I_j$ esetén $x \in E_i$, ezért $x \in \bigcap_{i\in I_j} E_i$, következésképpen $x \in \bigcap_{j\in J}\bigcap_{i\in I_j} E_i$. Ezzel megmutattuk, hogy $\bigcap_{i\in I} E_i \subseteq \bigcap_{j\in J}\bigcap_{i\in I_j} E_i$.

Megfordítva, legyen $I \neq \emptyset$, és $x \in \bigcap_{j\in J}\bigcap_{i\in I_j} E_i$. Legyen $i_* \in I$ tetszőleges. Ekkor $I = \bigcup_{j\in J} I_j$ miatt választhatunk olyan $j_* \in J$ elemet, amelyre $i_* \in I_{j_*}$. Ekkor $x \in \bigcap_{i\in I_{j_*}} E_i$, így $x \in E_{i_*}$. Az $i_* \in I$ elem tetszőleges volt, ezért $x \in \bigcap_{i\in I} E_i$. Ezzel megmutattuk, hogy $\bigcap_{j\in J}\bigcap_{i\in I_j} E_i \subseteq \bigcap_{i\in I} E_i$. ■

6.9.5. Állítás. (**A halmazszorzás asszociativitása**) *Legyen* $(E_i)_{i\in I}$ *olyan halmazrendszer, amelyre* $I \neq \emptyset$, *és legyen* $(I_j)_{j\in J}$ *olyan diszjunkt halmazrendszer, hogy* $I = \bigcup_{j\in J} I_j$ *és minden* $j \in J$ *indexre* $I_j \neq \emptyset$ (*ezt röviden úgy fejezzük ki, hogy* $(I_j)_{j\in J}$ *az* I *halmaz* **partíciója**). *Ekkor az*

$$\prod_{i\in I} E_i \to \prod_{j\in J}\prod_{i\in I_j} E_i \quad ; \quad f \mapsto (j \mapsto f|_{I_j})$$

leképezés bijekció. (*Ezt leképezést nevezzük az* I *indexhalmaz* $(I_j)_{j\in J}$ *partíciója által meghatározott* **kanonikus bijekciónak**.)

Bizonyítás. Legyenek $f, f' \in \prod_{i\in I} E_i$ olyanok, hogy minden $j \in J$ esetén $f|_{I_j} = f'|_{I_j}$. Ekkor $f = f'$, mert $I = \bigcup_{j\in J} I_j$ és $\mathrm{Dom}(f) = I = \mathrm{Dom}(f')$. Ez azt jelenti, hogy a vizsgált függvény injektív.

Minden $i \in I$ esetén létezik egyetlen olyan $j \in I$, amelyre $i \in I_j$, ezért a

$$\sigma := \{\ (i,j) \in I \times J \mid i \in J_j\ \}$$

halmaz olyan függvény, hogy $\mathrm{Dom}(\sigma) = I$ és $\mathrm{Im}(\sigma) \subseteq J$.

Legyen $g \in \prod_{j\in J}\prod_{i\in I_j} E_i$. Ha $i \in I$, akkor $\sigma(i) \in J$ az az index, amelyre $i \in J_{\sigma(i)}$, ugyanakkor

$g(\sigma(i)) \in \prod_{i' \in I_{\sigma(i)}} E_{i'}$, ezért $(g(\sigma(i)))(i) \in E_i$. Tehát az

$$f := \{ (i, (g(\sigma(i)))(i)) \mid i \in I \}$$

halmaz olyan függvény, amelyre $\mathrm{Dom}(f) = I$, és minden $i \in I$ esetén $f(i) \in E_i$, vagyis $f \in \prod_{i \in I} E_i$. Továbbá, ha $j \in J$, akkor minden $I_j \ni i$-re $f(i) = (g(\sigma(i)))(i) = (g(j))(i)$, tehát $f|_{I_j} = g(j)$. Ez azt jelenti, hogy a vizsgált függvény szürjektív. ■

6.9.6. Állítás. (**Disztributivitás-formulák**) *Legyen* $(I_j)_{j \in J}$ *olyan halmazrendszer, hogy minden* $j \in J$ *indexre* $I_j \neq \emptyset$. *Legyen* $\left((E_{i,j})_{i \in I_j}\right)_{j \in J}$ *halmazrendszer. Ha* $I := \prod_{j \in J} I_j$, *akkor* $I \neq \emptyset$, *és*

$$\bigcup_{j \in J} \bigcap_{i \in I_j} E_{i,j} = \bigcap_{f \in I} \bigcup_{j \in J} E_{f(j),j},$$

$$\bigcap_{j \in J} \bigcup_{i \in I_j} E_{i,j} = \bigcup_{f \in I} \bigcap_{j \in J} E_{f(j),j}.$$

Bizonyítás. Az I halmaz a kiválasztási axióma miatt nem üres.

(I) Legyen $x \in \bigcup_{j \in J} \bigcap_{i \in I_j} E_{i,j}$, és vegyünk egy olyan $j_* \in J$ elemet, amelyre $x \in \bigcap_{i \in I_{j_*}} E_{i,j_*}$. Ha $f \in I$, akkor minden $j \in J$ esetén $f(j) \in I_j$, következésképpen $f(j_*) \in I_{j_*}$, így $x \in E_{f(j_*),j_*}$, hiszen minden $I_{j_*} \ni i$-re $x \in E_{i,j_*}$. Ez azt jelenti, hogy $f \in I$ esetén van olyan $j \in J$, hogy $x \in E_{f(j),j}$ (ti. $j := j_*$ ilyen), vagyis $x \in \bigcup_{j \in J} E_{f(j),j}$. Ezzel beláttuk, hogy $\bigcup_{j \in J} \bigcap_{i \in I_j} E_{i,j} \subseteq \bigcap_{f \in I} \bigcup_{j \in J} E_{f(j),j}$.

Megfordítva, tegyük fel, hogy $x \notin \bigcup_{j \in J} \bigcap_{i \in I_j} E_{i,j}$. Ekkor minden $j \in J$ indexhez van olyan $i \in I_j$, hogy $x \notin E_{i,j}$. Másként fogalmazva: minden $j \in J$ esetén $\{i \in I_j | x \notin E_{i,j}\} \neq \emptyset$, ezért a kiválasztási axióma szerint vehetünk egy $f_* \in \prod_{j \in J} \{i \in I_j | x \notin E_{i,j}\}$ elemet. Világos, hogy $\prod_{j \in J} \{i \in I_j | x \notin E_{i,j}\} \subseteq \prod_{j \in J} I_j =: I$, tehát $f_* \in I$. Ha $j \in J$, akkor az f_* definíciója szerint $f_*(j) \in \{i \in I_j | x \notin E_{i,j}\}$, vagyis $x \notin E_{f_*(j),j}$, ezért $x \notin \bigcup_{j \in J} E_{f_*(j),j}$. Ez azt jelenti, hogy létezik olyan $f \in I$, amelyre $x \notin \bigcup_{j \in J} E_{f(j),j}$ (ti. $f := f_*$ ilyen), tehát $x \notin \bigcap_{f \in I} \bigcup_{j \in J} E_{f(j),j}$. Ezzel beláttuk, hogy $\bigcap_{f \in I} \bigcup_{j \in J} E_{f(j),j} \subseteq \bigcup_{j \in J} \bigcap_{i \in I_j} E_{i,j}$.

(II) Legyen $x \in \bigcap_{j \in J} \bigcup_{i \in I_j} E_{i,j}$. Ekkor minden $j \in J$ esetén van olyan $i \in I_j$, hogy $x \in E_{i,j}$. Másként fogalmazva: minden $j \in J$ esetén $\{i \in I_j | x \in E_{i,j}\} \neq \emptyset$, ezért a kiválasztási axióma szerint vehetünk egy $f_* \in \prod_{j \in J} \{i \in I_j | x \in E_{i,j}\}$ elemet. Világos, hogy $\prod_{j \in J} \{i \in I_j | x \in E_{i,j}\} \subseteq \prod_{j \in J} I_j =: I$, tehát $f_* \in I$. Ha $j \in J$, akkor az f_* definíciója szerint

$f_*(j) \in \{i \in I_j | x \in E_{i,j}\}$, vagyis $x \in E_{f_*(j),j}$, ezért $x \in \bigcup_{j\in J} E_{f_*(j),j}$. Ez azt jelenti, hogy létezik olyan $f \in I$, amelyre $x \in \bigcap_{j\in J} E_{f(j),j}$ (ti. $f := f_*$ ilyen), tehát $x \in \bigcup_{f\in I} \bigcap_{j\in J} E_{f(j),j}$. Ezzel beláttuk, hogy $\bigcap_{j\in J} \bigcup_{i\in I_j} E_{i,j} \subseteq \bigcup_{f\in I} \bigcap_{j\in J} E_{f(j),j}$.

Megfordítva, tegyük fel, hogy $x \in \bigcup_{f\in I} \bigcap_{j\in J} E_{f(j),j}$, és vegyünk egy olyan $f_* \in I$ elemet, amelyre $x \in \bigcap_{j\in J} E_{f_*(j),j}$. Ha $j \in J$, akkor $x \in E_{f_*(j),j}$, tehát van olyan $i \in I_j$, hogy $x \in E_{i,j}$ (ti. $i := f_*(j)$ ilyen). Ez azt jelenti, hogy minden $j \in J$ esetén $x \in \bigcup_{i\in I_j} E_{i,j}$. Ezzel beláttuk, hogy $\bigcup_{f\in I} \bigcap_{j\in J} E_{f(j),j} \subseteq \bigcap_{j\in J} \bigcup_{i\in I_j} E_{i,j}$. ■

6.9.7. Következmény. *Ha $(E_i)_{i\in I}$ és $(F_j)_{j\in J}$ halmazrendszerek, akkor*

$$\Big(\bigcup_{i\in I} E_i\Big) \cap \Big(\bigcup_{j\in J} F_j\Big) = \bigcup_{(i,j)\in I\times J} (E_i \cap F_j),$$

és ha I és J nem üresek, akkor

$$\Big(\bigcap_{i\in I} E_i\Big) \cup \Big(\bigcap_{j\in J} F_j\Big) = \bigcap_{(i,j)\in I\times J} (E_i \cup F_j).$$

Bizonyítás. Mindkét állítás bebizonyítható az előző állítás és 6.7.6. alkalmazásával. Itt közvetlen bizonyítás adunk.

(I) Legyen $x \in \Big(\bigcup_{i\in I} E_i\Big) \cap \Big(\bigcup_{j\in J} F_j\Big)$. Ekkor $x \in \bigcup_{i\in I} E_i$ és $x \in \bigcup_{j\in J} F_j$, ezért vehetünk olyan $i_* \in I$ és $j_* \in J$ indexeket, hogy $x \in E_{i_*}$ és $x \in F_{j_*}$, vagyis $x \in E_{i_*} \cap F_{j_*}$. Ebből következik, hogy $x \in \bigcup_{(i,j)\in I\times J} (E_i \cap F_j)$. Megfordítva, tegyük fel, hogy $x \in \bigcup_{(i,j)\in I\times J} (E_i \cap F_j)$, és rögzítsünk olyan $(i_*, j_*) \in I \times J$ párt, amelyre $x \in E_{i_*} \cap F_{j_*}$. Ekkor $x \in E_{i_*} \subseteq \bigcup_{i\in I} E_i$ és $x \in F_{j_*} \subseteq \bigcup_{j\in J} F_j$, tehát $x \in \Big(\bigcup_{i\in I} E_i\Big) \cap \Big(\bigcup_{j\in J} F_j\Big)$.

(II) Tegyük fel, hogy I és J nem üresek. Legyen $x \in \Big(\bigcap_{i\in I} E_i\Big) \cup \Big(\bigcap_{j\in J} F_j\Big)$. Ha $x \in \bigcap_{i\in I} E_i$, akkor minden $i \in I$ és $j \in J$ esetén $x \in E_i \subseteq E_i \cup F_j$, tehát $x \in \bigcap_{(i,j)\in I\times J} (E_i \cup F_j)$. Ha $x \in \bigcap_{j\in J} F_j$, akkor minden $i \in I$ és $j \in J$ esetén $x \in F_j \subseteq E_i \cup F_j$, tehát $x \in \bigcap_{(i,j)\in I\times J} (E_i \cup F_j)$. Ebből következik, hogy $x \in \bigcap_{(i,j)\in I\times J} (E_i \cup F_j)$. Megfordítva, tegyük fel, hogy $x \notin \Big(\bigcap_{i\in I} E_i\Big) \cup \Big(\bigcap_{j\in J} F_j\Big)$. Ekkor $x \notin \bigcap_{i\in I} E_i$ és $x \notin \bigcap_{j\in J} F_j$, tehát vehetünk olyan $i_* \in I$ és $j_* \in J$ indexeket, hogy $x \notin E_{i_*}$ és $x \notin F_{j_*}$. Világos, hogy $x \notin E_{i_*} \cup F_{j_*}$, tehát $x \notin \bigcap_{(i,j)\in I\times J} (E_i \cup F_j)$. ■

6.9.8. Állítás. (**Disztributivitás-formulák**) *Legyenek* $(I_j)_{j\in J}$ *és* $\big((E_{i,j})_{i\in I_j}\big)_{j\in J}$ *halmazrendszerek. Ha* $I := \prod_{j\in J} I_j$, *akkor*

$$\prod_{j\in J}\bigcup_{i\in I_j} E_{i,j} = \bigcup_{f\in I}\prod_{j\in J} E_{f(j),j},$$

és ha minden $j \in J$ *indexre* $I_j \neq \emptyset$, *akkor* $I \neq \emptyset$, *és*

$$\prod_{j\in J}\bigcap_{i\in I_j} E_{i,j} = \bigcap_{f\in I}\prod_{j\in J} E_{f(j),j}.$$

Bizonyítás. (I) Legyen $g \in \prod_{j\in J}\bigcup_{i\in I_j} E_{i,j}$. Ekkor minden $j \in J$ esetén $g(j) \in \bigcup_{i\in I_j} E_{i,j}$, tehát van olyan $i \in I_j$, hogy $g(j) \in E_{i,j}$. Másként fogalmazva: minden $j \in J$ esetén $\{i \in I_j | g(j) \in E_{i,j}\} \neq \emptyset$, ezért a kiválasztási axióma szerint vehetünk egy $f_* \in \prod_{j\in J}\{i \in I_j | g(j) \in E_{i,j}\}$ elemet. Világos, hogy $\prod_{j\in J}\{i \in I_j | g(j) \in E_{i,j}\} \subseteq \prod_{j\in J} I_j =: I$, tehát $f_* \in I$. Az f_* definíciója alapján, minden $j \in J$ esetén $g(j) \in E_{f_*(j),j}$, tehát $g \in \prod_{j\in J} E_{f_*(j),j}$. Ez azt jelenti, hogy van olyan $f \in I$, amelyre $g \in \prod_{j\in J} E_{f(j),j}$ (ti. $f := f_*$ ilyen), ezért $g \in \bigcup_{f\in I}\prod_{j\in J} E_{f(j),j}$. Ezzel megmutattuk, hogy $\prod_{j\in J}\bigcup_{i\in I_j} E_{i,j} \subseteq \bigcup_{f\in I}\prod_{j\in J} E_{f(j),j}$.

Megfordítva, tegyük fel, hogy $g \in \bigcup_{f\in I}\prod_{j\in J} E_{f(j),j}$ és vegyünk egy $f_* \in I$ elemet, amelyre $g \in \prod_{j\in J} E_{f_*(j),j}$. Ha $j \in J$, akkor $g(j) \in E_{f_*(j),j}$, tehát van olyan $i \in I_j$, hogy $g(j) \in E_{i,j}$ (ti. $i := f_*(j)$ ilyen), így $g(j) \in \bigcup_{i\in I_j} E_{i,j}$. Ez azt jelenti, hogy $g \in \prod_{j\in J}\bigcup_{i\in I_j} E_{i,j}$. Ezzel megmutattuk, hogy $\bigcup_{f\in I}\prod_{j\in J} E_{f(j),j} \subseteq \prod_{j\in J}\bigcup_{i\in I_j} E_{i,j}$.

(II) Tegyük fel, hogy minden $j \in J$ indexre $I_j \neq \emptyset$. Ekkor a kiválasztási axióma szerint $I := \prod_{j\in J} I_j \neq \emptyset$.

Legyen $g \in \prod_{j\in J}\bigcap_{i\in I_j} E_{i,j}$. Ekkor minden $j \in J$ esetén $g(j) \in \bigcap_{i\in I_j} E_{i,j}$, tehát minden $i \in I_j$ esetén $g(j) \in E_{i,j}$. Ebből következik, hogy ha $f \in I$, akkor minden $j \in J$ esetén $g(j) \in E_{f(j),j}$ (hiszen $f(j) \in I_j$), vagyis $g \in \prod_{j\in J} E_{f(j),j}$. Ez minden $f \in I$ esetén igaz, tehát $g \in \bigcap_{f\in I}\prod_{j\in J} E_{f(j),j}$. Ezzel megmutattuk, hogy $\prod_{j\in J}\bigcap_{i\in I_j} E_{i,j} \subseteq \bigcap_{f\in I}\prod_{j\in J} E_{f(j),j}$.

Megfordítva, legyen $g \in \bigcap_{f\in I}\prod_{j\in J} E_{f(j),j}$, és rögzítsünk egy $j \in J$ és egy $i \in I_j$ indexet. A kiválasztási axióma miatt vehetünk egy $f_* \in \prod_{j'\in J\setminus\{j\}} I_{j'}$ függvényt. Képezzük az $f := f_* \cup \{(j,i)\}$ halmazt. Ez olyan függvény, amelyre $\mathrm{Dom}(f) = J$ és minden $j' \in J$ esetén $f(j') \in I_{j'}$, és $f(j) = i$, vagyis $f \in I$ és $f(j) = i$. A g-re vonatkozó hipotézis szerint $g \in \prod_{j' \in J} E_{f(j'),j'}$, ezért $g(j) \in E_{f(j),j} = E_{i,j}$. Tehát minden $j \in J$ és $i \in I_j$ esetén $g(j) \in E_{i,j}$, ami azt jelenti, hogy $g \in \prod_{j \in J} \bigcap_{i \in I_j} E_{i,j}$. Ezzel megmutattuk, hogy $\bigcap_{f \in I} \prod_{j \in J} E_{f(j),j} \subseteq \prod_{j \in J} \bigcap_{i \in I_j} E_{i,j}$. ■

6.9.9. Következmény. *Ha $(E_i)_{i \in I}$ és $(F_j)_{j \in J}$ halmazrendszerek, akkor*

$$\Big(\bigcup_{i \in I} E_i\Big) \times \Big(\bigcup_{j \in J} F_j\Big) = \bigcup_{(i,j) \in I \times J} (E_i \times F_j),$$

és ha I és J nem üresek, akkor

$$\Big(\bigcap_{i \in I} E_i\Big) \times \Big(\bigcap_{j \in J} F_j\Big) = \bigcap_{(i,j) \in I \times J} (E_i \times F_j).$$

Bizonyítás. Mindkét állítás bebizonyítható az előző állítás és 6.7.6. alkalmazásával. Itt egy közvetlen bizonyítást adunk.

(I) Legyen $(x, y) \in \Big(\bigcup_{i \in I} E_i\Big) \times \Big(\bigcup_{j \in J} F_j\Big)$. Ekkor $x \in \bigcup_{i \in I} E_i$ és $y \in \bigcup_{j \in J} F_j$, így vehetünk olyan $i_* \in I$ és $j_* \in J$ indexeket, hogy $x \in E_{i_*}$ és $y \in F_{j_*}$. Világos, hogy $(x, y) \in E_{i_*} \times F_{j_*} \subseteq \bigcup_{(i,j) \in I \times J} (E_i \times F_j)$, tehát $(x, y) \in \bigcup_{(i,j) \in I \times J} (E_i \times F_j)$. Megfordítva, ha $(x, y) \in\subseteq \bigcup_{(i,j) \in I \times J} (E_i \times F_j)$, akkor vehetünk olyan $(i_*, j_*) \in I \times J$ párt, hogy $(x, y) \in E_{i_*} \times F_{j_*}$. Ekkor $x \in E_{i_*} \subseteq \bigcup_{i \in I} E_i$ és $y \in F_{j_*} \subseteq \bigcup_{j \in J} F_j$, tehát $(x, y) \in \Big(\bigcup_{i \in I} E_i\Big) \times \Big(\bigcup_{j \in J} F_j\Big)$.

(II) Tegyük fel, hogy I és J nem üresek. Legyen $(x, y) \in \Big(\bigcap_{i \in I} E_i\Big) \times \Big(\bigcap_{j \in J} F_j\Big)$. Ekkor $x \in \bigcap_{i \in I} E_i$ és $y \in \bigcap_{j \in J} F_j$, tehát minden $i \in I$ és $j \in J$ esetén $x \in E_i$ és $y \in F_j$, vagyis $(x, y) \in E_i \times F_j$. Ez azt jelenti, hogy $(x, y) \in \bigcap_{(i,j) \in I \times J} (E_i \times F_j)$. Megfordítva, legyen $(x, y) \in \bigcap_{(i,j) \in I \times J} (E_i \times F_j)$. Ekkor minden $i \in I$ és $j \in J$ esetén $(x, y) \in E_i \times F_j$, vagyis $x \in E_i$ és $y \in F_j$. Ez azt jelenti, hogy $x \in \bigcap_{i \in I} E_i$ és $y \in \bigcap_{j \in J} F_j$, tehát $(x, y) \in \Big(\bigcap_{i \in I} E_i\Big) \times \Big(\bigcap_{j \in J} F_j\Big)$. ■

Vigyázzunk arra, hogy ha $(E_i)_{i \in I}$ halmazrendszer, akkor nyilvánvalóan Z

$$\bigcup_{i \in I} (E_i \times E_i) \subseteq \Big(\bigcup_{i \in I} E_i\Big) \times \Big(\bigcup_{i \in I} E_i\Big),$$

de könnyen látható, hogy előfordulhat az, hogy itt nincs egyenlőség. Azonban fennáll a következő állítás.

6.9.10. Állítás. *Legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i, j \in E$ esetén $E_i \subseteq E_j$ vagy $E_j \subseteq E_i$. (Ilyenkor azt mondjuk, hogy az $(E_i)_{i\in I}$ halmazrendszer tartalmazás tekintetében* **felfelé irányított**.) *Ekkor*

$$\bigcup_{i\in I}(E_i \times E_i) = \Big(\bigcup_{i\in I} E_i\Big) \times \Big(\bigcup_{i\in I} E_i\Big).$$

Bizonyítás. Legyenek $x, y \in \bigcup_{i\in I} E_i$ tetszőlegesek, és vegyünk olyan $i_*, j_* \in I$ indexeket, amelyekre $x \in E_{i_*}$ és $y \in E_{j_*}$. A hipotézis szerint $E_{i_*} \subseteq E_{j_*}$ vagy $E_{j_*} \subseteq E_{i_*}$. Az első esetben $(x, y) \in E_{i_*} \times E_{j_*} \subseteq E_{j_*} \times E_{j_*}$. A második esetben $(x, y) \in E_{i_*} \times E_{j_*} \subseteq E_{i_*} \times E_{i_*}$. Ezért $(x, y) \in \bigcup_{i\in I}(E_i \times E_i)$, így az egyenlőség jobb oldalán álló halmaz részhalmaza a bal oldalon álló halmaznak. ■

6.9.11. Állítás. *Ha I, J halmazok, $(E_{i,j})_{(i,j)\in I\times J}$ halmazrendszer és $J \neq \emptyset$, akkor*

$$\bigcap_{j\in J}\prod_{i\in I} E_{i,j} = \prod_{i\in I}\bigcap_{j\in J} E_{i,j}.$$

Bizonyítás. Legyen $f \in \bigcap_{j\in J}\prod_{i\in I} E_{i,j}$. Ekkor minden $j \in J$ esetén $f \in \prod_{i\in I} E_{i,j}$. A hipotézis szerint $J \neq \emptyset$, tehát rögzíthetünk egy $j_* \in J$ indexet. Erre a j_* indexre is fennáll az, hogy $f \in \prod_{i\in I} E_{i,j_*}$, ezért f olyan függvény, amelyre $\mathrm{Dom}(f) = I$, és minden $i \in I$ esetén $f(i) \in E_{i,j_*}$. Az f-re vonatkozó hipotézis szerint minden $j \in J$ és $i \in I$ esetén $f(i) \in E_{i,j}$. Ez azzal ekvivalens, hogy minden $i \in I$ és $j \in J$ esetén $f(i) \in E_{i,j}$, azaz minden $I \ni i$-re $f(i) \in \bigcap_{j\in J} E_{i,j}$. Ez azt jelenti, hogy $f \in \prod_{i\in I}\bigcap_{j\in J} E_{i,j}$, amivel igazoltuk a $\bigcap_{j\in J}\prod_{i\in I} E_{i,j} \subseteq \prod_{i\in I}\bigcap_{j\in J} E_{i,j}$ összefüggést.

Megfordítva, legyen $f \in \prod_{i\in I}\bigcap_{j\in J} E_{i,j}$. Ekkor f olyan függvény, hogy $\mathrm{Dom}(f) = I$ és minden $i \in I$ esetén $f(i) \in \bigcap_{j\in J} E_{i,j}$, vagyis minden $J \ni j$-re $f(i) \in E_{i,j}$. Tehát minden $j \in J$ esetén minden $I \in i$-re $f(i) \in E_{i,j}$, így $f \in \prod_{i\in I} E_{i,j}$, vagyis $f \in \bigcap_{j\in J}\prod_{i\in I} E_{i,j}$. Ezzel megmutattuk, hogy $\prod_{i\in I}\bigcap_{j\in J} E_{i,j} \subseteq \bigcap_{j\in J}\prod_{i\in I} E_{i,j}$. ■

6.9.12. Következmény. *Ha $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ egyenlő indexhalmazú halmazrendszerek, akkor*

$$\Big(\prod_{i\in I} E_i\Big) \cap \Big(\prod_{i\in I} F_i\Big) = \prod_{i\in I}(E_i \cap F_i),$$

és ha $I \neq \emptyset$, akkor

$$\Big(\bigcap_{i\in I} E_i\Big) \times \Big(\bigcap_{i\in I} F_i\Big) = \bigcap_{i\in I}(E_i \times F_i).$$

Bizonyítás. (I) Legyen $J := \{0,1\}$ (ahol $0 := \emptyset$ és $1 := \{\emptyset\}$). Továbbá, minden $i \in I$ esetén legyen $E_{i,0} := E_i$ és $E_{i,1} = F_i$. Ekkor

$$\Big(\prod_{i\in I} E_i\Big) \cap \Big(\prod_{i\in I} F_i\Big) = \Big(\prod_{i\in I} E_{i,0}\Big) \cap \Big(\prod_{i\in I} E_{i,1}\Big) = \bigcap_{j\in J}\prod_{i\in I} E_{i,j} \overset{(*)}{=}$$
$$\overset{(*)}{=} \prod_{i\in I}\bigcap_{j\in J} E_{i,j} = \prod_{i\in I}(E_{i,0}\cap E_{i,1}) = \prod_{i\in I}(E_i \cap F_i),$$

ahol a $\overset{(*)}{=}$ egyenlőségnél kell hivatkozni az előző állításra.

(II) A második egyenlőség bebizonyítható az $I \neq \emptyset$ feltétel mellett úgy, hogy hivatkozunk az előző állításra és 6.7.6.-re. Itt egy közvetlen bizonyítást adunk.

Legyen $z \in \Big(\bigcap_{i\in I} E_i\Big) \times \Big(\bigcap_{i\in I} F_i\Big)$. Ekkor vehetünk olyan $x \in \bigcap_{i\in I} E_i$ és $y \in \bigcap_{i\in I} F_i$ elemeket, hogy $z = (x,y)$. Ha $i \in I$, akkor $x \in E_i$ és $y \in F_i$, tehát $z = (x,y) \in E_i \times F_i$, vagyis $z \in \bigcap_{i\in I}(E_i \times F_i)$. Ezzel megmutattuk, hogy $\Big(\bigcap_{i\in I} E_i\Big) \times \Big(\bigcap_{i\in I} F_i\Big) \subseteq \bigcap_{i\in I}(E_i \times F_i)$.

Megfordítva, legyen $z \in \bigcap_{i\in I}(E_i \times F_i)$, tehát minden $i \in I$ esetén $z \in E_i \times F_i$. Az $I \neq \emptyset$ feltétel miatt vehetünk egy $i_* \in I$ indexet, és erre is teljesül az, hogy $z \in E_{i_*} \times F_{i_*}$. Ebből következik, hogy z pár, tehát vehetünk olyan x és y halmazokat, hogy $z = (x,y)$. A z-re vonatkozó hipotézis szerint minden $i \in I$ esetén $(x,y) = z \in E_i \times F_i$, ezért $x \in E_i$ és $y \in F_i$, vagyis $x \in \bigcap_{i\in I} E_i$ és $y \in \bigcap_{i\in I} F_i$. Ez azt jelenti, hogy $z = (x,y) \in \Big(\bigcap_{i\in I} E_i\Big) \times \Big(\bigcap_{i\in I} F_i\Big)$. Ezzel megmutattuk, hogy $\bigcap_{i\in I}(E_i \times F_i) \subseteq \Big(\bigcap_{i\in I} E_i\Big) \times \Big(\bigcap_{i\in I} F_i\Big)$. ■

6.9.13. Állítás. *Legyen f függvény.*

a) *Ha $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ halmazrendszerek, akkor*

$$f\Big\langle\bigcup_{i\in I} E_i\Big\rangle = \bigcup_{i\in I} f\langle E_i\rangle, \qquad \overset{-1}{f}\Big\langle\bigcup_{i\in I} F_i\Big\rangle = \bigcup_{i\in I} \overset{-1}{f}\langle F_i\rangle,$$

és ha $I \neq \emptyset$, akkor

$$f\Big\langle\bigcap_{i\in I} E_i\Big\rangle \subseteq \bigcap_{i\in I} f\langle E_i\rangle, \qquad \overset{-1}{f}\Big\langle\bigcap_{i\in I} F_i\Big\rangle = \bigcap_{i\in I} \overset{-1}{f}\langle F_i\rangle.$$

b) *Ha f injektív, $(E_i)_{i\in I}$ halmazrendszer, és $I \neq \emptyset$, akkor*

$$f\Big\langle\bigcap_{i\in I} E_i\Big\rangle = \bigcap_{i\in I} f\langle E_i\rangle.$$

c) *Ha F és Y halmazok, akkor*

$$\overset{-1}{f}\langle F \setminus Y\rangle = \overset{-1}{f}\langle F\rangle \setminus \overset{-1}{f}\langle Y\rangle,$$

továbbá, ha E és X halmazok, akkor

$$f\langle E\rangle \setminus f\langle X\rangle \subseteq f\langle E \setminus X\rangle,$$

d) *Ha f injektív és E és X halmazok, akkor*

$$f\langle E\rangle \setminus f\langle X\rangle = f\langle E \setminus X\rangle.$$

Bizonyítás. a) Legyen $y \in f\Big\langle \bigcup_{i\in I} E_i \Big\rangle$. Ekkor vehetünk olyan $x \in \mathrm{Dom}(f)$ elemet, amelyre $x \in \bigcup_{i\in I} E_i$ és $f(x) = y$. Rögzítsünk olyan $i_* \in I$ indexet, amelyre $x \in E_{i_*}$. Világos, hogy $y = f(x) \in f\langle E_{i_*}\rangle$, ezért $y \in \bigcup_{i\in I} f\langle E_i\rangle$. Megfordítva, legyen $y \in \bigcup_{i\in I} f\langle E_i\rangle$, és vegyünk olyan $i_* \in I$ indexet, hogy $y \in f\langle E_{i_*}\rangle$. Ekkor rögzíthetünk olyan $x \in \mathrm{Dom}(f)$ elemet, hogy $x \in E_{i_*}$ és $y = f(x)$. Világos, hogy $x \in \bigcup_{i\in I} E_i$, ezért $y = f(x) \in f\Big\langle \bigcup_{i\in I} E_i \Big\rangle$. Ezzel megmutattuk, hogy $\bigcup_{i\in I} f\langle E_i\rangle = f\Big\langle \bigcup_{i\in I} E_i \Big\rangle$.

Legyen $x \in \overset{-1}{f}\Big\langle \bigcup_{i\in I} F_i \Big\rangle$. Ekkor $x \in \mathrm{Dom}(f)$ és $f(x) \in \bigcup_{i\in I} F_i$, tehát vehetünk olyan $i_* \in I$ indexet, hogy $f(x) \in F_{i_*}$. Ez azt jelenti, hogy $x \in \overset{-1}{f}\langle F_{i_*}\rangle \subseteq \bigcup_{i\in I} \overset{-1}{f}\langle F_i\rangle$, tehát $x \in \bigcup_{i\in I} \overset{-1}{f}\langle F_i\rangle$. Megfordítva, legyen $x \in \bigcup_{i\in I} \overset{-1}{f}\langle F_i\rangle$ és vegyünk olyan $i_* \in I$ indexet, hogy $x \in \overset{-1}{f}\langle F_{i_*}\rangle$. Ekkor $x \in \mathrm{Dom}(f)$ és $f(x) \in F_{i_*} \subseteq \bigcup_{i\in I} F_i$, így $x \in \overset{-1}{f}\Big\langle \bigcup_{i\in I} F_i \Big\rangle$. Ezzel megmutattuk, hogy $\overset{-1}{f}\Big\langle \bigcup_{i\in I} F_i \Big\rangle = \bigcup_{i\in I} \overset{-1}{f}\langle F_i\rangle$.

Tegyük fel, hogy $I \neq \emptyset$.

Legyen $y \in f\Big\langle \bigcap_{i\in I} E_i \Big\rangle$. Ekkor vehetünk olyan $x \in \mathrm{Dom}(f)$ elemet, hogy $x \in \bigcap_{i\in I} E_i$ és $f(x) = y$. Ha $i \in I$ tetszőleges, akkor $x \in E_i$ és $x \in \mathrm{Dom}(f)$, ezért $f(x) \in f\langle E_i\rangle$, így $y = f(x) \in \bigcap_{i\in I} f\langle E_i\rangle$. Ezzel megmutattuk, hogy $f\Big\langle \bigcap_{i\in I} E_i \Big\rangle \subseteq \bigcap_{i\in I} f\langle E_i\rangle$.

Legyen $x \in \overset{-1}{f}\Big\langle \bigcap_{i\in I} F_i \Big\rangle$. Ekkor $x \in \mathrm{Dom}(f)$ és $f(x) \in \bigcap_{i\in I} F_i$, tehát minden $i \in I$ esetén $f(x) \in F_i$. Ez azt jelenti, hogy minden $I \ni i$-re $x \in \overset{-1}{f}\langle F_i\rangle$, vagyis $x \in \bigcap_{i\in I} \overset{-1}{f}\langle F_i\rangle$. Megfordítva, ha $x \in \bigcap_{i\in I} \overset{-1}{f}\langle F_i\rangle$, akkor minden $i \in I$ esetén $x \in \overset{-1}{f}\langle F_i\rangle$, vagyis $x \in \mathrm{Dom}(f)$ és $f(x) \in F_i$. Az $I \neq \emptyset$ feltétel alapján rögzíthetünk egy $i_* \in I$ indexet, és erre is teljesül az, hogy $x \in \overset{-1}{f}\langle F_{i_*}\rangle$, ezért $x \in \mathrm{Dom}(f)$. Tehát $x \in \mathrm{Dom}(f)$ és minden $i \in I$ esetén $f(x) \in F_i$, vagyis $f(x) \in \bigcap_{i\in I} F_i$. Ez azt jelenti, hogy $x \in \overset{-1}{f}\Big\langle \bigcap_{i\in I} F_i \Big\rangle$. Ezzel megmutattuk, hogy $\overset{-1}{f}\Big\langle \bigcap_{i\in I} F_i \Big\rangle = \bigcap_{i\in I} \overset{-1}{f}\langle F_i\rangle$.

b) Legyen $y \in \bigcap_{i\in I} f\langle E_i\rangle$, tehát minden $i \in I$ esetén $y \in f\langle E_i\rangle$, vagyis minden $i \in I$ indexhez van olyan $x \in \mathrm{Dom}(f)$, hogy $x \in E_i$ és $y = f(x)$. Az $I \neq \emptyset$ feltétel alapján rögzíthetünk egy $i_* \in I$ indexet, és ehhez vehetünk olyan $x_* \in \mathrm{Dom}(f)$ elemet, hogy $x_* \in E_i$ és $y = f(x_*)$. Ha $i \in I$ tetszőleges, akkor van olyan $x \in \mathrm{Dom}(f)$, hogy $x \in E_i$ és $f(x) = y = f(x_*)$, így az f injektivitása miatt $x = x_*$, tehát $x_* \in E_i$. Ez azt jelenti, hogy $x_* \in \mathrm{Dom}(f)$ és $x_* \in \bigcap_{i \in I} E_i$, valamint $y = f(x_*)$, tehát $y \in f\left\langle \bigcap_{i \in I} E_i \right\rangle$. Ezzel megmutattuk, hogy $\bigcap_{i \in I} f\langle E_i \rangle \subseteq f\left\langle \bigcap_{i \in I} E_i \right\rangle$, tehát az a) állítás alapján $f\left\langle \bigcap_{i \in I} E_i \right\rangle = \bigcap_{i \in I} f\langle E_i \rangle$.

c) Legyen $x \in \overset{-1}{f}\langle F \setminus Y \rangle$. Ekkor $x \in \mathrm{Dom}(f)$ és $f(x) \in F \setminus Y$, vagyis $f(x) \in F$ és $f(x) \notin Y$. Ekkor $x \in \overset{-1}{f}\langle F \rangle$ és $x \notin \overset{-1}{f}\langle Y \rangle$, vagyis $x \in \overset{-1}{f}\langle F \rangle \setminus \overset{-1}{f}\langle Y \rangle$. Megfordítva, tegyük fel, hogy $x \in \overset{-1}{f}\langle F \rangle \setminus \overset{-1}{f}\langle Y \rangle$. Ekkor $x \in \overset{-1}{f}\langle F \rangle$, tehát $x \in \mathrm{Dom}(f)$ és $f(x) \in F$, valamint $x \notin \overset{-1}{f}\langle Y \rangle$, így $f(x) \notin Y$. Ezért $x \in \mathrm{Dom}(f)$ és $f(x) \in F \setminus Y$, ami azt jelenti, hogy $x \in \overset{-1}{f}\langle F \rangle \setminus \overset{-1}{f}\langle Y \rangle$.

Legyen $y \in f\langle E \rangle \setminus f\langle X \rangle$, vagyis $y \in f\langle E \rangle$ és $y \notin f\langle X \rangle$. Vegyünk olyan $x \in \mathrm{Dom}(f)$ elemet, amelyre $x \in \mathrm{Dom}(f)$ és $x \in E$, valamint $y = f(x)$. Ekkor $x \notin X$, különben $x \in \mathrm{Dom}(f)$, $x \in X$ és $y = f(x)$ miatt $y \in f\langle X \rangle$ teljesülne. Ez azt jelenti, hogy $x \in \mathrm{Dom}(f)$ és $x \in E \setminus X$, valamint $y = f(x)$, tehát $y \in f\langle E \setminus X \rangle$. Ezzel megmutattuk, hogy $f\langle E \rangle \setminus f\langle X \rangle \subseteq f\langle E \setminus X \rangle$.

d) Tegyük fel, hogy f injektív és legyen $y \in f\langle E \setminus X \rangle$. Vegyünk olyan $x \in \mathrm{Dom}(f)$ elemet, amelyre $x \in E \setminus X$ és $y = f(x)$. Ekkor $x \in \mathrm{Dom}(f)$, $x \in E$ és $y = f(x)$, ezért $y \in f\langle E \rangle$. Ha $y \in f\langle X \rangle$ teljesülne, akkor létezne olyan $x' \in \mathrm{Dom}(f)$, hogy $x' \in X$ és $y = f(x')$, tehát az f injektivitása folytán $x = x' \in X$, holott $x \notin X$. Ezért $y \in f\langle E \rangle \setminus f\langle X \rangle$. Ezzel megmutattuk, hogy $f\langle E \setminus X \rangle \subseteq f\langle E \rangle \setminus f\langle X \rangle$, tehát a c) állítás alapján $f\langle E \rangle \setminus f\langle X \rangle = f\langle E \setminus X \rangle$. ■

6.10. Rendezések és ekvivalenciák

6.10.1. Definíció. *Legyen R reláció.*

– R **szimmetrikus**, *ha*

$$(\forall x)(\forall y)(((x, y) \in R) \Rightarrow ((y, x) \in R)),$$

ahol az x és y változók nem szerepelnek R-ben.

– R **antiszimmetrikus**, *ha*

$$(\forall x)(\forall y)(((x, y) \in R) \wedge ((y, x) \in R)) \Rightarrow x = y),$$

ahol az x és y változók nem szerepelnek R-ben.

– R **tranzitív**, *ha*

$$(\forall x)(\forall y)(\forall z)(((x, y) \in R) \wedge ((y, z) \in R)) \Rightarrow ((x, z) \in R)),$$

ahol az x, y és z változók nem szerepelnek R-ben.

– R **reflexív** *az E halmazon, ha*

$$(\forall x)((x \in E) \Rightarrow ((x, x) \in R)),$$

ahol az x változó nem szerepel R-ben.

– R **trichotóm** *az E halmazon, ha*

$$(\forall x)(\forall y)(((x \in E) \wedge (y \in E)) \Rightarrow (((x, y) \in R) \vee ((y, x) \in R))),$$

ahol az x és y változók nem szerepelnek R-ben.

6.10.2. Definíció. *Ha R reláció és E halmaz, akkor az*

$$R \cap (E \times E)$$

halmazt az R reláció E halmazra vett **megszorításának** *nevezzük. Azt mondjuk, hogy R* **reláció az E halmaz felett**, *ha $R \subseteq E \times E$ (vagyis az R reláció E halmazra vett megszorítása egyenlő R-rel).*

Könnyen látható, hogy szimmetrikus (ill. antiszimmetrikus, ill. tranzitív) reláció megszorítása bármely halmazra szintén szimmetrikus (ill. antiszimmetrikus, ill. tranzitív) reláció. Ha az R reláció reflexív (ill. trichotóm) az E halmazon, akkor az R megszorítása az E bármely részhalmazára szintén reflexív (ill. trichotóm) reláció a részhalmazon.

6.10.3. Állítás. *Legyen R reláció.*

a) *R pontosan akkor szimmetrikus, ha $\overset{-1}{R} = R$.*

b) *R pontosan akkor antiszimmetrikus, ha $R \cap \overset{-1}{R} \subseteq \mathrm{id}_{\mathrm{pr}_1 R}$.*

c) *R pontosan akkor tranzitív, ha $R \circ R \subseteq R$.*

d) *R pontosan akkor reflexív az E halmazon, ha $\mathrm{id}_E \subseteq R$.*

Bizonyítás. a) Az $\overset{-1}{R} = R$ kijelentés azzal ekvivalens, hogy minden x-re és minden y-ra $((x, y) \in R) \Leftrightarrow ((y, x) \in R)$. Ez utóbbi állítás egyenértékű az R reláció szimmetrikusságával.

b) Az $(x, y) \in R \cap \overset{-1}{R}$ kijelentés azzal ekvivalens, hogy $((x, y) \in R) \wedge ((y, x) \in R)$. Tehát ha R antiszimmetrikus, akkor $(x, y) \in R \cap \overset{-1}{R}$ esetén $x = y$, így $(x, y) \in \mathrm{id}_{\mathrm{pr}_1 R}$. Megfordítva, ha $R \cap \overset{-1}{R} \subseteq \mathrm{id}_{\mathrm{pr}_1 R}$ és $((x, y) \in R) \wedge ((y, x) \in R)$, akkor $(x, y) \in \mathrm{id}_{\mathrm{pr}_1 R}$, ezért $x = y$, vagyis R antiszimmetrikus.

c) Ha $(x, y) \in R \circ R$, akkor van olyan z, hogy $(x, z) \in R$ és $(z, y) \in R$, így R tranzitivitásából $(x, y) \in R$ következik, tehát ha R tranzitív, akkor $R \circ R \subseteq R$. Megfordítva, ha $R \circ R \subseteq R$, akkor $(x, y) \in R$ és $(y, z) \in R$ esetén $(x, z) \in R \circ R \subseteq R$, vagyis R tranzitív.

d) Világos, hogy $(x, y) \in \mathrm{id}_E$ esetén $x \in E$ és $x = y$, tehát ha R reflexív az E halmazon, akkor az $(x, y) \in \mathrm{id}_E$ állításból $(x, y) = (x, x) \in R$ következik, vagyis $\mathrm{id}_E \subseteq R$. Megfordítva, ha $\mathrm{id}_E \subseteq R$ és $x \in E$, akkor $(x, x) \in \mathrm{id}_E \subseteq R$, tehát R reflexív az E halmazon. ■

6.10.4. Definíció. *Ha E és F halmazok, $f : E \to F$ függvény és S reláció F felett, akkor*

$$f_*(S) \ := \ \{ \ (x, y) \in E \times E \mid (f(x), f(y)) \in S \ \}.$$

6.10.5. Állítás. *Legyenek E és F halmazok, $f : E \to F$ függvény és S reláció az F halmaz felett.*

a) *Ha az S reláció szimmetrikus (illetve tranzitív), akkor az $f_*(S)$ reláció is szimmetrikus (illetve tranzitív).*

b) *Ha az S reláció reflexív (illetve trichotóm) az* $\mathrm{Im}(f)$ *halmazon, akkor az $f_*(S)$ reláció reflexív (illetve trichotóm) az E halmazon.*

c) *Ha az S reláció antiszimmetrikus és f injektív, akkor az $f_*(S)$ reláció is antiszimmetrikus.*

Bizonyítás. a) Ha S szimmetrikus és $(x, y) \in f_*(S)$, akkor $(f(x), f(y)) \in S$, tehát $(f(y), f(x)) \in S$, ezért $(y, x) \in f_*(S)$, tehát $f_*(S)$ szimmetrikus. Ha S tranzitív és $(x, y) \in\in f_*(S)$ és $(y, z) \in f_*(S)$, akkor $(f(x), f(y)) \in S$ és $(f(y), f(z)) \in S$, ezért $(f(x), f(z)) \in S$, vagyis $(x, z) \in f_*(S)$, tehát $f_*(S)$ tranzitív.

b) Ha S reflexív az $\mathrm{Im}(f)$ halmazon, akkor minden $x \in E$ esetén $(f(x), f(x)) \in S$, ezért $(x, x) \in f_*(S)$, tehát $f_*(S)$ reflexív az E halmazon. Ha S trichotóm az $\mathrm{Im}(f)$ halmazon, akkor minden $x, y \in E$ esetén $(f(x), f(y)) \in S$ vagy $(f(y), f(x)) \in S$, ezért $(x, y) \in f_*(S)$ vagy $(y, x) \in f_*(S)$, tehát $f_*(S)$ trichotóm az E halmazon.

c) Ha S antiszimmetrikus és f injektív, valamint $x, y \in E$ olyanok, hogy $(x, y) \in f_*(S)$ és $(y, x) \in f_*(S)$, akkor $(f(x), f(y)) \in S$ és $(f(y), f(x)) \in S$, ezért $f(x) = f(y)$, így $x = y$, tehát az $f_*(S)$ reláció is antiszimmetrikus. ■

6.10.6. Definíció. *Azt mondjuk, hogy az R reláció* **ekvivalencia az E halmaz felett***, ha $R \subseteq E \times E$ és R szimmetrikus, tranzitív és reflexív az E halmazon. Azt mondjuk, hogy az R reláció* **rendezés az E halmaz felett***, ha $R \subseteq E \times E$ és R antiszimmetrikus, tranzitív és reflexív az E halmazon. Azt mondjuk, hogy az R reláció* **lineáris rendezés az E halmaz felett***, ha R olyan rendezés az E halmaz felett, amely trichotóm az E halmazon.*

A 6.10.5. állítás a) és b) pontja szerint nyilvánvaló, hogy ha E és F halmazok, $f : E \to F$ függvény és S ekvivalencia F felett, akkor $f_*(S)$ ekvivalencia E felett. A 6.10.5. állítás c) pontja szerint nyilvánvaló, hogy ha E és F halmazok, $f : E \to F$ injektív függvény és S rendezés (illetve lineáris rendezés) F felett, akkor $f_*(S)$ rendezés (illetve lineáris rendezés) E felett.

Példák. 1) Ha E halmaz, akkor az

$$=_E := \{(x, y) | (x \in E) \wedge (y \in E) \wedge (x = y)\}$$

reláció ekvivalencia az E halmaz felett; ezt nevezzük az E feletti *egyenlőség-relációnak*. Ez a reláció egyben rendezés is E felett.

2) Ha E halmaz, akkor az

$$\approx_E := \{(x, y) | (x \in E) \wedge (y \in E) \wedge (\text{"}x \text{ ekvipotens } y\text{-nal"})\}$$

reláció ekvivalencia az E halmaz felett; ezt nevezzük az E feletti *ekvipotencia-relációnak*.

3) Ha E halmaz, akkor az

$$\subseteq_E := \{(x, y) | (x \in E) \wedge (y \in E) \wedge (x \subseteq y)\}$$

reláció rendezés az E halmaz felett; ezt nevezzük az E feletti *tartalmazás-relációnak*.

4) Ha E halmaz, akkor az

$$\{(x,y)|(x \in E) \wedge (y \in E) \wedge (x \text{ kisebb-egyenlő számosságú } y\text{-nál})\}$$

reláció tranzitív és reflexív az E halmazon, de általában nem rendezés és nem ekvivalencia az E halmaz felett.

5) Ha E halmaz, akkor az

$$\in_E := \{(x,y)|(x \in E) \wedge (y \in E) \wedge (x \in y)\}$$

relációt az E feletti *elem-relációnak* nevezzük.

6.10.7. Állítás. *Legyen $(R_i)_{i\in I}$ relációk tetszőleges rendszere.*

a) *Ha minden $i \in I$ esetén az R_i reláció szimmetrikus, akkor az $\bigcup_{i\in I} R_i$ reláció is szimmetrikus.*

b) *Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén az R_i reláció reflexív az E_i halmazon, akkor az $\bigcup_{i\in I} R_i$ reláció reflexív az $\bigcup_{i\in I} E_i$ halmazon.*

c) *Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén az R_i reláció trichotóm az E_i halmazon, és teljesül az, hogy minden $i,j \in E$ esetén $E_i \subseteq E_j$ vagy $E_j \subseteq E_i$, akkor az $\bigcup_{i\in I} R_i$ reláció trichotóm az $\bigcup_{i\in I} E_i$ halmazon.*

Bizonyítás. Legyen $R := \bigcup_{i\in I} R_i$ és $E := \bigcup_{i\in I} E_i$.

a) Tegyük fel, hogy minden $i \in I$ esetén az R_i reláció szimmetrikus. Ha $(x,y) \in R$, akkor van olyan $i \in I$, hogy $(x,y) \in R_i$, ezért R_i szimmetrikussága miatt $(y,x) \in R_i \subseteq R$, tehát R is szimmetrikus reláció.

b) Tegyük fel, hogy hogy minden $i \in I$ esetén az R_i reláció reflexív az E_i halmazon. Ha $x \in E$, akkor van olyan $i \in I$, hogy $x \in E_i$, és mivel R_i reflexív az E_i halmazon, így $(x,x) \in R_i \subseteq R$. Tehát az R reláció reflexív az E halmazon.

c) Tegyük fel, hogy hogy minden $i \in I$ esetén az R_i reláció trichotóm az E_i halmazon, és teljesül az, hogy minden $i,j \in E$ esetén $E_i \subseteq E_j$ vagy $E_j \subseteq E_i$. Legyenek $x,y \in E$ tetszőlegesek. Ekkor léteznek olyan $i,j \in I$ indexek, hogy $x \in E_i$ és $y \in E_j$. Ha $E_i \subseteq E_j$, akkor $x,y \in E_j$ és R_j trichotóm az E_j halmazon, ezért $(x,y) \in R_j \subseteq R$ vagy $(y,x) \in R_j \subseteq R$. Ha $E_j \subseteq E_i$, akkor $x,y \in E_i$ és R_i trichotóm az E_i halmazon, ezért $(x,y) \in R_i \subseteq R$ vagy $(y,x) \in R_i \subseteq R$. Tehát ekkor $(x,y) \in R$ vagy $(y,x) \in R$, ami azt jelenti, hogy az R reláció trichotóm az E halmazon. ■

6.10.8. Állítás. *Legyen $(R_i)_{i\in I}$ relációk olyan rendszere, hogy minden $i,j \in I$ esetén $R_i \subseteq R_j$ vagy $R_j \subseteq R_i$. Ha minden $i \in I$ esetén az R_i reláció antiszimmetrikus (illetve tranzitív), akkor az $\bigcup_{i\in I} R_i$ reláció is antiszimmetrikus (illetve tranzitív).*

Bizonyítás. Legyen $R := \bigcup_{i\in I} R_i$.

Tegyük fel, hogy minden $i \in I$ esetén az R_i reláció antiszimmetrikus, és legyenek $(x,y) \in R$ és $(y,x) \in R$. Léteznek olyan $i,j \in I$ indexek, hogy $(x,y) \in R_i$ és $(y,x) \in R_j$. A hipotézis szerint $R_i \subseteq R_j$ vagy $R_j \subseteq R_i$. Ha $R_i \subseteq R_j$, akkor $(x,y) \in R_i \subseteq R_j$ és

$(y,x) \in R_j$, így R_j antiszimmetrikussága miatt $x = y$. Ha $R_j \subseteq R_i$, akkor $(x,y) \in R_i$ és $(y,x) \in R_j \subseteq R_i$, így R_i antiszimmetrikussága miatt $x = y$. Tehát az R reláció antiszimmetrikus.

Tegyük fel, hogy minden $i \in I$ esetén az R_i reláció tranzitív, és legyenek $(x,y) \in R$ és $(y,z) \in R$. Léteznek olyan $i, j \in I$ indexek, hogy $(x,y) \in R_i$ és $(y,z) \in R_j$. A hipotézis szerint $R_i \subseteq R_j$ vagy $R_j \subseteq R_i$. Ha $R_i \subseteq R_j$, akkor $(x,y) \in R_i \subseteq R_j$ és $(y,z) \in R_j$, így R_j tranzitivitása miatt $(x,z) \in R_j \subseteq R$. Ha $R_j \subseteq R_i$, akkor $(x,y) \in R_i$ és $(y,z) \in R_j \subseteq R_i$, így R_i tranzitivitása miatt $(x,z) \in R_i \subseteq R$. Tehát az R reláció tranzitív. ■

6.10.9. Állítás. (**Rendezések és ekvivalenciák összeragasztása**) *Legyen $(R_i)_{i\in I}$ relációk olyan rendszere, hogy minden $i, j \in I$ esetén $R_i \subseteq R_j$ vagy $R_j \subseteq R_i$. Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén az R_i reláció ekvivalencia (illetve rendezés, illetve lineáris rendezés) az E_i halmaz felett, akkor az $\bigcup\limits_{i\in I} R_i$ reláció ekvivalencia (illetve rendezés, illetve lineáris rendezés) az $\bigcup\limits_{i\in I} E_i$ halmaz felett.*

Bizonyítás. Először megjegyezzük, hogy bármelyik hipotézis alapján teljesül az, hogy minden $i \in I$ esetén $R_i \subseteq E_i \times E_i$, ezért nyilvánvaló, hogy

$$\bigcup_{i\in I} R_i \subseteq \bigcup_{i\in I} (E_i \times E_i) \subseteq \Big(\bigcup_{i\in I} E_i\Big) \times \Big(\bigcup_{i\in I} E_i\Big).$$

Továbbá, minden $i \in I$ esetén R_i reflexív az E_i halmazon és $R_i \subseteq E_i \times E_i$, így $E_i = \mathrm{pr}_1 R_i$, tehát az $(R_i)_{i\in I}$ reláció-rendszerre vonatkozó feltevés alapján $i, j \in I$ esetén $R_i \subseteq R_j$, ezért $E_i = \mathrm{pr}_1 R_i \subseteq \mathrm{pr}_1 R_j = E_j$ vagy $R_j \subseteq R_i$, ezért $E_j = \mathrm{pr}_1 R_j \subseteq \mathrm{pr}_1 R_i = E_i$. Ez azt jelenti, hogy bármelyik hipotézis esetén az $(E_i)_{i\in I}$ halmazrendszer tartalmazás tekintetében felfelé irányított (6.9.10.).

Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén az R_i reláció ekvivalencia E_i felett, akkor minden $i \in I$ esetén R_i szimmetrikus, tranzitív és reflexív az E_i halmazon, így 6.10.7. a) és b), valamint 6.10.8. alapján az $\bigcup\limits_{i\in I} R_i$ reláció szimmetrikus, tranzitív, és reflexív az $\bigcup\limits_{i\in I} E_i$ halmazon. Ezért ekkor az $\bigcup\limits_{i\in I} R_i$ reláció ekvivalencia az $\bigcup\limits_{i\in I} E_i$ halmaz felett.

Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén az R_i reláció rendezés (illetve lineáris rendezés) E_i felett, akkor minden $i \in I$ esetén R_i antiszimmetrikus, tranzitív és reflexív (illetve reflexív és trichotóm) az E_i halmazon, így 6.10.8., valamint 6.10.7. b) és c) alapján az $\bigcup\limits_{i\in I} R_i$ reláció antiszimmetrikus, tranzitív és reflexív (illetve reflexív és trichotóm) az $\bigcup\limits_{i\in I} E_i$ halmazon. Ezért ekkor az $\bigcup\limits_{i\in I} R_i$ reláció rendezés (illetve lineáris rendezés) az $\bigcup\limits_{i\in I} E_i$ halmaz felett. ■

Jelölés. Az ekvivalenciákra és rendezésekre gyakran speciális infix jelölést alkalmazunk.

– Az ekvivalenciákat gyakran a $\approx$ szimbólummal jelöljük, és ha $\approx$ ekvivalencia az E halmaz felett, akkor $x, y \in E$ esetén $(x,y) \in \approx$ helyett azt írjuk, hogy $x \approx y$.

– A rendezéseket gyakran a $\leq$ szimbólummal jelöljük, és ha $\leq$ rendezés az E halmaz felett, akkor $x, y \in E$ esetén $(x,y) \in \leq$ helyett azt írjuk, hogy $x \leq y$.

6.11. Faktorhalmazok és függvények faktorizációja

6.11.1. Definíció. *Ha $\approx$ evivalencia az E halmaz felett, akkor $\approx$ szerinti* **ekvivalencia-osztálynak** *nevezünk minden olyan $X \subseteq E$ halmazt, amelyre teljesülnek az alábbiak.*

a) *$X \neq \emptyset$ és minden $x, x' \in X$ elemre $x \approx x'$.*

b) *Minden $x \in X$ és $x' \in E$ elemre, ha $x \approx x'$, akkor $x' \in X$.*

6.11.2. Állítás. *Legyen $\approx$ evivalencia az E halmaz felett.*

a) *Ha X és X' ekvivalencia-osztályok $\approx$ szerint és $X \cap X' \neq \emptyset$, akkor $X = X'$.*

b) *Minden $x \in E$ elemhez létezik egyetlen olyan X ekvivalencia-osztály $\approx$ szerint, hogy $x \in X$; ez a halmaz egyenlő az $\{x' \in E | x \approx x'\}$ halmazzal.*

c) *Az "X ekvivalencia-osztály $\approx$ szerint" kijelentés kollektivizáló az X változóban.*

d) *Vezessük be az $E/\approx := \{X | X$ ekvivalencia-osztály $\approx$ szerint $\}$ jelölést. Ekkor az $\{(x, X) | (X \in E/\approx) \wedge (x \in X)\}$ halmaz olyan E-n értelmezett, $E/\approx$-ba érkező függvény, amely ráképez $E/\approx$-ra.*

Bizonyítás. a) Legyenek X és X' ekvivalencia-osztályok $\approx$ szerint és tegyük fel, hogy $X \cap X' \neq \emptyset$. Legyen $z \in X \cap X'$ tetszőlegesen rögzített elem. Ha $x \in X$, akkor $z \in X$ miatt $x \approx z$. Ekkor $z \approx x$ is teljesül és $z \in X'$, ezért $x \in X'$. Ez azt jelenti, hogy $X \subseteq X'$. Felcserélve X-t és X'-t, valamint x-t es x'-t; az előző érvelés azt adja, hogy $X' \subseteq X$, tehát a meghatározottsági axióma alapján $X = X'$.

b) Legyen $x \in E$ és tekintsük az $X := \{x' | (x' \in E) \wedge (x \approx x')\}$ halmazt. Világos, hogy $X \subseteq E$ olyan halmaz, hogy $x \in X$, mivel a $\approx$ reláció reflexív az E halmazon. Ha $x', x'' \in X$, akkor $x \approx x'$ és $x \approx x''$, tehát $\approx$ szimmetrikussága és tranzitivitása folytán $x' \approx x''$. Ha $x' \in E$, $x'' \in X$ és $x' \approx x''$, akkor $x \approx x''$, tehát ismét az $\approx$ reláció szimmetrikussága és tranzitivitása miatt $x \approx x'$, így $x' \in X$. Ez azt jelenti, hogy X ekvivalencia-osztály $\approx$ szerint és $x \in X$. Ha X' is ekvivalencia-osztály $\approx$ szerint és $x \in X'$, akkor $x \in X \cap X'$, tehát az a) alapján $X = X'$.

c) Ha X ekvivalencia-osztály $\approx$ szerint, akkor $X \in \mathscr{P}(E)$, tehát a részhalmaz axióma alapján c) teljesül.

d) Legyen $F := \{(x, X) | (X \in E/\approx) \wedge (x \in X)\}$. Ha $(x, X), (x, X') \in F$, akkor X és X' olyan ekvivalencia-osztályok $\approx$ szerint, hogy $x \in X \cap X'$, tehát az a) szerint $X = X'$. Ezért F függvény és b) következtében $\mathrm{pr}_1\langle F\rangle$ ($= \mathrm{Dom}(F)$) egyenlő E-vel és c) alapján nyilvánvaló, hogy $\mathrm{pr}_2\langle F\rangle$ ($= \mathrm{Im}(F)$) egyenlő az összes $\approx$ szerinti ekvivalencia-osztályok halmazával, vagyis $E/\approx$-mal. ■

6.11.3. Definíció. *Legyen $\approx$ ekvivalencia E felett. Ekkor*

$$E/\approx := \{X | X \text{ ekvivalencia-osztály } \approx \text{ szerint}\},$$

és ezt a halmazt az E halmaz $\approx$ ekvivalencia szerinti **faktorhalmazának** *nevezzük. Minden $x \in E$ esetén az x elem $\approx$ szerinti ekvivalencia-osztályát a $\underset{\approx}{\mathrm{Class}}(x)$ szimbólummal jelöljük, vagyis $\underset{\approx}{\mathrm{Class}}(x) := \{x' \in E | x \approx x'\}$, továbbá a*

$$\pi_{E/\approx} : E \to E/\approx; \quad x \mapsto \underset{\approx}{\mathrm{Class}}(x)$$

függvényt az E és $E/\approx$ halmazok közötti **kanonikus szürjekciónak** *nevezzük.*

6.11.4. Állítás. *Legyen f függvény, és*

$$\mathrm{R}_f \ := \ \{\ (x,x') \in \mathrm{Dom}(f) \times \mathrm{Dom}(f) \mid f(x) = f(x')\ \}.$$

Ekkor R_f *ekvivalencia a* $\mathrm{Dom}(f)$ *halmaz felett és létezik egyetlen olyan* $\dot{f} : \mathrm{Dom}(f)/\mathrm{R}_f \to \mathrm{Im}(f)$ *függvény, amelyre* $\dot{f} \circ \pi_{\mathrm{Dom}(f)/\mathrm{R}_f} = f$*, vagyis a következő diagram kommutatív:*

$$\begin{tikzcd} \mathrm{Dom}(f)/\mathrm{R}_f \arrow[r, "\dot{f}"] & \mathrm{Im}(f) \\ \mathrm{Dom}(f) \arrow[u, "\pi_{\mathrm{Dom}(f)/\mathrm{R}_f}"] \arrow[ur, "f"'] & \end{tikzcd}$$

Az $\dot{f}$ *függvény bijekció a* $\mathrm{Dom}(f)/\mathrm{R}_f$ *faktorhalmaz és* $\mathrm{Im}(f)$ *között.*

Bizonyítás. Az R_f reláció triviálisan reflexív a $\mathrm{Dom}(f)$ halmaz felett, és szimmetrikus is, mert a logikai egyenlőség szimmetrikus. Ha $(x,x') \in \mathrm{R}_f$ és $(x',x'') \in \mathrm{R}_f$, akkor $f(x) = f(x')$ és $f(x') = f(x'')$, így a logikai egyenlőség tranzitivitása miatt $f(x) = f(x'')$, vagyis $(x,x'') \in \mathrm{R}_f$, tehát a R_f reláció tranzitív. Ez azt jelenti, hogy R_f ekvivalencia $\mathrm{Dom}(f)$ felett.

Ha $g, g' : \mathrm{Dom}(f)/\mathrm{R}_f \to \mathrm{Im}(f)$ mindketten olyan függvények, hogy $g \circ \pi_{\mathrm{Dom}(f)/\mathrm{R}_f} = f = g' \circ \pi_{\mathrm{Dom}(f)/\mathrm{R}_f}$, akkor a $\pi_{\mathrm{Dom}(f)/\mathrm{R}_f} : \mathrm{Dom}(f)/\mathrm{R}_f \to \mathrm{Im}(f)$ függvény szürjektivitása folytán $g = g'$, vagyis az $\dot{f}$ függvény egyértelmű. Az $\dot{f}$ függvény létezésének bizonyításához tekintsük a

$$F \ := \ \{\ (\xi, y) \mid (\xi \in \mathrm{Dom}(f)/\mathrm{R}_f) \wedge (\exists x \in \xi)\ y = f(x)\ \}$$

halmazt. Az F halmaz minden eleme pár, tehát F reláció. Ha $(\xi, y), (\xi, y') \in F$, akkor vehetünk olyan $x \in \xi$ elemet, hogy $y = f(x)$, és vehetünk olyan $x' \in \xi$ elemet, hogy $y' = f(x')$. Ekkor $x, x' \in \xi$ miatt $(x,x') \in \mathrm{R}_f$, hiszen ξ ekvivalenciaosztály R_f szerint, következésképpen $y = f(x) = f(x') = y'$. Ez azt jelenti, hogy F függvényreláció. Világos, hogy $\mathrm{Dom}(F) = \mathrm{pr}_1\langle F\rangle \subseteq \mathrm{Dom}(f)/\mathrm{R}_f$. Ha $\xi \in \mathrm{Dom}(f)/\mathrm{R}_f$, akkor $\xi \neq \emptyset$ alapján véve tetszőleges $x \in \xi$ elemet kapjuk, hogy $(\xi, f(x)) \in F$, tehát $\mathrm{Dom}(f)/\mathrm{R}_f \subseteq \mathrm{Dom}(F)$. Ezért $\mathrm{Dom}(F) = \mathrm{Dom}(f)/\mathrm{R}_f$, és $y \in \mathrm{Im}(F)$ esetén van olyan $\xi \in \mathrm{Dom}(f)/\mathrm{R}_f$, hogy $(\xi, y) \in F$, tehát van olyan $x \in \xi$, hogy $y = f(x)$, így $F(\xi) = y = f(x) \in \mathrm{Im}(f)$. Ez azt jelenti, hogy $\mathrm{Im}(F) \subseteq \mathrm{Im}(f)$, vagyis $F : \mathrm{Dom}(f)/\mathrm{R}_f \to \mathrm{Im}(f)$ függvény.

Ha $x \in \mathrm{Dom}(f)$, akkor $\xi := \pi_{\mathrm{Dom}(f)/\mathrm{R}_f}(x)$ olyan, hogy $\xi \in \mathrm{Dom}(f)/\mathrm{R}_f$ és $x \in \xi$, ezért $(\xi, f(x)) \in F$, vagyis $F(\xi) = f(x)$, azaz $F\left(\pi_{\mathrm{Dom}(f)/\mathrm{R}_f}(x)\right) = f(x)$. Ez azt jelenti, hogy F olyan függvény, amelyre az $F \circ \pi_{\mathrm{Dom}(f)/\mathrm{R}_f} = f$ egyenlőség teljesül, amivel $\dot{f}$ egzisztenciáját is igazoltuk.

Ha $y \in \mathrm{Im}(f)$, akkor van olyan $x \in \mathrm{Dom}(f)$, hogy $y = f(x)$, és ekkor $\dot{f}\left(\pi_{\mathrm{Dom}(f)/\mathrm{R}_f}(x)\right) = f(x) = y$, tehát $\xi := \pi_{\mathrm{Dom}(f)/\mathrm{R}_f}(x) \in \mathrm{Dom}(f)/\mathrm{R}_f$ olyan elem, amelyre $\dot{f}(\xi) = y$. Ezért $\mathrm{Im}\left(\dot{f}\right) = \mathrm{Im}(f)$, vagyis az $\dot{f} : \mathrm{Dom}(f)/\mathrm{R}_f \to \mathrm{Im}(f)$ függvény szürjektív. Ha $\xi, \xi' \in \mathrm{Dom}(f)/\mathrm{R}_f$ olyanok, hogy $\dot{f}(\xi) = \dot{f}(\xi')$, akkor tetszőlegesen kijelölve $x \in \xi$ és $x' \in \xi'$ pontokat kapjuk, hogy $\dot{f}(\xi) = f(x)$ és $\dot{f}(\xi') = f(x')$, ezért $f(x) = f(x')$, vagyis $(x,x') \in \mathrm{R}_f$, azaz $\xi = \pi_{\mathrm{Dom}(f)/\mathrm{R}_f}(x) = \pi_{\mathrm{Dom}(f)/\mathrm{R}_f}(x') = \xi'$. Ezzel bebizonyítottuk, hogy $\dot{f}$ injekció. ■

6.11.5. Definíció. *Ha f függvény, akkor az előző állításban értelmezett R_f ekvivalenciát az f* **függvény által meghatározott ekvivalenciának** *nevezzük, továbbá az $\dot{f}$: $\mathrm{Dom}(f)/\mathrm{R}_f \to \mathrm{Im}(f)$ bijekciót az f függvény* **kanonikus faktorizáltjának** *nevezzük.*

6.11.6. Állítás. *Legyenek R és S olyan ekvivalenciák az E halmaz felett, hogy $R \subseteq S$. Legyen*

$$S/R := \{(\xi, \xi') \in (E/R) \times (E/R) | (\exists x \in \xi)(\exists x' \in \xi')\ (x, x') \in S\}.$$

Ekkor S/R ekvivalencia az E/R faktorhalmaz felett, és létezik egyetlen olyan $f : E/S \to (E/R)/(S/R)$ függvény, amelyre $f \circ \pi_{E/S} = \pi_{(E/R)/(S/R)} \circ \pi_{E/R}$, vagyis a következő diagram kommutatív:

$$\begin{tikzcd}
E/S \arrow[r, "f"] & (E/R)/(S/R) \\
E \arrow[u, "\pi_{E/S}"] \arrow[r, "\pi_{E/R}"'] & E/R \arrow[u, "\pi_{(E/R)/(S/R)}"']
\end{tikzcd}$$

Ez az f függvény bijekció az E/S és $(E/R)/(S/R)$ faktorhalmazok között.

Bizonyítás. Ha $\xi \in E/R$, akkor bármely $x \in \xi$ esetén $(x, x) \in S$, hiszen $\xi \subseteq E$ miatt $x \in E$ és S reflexív az E halmazon; ezért $(\xi, \xi) \in S/R$, tehát az S/R reláció reflexív az E/R halmazon. Ha $(\xi, \xi') \in S/R$, akkor léteznek olyan $x \in \xi$ és $x' \in \xi'$, hogy $(x, x') \in S$; ekkor $x' \in \xi'$ és $x \in \xi$, valamint S szimmetrikussága miatt $(x', x) \in S$, így S/R definíciója alapján $(\xi', \xi) \in S/R$, vagyis az S/R reláció szimmetrikus. Ha $(\xi, \xi') \in S/R$ és $(\xi', \xi'') \in S/R$, akkor léteznek olyan $x \in \xi$ és $x' \in \xi'$ elemek, hogy $(x, x') \in S$, valamint léteznek olyan $\tilde{x}' \in \xi'$ és $x'' \in \xi''$ elemek, hogy $(\tilde{x}', x'') \in S$. Mivel $x', \tilde{x}' \in \xi'$, így $(x', \tilde{x}') \in R \subseteq S$ és $(x, x') \in S$, ezért az S reláció tranzitivitása folytán $(x, \tilde{x}') \in S$. Ugyanakkor $(\tilde{x}', x'') \in S$ is teljesül, így ismét S tranzitivitását alkalmazva $(x, x'') \in S$, ami azt jelenti, hogy $(\xi, \xi'') \in S/R$, tehát az S/R reláció tranzitív. Ezzel beláttuk, hogy S/R ekvivalencia az E/R faktorhalmaz felett.

Ha $g, g' : E/S \to (E/R)/(S/R)$ olyan függyények, hogy $g \circ \pi_{E/S} = \pi_{(E/R)/(S/R)} \circ \pi_{E/R}$ és $g' \circ \pi_{E/S} = \pi_{(E/R)/(S/R)} \circ \pi_{E/R}$, akkor $g \circ \pi_{E/S} = g' \circ \pi_{E/S}$, így a $\pi_{E/S} : E \to E/S$ leképezés szürjektivitásából következik, hogy $g = g'$. Ezért az előírt tulajdonságú $E/S \to (E/R)/(S/R)$ leképezés egyértelmű.

Az előírt tulajdonságú $E/S \to (E/R)/(S/R)$ leképezés létezésének bizonyításához tekintsük a következő halmazt:

$$f \;:=\; \{\; (\xi, \eta) \in (E/S) \times (E/R)/(S/R) \mid (\exists x \in \xi)\ \eta = \pi_{(E/R)/(S/R)}\big(\pi_{E/R}(x)\big)\; \}.$$

Az f halmaz minden eleme pár, tehát f reláció, és a definíció szerint $f \subseteq (E/S) \times (E/R)/(S/R)$, ezért $\mathrm{pr}_1 f \subseteq E/S$ és $\mathrm{pr}_2 f \subseteq (E/R)/(S/R)$. Ha $(\xi, \eta) \in f$ és $(\xi, \eta') \in f$, akkor léteznek olyan $x, x' \in \xi$, hogy $\eta = \pi_{(E/R)/(S/R)}\big(\pi_{E/R}(x)\big)$ és $\eta' = \pi_{(E/R)/(S/R)}\big(\pi_{E/R}(x')\big)$; ekkor $\xi \in E/S$ miatt $\pi_{E/S}(x) = \pi_{E/S}(x')$, és $x \in \pi_{E/S}(x)$, valamint $x' \in \pi_{E/S}(x')$, így $(x, x') \in S$, amiből S/R definíciója alapján kapjuk, hogy $\big(\pi_{E/R}(x), \pi_{E/R}(x')\big) \in S/R$, tehát $\eta = \pi_{(E/R)/(S/R)}\big(\pi_{E/R}(x)\big) = \pi_{(E/R)/(S/R)}\big(\pi_{E/R}(x')\big) = \eta'$. Ez azt jelenti, hogy f függvényreláció, és $\mathrm{Dom}(f) \subseteq E/S$, valamint $\mathrm{Im}(f) \subseteq (E/R)/(S/R)$, tehát $f : E/S \rightarrowtail (E/R)/(S/R)$ függvény.

Ha $\xi \in E/S$, akkor a $\pi_{E/S} : E \to E/S$ függvény szürjektivitása miatt van olyan $x \in E$, hogy $\xi = \pi_{E/S}(x)$, azaz $x \in \xi$, és ekkor f definíciója szerint $\big(\xi, \pi_{(E/R)/(S/R)}\big(\pi_{E/R}(x)\big)\big) \in f$, vagyis $\xi \in \mathrm{Dom}(f)$ és $f\big(\pi_{E/S}(x)\big) = f(\xi) = \pi_{(E/R)/(S/R)}\big(\pi_{E/R}(x)\big)$. Ez azt jelenti, hogy $\mathrm{Dom}(f) = E/S$, és fennáll az $f \circ \pi_{E/S} = \pi_{(E/R)/(S/R)} \circ \pi_{E/R}$ egyenlőség, amivel az előírt tulajdonságú $E/S \to (E/R)/(S/R)$ leképezés egzisztenciáját is igazoltuk.

Az $f : E/S \to (E/R)/(S/R)$ függvény injektivitásának bizonyításához legyenek $\xi, \xi' \in E/S$ olyanok, hogy $f(\xi) = f(\xi')$. Ekkor véve $x \in \xi$ és $x' \in \xi'$ elemeket kapjuk, hogy $\pi_{E/S}(x) = \xi$ és $\pi_{E/S}(x') = \xi'$, tehát $\pi_{(E/R)/(S/R)}\left(\pi_{E/R}(x)\right) = f\left(\pi_{E/S}(x)\right) = f(\xi) = f(\xi') = f\left(\pi_{E/S}(x')\right) = \pi_{(E/R)/(S/R)}\left(\pi_{E/R}(x')\right)$, ezért $\left(\pi_{E/R}(x), \pi_{E/R}(x')\right) \in S/R$. Az S/R reláció definíciója szerint léteznek olyan $\tilde{x} \in \pi_{E/R}(x)$ és $\tilde{x}' \in \pi_{E/R}(x')$ elemek, amelyekre $(\tilde{x}, \tilde{x}') \in S$. Mivel $(x, \tilde{x}) \in R \subseteq S$ és $(x', \tilde{x}') \in R \subseteq S$, így fennállnak az $(x, \tilde{x}) \in S$, $(\tilde{x}, \tilde{x}') \in S$ és $(x', \tilde{x}') \in S$ összefüggések. Ezekből S szimmetrikussága és tranzitivitása alapján következik, hogy $(x, x') \in S$, vagyis $\xi = \pi_{E/S}(x) = \pi_{E/S}(x') = \xi'$, tehát az f függvény injektív.

Az $f : E/S \to (E/R)/(S/R)$ függvény szürjektivitása az $f \circ \pi_{E/S} = \pi_{(E/R)/(S/R)} \circ \pi_{E/R}$ egyenlőségből következik, mert a jobb oldalon a $\pi_{E/R} : E \to E/R$ és $\pi_{(E/R)/(S/R)} : E/R \to (E/R)/(S/R)$ szürjekciók kompozíciója áll, tehát a $\pi_{(E/R)/(S/R)} \circ \pi_{E/R} : E \to (E/R)/(S/R)$ szürjektív, ezért még a $\pi_{E/S} : E \to E/S$ függvény szürjektivitását is felhasználva nyerjük, hogy $\mathrm{Im}(f) = f\langle E/S\rangle = f\langle \mathrm{Im}\left(\pi_{E/S}\right) = \mathrm{Im}\left(\pi_{(E/R)/(S/R)} \circ \pi_{E/R}\right) = (E/R)/(S/R)$, vagyis az $f : E/S \to (E/R)/(S/R)$ függvény szürjektív. ■

6.11.7. Definíció. *Ha R és S olyan ekvivalenciák az E halmaz felett, hogy $R \subseteq S$, akkor az előző állításban értelmezett $E/S \to (E/R)/(S/R)$ bijekciót az E/S és $(E/R)/(S/R)$ faktorhalmazok közötti* **kanonikus bijekciónak nevezzük**.

6.11.8. Állítás. *Legyenek E és F halmazok, R ekvivalencia E felett, S ekvivalencia F felett, és $f : E \to F$ olyan függvény, hogy $(f \times f)\langle R\rangle \subseteq S$ (azaz minden $(x, x') \in R$ esetén $(f(x), f(x')) \in S$).*

a) *Létezik egyetlen olyan $\dot{f}_{R,S} : E/R \to F/S$ függvény, amelyre $\dot{f}_{R,S} \circ \pi_{E/R} = \pi_{F/S} \circ f$, vagyis a következő diagram kommutatív:*

$$\begin{tikzcd}
E/R \arrow[r, "\dot{f}_{R,S}"] & F/S \\
E \arrow[u, "\pi_{E/R}"] \arrow[r, "f"'] & F \arrow[u, "\pi_{F/S}"']
\end{tikzcd}$$

b) *Ha f injekció és $(f \times f)\langle R\rangle = S$, akkor $\dot{f}_{R,S}$ injekció.*

c) *Ha az $f : E \to F$ függvény szürjekció, akkor az $\dot{f}_{R,S} : E/R \to F/S$ függvény szürjekció.*

d) *Ha az $f : E \to F$ függvény bijekció az E és F halmazok között, és $(f \times f)\langle R\rangle = S$, akkor az $\dot{f}_{R,S} : E/R \to F/S$ függvény bijekció az E/R és F/S faktorhalmazok között.*

Bizonyítás. a) Ha $g, g' : E/R \to F/S$ olyan függvények, amelyekre $g \circ \pi_{E/R} = \pi_{F/S} \circ f$ és $g' \circ \pi_{E/R} = \pi_{F/S} \circ f$, akkor $g \circ \pi_{E/R} = g' \circ \pi_{E/R}$, ezért a $\pi_{E/R} : E \to E/R$ függvény szürjektivitása miatt $g = g'$, tehát az előírt tulajdonságú függvény egyértelmű. Az egzisztencia bizonyításához tekintsük a következő halmazt:

$$G := \{\, (\xi, \eta) \in (E/R) \times (F/S) \mid (\exists x \in \xi)\ \eta = \pi_{F/S}(f(x)) \,\}.$$

A G halmaz minden eleme pár, ezért G reláció, és a definíció szerint $G \subseteq (E/R) \times (F/S)$, tehát $\mathrm{pr}_1 G \subseteq E/R$ és $\mathrm{pr}_2 G \subseteq F/S$. Ha $(\xi, \eta) \in G$ és $(\xi, \eta') \in G$, akkor G definíciója szerint léteznek olyan $x, x' \in \xi$, hogy $\eta = \pi_{F/S}(f(x))$ és $\eta' = \pi_{F/S}(f(x'))$; ekkor $(x, x') \in R$, így $(f(x), f(x')) \in S$, tehát $\eta = \pi_{F/S}(f(x)) = \pi_{F/S}(f(x')) = \eta'$. Ez azt jelenti, hogy G függvényreláció, és $\mathrm{Dom}(G) \subseteq E/R$, valamint $\mathrm{Im}(G) \subseteq F/S$, tehát $G : E/R \rightarrowtail F/S$ függvény.

Ha $\xi \in E/R$, akkor $x \in \xi$ esetén G definíciója szerint $\big(\xi, \pi_{F/S}(f(x))\big) \in G$, ezért $\xi \in \mathrm{Dom}(G)$. Ez azt jelenti, hogy $\mathrm{Dom}(G) = E/S$, továbbá minden $x \in E$ esetén $x \in \pi_{E/R}(x)$, így $G\left(\pi_{E/R}(x)\right) = \pi_{F/S}(f(x))$, vagyis fennáll a $G \circ \pi_{E/R} = \pi_{F/S} \circ \pi_{E/R}$ egyenlőség, amivel az előírt tulajdonságú $E/R \to F/S$ leképezés egzisztenciáját is igazoltuk.

b) Tegyük fel, hogy f injekció és $(f \times f)\langle R \rangle = S$. Legyenek $\xi, \xi' \in E/R$ olyanok, hogy $\dot{f}_{R,S}(\xi) = \dot{f}_{R,S}(\xi')$. Legyenek $x \in \xi$ és $x' \in \xi'$ rögzített elemek, tehát $\xi = \pi_{E/R}(x)$ és $\xi' = \pi_{E/R}(x')$. Ekkor $\pi_{F/S}(f(x)) = \dot{f}_{R,S}\left(\pi_{E/R}(x)\right) = \dot{f}_{R,S}(\xi) = \dot{f}_{R,S}(\xi') = \dot{f}_{R,S}\left(\pi_{E/R}(x')\right) = \pi_{F/S}(f(x'))$, tehát $(f(x), f(x')) \in S$. Az $(f \times f)\langle R \rangle = S$ hipotézis szerint létezik olyan $(\tilde{x}, \tilde{x}') \in R$ pár, hogy $(f(\tilde{x}), f(\tilde{x}')) = (f(x), f(x'))$, azaz $f(\tilde{x}) = f(x)$ és $f(\tilde{x}') = f(x')$. Az f függvény injektivitása miatt $\tilde{x} = x$ és $\tilde{x}' = x'$. Tehát $(x, x') \in R$, így $\xi = \pi_{E/R}(x) = \pi_{E/R}(x') = \xi'$, ami azt jelenti, hogy $\dot{f}_{R,S}$ injekció.

c) Tegyük fel, hogy az $f : E \to F$ függvény szürjekció. Mivel $\pi_{F/S} : F \to F/S$ is szürjekció, így az $\dot{f}_{R,S} \circ \pi_{E/R} = \pi_{F/S} \circ f$ egyenlőség alapján az $\dot{f}_{R,S} \circ \pi_{E/R} : E \to F/S$ függvény is szürjekció, így kihasználva a $\pi_{E/R} : E \to E/R$ függvény szürjektivitását kapjuk, hogy $\mathrm{Im}\left(\dot{f}_{R,S}\right) = \dot{f}_{R,S}\langle E/R \rangle = \dot{f}_{R,S}\langle \mathrm{Im}\left(\pi_{E/R}\right) \rangle = F/S$, tehát az $\dot{f}_{R,S} : E/R \to F/S$ függvény szürjekció.

d) Ha $(f \times f)\langle R \rangle = S$ és az $f : E \to F$ függvény bijekció, akkor f injekció, így b) szerint $\dot{f}_{R,S}$ injekció, továbbá az $f : E \to F$ függvény szürjekció, tehát c) szerint az $\dot{f}_{R,S} : E/R \to F/S$ függvény szürjekció. ■

6.11.9. Definíció. *Legyenek E és F halmazok, R ekvivalencia E felett, S ekvivalencia F felett, és $f : E \to F$ olyan függvény, hogy $(f \times f)\langle R \rangle \subseteq S$ akkor az előző állításban értelmezett $\dot{f}_{R,S} : E/R \to F/S$ függvényt az f függvény R-S* **faktorizáltjának** *nevezzük.*

6.11.10. Állítás. *Legyen $((E_i, R_i))_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén R_i ekvivalencia az E_i halmaz felett és*

$$\mathop{\times}_{i \in I} R_i := \left\{ ((x_i)_{i \in I}, (x'_i)_{i \in I}) \in \left(\prod_{i \in I} E_i\right) \times \left(\prod_{i \in I} E_i\right) \;\middle|\; (\forall i \in I)\ (x_i, x'_i) \in R_i \right\}.$$

Ekkor a $\mathop{\times}\limits_{i \in I} R_i$ halmaz ekvivalencia a $\prod\limits_{i \in I} E_i$ szorzathalmaz felett, és létezik egyetlen olyan

$$f : \left(\prod_{i \in I} E_i\right) \Big/ \left(\mathop{\times}_{i \in I} R_i\right) \to \prod_{i \in I} (E_i/R_i)$$

függvény, amelyre $f \circ p = \mathop{\times}\limits_{i \in I} \pi_{E_i/R_i}$, ahol $p : \prod\limits_{i \in I} E_i \to \left(\prod\limits_{i \in I} E_i\right) \Big/ \left(\mathop{\times}\limits_{i \in I} R_i\right)$ a kanonikus *szürjekció, vagyis a következő diagram kommutatív:*

$$\begin{tikzcd}
\left(\prod\limits_{i\in I} E_i\right)\Big/\left(\mathop{\times}\limits_{i\in I} R_i\right) \arrow[r, "f"] & \prod\limits_{i\in I}(E_i/R_i) \\
\prod\limits_{i\in I} E_i \arrow[u, "p"] \arrow[ur, "\mathop{\times}\limits_{i\in I}\pi_{E_i/R_i}"'] &
\end{tikzcd}$$

Az f függvény bijekció.

Bizonyítás. Vezessük be az $E := \prod\limits_{i\in I} E_i$ és $R := \mathop{\times}\limits_{i\in I} R_i$ jelöléseket. Világos, hogy ekkor $p = \pi_{E/R}$.

Ha $(x_i)_{i\in I} \in E$, akkor minden $i \in I$ esetén $(x_i, x_i) \in R_i$, mivel $x_i \in E_i$ és R_i reflexív az E_i halmazon, tehát $((x_i)_{i\in I}, (x_i)_{i\in I}) \in R$, vagyis az R reláció reflexív az E halmazon. Ha $((x_i)_{i\in I}, (x'_i)_{i\in I}) \in R$, akkor minden $i \in I$ esetén $(x_i, x'_i) \in R_i$, ezért R_i szimmetrikussága miatt $(x'_i, x_i) \in R_i$, vagyis $((x'_i)_{i\in I}, (x_i)_{i\in I}) \in R$, ami azt jelenti, hogy az R reláció szimmetrikus. Ha $((x_i)_{i\in I}, (x'_i)_{i\in I}) \in R$ és $((x'_i)_{i\in I}, (x''_i)_{i\in I}) \in R$, akkor minden $i \in I$ esetén $(x_i, x'_i) \in R_i$ és $(x'_i, x''_i) \in R_i$, ezért R_i tranzitivitása miatt $(x_i, x''_i) \in R_i$, vagyis $((x_i)_{i\in I}, (x''_i)_{i\in I}) \in R$, ami azt jelenti, hogy az R reláció tranzitív. Ezzel beláttuk, hogy R ekvivalencia E felett.

Ha $g, g' : E/R \to \prod\limits_{i\in I}(E_i/R_i)$ olyan függvények, hogy $g\circ p = \mathop{\times}\limits_{i\in I} \pi_{E_i/R_i}$ és $g'\circ p = \mathop{\times}\limits_{i\in I} \pi_{E_i/R_i}$, akkor $g \circ p = g' \circ p$, ezért a $p = \pi_{E/R} : E \to E/R$ függvény szürjektivitása miatt $g = g'$, vagyis az előírt tulajdonságú függvény egyértelmű. Az egzisztencia bizonyításához legyen

$$f := \left\{ (\xi, (y_i)_{i\in I}) \in (E/R) \times \prod_{i\in I}(E_i/R_i) \;\middle|\; (\exists (x_i)_{i\in I} \in \xi)\, (\forall i \in I)\; y_i = \pi_{E_i/R_i}(x_i) \right\}.$$

Az F halmaz minden eleme pár, tehát F reláció, és a definíció szerint $F \subseteq (E/R) \times \prod\limits_{i\in I}(E_i/R_i)$, tehát $\mathrm{pr}_1 F \subseteq E/R$ és $\mathrm{pr}_2 F \subseteq \prod\limits_{i\in I}(E_i/R_i)$. Ha $(\xi, (y_i)_{i\in I}) \in f$ és $(\xi, (y'_i)_{i\in I}) \in f$, akkor léteznek olyan $(x_i)_{i\in I}, (x'_i)_{i\in I} \in \xi$ rendszerek, hogy minden $i \in I$ esetén $y_i = \pi_{E_i/R_i}(x_i)$ és $y'_i = \pi_{E_i/R_i}(x'_i)$, mivel pedig $(x_i, x'_i) \in R_i$, így $y_i = \pi_{E_i/R_i}(x_i) = \pi_{E_i/R_i}(x'_i) = y'_i$, vagyis $(y_i)_{i\in I} = (y'_i)_{i\in I}$. Ez azt jelenti, hogy f függvényreláció, és $\mathrm{Dom}(f) \subseteq E/R$, valamint $\mathrm{Im}(f) \subseteq \prod\limits_{i\in I}(E_i/R_i)$, vagyis $f : E/R \rightarrowtail \prod\limits_{i\in I}(E_i/R_i)$ függvény.

Ha $\xi \in E/R$, akkor véve egy $(x_i)_{i\in I} \in \xi$ elemet az f függvény definíciójából nyilvánvalóan adódik, hogy $\left(\xi, \left(\pi_{E_i/R_i}(x_i)\right)_{i\in I}\right) \in f$, ezért $\xi \in \mathrm{Dom}(f)$, így $\mathrm{Dom}(f) = E/R$. Továbbá, minden $(x_i)_{i\in I} \in E$ esetén $\left(\pi_{E/R}\left((x_i)_{i\in I}\right), \left(\pi_{E_i/R_i}(x_i)\right)_{i\in I}\right) \in f$, vagyis fennáll az $f\left(\pi_{E/R}\left((x_i)_{i\in I}\right)\right) = \left(\pi_{E_i/R_i}(x_i)\right)_{i\in I} = \left(\mathop{\times}\limits_{i\in I} \pi_{E_i/R_i}\right)((x_i)_{i\in I})$ egyenlőség. Ez azt jelenti, hogy az $f : E/R \to \prod\limits_{i\in I}(E_i/R_i)$ függvény olyan, hogy $f \circ p = \mathop{\times}\limits_{i\in I} \pi_{E_i/R_i}$, hiszen $p = \pi_{E/R}$. Tehát az előírt tulajdonságú függvény létezését igazoltuk.

Legyenek $\xi, \xi' \in E/R$ olyanok, hogy $f(\xi) = f(\xi')$, és válasszunk ki egy $(x_i)_{i\in I} \in \xi$ és $(x'_i)_{i\in I} \in \xi'$ pontot. Ekkor $\xi = \pi_{E/R}\left((x_i)_{i\in I}\right)$ és $\xi' = \pi_{E/R}\left((x'_i)_{i\in I}\right)$, következésképpen $\left(\pi_{E_i/R_i}(x_i)\right)_{i\in I} = f\left(\pi_{E/R}\left((x_i)_{i\in I}\right)\right) = f(\xi) = f(\xi') = f\left(\pi_{E/R}\left((x'_i)_{i\in I}\right)\right) =$

$\left(\pi_{E_i/R_i}(x_i')\right)_{i\in I}$, vagyis minden $i \in I$ esetén $\pi_{E_i/R_i}(x_i) = \pi_{E_i/R_i}(x_i')$, azaz $(x_i, x_i') \in R_i$. Ezért $((x_i)_{i\in I}, (x_i)_{i\in I}) \in R$, tehát $\xi = \pi_{E/R}\left((x_i)_{i\in I}\right) = \pi_{E/R}\left((x_i')_{i\in I}\right) = \xi'$. Ez azt jelenti, hogy f injekció.

Az $f : E/R \rightarrowtail \prod_{i\in I}(E_i/R_i)$ függvény szürjektív, mert $(y_i)_{i\in I} \in \prod_{i\in I}(E_i/R_i)$ esetén minden $i \in I$ indexre $y_i \in E_i/R_i$, így a $\pi_{E_i/R_i} : E_i \to E_i/R_i$ függvény szürjektivitása folytán létezik olyan $x_i \in E_i$, hogy $y_i = \pi_{E_i/R_i}(x_i)$, ezért a kiválasztási axióma alkalmazásával kiválaszthatunk olyan $(x_i)_{i\in I} \in E$ rendszert, amelyre $(y_i)_{i\in I} = \left(\pi_{E_i/R_i}(x_i)\right)_{i\in I} = f\left(\pi_{E/R}\left((x_i)_{i\in I}\right)\right) \in \operatorname{Im}(f)$. Ezért az $f : E/R \rightarrowtail \prod_{i\in I}(E_i/R_i)$ függvény bijekció. ■

6.11.11. Definíció. *Ha $((E_i, R_i))_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén R_i ekvivalencia az E_i halmaz felett, akkor az előző állításban értelmezett $\times_{i\in I} R_i$ ekvivalenciát az $(R_i)_{i\in I}$* **ekvivalencia-rendszer szorzatának** *nevezzük, és az előző állításban értelmezett $\left(\prod_{i\in I} E_i\right)\Big/\left(\times_{i\in I} R_i\right) \to \prod_{i\in I}(E_i/R_i)$ függvényt az $\left(\prod_{i\in I} E_i\right)\Big/\left(\times_{i\in I} R_i\right)$ faktorhalmaz és $\prod_{i\in I}(E_i/R_i)$ szorzathalmaz közötti* **kanonikus bijekciónak** *nevezzük.*

6.12. Rendezett halmazok

6.12.1. Definíció. *Az $(E, \leq)$ párt* **rendezett halmaznak** *nevezzük, ha $\leq$ rendezés az E halmaz felett. Ha $(E, \leq)$ rendezett halmaz, akkor az $x, x' \in E$ elemeket* **összehasonlíthatóknak** *nevezzük a $\leq$ rendezés szerint, ha $x \leq x'$ vagy $x' \leq x$ teljesül. Az $(E, \leq)$ párt* **lineárisan rendezett halmaznak** *nevezzük, ha $(E, \leq)$ olyan rendezett halmaz, hogy az E bármely két eleme összehasonlítható a $\leq$ rendezés szerint. Az E halmaz feletti $\leq$ relációt* **lineáris rendezésnek** *nevezzük, ha $(E, \leq)$ lineárisan rendezett halmaz.*

Ha E legalább két elemű halmaz, akkor a $(\mathscr{P}(E), \subseteq_{\mathscr{P}(E)})$ pár rendezett halmaz, de nem lineárisan rendezett.

Megjegyezzük, hogy ha $(E, \leq)$ rendezett halmaz, akkor minden $F \subseteq E$ halmazra a $\leq_F$ megszorított reláció nyilvánvalóan szintén rendezés F felett, tehát az $(F, \leq_F)$ pár is rendezett halmaz.

Ha $(E, \leq)$ rendezett halmaz, akkor az $\overset{-1}{\leq}$ inverz reláció nyilvánvalóan szintén rendezés E felett, tehát $(E, \overset{-1}{\leq})$ rendezett halmaz.

6.12.2. Definíció. *Ha $(E, \leq)$ rendezett halmaz, akkor a $\overset{-1}{\leq}$ inverz relációt a $\leq^\circ$ szimbólummal jelöljük, és az $(E, \leq^\circ)$ rendezett halmazt az $(E, \leq)$ rendezett halmaz* **ellentettjének** *nevezzük.*

6.12.3. Definíció. *Legyen $(E, \leq)$ rendezett halmaz.*

– *Az $X \subseteq E$ halmaz* **felső** *(illetve* **alsó***)* **korlátjának** *nevezünk a $\leq$ rendezés szerint minden olyan $y \in E$ elemet, amelyre teljesül az, hogy minden $x \in X$ elemre $x \leq y$ (illetve $y \leq x$). Az $X \subseteq E$ halmaz* **felülről** *(illetve* **alulról***)* **korlátos** *a $\leq$ rendezés szerint, ha létezik X-nek felső (illetve alsó) korlátja a $\leq$ rendezés szerint. Az $X \subseteq E$ halmaz* **korlátos** *a $\leq$ rendezés szerint, ha X felülről és alulról is korlátos a $\leq$ rendezés szerint.*

– *Az $X \subseteq E$ halmaz* **legnagyobb** *(illetve* **legkisebb***) elemének nevezzük a $\leq$ rendezés* *szerint az E halmaz minden olyan elemét, amely felső (illetve alsó) korlátja X-nek a $\leq$ rendezés szerint és eleme X-nek.*

– *Az $X \subseteq E$ halmaz* **felső** (*illetve* **alsó**) **határának** *nevezzük a $\leq$ rendezés szerint az X halmaz legkisebb (illetve legnagyobb) felső (illetve alsó) korlátját a $\leq$ rendezés szerinti. A felső (illetve alsó) határ elnevezés helyett gyakran a* **szuprémum** (*illetve* **infimum**)*elnevezést is használjuk.*

Ha világos, hogy az E halmaz felett melyik $\leq$ rendezésről van szó, akkor az imént bevezetett elnevezésekből elhagyjuk a "$\leq$ rendezés szerint" kifejezést.

6.12.4. Állítás. *Ha $(E, \leq)$ rendezett halmaz és $X \subseteq E$, akkor X-nek legfeljebb egy legkisebb eleme (illetve legnagyobb eleme, illetve infimuma, illetve szuprémuma) létezik.*

Bizonyítás. Ha $a, b \in X$ legkisebb (illetve legnagyobb) elemei E-nek, akkor minden $x \in X$ esetén $a \leq x$ és $b \leq x$ (illetve $x \leq a$ és $x \leq b$), ezért $a \leq b$ és $b \leq a$ is teljesül, így az $\leq$ reláció antiszimmetrikussága miatt $a = b$. Tehát az X halmaz legkisebb (illetve legnagyobb) eleme egyértelműen van meghatározva.

Ebből már következik, hogy az X halmaz infimuma és szuprémuma is egyértelmű, mert az infimum (illetve szuprémum) az X halmaz alsó (illetve felső) korlátjai halmazának a legnagyobb (illetve legkisebb) eleme. ■

Jelölés. Legyen $(E, \leq)$ rendezett halmaz.

– Ha az $X \subseteq E$ halmaznak létezik legnagyobb (illetve legkisebb) eleme, akkor azt a $\max(X)$ (illetve $\min(X)$(szimbólummal jelöljük, vagy ha szükséges kiemelni, hogy melyik E feletti $\leq$ rendezés szerint vesszük ezt az elemet, akkor a $\max_{\leq}(X)$ (illetve $\min_{\leq}(X)$) szimbólumot alkalmazzuk.

– Ha az $X \subseteq E$ halmaznak létezik szuprémuma (illetve infimuma), akkor azt a $\sup(X)$ (illetve $\inf(X)$) szimbólummal jelöljük, vagy ha szükséges kiemelni, hogy melyik E feletti $\leq$ rendezés szerint vesszük ezt az elemet, akkor a $\sup_{\leq}(X)$ (illetve $\inf_{\leq}(X)$) szimbólumot alkalmazzuk.

6.12.5. Definíció. *Legyen $(E, \leq)$ rendezett halmaz.*

– *Ha T halmaz, és $f : T \to E$ olyan függvény, hogy az $\mathrm{Im}(f)$ halmaznak létezik legnagyobb (illetve legkisebb) eleme, akkor a*

$$\max(f) := \max(\mathrm{Im}(f)), \qquad (\text{ \textit{illetve} } \min(f) := \min(\mathrm{Im}(f))\ )$$

jelölést alkalmazzük, és ezt az elemet az f **függvény maximumának** (*illetve* **minimumának**) *nevezzük. Speciálisan, ha $(x_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ indexre $x_i \in E$, akkor a*

$$\max_{i \in I} x_i := \max(\{x_i | i \in I\}), \qquad (\text{ \textit{illetve} } \min_{i \in I} x_i := \min(\{x_i | i \in I\})\ )$$

elemet az E-ben haladó $(x_i)_{i \in I}$ **rendszer maximumának** (*illetve* **minimumának**) *nevezzük.*

– *Ha T halmaz, és $f : T \to E$ olyan függvény, hogy az $\mathrm{Im}(f)$ halmaznak létezik szuprémuma (illetve infimuma), akkor a*

$$\sup(f) := \sup(\mathrm{Im}(f)), \qquad (\text{ \textit{illetve} } \inf(f) := \inf(\mathrm{Im}(f))\ )$$

elemet az f **függvény szuprémumának** (*illetve* **infimumának**) *nevezzük. Speciálisan, ha $(x_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ indexre $x_i \in E$, akkor a*

$$\sup_{i\in I} x_i := \sup(\{x_i | i \in I\}, \qquad (\text{ illetve } \inf_{i\in I} x_i := \inf(\{x_i | i \in I\})\ )$$

elemet az E-ben haladó $(x_i)_{i\in I}$ **rendszer szuprémumának** (*illetve* **infimumának**) *nevezzük.*

Természetesen, ha $(E, \leq)$ rendezett halmaz és $X \subseteq E$, akkor X-nek nem szükségképpen létezik legkisebb vagy legnagyobb eleme (ez a helyzet például ha $X = \emptyset$), és X-nek nem szükségképpen létezik infimuma vagy szuprémuma (ez a helyzet például ha X nem korlátos alulról vagy felülről).

6.12.6. Definíció. *Azt mondjuk, hogy az E halmaz feletti $\leq$ rendezés* **teljes**, *ha E minden nem üres felülről korlátos részhalmazának létezik szuprémuma a $\leq$ rendezés szerint. Azt mondjuk, hogy $(E, \leq)$* **teljesen rendezett halmaz**, *ha $\leq$ teljes rendezés E felett.*

A definíció alapján nyilvánvaló, hogy ha $(E, \leq)$ rendezett halmaz, akkor az üres halmaznak pontosan akkor létezik infimuma (illetve szuprémuma) a $\leq$ rendezés szerint, ha E-nek létezik legnagyobb (illetve legkisebb) eleme, és ha ez létezik, akkor $\emptyset$ infimuma (illetve szuprémuma) egyenlő az E halmaz $\leq$ rendezés szerinti legnagyobb (illetve legkisebb) elemével.

6.12.7. Állítás. *Legyen $(E, \leq)$ rendezett halmaz és $X \subseteq E$.*

a) *Az $y \in E$ elem pontosan akkor felső* (*illetve alsó*) *korlátja X-nek a $\leq$ rendezés szerint, ha y alsó* (*illetve felső*) *korlátja X-nek a $\leq^\circ$ rendezés szerint.*

b) *Az $y \in E$ elem pontosan akkor a legnagyobb* (*illetve legkisebb*) *eleme X-nek a $\leq$ rendezés szerint, ha y az X halmaz legkisebb* (*illetve legnagyobb*) *eleme X-nek a $\leq^\circ$ rendezés szerint, vagyis fennáll a $\max_{\leq}(X) = \min_{\leq^\circ}(X)$* (*illetve* $\min_{\leq}(X) = \max_{\leq^\circ}(X)$) *egyenlőség.*

c) *Az X-nek halmaznak pontosan akkor létezik szuprémuma* (*illetve infimuma*) *a $\leq$ rendezés szerint, ha X-nek létezik infimuma* (*illetve szuprémuma*) *a $\leq^\circ$ rendezés szerint, és fennáll a $\sup_{\leq}(X) = \inf_{\leq^\circ}(X)$* (*illetve* $\inf_{\leq}(X) = \sup_{\leq^\circ}(X)$) *egyenlőség.*

Bizonyítás. a) Az $y \in E$ elem pontosan akkor felső (illetve alsó) korlátja X-nek a $\leq$ rendezés szerint, ha minden $x \in X$ esetén $x \leq y$ (illetve $y \leq x$), ami azzal ekvivalens, hogy minden $x \in X$ esetén $y \leq^\circ x$ (illetve $x \leq^\circ y$), vagyis y alsó (illetve felső) korlátja X-nek a $\leq^\circ$ rendezés szerint.

b) Az $y \in E$ elem pontosan akkor a legnagyobb (illetve legkisebb) eleme X-nek a $\leq$ rendezés szerint, ha $y \in X$ és y felső (illetve alsó) korlátja X-nek a $\leq$ rendezés szerint, ami a) alapján ekvivalens azzal, hogy $y \in X$ és y alsó (illetve felső) korlátja X-nek a $\leq^\circ$ rendezés szerint, vagyis y az X halmaz legkisebb (illetve legnagyobb) eleme a $\leq^\circ$ rendezés szerint.

c) Az a) állítás alapján az X halmaz $\leq$ szerinti felső (illetve alsó) korlátjainak halmaza *egyenlő* az X halmaz $\leq^\circ$ szerinti alsó (illetve felső) korlátjainak halmazával, így b) alapján pontosan akkor létezik az X halmaz $\leq$ szerinti felső (illetve alsó) korlátjai halmazának $\leq$ szerinti legkisebb (illetve legnagyobb) eleme, ha létezik az X halmaz $\leq^\circ$ szerinti alsó (illetve felső) korlátjai halmazának $\leq^\circ$ szerinti legnagyobb (illetve legkisebb) eleme és szintén b) alapján írható, hogy $\sup_{\leq}(X) = \inf_{\leq^\circ}(X)$ (llletve $\inf_{\leq}(X) = \sup_{\leq^\circ}(X)$). ■

6.12.8. Állítás. *Legyen $(E, \leq)$ rendezett halmaz. A következő állítások ekvivalensek.*
(i) *Az E halmaz minden nem üres, felülről korlátos részhalmazának létezik szuprémuma (vagyis $(E, \leq)$ teljesen rendezett halmaz).*

(ii) *Az E halmaz minden nem üres, alulról korlátos részhalmazának létezik infimuma.*

Bizonyítás. (i)$\Rightarrow$(ii) Legyen $X \subseteq E$ nem üres, $\leq$ szerint alulról korlátos halmaz, és jelölje X_* az X halmaz $\leq$ rendezés szerinti alsó korlátjainak halmazát, vagyis

$$X_* := \{y \in E | (\forall x \in X) : \ y \leq x\}.$$

Az X halmaz alulról korlátos $\leq$ szerint, ezért $X_* \neq \emptyset$. Másfelől, $X \neq \emptyset$, és ha $x \in X$, akkor X_* definíciója alapján minden $y \in X_*$ esetén $y \leq x$, vagyis x felső korlátja X_*-nak $\leq$ szerint. Tehát $X_* \subseteq E$ nem üres, $\leq$ szerint felülről korlátos halmaz, így (i) alapján létezik az $x_* := \sup(X_*)$ szuprémum. Megmutatjuk, hogy x_* az X halmaz legnagyobb alsó korlátja a $\leq$ rendezés szerint, vagyis $x_* = \inf(X)$.

Ha $x \in X$, akkor x felső korlátja X_*-nak $\leq$ szerint, így $x_* \leq x$, hiszen a definíció alapján x_* a legkisebb felső korlátja X_*-nak $\leq$ szerint. Ez azt jelenti, hogy x_* alsó korlátja X-nek $\leq$ szerint. Ha $y \in E$ a $\leq$ rendezés szerint alsó korlátja X-nek, akkor a definíció szerint $y \in X_*$, ezért $y \leq x_*$, hiszen x_* felső korlátja X_*-nak $\leq$ szerint. Ez azt jelenti, hogy x_* a legnagyobb alsó korlátja X-nek a $\leq$ rendezés szerint, vagyis $x_* = \inf(X)$.

(ii)$\Rightarrow$(i) Az előző állítás szerint (ii) azzal ekvivalens, hogy az Az E halmaz minden nem üres, felülről korlátos részhalmazának létezik szuprémuma a $\leq^\circ$ rendezés szerint. Ezért az imént igazolt (i)$\Rightarrow$(ii) következtetést alkalmazva az $(E, \leq)$ rendezett halmaz helyett az $(E, \leq^\circ)$ rendezett halmazra kapjuk, hogy az E halmaz minden nem üres, alulról korlátos részhalmazának létezik infimuma $\leq^\circ$ szerint. Ez viszont ismét az előző állítás szerint azzal ekvivalens, hogy az E halmaz minden nem üres, felülről korlátos részhalmazának létezik szuprémuma $(\leq^\circ)^\circ$ szerint, ami egyenlő az $\leq$ rendezéssel. ■

6.12.9. Állítás. (**A szuprémum és infimum kommutativitása**) *Legyen $(E, \leq)$ rendezett halmaz, $(x_i)_{i\in I}$ E-ben haladó rendszer, J halmaz, és $\sigma : J \to I$ szürjektív leképezés. Az $(x_i)_{i\in I}$ rendszernek pontosan akkor létezik szuprémuma (illetve infimuma), ha az $(x_{\sigma(j)})_{j\in J}$ rendszernek létezik szuprémuma (illetve infimuma), továbbá, ha az $(x_i)_{i\in I}$ rendszernek létezik szuprémuma (illetve infimuma), akkor*

$$\sup_{i\in I} x_i = \sup_{j\in J} x_{\sigma(j)}, \qquad \left(\textit{illetve } \inf_{i\in I} x_i = \inf_{j\in J} x_{\sigma(j)} \right).$$

Bizonyítás. A szuprémum (illetve infimum) definíciója szerint $\sup\limits_{i\in I} x_i$ (illetve $\inf\limits_{i\in I} x_i$) pontosan akkor létezik, ha az $X := \{x_i | i \in I\}$ halmaznak létezik szuprémuma (illetve infimuma) az $(E, \leq)$ rendezett halmazban. Hasonlóan, $\sup\limits_{j\in J} x_{\sigma(j)}$ (illetve $\inf\limits_{j\in J} x_{\sigma(j)}$) pontosan akkor létezik, ha az $X_\sigma := \{x_{\sigma(j)} | j \in J\}$) halmaznak létezik szuprémuma (illetve infimuma) az $(E, \leq)$ rendezett halmazban. Triviális, hogy $X_\sigma \subseteq X$, és mivel a $\sigma : J \to I$ leképezés szürjektív, így $X \subseteq X_\sigma$. Tehát $X = X_\sigma$, amiből azonnal következik az állítás. ■

6.12.10. Állítás. (**A szuprémum és infimum assszociativitása**) *Legyen $(E, \leq)$ rendezett halmaz, $(x_i)_{i\in I}$ E-ben haladó rendszer és $(I_j)_{j\in J}$ olyan halmazrendszer, hogy $I = \bigcup\limits_{j\in J} I_j$. Tegyük fel, hogy minden $j \in J$ esetén az $(x_i)_{i\in I_j}$ rendszernek létezik szuprémuma (illetve infimuma). Az $(x_i)_{i\in I}$ rendszernek pontosan akkor létezik szuprémuma (illetve* *infimuma), ha a* $\left(\sup_{i\in I_j} x_i\right)_{j\in J}$ *(illetve* $\left(\inf_{i\in I_j} x_i\right)_{j\in J}$*) rendszernek létezik szuprémuma (illetve infimuma), továbbá, ha az* $(x_i)_{i\in I}$ *rendszernek létezik szuprémuma (illetve infimuma), akkor*

$$\sup_{i\in I} x_i = \sup_{j\in J}\left(\sup_{i\in I_j} x_i\right), \qquad \left(\textit{illetve } \inf_{i\in I} x_i = \inf_{j\in J}\left(\inf_{i\in I_j} x_i\right)\right).$$

Bizonyítás. Minden $j \in J$ esetén legyen $y_j := \sup_{i\in I_j} x_i$.

Tegyük fel, hogy az $(y_j)_{j\in J}$ rendszernek létezik szuprémuma, és legyen $y := \sup_{j\in J} y_j$. Ha $i \in I$, akkor $I = \bigcup_{j\in J} I_j$ miatt van olyan $j \in J$, hogy $i \in I_j$, és ekkor $x_i \leq y_j \leq y$. Ez azt jelenti, hogy y felső korlátja az $(x_i)_{i\in I}$ rendszernek. Legyen $y' \in E$ tetszőleges felső korlátja az $(x_i)_{i\in I}$ rendszernek. Ha $j \in J$, akkor minden $i \in I_j \subseteq I$ esetén $x_i \leq y'$, tehát az y' felső korlátja az $(x_i)_{i\in I_j}$ rendszernek, így y_j definíciója szerint $y_j \leq y'$. Ez azt jelenti, hogy y' felső korlátja az $(y_j)_{j\in J}$ rendszernek is, tehát az y értelmezése alapján $y \leq y'$. Ezzel megmutattuk, hogy y az $(x_i)_{i\in I}$ rendszer legkisebb felső korlátja, vagyis az $(x_i)_{i\in I}$ rendszernek létezik szuprémuma, és

$$\sup_{i\in I} x_i = y = \sup_{j\in J} y_j = \sup_{j\in J}\left(\sup_{i\in I_j} x_i\right).$$

Megfordítva, tegyük fel, hogy az $(x_i)_{i\in I}$ rendszernek létezik szuprémuma, és legyen $x := \sup_{i\in I} x_i$. Ha $j \in J$, akkor minden $i \in I_j \subseteq I$ esetén $x_i \leq x$, ezért $y_j \leq x$. Tehát x felső korlátja az $(y_j)_{j\in J}$ rendszernek. Legyen $x' \in E$ tetszőleges felső korlátja az $(y_j)_{j\in J}$ rendszernek. Ekkor $i \in I$ esetén, $I = \bigcup_{j\in J} I_j$ miatt van olyan $j \in J$, hogy $i \in I_j$, ezért $x_i \leq y_i \leq x'$. Ez azt jelenti, hogy x' felső korlátja az $(x_i)_{i\in I}$ rendszernek, így az x definíciója szerint $x \leq x'$. Tehát x az $(y_j)_{j\in J}$ rendszer legkisebb felső korlátja, vagyis az $(y_j)_{j\in J}$ rendszernek létezik szuprémuma, és

$$\sup_{j\in J}\left(\sup_{i\in I_j} x_i\right) = \sup_{j\in J} y_j = x = \sup_{i\in I} x_i.$$

Az infimumokra vonatkozó állítás hasonló meggondolásokkal igazolható. ■

6.12.11. Állítás. *Legyen* $(E, \leq)$ *rendezett halmaz és* $(x_{i,j})_{(i,j)\in I\times J}$ *tetszőleges* E*-ben haladó rendszer.*

a) *Tegyük fel, hogy minden* $j \in J$ *esetén az* $(x_{i,j})_{i\in I}$ *rendszernek létezik szuprémuma (illetve infimuma). Az* $(x_{i,j})_{(i,j)\in I\times J}$ *rendszernek pontosan akkor létezik szuprémuma (illetve infimuma), ha a* $\left(\sup_{i\in I} x_{i,j}\right)_{j\in J}$ *(illetve* $\left(\inf_{i\in I} x_{i,j}\right)_{j\in J}$*) rendszernek létezik szuprémuma (illetve infimuma), továbbá, ha az* $(x_{i,j})_{(i,j)\in I\times J}$ *rendszernek létezik szuprémuma (illetve infimuma), akkor*

$$\sup_{(i,j)\in I\times J} x_{i,j} = \sup_{j\in J}\left(\sup_{i\in I} x_{i,j}\right)$$

$$\left(\textit{illetve:} \quad \inf_{(i,j)\in I\times J} x_{i,j} = \inf_{j\in J}\left(\inf_{i\in I} x_{i,j}\right)\right).$$

b) *Tegyük fel, hogy minden $i \in I$ esetén az $(x_{i,j})_{j\in J}$ rendszernek létezik szuprémuma (illetve infimuma). Az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek pontosan akkor létezik szuprémuma (illetve infimuma), ha a $\left(\sup_{j\in J} x_{i,j}\right)_{i\in I}$ (illetve $\left(\inf_{j\in J} x_{i,j}\right)_{i\in I}$) rendszernek létezik szuprémuma (illetve infimuma), továbbá, ha az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek létezik szuprémuma (illetve infimuma), akkor*

$$\sup_{(i,j)\in I\times J} x_{i,j} = \sup_{i\in I}\left(\sup_{j\in J} x_{i,j}\right)$$

$$\left(\textit{illetve:}\quad \inf_{(i,j)\in I\times J} x_{i,j} = \inf_{i\in I}\left(\inf_{j\in J} x_{i,j}\right)\right).$$

c) *Tegyük fel, hogy minden $j \in J$ esetén az $(x_{i,j})_{i\in I}$ rendszernek létezik szuprémuma (illetve infimuma), és minden $i \in I$ esetén az $(x_{i,j})_{j\in J}$ rendszernek létezik szuprémuma (illetve infimuma). Tegyük fel, hogy az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek létezik szuprémuma (illetve infimuma). Ekkor a $\left(\sup_{i\in I} x_{i,j}\right)_{j\in J}$ (illetve $\left(\inf_{i\in I} x_{i,j}\right)_{j\in J}$) rendszernek létezik szuprémuma (illetve infimuma), és a $\left(\sup_{j\in J} x_{i,j}\right)_{i\in I}$ (illetve $\left(\inf_{j\in J} x_{i,j}\right)_{i\in I}$) rendszernek létezik szuprémuma (illetve infimuma), továbbá*

$$\sup_{(i,j)\in I\times J} x_{i,j} = \sup_{j\in J}\left(\sup_{i\in I} x_{i,j}\right) = \sup_{i\in I}\left(\sup_{j\in J} x_{i,j}\right)$$

$$\left(\textit{illetve:}\quad \inf_{(i,j)\in I\times J} x_{i,j} = \inf_{j\in J}\left(\inf_{i\in I} x_{i,j}\right) = \inf_{i\in I}\left(\inf_{j\in J} x_{i,j}\right)\right).$$

Bizonyítás. a) Minden $j \in J$ esetén legyen $x_j := \sup_{i\in I} x_{i,j}$.

Tegyük fel, hogy az $(x_j)_{j\in J}$ rendszernek létezik szuprémuma, és legyen $x := \sup_{j\in J} x_j$. Ekkor minden $(i,j) \in I \times J$ esetén $x_{i,j} \le x_j \le x$, tehát x felső korlátja az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek a $\le$ rendezés szerint. Legyen $x' \in E$ tetszőleges felső korlátja az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek. Ekkor $j \in J$ esetén minden $I \in i$-re $x_{i,j} \le x'$, vagyis x' felső korlátja az $(x_{i,j})_{i\in I}$ rendszernek, így $x_j \le x'$. Ez azt jelenti, hogy x' felső korlátja az $(x_j)_{j\in J}$ rendszernek, tehát az x definíciója szerint $x \le x'$. Ez azt jelenti, hogy x a legkisebb felső korlátja az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek, vagyis az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek létezik szuprémuma, és

$$\sup_{(i,j)\in I\times J} x_{i,j} = x = \sup_{j\in J} x_j = \sup_{j\in J}\left(\sup_{i\in I} x_{i,j}\right).$$

Megfordítva, tegyük fel, hogy az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek létezik szuprémuma, és legyen $x := \sup_{(i,j)\in I\times J} x_{i,j}$. Ha $j \in J$, akkor minden $I \ni i$-re $x_{i,j} \le x$, ezért az x_j definíciója szerint $x_j \le x$, vagyis x felső korlátja az $(x_j)_{j\in J}$ rendszernek. Legyen $x' \in E$ tetszőleges felső korlátja az $(x_j)_{j\in J}$ rendszernek. Ekkor minden $i \in I$ és $j \in J$ esetén $x_{i,j} \le x_j \le x'$, tehát x' felső korlátja az $(x_{i,j})_{(i,j)\in I\times J}$ rendszernek, tehát az x definíciója szerint $x \le x'$. Ez azt jelenti, hogy x a legkisebb felső korlátja az $(x_j)_{j\in J}$ rendszernek, vagyis az $\left(\sup_{i\in I} x_{i,j}\right)_{j\in J}$ rendszernek létezik szuprémuma, és

$$\sup_{j\in J}\left(\sup_{i\in I} x_{i,j}\right) = \sup_{j\in J} x_j = x = \sup_{(i,j)\in I\times J} x_{i,j}.$$

Az infimumokra vonatkozó állítás hasonló meggondolásokkal igazolható.

b) Az a) állítás bizonyításának mintájára végezhető el.

c) Az a) és b) állításokból azonnal következik. ■

6.12.12. Definíció. *Ha $(E, \leq)$ rendezett halmaz, akkor $x, x' \in E$ esetén $x < x'$ vagy $x' > x$ az $(x \leq x') \wedge (x \neq x')$ kijelentés rövidítése, és ha $x < x'$, akkor azt mondjuk, hogy x'* **szigorúan nagyobb** *x-nél a $\leq$ rendezés szerint, vagy x* **szigorúan kisebb** *x-nél a $\leq$ rendezés szerint*

6.12.13. Állítás. *Legyen $(E, \leq)$ lineárisan rendezett halmaz és $X \subseteq E$. Az $y \in E$ elem pontosan akkor szuprémuma az X halmaznak, ha y felső korlátja X-nek és minden $z \in E$ elemhez, $z < y$ esetén létezik olyan $x \in X$, hogy $z < x$.*

Bizonyítás. Tegyük fel, hogy y rendelkezik ezekkel a tulajdonságokkal. Ekkor y felső korlátja X-nek, és ha z szintén felső korlátja X-nek, akkor $z < y$ lehetetlen, különben a feltevés alapján létezne olyan $x \in X$, hogy $z < x$, ami ellentmond annak, hogy z felső korlátja X-nek. Tehát ha z felső korlátja X-nek, akkor $z < y$ nem igaz, ugyanakkor $(E, \leq)$ lineárisan rendezett halmaz, ezért $y \leq z$, vagyis y a legkisebb felső korlátja X-nek. Megfordítva, legyen y szuprémuma X-nek. Ekkor y a legkisebb felső korlátja X-nek, tehát ha $z \in E$ olyan elem, hogy $z < y$, akkor z nem lehet felső korlátja X-nek, így létezik olyan $x \in X$, hogy $x \leq z$ nem igaz. De $(E, \leq)$ lineárisan rendezett halmaz, ezért ekkor szükségképpen $z < x$. ■

6.12.14. Állítás. *Legyen $(E, \leq)$ lineárisan rendezett halmaz és $x, y \in E$. A következő állítások ekvivalensek.*

(i) $x \leq y$.

(ii) *Minden $z \in E$ esetén, ha $z < x$, akkor $z \leq y$.*

(iii) *Minden $z \in E$ esetén, ha $y < z$, akkor $x \leq z$.*

Bizonyítás. (i)⇒(ii) és (i)⇒(iii) a $\leq$ rendezés tranzitivitása miatt nyilvánvaló, mert ha $x \leq y$ és $z \in E$ olyan, hogy $z < x$ (illetve $y < z$), akkor $z \leq x$ (illetve $y \leq z$), ezért $z \leq y$ (illetve $x \leq z$). (Ezek az implikációk tehát akkor is igazak, ha a $\leq$ rendezés nem lineáris.)

Ha (i) nem igaz, akkor a $\leq$ rendezés linearitása folytán $y < x$, ezért $z := y$ (illetve $z := x$) olyan eleme E-nek, hogy $z < x$ (illetve $y < z$), azonban $y < z$ (illetve $z < x$), tehát $z \leq y$ (illetve $x \leq z$) nem igaz. Ez azt jelenti, hogy a $\neg$(i) $\Rightarrow \neg$(ii) és $\neg$(i) $\Rightarrow \neg$(iii) implikációk igazak, ezért a (ii)⇒(i) és (iii)⇒(i) következtetések is igazak. ■

6.12.15. Definíció. *Legyen $(E, \leq)$ rendezett halmaz. Minden $x, y \in E$ esetén*

$$\begin{aligned}
&[x, y] := \{z | (z \in E) \wedge (x \leq z) \wedge (z \leq y)\} && [x, \rightarrow [:= \{z | (z \in E) \wedge (x \leq z)\} \\
&[x, y[:= \{z | (z \in E) \wedge (x \leq z) \wedge (z < y)\} &&]x, \rightarrow [:= \{z | (z \in E) \wedge (x < z)\} \\
&]x, y] := \{z | (z \in E) \wedge (x < z) \wedge (z \leq y)\} &&] \leftarrow, x] := \{z | (z \in E) \wedge (z \leq x)\} \\
&]x, y[:= \{z | (z \in E) \wedge (x < z) \wedge (z < y)\} &&] \leftarrow, x[:= \{z | (z \in E) \wedge (z < x)\}
\end{aligned}$$

Az ilyen alakú halmazokat **intervallumoknak** *nevezzük. Továbbá, $x, y \in E$ esetén az $]x, y[$, $]x, \rightarrow [$ és $] \leftarrow, x[$ alakú intervallumokat* **nyílt** *intervallumoknak, valamint az $[x, y]$, $[x, \rightarrow [$ és $] \leftarrow, x]$ alakú intervallumokat* **zárt** *intervallumoknak nevezzük. Ha $x, y \in E$, akkor az $[x, y[$ és $[x, \rightarrow [$ (illetve $]x, y]$ és $] \leftarrow, x]$) alakú intervallumokat* **balról zárt, jobbról nyílt** (*illetve* **balról nyílt, jobbról zárt**) *intervallumoknak nevezzük.*

6.12.16. Definíció. *Legyenek $(E, \leq)$ és $(E', \leq')$ rendezett halmazok.*

– *Azt mondjuk, hogy az $f : E \to E'$ függvény* **monoton növő** *(illetve* **monoton fogyó***), ha minden $x, y \in E$ elemre, $x \leq y$ esetén $f(x) \leq' f(y)$ (illetve $f(y) \leq' f(x)$).*

– *Azt mondjuk, hogy az $f : E \to E'$ függvény* **szigorúan monoton növő** *(illetve* **szigorúan monoton fogyó***), ha minden $x, y \in E$ elemre, $x < y$ esetén $f(x) <' f(y)$ (illetve $f(y) <' f(x)$).*

– *Azt mondjuk, hogy az $f : E \to E'$ függvény* **izomorfizmus** *az $(E, \leq)$ és $(E', \leq')$ rendezett halmazok között, ha f bijekció és minden $x, y \in E$ elemre $x \leq y$ ekvivalens azzal, hogy $f(x) \leq' f(y)$.*

– *Az $(E, \leq)$ és $(E', \leq')$ rendezett halmazokat* **izomorfaknak** *mondjuk, ha létezik izomorfizmus az $(E, \leq)$ és $(E', \leq')$ rendezett halmazok között.*

Könnyen látható, hogy ha $(E, \leq)$ rendezett halmaz és $(E', \leq')$ lineárisan rendezett halmaz, akkor egy $f : E \to E'$ függvény pontosan akkor izomorfizmus $(E, \leq)$ és $(E', \leq')$ között, ha f bijekció E és E' között, valamint f és f^{-1} mindketten monoton növekvőek. Azonban, ha $(E', \leq')$ nem lineárisan rendezett, akkor az f szigorú monoton növéséből nem következik az f injektivitása, de még ha injektív is az f függvény, akkor is előfordulhat, hogy $x, y \in E$, $f(x) <' f(y)$, de $x < y$ nem igaz.

6.13. Jólrendezett halmazok

6.13.1. Definíció. *A $(E, \leq)$ párt* **jólrendezett halmaznak** *nevezzük, ha rendezett halmaz és az E minden nem üres részhalmazának létezik legkisebb eleme. Az E halmaz feletti $\leq$ relációt* **jólrendezésnek** *nevezzük, ha $(E, \leq)$ jólrendezett halmaz.*

Minden $(E, \leq)$ jólrendezett halmaz lineárisan rendezett, mert ha $x, y \in E$, akkor a jólrendezettség miatt az $\{x, y\}$ halmaznak van legkisebb eleme, ezért x és y összehasonlíthatók a $\leq$ rendezés szerint.

Egyáltalán nem nyilvánvaló az, hogy minden halmaz felett létezik jólrendezés, pedig ez a helyzet; ezt mondja ki a *Zermelo-féle jólrendezési tétel* (6.15.2.). Például a valós számok halmazán (amelyről a **23.5.** pontban lesz szó) szintén létezik jólrendezés, de eddig még nem sikerült konkrét jólrendezést megadni ezen a halmazon.

6.13.2. Állítás. *Ha $(E, \leq)$ jólrendezett halmaz, $E' \subseteq E$ és $\leq'$ jelöli a $\leq$ reláció megszorítását E'-re, akkor $(E', \leq')$ is jólrendezett halmaz.*

Bizonyítás. Legyen $H \subseteq E'$ tetszőleges nem üres halmaz. Ekkor $H \subseteq E$ nem üres halmaz, és $\leq$ jólrendezés E felett, így létezik H-nak legkisebb eleme a $\leq$ rendezés szerint: legyen ez x. Ekkor $y \in H$ esetén $x \leq y$, így $x, y \in E'$ miatt $x \leq' y$ is teljesül, tehát x a H halmaz legkisebb eleme a $\leq'$ rendezés szerint is. ■

6.13.3. Állítás. *Legyen $(E, \leq)$ jólrendezett halmaz és $\mathfrak{a}$ olyan halmaz, hogy $\mathfrak{a} \notin E$. Ha $E' := E \cup \{\mathfrak{a}\}$ és*

$$\leq' := \leq \cup (E \times \{\mathfrak{a}\}) \cup \{(\mathfrak{a}, \mathfrak{a})\}$$

akkor $\leq'$ olyan jólrendezés a E' halmaz felett, amely szerint $\mathfrak{a}$ az E' legnagyobb eleme és amelynek megszorítása E-re egyenlő a $\leq$ relációval.

Bizonyítás. Egyszerű esetszétválasztásokkal könnyen belátható, hogy $\leq'$ rendezés E' felett. Az is nyilvánvaló, hogy $\mathfrak{a}$ az E' halmaz legnagyobb eleme $\leq'$ szerint, és $\leq'$ megszorítása E-re egyenlő a $\leq$ relációval.

Legyen $H \subseteq E'$ nem üres halmaz, ekkor két eset lehetséges.

– Ha $H \cap E = \emptyset$, akkor $H = \{\mathfrak{a}\}$, tehát $\mathfrak{a}$ a H halmaz legkisebb eleme a $\leq'$ rendezés szerint.

– Ha $H \cap E \neq \emptyset$, akkor legyen x a $H \cap E$ halmaz legkisebb eleme a $\leq$ jólrendezés szerint. Ha $x' \in H$ és $x' \notin E$, akkor $x' = \mathfrak{a}$, így $x \leq' x'$. Ha $x' \in H$ és $x' \in E$, akkor $x' \in H \cap E$, tehát $x \leq x'$, így $x \leq' x'$. Ezért x a H halmaz legkisebb eleme a $\leq'$ rendezés szerint. ■

6.13.4. Definíció. *Legyen $(E, \leq)$ rendezett halmaz. Az $X \subseteq E$ halmaz* **maximális** *(illetve* **minimális***) elemének nevezünk minden olyan $x \in X$ elemet, amelyre teljesül az, hogy X-nek nem létezik x-nél szigorúan nagyobb (illetve szigorúan kisebb) eleme, vagyis minden $x' \in X$ esetén, ha $x \leq x'$ (illetve $x' \leq x$), akkor $x = x'$.*

Legyen $(E, \leq)$ rendezett halmaz, $X \subseteq E$, és $x \in X$. Ekkor az "x maximális eleme X-nek a $\leq$ rendezés szerint" kijelentés a következő ekvivalencia-lánc fennállása miatt ekvivalens azzal, hogy "minden $x' \in X$ esetén, ha $x \leq x'$ akkor $x = x'$":

$$\neg(\exists x')(\ x' \in X \wedge (x \leq x' \wedge x \neq x')\ ) \Leftrightarrow (\forall x')(\ x' \notin X \vee (x \nleq x' \vee x = x'))\ ) \Leftrightarrow$$
$$\Leftrightarrow (\forall x')(\ x' \in X \Rightarrow (x \leq x' \Rightarrow x = x'))\ ) \Leftrightarrow (\forall x' \in X)(\ x \leq x' \Rightarrow x = x'\ ).$$

Látható, hogy itt az egzisztenciális kvantor negációjának szabályát (**LOG** 2.6.2.), a logikai de Morgan-tételt (**LOG** 2.5.12.), az implikáció definícióját (**LOG** 2.1.9.), a feltételes univerzális kvantor definícióját (**LOG** 2.2.5.), az általánosítás szabályát (**LOG** 2.6.7.), és a szigorú egyenlőtlenség definícióját (6.12.12.) alkalmaztuk. Hasonlóan kapjuk, hogy az "x minimális eleme X-nek a $\leq$ rendezés szerint" kijelentés a következő ekvivalencia-lánc fennállása miatt ekvivalens azzal, hogy "minden $x' \in X$ esetén, ha $x' \leq x$ akkor $x = x'$":

$$\neg(\exists x')(\ x' \in X \wedge (x' \leq x \wedge x \neq x')\ ) \Leftrightarrow (\forall x')(\ x' \notin X \vee (x' \nleq x \vee x = x'))\ ) \Leftrightarrow$$
$$\Leftrightarrow (\forall x')(\ x' \in X \Rightarrow (x' \leq x \Rightarrow x = x'))\ ) \Leftrightarrow (\forall x' \in X)(\ x' \leq x \Rightarrow x = x'\ ).$$

Vigyázzunk arra, hogy ha $(E, \leq)$ rendezett halmaz és $X \subseteq E$, akkor az X legnagyobb (illetve legkisebb) eleme (ha létezik) az X-nek maximális (illetve minimális) eleme, azonban létezhetnek X-nek olyan maximális (illetve minimális) elemei, amelyek az X bizonyos elemeivel nem hasonlíthatók össze. A definíció alapján nyilvánvaló, hogy ha az $x \in X$ elem nem hasonlítható össze X egyetlen x-től különböző elemével sem, akkor x egyszerre maximális és minimális eleme is X-nek.

Bizonyos matematikai objektumok egyes tulajdonságai egyenértékűek valamely rendezés szerinti maximalitással, ezért ilyen tulajdonságú objektumok *létezésének* bizonyíthatósága szempontjából fontos szerepe lehet minden olyan állításnak, amely – eléggé általános feltételek mellett – maximális elemek létezését mondja ki rendezett halmazokban. Ilyen állítás a *Kuratowski–Zorn-lemma*, amelyről a következő pontban lesz szó, és amelynek bizonyításához szükség lesz a következő definícióra és állításra.

6.13.5. Definíció. *Az $(E, \leq)$ rendezett halmaz* **szegmensének** *nevezünk minden olyan $S \subseteq E$ halmazt, amelyre teljesül az, hogy minden $x \in S$ elemre $]\leftarrow, x] \subseteq S$. Az $(E, \leq)$ rendezett halmaz E-től különböző szegmenseit* **valódi szegmenseknek** *nevezzük.*

Nyilvánvaló, hogy ha $(E, \leq)$ rendezett halmaz, akkor minden $x \in E$ elemre az $]\leftarrow, x]$ intervallum szegmens, és az $]\leftarrow, x[$ intervallum valódi szegmens.

6.13.6. Állítás. *Legyen $(E, \leq)$ jólrendezett halmaz és E^* az E valódi szegmenseinek hamaza. Ekkor az*

$$E \to E^*; \quad x \mapsto]\leftarrow, x[$$

leképezés izomorfizmus az $(E, \leq)$ és $(E^*, \subseteq_{E^*})$ rendezett halmazok között. (*Vagyis olyan bijekció az E és E^* halmazok között, hogy minden $x, x' \in E$ elemre, $x \leq x'$ ekvivalens azzal, hogy $]\leftarrow, x[\subseteq]\leftarrow, x'[$.*)

Bizonyítás. Ha $x, x' \in E$ és $x \leq x'$, akkor a $\leq$ rendezés tranzitivitása következtében $]\leftarrow, x[\subseteq]\leftarrow, x'[$, tehát az adott függvény monoton növő az $(E, \leq)$ és $(E^*, \subseteq_{E^*})$ rendezett halmazok között.

Megfordítva: legyenek $x, x' \in E$ és tegyük fel, hogy $x \not\leq x'$. Ekkor a $\leq$ rendezés linearitása folytán $x' < x$, azaz $x' \in]\leftarrow, x[$, ugyanakkor nyilvánvalóan $x' \notin]\leftarrow, x'[$, tehát $]\leftarrow, x[\not\subseteq]\leftarrow, x'[$. Ez azt jelenti, hogy ha $x, x' \in E$ és $]\leftarrow, x[\subseteq]\leftarrow, x'[$, akkor $x \leq x'$.

Ezzel megmutattuk, hogy minden $x, x' \in E$ esetén az $x \leq x'$ és $]\leftarrow, x[\subseteq]\leftarrow, x'[$ kijelentések ekvivalensek. A $\leq$ rendezés tranzitivitása miatt ebből következik az adott függvény injektivitása. (Megjegyezzük, hogy eddig csak azt használtuk fel, hogy $(E, \leq)$ *lineárisan* rendezett halmaz.)

Megmutatjuk, hogy a szóban forgó függvény szürjekció. Ehhez legyen $S \subseteq E$ valódi szegmens, és olyan $x \in E$ elemet keresünk, hogy $S =]\leftarrow, x[$. Ekkor $E \setminus S \neq \emptyset$, tehát van olyan $x \in E \setminus S$, hogy x az $E \setminus S$ legkisebb eleme. Ha $y \in]\leftarrow, x[$, akkor $y \in S$, különben $y \in E \setminus S$ teljesülne, tehát $x \leq y$ igaz volna. Ezért $]\leftarrow, x[\subseteq S$. Ha $y \in S$, akkor $y \leq x$ vagy $x \leq y$; világos, hogy $x \leq y$ lehetetlen, mert S szegmens, $y \in S$ és $x \notin S$, így $y \leq x$ és persze $x \neq y$, tehát $y \in]\leftarrow, x[$. Ezért $S \subseteq]\leftarrow, x[$ is teljesül. ■

Megjegyezzük, hogy az előző állítás továbbiak szempontjából legfontosabb része az, hogy ha $(E, \leq)$ jólrendezett halmaz, akkor minden $S \subseteq E$ valódi szegmenshez létezik olyan $x \in E$, amelyre $S =]\leftarrow, x[$ (vagyis az $E \to E^*;\ x \mapsto]\leftarrow, x[$ leképezés *szürjektív*).

6.13.7. Állítás. *Ha $(E, \leq)$ jólrendezett halmaz és $(S_i)_{i \in I}$ szegmensek tetszőleges rendszere, akkor $\bigcup_{i \in I} S_i$ is szegmens.*

Bizonyítás. Feltehető, hogy az $S := \bigcup_{i \in I} S_i$ halmaz nem egyenlő E-vel (különben az állítás igaz). Legyen x az $E \setminus S$ halmaz legkisebb eleme; igazoljuk, hogy $S =]\leftarrow, x[$. Valóban, minden $y \in E \setminus S$ elemre $x \leq y$, vagyis $y \in E \setminus]\leftarrow, x[$, ezért $]\leftarrow, x[\subseteq S$. Megfordítva, ha $y \in S$, akkor van olyan $i \in I$, hogy $y \in S_i$. Ha $x \leq y$ teljesülne, akkor $x \in S_i$, mert S_i szegmens, tehát $x \in S$ igaz volna, holott $x \notin S$. Ezért $y < x$, ami azt jelenti, hogy $S \subseteq]\leftarrow, x[$. ■

6.13.8. Állítás. (**Jólrendezett halmazok összeragasztása**) *Legyen $((E_i, \leq_i))_{i \in I}$ jólrendezett halmazoknak olyan rendszere, hogy minden $i, j \in I$ indexre a következő állítások valamelyike teljesül:*

1) *az E_i halmaz szegmense az $(E_j, \leq_j)$ jólrendezett halmaznak és $\leq_i$ egyenlő a $\leq_j$ rendezés E_i-re vett megszorításával;*

2) *az E_j halmaz szegmense az $(E_i, \leq_i)$ jólrendezett halmaznak és $\leq_j$ egyenlő a $\leq_i$ rendezés E_j-re vett megszorításával.*

Legyen továbbá $E := \bigcup_{i \in I} E_i$. Ekkor teljesülnek a következő állítások.

a) *Az E halmaz felett létezik egyetlen olyan $\leq$ rendezés, hogy minden $i \in I$ indexre $\leq_i$ egyenlő a $\leq$ rendezés E_i-re vett megszorításával; ez a rendezés jólrendezés E felett.*

b) *Minden $i \in I$ esetén az $(E_i, \leq_i)$ jólrendezett halmaz minden szegmense az $(E, \leq)$ jólrendezett halmaznak is szegmense.*

c) *Minden $i \in I$ és $x \in E_i$ esetén az $]\leftarrow, x[$ intervallum az $(E_i, \leq_i)$ jólrendezett halmazban ugyanaz, mint az $(E, \leq)$ jólrendezett halmazban.*

d) *Az $(E, \leq)$ jólrendezett halmaz minden S valódi szegmenséhez létezik olyan $i \in I$, hogy S valódi szegmense az $(E_i, \leq_i)$ jólrendezett halmaznak.*

Bizonyítás. a) A hipotézis alapján minden $i, j \in I$ esetén $E_i \subseteq E_j$ és $\leq_i$ részhalmaza $\leq_j$-nek, vagy $E_j \subseteq E_i$ és $\leq_j$ részhalmaza $\leq_i$-nek. Ezért a 6.10.9. állítás alapján a $\leq := \bigcup_{i \in I} \leq_i$ reláció *lineáris rendezés* az E halmaz felett.

Megmutatjuk, hogy minden $i \in I$ indexre $\leq_i$ egyenlő a $\leq$ rendezés E_i-re vett megszorításával. Nyilvánvaló, hogy $i \in I$, $x, y \in E_i$ és $x \leq_i y$ esetén $x \leq y$ és $(x, y) \in E_i \times E_i$. Ez azt jelenti, hogy minden $i \in I$ esetén $\leq_i$ részhalmaza az $\leq \cap (E_i \times E_i)$ megszorításnak. Megfordítva: tegyük fel, hogy $i \in I$, és $(x, y) \in \leq \cap (E_i \times E_i)$, vagyis $x, y \in E_i$ és $x \leq y$. Ekkor a $\leq$ reláció definíciója szerint vehetünk olyan $j \in I$ indexet, hogy $(x, y) \in \leq_j$, vagyis $(x, y) \in E_j \times E_j$ és $x \leq_j y$. A hipotézis alapján $E_i \subseteq E_j$ és $\leq_j$ megszorítása E_i-re egyenlő $\leq_i$-vel, vagy $E_j \subseteq E_i$ és $\leq_i$ megszorítása E_j-re egyenlő $\leq_j$-vel. Az első esetben $(x, y) \in \leq_j \cap (E_i \times E_i) = \leq_i$. A második esetben $(x, y) \in \leq_j = \leq_i \cap (E_j \times E_j)$, tehát $(x, y) \in \leq_i$. Ez azt jelenti, hogy minden $i \in I$ esetén a $\leq \cap (E_i \times E_i)$ megszorítás részhalmaza $\leq_i$-nek.

Most megmutatjuk, hogy $\leq$ jólrendezés E felett. Ehhez legyen $H \subseteq E$ nem üres halmaz. Ekkor $H = E \cap H = \bigcup_{i \in I} (E_i \cap H)$ miatt vehetünk olyan $i \in I$ indexet, amelyre $E_i \cap H \neq \emptyset$. A $\leq_i$ reláció jólrendezés az E_i halmaz felett, ezért az $E_i \cap H$ halmaznak létezik a legkisebb eleme a $\leq_i$ rendezés szerint: jelölje ezt az elemet x. Igazolni fogjuk, hogy x a H halmaz legkisebb eleme a $\leq$ rendezés szerint. Ehhez legyen $y \in H$ tetszőleges elem, és vegyünk olyan $j \in I$ indexet, amelyre $y \in E_j$. Azt kell bizonyítani, hogy $x \leq y$. A hipotézis szerint az i és j indexekre az 1) vagy a 2) eset lehetséges.

Tegyük fel, hogy az első eset teljesül, és indirekt tegyük fel, hogy $x \not\leq y$, vagyis a $\leq$ rendezés linearitása folytán $y < x$. Az 1) feltétel alapján $x \in E_i \cap H \subseteq E_j \cap H$, ugyanakkor $y \in E_j \cap H$ is teljesül, ezért $x \leq_j y$ lehetetlen, különben $x \leq y$, ami ellentmond az $y < x$ indirekt hipotézisnek. Tehát $y <_j x$, és mivel $x \in E_i$ és E_i szegmense az $(E_j, \leq_j)$ jólrendezett halmaznak, így $y \in E_i$. Ez azt jelenti, hogy $y \in E_i \cap H$, tehát az x elem definíciója szerint $x \leq_i y$. Ebből következik, hogy $x \leq_j y$, mert $\leq_i$ egyenlő $\leq_j$ megszorításával E_i-re. Ez viszont ellentmond annak, hogy $y <_j x$.

Tegyük fel, hogy a második eset teljesül. Ekkor $y \in E_j \subseteq E_i$, tehát $y \in E_i \cap H$, így az x elem definíciója szerint $x \leq_i y$. Ebből azonnal következik, hogy $x \leq y$, mert $\leq_i$ egyenlő a $\leq$ rendezés E_i-re vett megszorításával.

Tehát $\leq$ olyan jólrendezés az E halmaz felett, hogy minden $i \in I$ indexre $\leq_i$ egyenlő a $\leq$ reláció E_i-re vett megszorításával. Ez a $\leq$ jólrendezés ezzel a tulajdonsággal még az összes E feletti relációk halmazában is egyértelműen van meghatározva. Valóban, ha R olyan reláció, hogy $R \subseteq E \times E$ és minden $i \in I$ esetén $\leq_i$ egyenlő $R \cap (E_i \times E_i)$-vel, akkor

$$\leq \,=\, \bigcup_{i \in I} \leq_i \,=\, \bigcup_{i \in I} (R \cap (E_i \times E_i)) \;=\; R \cap \bigcup_{i \in I} (E_i \times E_i) \;=\; R \cap (E \times E) \;=\; R,$$

mert az $(E_i)_{i \in I}$ halmazrendszer tartalmazás tekintetében *felfelé irányított*, tehát

$$\bigcup_{i \in I} (E_i \times E_i) = \Big(\bigcup_{i \in I} E_i\Big) \times \Big(\bigcup_{i \in I} E_i\Big) = E \times E$$

(ld. 6.9.10.).

b) Legyen $i \in I$ és $S \subseteq E_i$ szegmense az $(E_i, \leq_i)$ jólrendezett halmaznak. Megmutatjuk, hogy ekkor S szegmense az $(E, \leq)$ jólrendezett halmaznak is. Ehhez legyen $x \in S$, $y \in E$ és $y \leq x$. Azt kell igazolni, hogy $y \in S$ teljesül. Ennek bizonyításához legyen $j \in I$ olyan, hogy $y \in E_j$. A hipotézis szerint az i és j indexekre az 1) vagy a 2) eset lehetséges.

Tegyük fel, hogy az első eset teljesül. Ekkor $x \in E_i \subseteq E_j$ miatt $x, y \in E_j$ és $y \leq x$, ezért $y \leq_j x$, hiszen $\leq_j$ egyenlő a $\leq$ reláció E_j-re vett megszorításával. Ugyanakkor $x \in E_i$ és a feltevés szerint E_i szegmense az $(E_j, \leq_j)$ jólrendezett halmaznak, ezért $y \in E_i$. Tehát $x, y \in E_i$ és $y \leq_j x$, ezért $y \leq_i x$, hiszen $\leq_i$ egyenlő az $\leq_j$ reláció E_i-re vett megszorításával. Mivel $x \in S$ és S szegmense az $(E_i, \leq_i)$ jólrendezett halmaznak, ebből kapjuk, hogy $y \in S$.

Tegyük fel, hogy a második eset teljesül. Ekkor $y \in E_j \subseteq E_i$ miatt $y \in E_i$. Tehát $x, y \in E_i$ és $y \leq_i x$, mert $\leq_i$ egyenlő az $\leq$ reláció E_i-re vett megszorításával és $y \leq x$. Mivel $x \in S$ és S szegmense az $(E_i, \leq_i)$ jólrendezett halmaznak, ebből következik, hogy $y \in S$.

c) Minden $i \in I$ és $x \in E_i$ esetén legyen $]\leftarrow, x[_i := \{y \in E_i | y <_i x\}$ és $]\leftarrow, x[:= \{y \in E | y < x\}$. Megmutatjuk, hogy ha $i \in I$ és $x \in E_i$, akkor $]\leftarrow, x[_i =]\leftarrow, x[$.

Ha $y \in]\leftarrow, x[_i$, akkor $x, y \in E_i$ és $y <_i x$, ezért $y < x$, mert $\leq_i$ egyenlő a $\leq$ reláció E_i-re vett megszorításával. Tehát $]\leftarrow, x[_i \subseteq]\leftarrow, x[$.

Megfordítva: legyen $y \in]\leftarrow, x[$, azaz $y < x$. Vegyünk olyan $j \in I$ indexet, hogy $y \in E_j$. A hipotézis szerint az i és j indexekre az 1) vagy a 2) eset lehetséges.

Tegyük fel, hogy az első eset teljesül. Ekkor $x \in E_i \subseteq E_j$ miatt $x, y \in E_j$ és $y < x$, ezért $y <_j x$, hiszen $\leq_j$ egyenlő a $\leq$ reláció E_j-re vett megszorításával. Ugyanakkor $x \in E_i$ és a feltevés szerint E_i szegmense az $(E_j, \leq_j)$ jólrendezett halmaznak, ezért $y \in E_i$. Tehát $x, y \in E_i$ és $y <_j x$, ezért $y <_i x$, hiszen $\leq_i$ egyenlő az $\leq_j$ reláció E_i-re vett megszorításával. Ez azt jelenti, hogy $y \in]\leftarrow, x[_i$.

Tegyük fel, hogy a második eset teljesül. Ekkor $y \in E_j \subseteq E_i$, tehát $x, y \in E_i$, és $y < x$, ezért $y <_i x$, mert $\leq_i$ egyenlő a $\leq$ reláció E_i-re vett megszorításával. Ez azt jelenti, hogy $y \in]\leftarrow, x[_i$.

d) Nyilvánvalóan következik c)-ből és a 6.13.6. állításból. ■

6.13.9. Állítás. *Legyen $(E_1, \leq_1)$ jólrendezett és $(E_2, \leq_2)$ lineárisan rendezett halmaz, és tegyük fel, hogy $f, g : E_1 \to E_2$ olyan monoton növő függvények, hogy $\mathrm{Im}(f)$ szegmens E_2-ben és g szigorúan monoton növő. Ekkor minden $x \in E_1$ elemre $f(x) \leq_2 g(x)$ teljesül.*

Bizonyítás. Indirekt tegyük fel, hogy az $S := \{x \in E_1 | f(x) \not\leq_2 g(x)\}$ halmaz nem üres. A $\leq_2$ rendezés linearitása miatt $S = \{x \in E_1 | g(x) <_2 f(x)\}$. A $\leq_1$ rendezés jólrendezés, ezért létezik S-nek legkisebb eleme $\leq_1$ szerint; legyen ez x. Ekkor $g(x) <_2 f(x) \in \mathrm{Im}(f)$ és $\mathrm{Im}(f)$ szegmense $(E_2, \leq_2)$-nek, ezért $g(x) \in \mathrm{Im}(f)$, így létezik olyan $x' \in E_1$, amelyre $f(x') = g(x)$. Ha $x' <_1 x$ teljesülne, akkor a g szigorú monoton növése folytán $g(x') <_2 g(x) = f(x')$ teljesülne, tehát $x' \in S$ is igaz lenne. Ez viszont lehetetlen, mert x az S legkisebb eleme $\leq_1$ szerint. Ezért $x \leq_1 x'$, így az f monoton növése miatt $f(x) \leq_2 f(x') = g(x)$, holott $g(x) <_2 f(x)$; ez ellentmondás. ■

6.13.10. Következmény. *Ha $(E_1, \leq_1)$ jólrendezett és $(E_2, \leq_2)$ lineárisan rendezett halmaz, akkor legfeljebb egy olyan $E_1 \to E_2$ szigorúan monoton növő függvény létezik, amelynek értékkészlete szegmense $(E_2, \leq_2)$-nek.*

Bizonyítás. Ha $f, g : E_1 \to E_2$ olyan szigorúan monoton növő függvények, amelyek értékkészlete szegmense $(E_2, \leq_2)$-nek, akkor alkalmazva az előző állítást az (f, g) függvénypárra kapjuk, hogy minden $x \in E_1$ esetén $f(x) \leq_2 g(x)$, majd alkalmazva a (g, f) függvénypárra kapjuk, hogy minden $x \in E_1$ esetén $g(x) \leq_2 f(x)$, ami azt jelenti, hogy $f = g$. ■

Azonban, ha $(E_1, \leq_1)$ jólrendezett és $(E_2, \leq_2)$ lineárisan rendezett halmaz, akkor sok olyan $E_1 \to E_2$ on növő függvény létezhet, amelynek értékkészlete nem szegmense $(E_2, \leq_2)$-nek. ° (Ilyenek például az $\mathbb{N} \to \mathbb{N}$ nem identikus indexsorozatok (7.8.5.), amelyek halmaza kontinuum-számosságú (10.3.6.).)$_\circ$

6.13.11. Következmény. *Ha $(E, \leq)$ jólrendezett halmaz, akkor* id_E *az egyetlen $E \to E$ szigorúan monoton növő bijekció.*

6.14. A Kuratowski–Zorn-lemma

6.14.1. Definíció. *Az $(E, \leq)$ rendezett halmaz* **jólrendezett részhalmazának** *nevezünk minden olyan $X \subseteq E$ halmazt, amelyre teljesül az, hogy a $\leq$ rendezés megszorítása X-re jólrendezés X felett.*

6.14.2. Tétel. (**Kuratowski–Zorn-lemma**) *Ha az $(E, \leq)$ rendezett halmaz minden jólrendezett részhalmaza felülről korlátos, akkor E-nek létezik maximális eleme a $\leq$ rendezés szerint.*

Bizonyítás. Jelölje $\mathscr{P}_0(E)$ az E nem üres részhalmazainak halmazát. A kiválasztási axiómából következik, hogy a $\prod_{X \in \mathscr{P}_0(E)} X$ szorzathalmaz nem üres; legyen f ennek tetszőleges eleme. Tehát f olyan függvény, amely az E nem üres részhalmazainak halmazán értelmezett és minden $X \subseteq E$ nem üres halmazra $f(X) \in X$. Megjegyezzük, hogy az $(E, \leq)$ rendezett halmazra vonatkozó hipotézis alapján $E \neq \emptyset$, mert az $\emptyset$ halmaz jólrendezett részhalmaza E-nek, tehát $\emptyset$-nak létezik felső korlátja E-ben, így E-nek van eleme.

Nevezzünk egy $H \subseteq E$ halmazt f-regulárisnak, ha teljesülnek rá a következők.

a) A $(H, \leq_H)$ pár olyan *jólrendezett* halmaz, amelynek $f(E)$ a legkisebb eleme.

b) Minden $x \in H$ elemre fennáll az

$$x = f(\{z | (z \in E) \wedge (H \cap] \leftarrow, x[\subseteq] \leftarrow, z[)\})$$

egyenlőség.

Például az $\{f(E)\}$ egy elemű halmaz nyilvánvalóan f-reguláris. Továbbá, ha $f(E)$ nem maximális eleme E-nek, vagyis $]f(E),\to[\neq\emptyset$, akkor az $\{f(E),f(]f(E),\to[)\}$ halmaz is f-reguláris. Továbbá, ha sem $f(E)$, sem $f(]f(E),\to[)$ nem maximális E-ben, akkor az $\{f(E),f(]f(E),\to[),f(]f(]f(E),\to[),\to[)\}$ halmaz is f-reguláris, s.í.t. Most néhány megállapítást teszünk f-reguláris halmazokkal kapcsolatban.

(I) Ha H és H' f-reguláris halmazok és $x\in H$, $x'\in H'$ és $H\cap]\leftarrow,x[=H'\cap]\leftarrow,x'[$, akkor $x=x'$. Valóban, ekkor

$$\{z|(z\in E)\wedge(H\cap]\leftarrow,x[\subseteq]\leftarrow,z[)\}=\{z|(z\in E)\wedge(H'\cap]\leftarrow,x'[\subseteq]\leftarrow,z[)\},$$

ezért az f-reguláris halmazok b) tulajdonsága miatt fennáll az

$$x=f(\{z|(z\in E)\wedge(H\cap]\leftarrow,x[\subseteq]\leftarrow,z[)\})=f(\{z|(z\in E)\wedge(H'\cap]\leftarrow,x'[\subseteq]\leftarrow,z[)\})=x'$$

egyenlőség.

(II) Ha H és H' f-reguláris halmazok, akkor H szegmense H'-nek vagy H' szegmense H-nak (a $\leq$ rendezés megfelelő halmazokra vett megszorítása szerint). Jelölje ugyanis S a H és H' közös szegmenseinek *unióját.* Az előző lemma szerint S szegmense H-nak is és H'-nek is, ezért ha $S\neq H$ és $S\neq H'$ teljesülne (vagyis S valódi szegmense volna H-nak is és H'-nek is), akkor a $H\setminus S$ halmaz x legkisebb elemére és a $H'\setminus S$ halmaz x' legkisebb elemére $H\cap]\leftarrow,x[=S=H'\cap]\leftarrow,x'[$ igaz volna. Ekkor (I) szerint $x=x'$ teljesülne, így a

$$H\cap]\leftarrow,x]=(H\cap]\leftarrow,x[)\cup\{x\}=(H'\cap]\leftarrow,x'[)\cup\{x'\}=H'\cap]\leftarrow,x']$$

halmaz szintén szegmense volna H-nak is és H'-nek is, vagyis $x\in H\cap]\leftarrow,x]\subseteq S$ teljesülne, holott $x\notin S$. Ezért szükségképpen $H=S$ vagy $H'=S$. Az első esetben H szegmense H'-nek, míg a második esetben H' szegmense H-nak.

(III) Ha $(H_i)_{i\in I}$ az E f-reguláris részhalmazainak tetszőleges rendszere, akkor a $H:=\bigcup\limits_{i\in I}H_i$ halmaz olyan, hogy minden $i\in I$ indexre és $x\in H_i$ elemre fennáll az $]\leftarrow,x[\cap H_i=]\leftarrow,x[\cap H$ egyenlőség. Valóban, az nyilvánvaló, hogy $]\leftarrow,x[\cap H_i\subseteq]\leftarrow,x[\cap H$. A fordított tartalmazást indirekt bizonyítjuk, tehát feltesszük, hogy létezik olyan $x'\in]\leftarrow,x[\cap H$, hogy $x'\notin]\leftarrow,x[\cap H_i$. Ekkor $x'\in H$ miatt létezik olyan $i'\in I$, hogy $x'\in H_{i'}$. A (II) alapján $H_{i'}$ szegmense H_i-nek vagy H_i szegmense $H_{i'}$-nek (a $\leq$ rendezés megfelelő halmazokra vett megszorítása szerint). A feltevés szerint $x'<x$, $x'\in H_{i'}$ és $x\in H_i$, ezért ha H_i szegmense volna $H_{i'}$-nek, akkor $x'\in H_i$ teljesülne, holott $x'\notin H_i$. Ezért H_i nem lehet szegmense $H_{i'}$-nek, következésképpen $H_{i'}$ szegmense H_i-nek. Ekkor viszont $x'\in H_{i'}\subseteq H_i$, így $x'\in]\leftarrow,x[\cap H_i$, ami ellentmond annak, hogy $x'\notin]\leftarrow,x[\cap H_i$.

(IV) Ha H f-reguláris részhalmaza E-nek és létezik E-nek olyan eleme, amely felső korlátja H-nak és nem eleme H-nak, akkor létezik E-nek olyan $\overline{H}$ f-reguláris részhalmaza, hogy $H\subseteq\overline{H}$ és $H\neq\overline{H}$. Valóban, ekkor nyilvánvaló, hogy $\{x'|(x'\in E)\wedge(H\subseteq]\leftarrow,x'[)\}\neq\emptyset$, és az $x:=f(\{x'|(x'\in E)\wedge(H\subseteq]\leftarrow,x'[)\})$ elem olyan, hogy $x\notin H$ és a $\overline{H}:=H\cup\{x\}$ halmaz nyilvánvalóan f-reguláris.

(V) Jelölje $\mathscr{H}$ az E összes f-reguláris részhalmazainak *unióját.* Megmutatjuk, hogy a $\mathscr{H}$ halmaz f-reguláris.

Az $\{f(E)\}$ halmaz f-reguláris, ezért $f(E)\in\mathscr{H}$. Ha $x\in\mathscr{H}$, akkor van olyan H f-reguláris részhalmaza E-nek, hogy $x\in H$, tehát $f(E)\leq x$, mert $f(E)$ minden f-reguláris halmaznak a legkisebb eleme.

Ha $x,x'\in\mathscr{H}$, akkor léteznek olyan H és H' f-reguláris halmazok, hogy $x\in H$ és $x'\in H'$. A (II)-ből következik, hogy $H\subseteq H'$ vagy $H'\subseteq H$, így $x,x'\in H$ vagy $x,x'\in H'$. De

a H és H' bármely két eleme összehasonlítható a $\leq$ rendezés szerint, ezért x és x' is összehasonlíthatók a $\leq$ rendezés szerint. Ez azt jelenti, hogy $\leq$ rendezés $\mathscr{H}$-ra vett megszorítása *lineáris rendezés* $\mathscr{H}$ felett.
Legyen $F \subseteq \mathscr{H}$ nem üres halmaz; megmutatjuk, hogy F-nek létezik legkisebb eleme a $\leq_{\mathscr{H}}$ rendezés szerint (és ez azt bizonyítja, hogy a $(\mathscr{H}, \leq_{\mathscr{H}})$ pár jólrendezett halmaz). Létezik E-nek olyan H f-reguláris részhalmaza, hogy $H \cap F \neq \emptyset$, így $H \cap F$-nek létezik legkisebb eleme a $\leq$ rendezés H-ra vett megszorítása szerint, mivel $(H, \leq_H)$ jólrendezett halmaz; legyen ez x. A (III) alapján $H \cap] \leftarrow, x[= \mathscr{H} \cap] \leftarrow, x[$, ezért a $\mathscr{H}$ minden x-nél kisebb eleme H-nak is eleme, így az F-nek nem eleme. Másként fogalmazva: az F minden eleme nagyobb-egyenlő x-nél, hiszen a $\mathscr{H}$ bármely két eleme összehasonlítható. Ez azt jelenti, hogy x az F halmaz legkisebb eleme a $\leq_{\mathscr{H}}$ rendezés szerint.
Végül, ha $x \in \mathscr{H}$ és H olyan f-reguláris részhalmaza E-nek, hogy $x \in H$, akkor a (III) alapján $H \cap] \leftarrow, x[= \mathscr{H} \cap] \leftarrow, x[$, így az f-reguláris halmazok b) tulajdonsága folytán

$$x = f(\{z | (z \in E) \wedge (H \cap] \leftarrow, x[\subseteq] \leftarrow, z[)\}) = f(\{z | (z \in E) \wedge (\mathscr{H} \cap] \leftarrow, x[\subseteq] \leftarrow, z[)\}),$$

tehát $\mathscr{H}$ f-reguláris halmaz.

(VI) Most már könnyen bizonyítható az állítás. Az (V) állítás szerint $\mathscr{H}$ jólrendezett részhalmaza az $(E, \leq)$ rendezett halmaznak. Az $(E, \leq)$ rendezett halmazra vonatkozó feltétel szerint $\mathscr{H}$-nak létezik felső korlátja. Állítjuk, hogy ha x felső korlátja $\mathscr{H}$-nak, akkor x maximális eleme E-nek. Valóban, ha x nem volna maximális, akkor létezne x-nél nagyobb eleme E-nek. Ekkor a (IV) alapján létezne $\mathscr{H}$-t valódi részhalmazként tartalmazó f-reguláris halmaz, ami lehetetlen, mert $\mathscr{H}$ az E minden f-reguláris részhalmazát tartalmazza. ∎

Vegyük észre, hogy a Kuratowski–Zorn-lemma bizonyításban a kiválasztási axiómát alkalmaztuk; ez nem véletlen. Elvileg nem volna kizárt az, hogy létezik a Kuratowski–Zorn-lemmának olyan bizonyítása, amely nem hivatkozik a kiválasztási axiómára. Azonban *nincs ilyen bizonyítás* (feltéve, hogy a halmazelmélet a kiálasztási axióma nélkül ellentmondásmentes), mert látni fogjuk, hogy a Kuratowski–Zorn-lemma *ekvivalens* a kiválasztási axiómával (6.15.3.).

6.14.3. Definíció. *Azt mondjuk, hogy az $(E, \leq)$ rendezett halmaz* **induktívan rendezett***, ha E minden olyan részhalmaza felülről korlátos, amelynek bármely két eleme összehasonlítható a $\leq$ rendezés szerint.*

6.14.4. Tétel. (**Zorn-lemma**) *Ha $(E, \leq)$ induktívan rendezett halmaz, akkor E-nek létezik maximális eleme a $\leq$ rendezés szerint.*

Bizonyítás. Mivel $(E, \leq)$ induktívan rendezett halmaz, így az E minden jólrendezett részhalmaza is felülről korlátos, hiszen jólrendezett halmaz bármely két eleme összehasonlítható a rendezés szerint. Ezért az állítás nyilvánvalóan következik a Kuratowski–Zorn-lemmából. ∎

Most bemutatjuk a Zorn-lemma egy fontos számosságelméleti következményét.

6.14.5. Állítás. *Ha E és F halmazok, akkor E kisebb-egyenlő számosságú F-nél, vagy F kisebb-egyenlő számosságú E-nél (vagyis bármely két halmaz számosság tekintetében összehasonlítható).*

Bizonyítás. Legyen $\mathbf{I}$ az $E \rightarrowtail F$ *injekciók* halmaza, és jelölje $\leq$ a tartalmazás-relációt $\mathbf{I}$ felett.

Megmutatjuk, hogy $\leq$ *induktív* rendezés $\mathbf{I}$ felett. Ehhez legyen $X \subseteq \mathbf{I}$ olyan halmaz, amelynek bármely két eleme összehasonlítható a $\leq$ rendezés szerint. Ekkor $f, g \in X$ esetén $f \subseteq g$ vagy $g \subseteq f$, ezért a függvények összeragasztásának 6.2.11. definícióját követő megjegyzés alapján $\overline{f} := \bigcup_{f \in X} f$ olyan injektív függvény, hogy $\mathrm{Dom}(\overline{f}) = \bigcup_{f \in X} \mathrm{Dom}(f) \subseteq E$ és $\mathrm{Im}(\overline{f}) = \bigcup_{f \in X} \mathrm{Im}(f) \subseteq F$, tehát $\overline{f} \in \mathbf{I}$. Nyilvánvaló, hogy $\overline{f}$ felső korlátja (sőt szuprémuma) az X halmaznak, tehát a $\leq$ rendezés induktív.

A Zorn-lemma alapján az $(\mathbf{I}, \leq)$ rendezett halmaznak létezik maximális eleme: legyen f ilyen. Tehát $f : E \rightarrowtail F$ olyan injekció, hogy nem létezik olyan $g : E \rightarrowtail F$ injekció, amelyre $f \subseteq g$ és $f \neq g$ teljesül. Igazoljuk, hogy ekkor $\mathrm{Dom}(f) = E$ *vagy* $\mathrm{Im}(f) = F$ teljesül.

Indirekt bizonyítunk, tehát feltesszük, hogy $\mathrm{Dom}(f) \neq E$ *és* $\mathrm{Im}(f) \neq F$. Legyenek $x \in E \setminus \mathrm{Dom}(f)$ és $y \in F \setminus \mathrm{Im}(f)$. Könnyen látható, hogy a $g := \{(x, y)\} \cup f$ halmaz olyan $E \rightarrowtail F$ injektív függvény, amelyre $f \subseteq g$ és $f \neq g$ teljesül, ami ellentmond az f függvény $\leq$ szerinti maximalitásának.

Ha $\mathrm{Dom}(f) = E$, akkor E kisebb-egyenlő számosságú F-nél, hiszen $f : E \to F$ injekció. Ha pedig $\mathrm{Im}(f) = F$, akkor F kisebb-egyenlő számosságú E-nél, hiszen $f^{-1} : F \to E$ injekció. ■

6.15. A Zermelo-féle jólrendezési tétel

6.15.1. Lemma. *Legyen* $(E, \leq)$ *rendezett halmaz.*

a) *Ha* $H \subseteq E$ *lineárisan rendezett részhalmaz, akkor létezik olyan* $\overline{H} \subseteq E$ *lineárisan rendezett részhalmaz, hogy* $H \subseteq \overline{H}$ *és* $\overline{H}$ *az* E *egyetlen ilyen tulajdonságú részhalmazának sem valódi részhalmaza.* (**Hausdorff-féle maximum-elv.**)

b) *Létezik* E*-nek olyan részhalmaza, amely tartalmazás tekintetében maximális az* E *lineárisan rendezett részhalmazai halmazában.*

Bizonyítás. a) Legyen $\mathfrak{H}$ azon $X \subseteq E$ lineárisan rendezett részhalmazok halmaza, amelyekre $H \subseteq X$, továbbá jelölje $\subseteq_{\mathfrak{H}}$ a tartalmazás relációt a $\mathfrak{H}$ halmaz felett.

Megmutatjuk, hogy a $\subseteq_{\mathfrak{H}}$ rendezés induktív. Ehhez legyen $\mathfrak{X} \subseteq \mathfrak{H}$ tartalmazás szerint lineárisan rendezett részhalmaz. Ekkor $\overline{X} := \bigcup_{X \in \mathfrak{X}} X$ olyan részhalmaza E-nek, amely lineárisan rendezett. Valóban, ha $x', x'' \in \overline{X}$, akkor vehetünk olyan $X' \in \mathfrak{X}$ és $X'' \in \mathfrak{X}$ halmazokat, hogy $x' \in X'$ és $x'' \in X''$. A $\mathfrak{X}$ halmaz tartalmazás reláció szerinti lineáris rendezettsége miatt $X' \subseteq X''$ vagy $X'' \subseteq X'$. Ha $X' \subseteq X''$, akkor $x', x'' \in X''$, és X'' lineárisan rendezett a $\leq$ rendezés szerint, ezért x' és x'' összehasonlíthatóak $\leq$ szerint. Ha $X'' \subseteq X'$, akkor $x', x'' \in X'$, és X' lineárisan rendezett a $\leq$ rendezés szerint, ezért x' és x'' összehasonlíthatóak $\leq$ szerint. Tehát $\overline{X}$ az E halmaznak $\leq$ szerint lineárisan rendezett részhalmaza, vagyis $\overline{X} \in \mathfrak{H}$, és nyilvánvaló, hogy $\overline{X}$ felső korlátja (sőt szuprémuma) $\mathfrak{X}$-nek a tartalmazás reláció szerint.

A Zorn-lemma szerint vehetünk egy $\overline{H} \in \mathfrak{H}$ elemet, amely maximális a tartalmazás reláció szerint. Ekkor $\overline{H}$ olyan lineárisan rendezett részhalmaza E-nek, hogy $H \subseteq \overline{H}$. Ha $H' \subseteq E$ olyan lineárisan rendezett halmaz, hogy $H \subseteq H'$, akkor $H' \in \mathfrak{H}$, ezért $\overline{H} \subseteq H'$ és $\overline{H} \neq H'$ lehetetlen, különben $\overline{H}$ nem lehetne tartalmazás tekintetében maximális eleme $\mathfrak{H}$-nak. Tehát $\overline{H}$ olyan lineárisan rendezett részhalmaza E-nek, amely tartalmazza H-t, és nem valódi részhalmaza az E egyetlen ilyen tulajdonságú részhalmazának sem.

b) Elegendő az a) állítást alkalmazni a $H := \emptyset$ választással, figyelembe véve, hogy az üres halmaz nyilvánvalóan lineárisan rendezett $\leq$ szerint. ■

6.15.2. Tétel. (**Zermelo-féle jólrendezési tétel**) *Minden halmaz felett létezik jólrendezés.*

Bizonyítás. Legyen E halmaz és tekintsük a következő $\mathscr{A}(x)$ kijelentést:

$$(\exists H)(\exists R)((x{=}(H,R)) \wedge (H \subseteq E) \wedge \text{"}R \text{ jólrendezés } H \text{ felett"}).$$

Ez a kijelentés kollektivizáló az x változóban, mert $\mathscr{A}(x)$-ből következik, hogy $x \in \mathscr{P}(E) \times \mathscr{P}(E \times E)$, tehát elég a részhalmaz-axiómát alkalmazni. Ezért tekinthetjük az

$$\mathbf{S} := \{(H,R) | (H \subseteq E) \wedge \text{"}R \text{ jólrendezés } H \text{ felett"}\}$$

halmazt. Az $\mathbf{S}$ halmazon bevezetjük a $\leq$ relációt úgy, hogy $(H,R),(H',R') \in \mathbf{S}$ esetén $(H,R) \leq (H',R')$ pontosan akkor teljesüljön, ha H szegmense a (H',R') jólrendezett halmaznak és $R = R' \cap (H \times H)$. Ekkor $(\mathbf{S}, \leq)$ rendezett halmaz, tehát az előző lemma b) pontja szerint van olyan $\mathbf{L} \subseteq \mathbf{S}$ halmaz, amit a $\leq$ reláció lineárisan rendez és amely tartalmazás tekintetében maximális ilyen tulajdonságú részhalmaza $\mathbf{S}$-nek.

Ekkor a $((H,R))_{(H,R)\in\mathbf{L}}$ rendszer jólrendezett halmazoknak olyan rendszere, amelyre teljesül az, hogy minden $(H,R),(H',R') \in \mathbf{L}$ esetén a következő állítások valamelyike igaz:

1) H szegmense a (H',R') jólrendezett halmaznak és $R = R' \cap (H \times H)$;

2) H' szegmense a (H,R) jólrendezett halmaznak és $R' = R \cap (H' \times H')$.

Ezért a jólrendezett halmazok összeragasztásának tétele (6.13.8.) alapján a $H := \bigcup_{(H',R')\in\mathbf{L}} H'$ halmazon létezik egyetlen olyan R rendezés, hogy minden $(H',R') \in \mathbf{L}$ párra H' szegmense a (H,R) rendezett halmaznak és $R' = R \cap (H' \times H')$, továbbá ekkor a (H,R) pár jólrendezett halmaz.

Ha $H \neq E$ teljesülne, akkor véve tetszőleges $x \in E \setminus H$ pontot, a $H' := H \cup \{x\}$ halmazt rendezhetjük azzal az R' relációval, amelynek megszorítása H-ra megegyezik R-rel és amely szerint x a legnagyobb elem H'-ben. Ekkor R' nyilvánvalóan jólrendezés H' felett, tehát $(H',R') \in \mathbf{S}$, ugyanakkor (H',R') a $\leq$ rendezés szerint *nagyobb* az $\mathbf{L}$ halmaz minden eleménél. Ekkor viszont $\mathbf{L}$ *valódi része* az $\mathbf{L}' := \mathbf{L} \cup \{(H',R')\}$ halmaznak, ugyanakkor az $\mathbf{L}'$ bármely két eleme összehasonlítható a $\leq$ rendezés szerint. Ez azonban ellentmond az $\mathbf{L}$ maximalitásának. Ezért $H = E$, tehát R jólrendezés az E halmaz felett. ■

6.15.3. Tétel. *A kiválasztási axióma, a Kuratowski–Zorn-lemma, a Zorn-lemma és a Zermelo-féle jólrendezési tétel ekvivalensek egymással.*

(**Megjegyzés**: Az állítás pontosan azt jelenti, hogy ha a halmazelméletnek azt a részelméletét tekintjük, amelynek axiómái a meghatározottsági axióma, a részhalmaz axiómaséma, a páraxióma, a hatványhalmaz-axióma és az unió axióma, akkor ebben az elméletben a fenti négy kijelentés páronként ekvivalens.)

Bizonyítás. Igazoltuk, hogy a kiválasztási axiómából következik a Kuratowski--Zorn-lemma (6.14.2.), és a Zorn-lemma nyilvánvalóan következik a Kuratowski--Zorn-lemmából (6.14.4.). A Zermelo-féle jólrendezési tételt a kiválasztási axióma alkalmazása nélkül vezettük le a Zorn-lemmából (6.15.2.) Ezért elegendő a Zermelo-féle jólrendezési tételből (a Kuratowski–Zorn-lemma alkalmazása nélkül) bizonyítani a kiválasztási axiómát.

Ehhez legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ indexre $E_i \neq \emptyset$. Az unió axióma szerint képezhetjük az $E := \bigcup_{i\in I} E_i$ halmazt. A Zermelo-féle jólrendezési tétel alapján létezik E felett olyan $\leq$ reláció, hogy $(E, \leq)$ jólrendezett halmaz. Minden $i \in I$ esetén $E_i \subseteq E$ és $E_i \neq \emptyset$, így létezik E_i-nek legkisebb eleme a $\leq$ rendezés szerint. Ekkor az

$$f := \{(i, x) \in I \times E | (x \in E_i) \wedge (\forall x')((x' \in E_i) \Rightarrow (x \leq x'))\}$$

halmaz a részhalmaz-axióma szerint létezik, és ez olyan függvény, hogy $\mathrm{Dom}(f) = I$ és minden $i \in I$ indexre $f(i) \in E_i$, vagyis $f \in \prod_{i\in I} E_i$. ■

6.15.4. Állítás. *Ha (E, R) és (E', R') jólrendezett halmazok, akkor a következő esetek közül az egyik teljesül:*
a) *Az (E', R') rendezett halmaznak létezik egyetlen olyan S' szegmense, hogy az (E, R) és $(S', R'|S')$ rendezett halmazok izomorfak.*
b) *Az (E, R) rendezett halmaznak létezik egyetlen olyan S szegmense, hogy az (E', R') és $(S, R|S)$ rendezett halmazok izomorfak.*
Ha a) *és* b) *egyszerre teljesül, akkor az (E, R) és (E', R') jólrendezett halmazok izomorfak.*

Bizonyítás. Jelölje $\mathbf{F}$ azon $f : E \to E'$ függvények halmazát, amelyekre $\mathrm{Dom}(f)$ szegmense az (E, R) rendezett halmaznak, $\mathrm{Im}(f)$ szegmense az (E', R') rendezett halmaznak, és f izomorfizmus a $(\mathrm{Dom}(f), R|\mathrm{Dom}(f))$ és $(\mathrm{Im}(f), R'|\mathrm{Im}(f))$ rendezett halmazok között. Jelölje $\leq$ a tartalmazás relációt az $\mathbf{F}$ halmaz felett. Nyilvánvaló, hogy $\mathbf{F} \neq \emptyset$, mert az üres függvény eleme $\mathbf{F}$-nek.

Az $(\mathbf{F}, \leq)$ pár *induktívan rendezett halmaz*, mert ha $\mathscr{F} \subseteq \mathbf{F}$ tartalmazás tekintetében lineárisan rendezett részhalmaz, akkor a függvények összeragasztásának tétele (6.2.10.) szerint a $\mathscr{F}$ függvényhalmaz összeragasztásával nyert $f : E \rightarrowtail E'$ függvény felső korlátja (sőt szuprémuma) az $\mathscr{F}$ halmaznak. Tehát a Kuratowski–Zorn-lemma alapján az $(\mathbf{F}, \leq)$ rendezett halmaznak létezik maximális eleme: legyen $f \in \mathbf{F}$ ilyen. Bebizonyítjuk, hogy $\mathrm{Dom}(f) = E$ *vagy* $\mathrm{Im}(f) = E'$.

Indirekt feltesszük, hogy $\mathrm{Dom}(f) \neq E$ *és* $\mathrm{Im}(f) \neq E'$ teljesül. Legyen $x \in E$ az $E\setminus\mathrm{Dom}(f)$ halmaz legkisebb eleme az R jólrendezés szerint és $y \in E'$ az $E'\setminus\mathrm{Im}(f)$ halmaz legkisebb elme az R' jólrendezés szerint. Legyen $f' := \{(x, y)\} \cup f$, tehát $f' : E \rightarrowtail E'$ az a kiterjesztése f-nek, amelyre $\mathrm{Dom}(f') = \mathrm{Dom}(f) \cup \{x\}$ és $\mathrm{Im}(f') = \mathrm{Im}(f) \cup \{y\}$, vagyis $f'(x) := y$. Könnyen látható, hogy ekkor $f' \in \mathbf{F}$, $f \subseteq f'$ és $f \neq f'$, ami ellentmond f maximalitásának.

Ezért $\mathrm{Dom}(f) = E$, így a) teljesül, vagy $\mathrm{Im}(f) = E'$, és akkor b) teljesül. ■

6.16. Gyakorlatok

1. Ha R reláció, akkor minden X halmazra $X \subseteq \mathrm{pr}_1\langle R\rangle$ ekvivalens az $X \subseteq \overset{-1}{R}\langle R\langle X\rangle\rangle$ tartalmazással.

2. Ha R és S relációk, akkor $\mathrm{pr}_1\langle R\rangle \subseteq \mathrm{pr}_1\langle S\rangle$ ekvivalens azzal, hogy $R \subseteq R \circ \overset{-1}{S} \circ S$. Ha R reláció, akkor $R \subseteq R \circ \overset{-1}{R} \circ R$.

3. Ha R reláció, akkor $\overset{-1}{R} \circ R = \emptyset$ pontosan akkor teljesül, ha $R = \emptyset$.

4. Ha R reláció és E, F halmazok, akkor

$$
\begin{aligned}
(E \times F) \circ R &= \overset{-1}{R}\langle E\rangle \times F \\
R \circ (E \times F) &= E \times R\langle F\rangle.
\end{aligned}
$$

5. Ha R, S és T relációk, akkor

$$(R \circ S) \cap T \subseteq (R \cap (T \circ \overset{-1}{S})) \circ (S \cap (\overset{-1}{R} \circ T)).$$

6. Ha E, F, E' és F' halmazok, akkor

$$(E \times F) \circ (E' \times F') = \begin{cases} \emptyset, & \text{ha } E \cap F' = \emptyset, \\ E' \times F, & \text{ha } E \cap F' \neq \emptyset. \end{cases}$$

7. Ha R reláció, akkor a következő állítások ekvivalensek.
a) Minden X és Y halmazra $\overset{-1}{R}\langle X \cap Y\rangle = \overset{-1}{R}\langle X\rangle \cap \overset{-1}{R}\langle Y\rangle$.
b) Minden X és Y halmazra, ha $X \cap Y = \emptyset$, akkor $\overset{-1}{R}\langle X\rangle \cap \overset{-1}{R}\langle Y\rangle = \emptyset$.
c) Minden X halmazra $R\langle \overset{-1}{R}\langle X\rangle\rangle \subseteq X$ teljesül.
d) Minden S és T relációra $(S \cap T) \circ R = (S \circ R) \cap (T \circ R)$.
e) R függvényreláció.

8. Ha $(R_i)_{i \in I}$ relációk tetszőleges rendszere, akkor minden X halmazra

$$\Big(\bigcup_{i \in I} R_i\Big)\langle X\rangle = \bigcup_{i \in I} R_i\langle X\rangle,$$

és ha $I \neq \emptyset$, akkor minden X *egy elemű* halmazra

$$\Big(\bigcap_{i \in I} R_i\Big)\langle X\rangle = \bigcap_{i \in I} R_i\langle X\rangle.$$

Azonban léteznek olyan R, S relációk és X halmaz, amelyekre

$$(R \cap S)\langle X\rangle \neq R\langle X\rangle \cap S\langle X\rangle.$$

9. Legyenek E, F, G és H halmazok, valamint $f : E \to F$, $g : F \to G$, $h : G \to H$ függvények. Ha $g \circ f$ és $h \circ g$ bijekciók, akkor f, g és h mindhárman bijekciók.

10. Legyenek E, F és G halmazok, valamint $f : E \to F$, $g : F \to G$, $h : G \to E$ függvények. Ha a $h \circ g \circ f$, $g \circ f \circ h$ és $f \circ h \circ g$ függvények közül bármely kettő injektív és a harmadik szürjektív, vagy bármely kettő szürjektív és a harmadik injektív, akkor f, g és h mindhárman bijekciók.

11. Ha van olyan függvény, amely eleme a saját definíciós tartományának, akkor léteznek olyan E, F és G halmazok, amelyekre $E{\in}F{\in}G{\in}E$ teljesül. (ld. I.3.**45**. gyakorlat: *a fundáltsági axióma.*)

12. Ha E, F halmazok és $X \subseteq E$, akkor az

$$\mathscr{F}(E; F) \to \mathscr{F}(X; F) \quad ; \quad f \mapsto f|_X$$

leképezés szürjekció, feltéve, hogy $F \neq \emptyset$, vagy $E = \emptyset = F$.

17. Legyenek E, F halmazok és minden $R \subseteq E \times F$ relációra értelmezzük a következő függvényt:

$$\hat{R} : E \to \mathscr{P}(F) \quad ; \quad x \mapsto R\langle\{x\}\rangle.$$

Ekkor a

$$\mathscr{P}(E \times F) \to \mathscr{F}(E; \mathscr{P}(F)) \quad ; \quad R \mapsto \hat{R}$$

függvény *bijekció.*

32. Legyen E halmaz és $f : \mathscr{P}(E) \to \mathscr{P}(E)$ olyan függvény, amelyre minden $X, Y \in \mathscr{P}(E)$ halmazra, ha $X \subseteq Y$, akkor $f(X) \subseteq f(Y)$ teljesül. Legyen E_- azon $X \subseteq E$ halmazok *metszete*, amelyekre $f(X) \subseteq X$ teljesül, továbbá legyen E_+ azon $X \subseteq E$ halmazok *uniója*, amelyekre $X \subseteq f(X)$ teljesül. Ekkor $E_- \subseteq E_+$, $f(E_-) = E_-$, $f(E_+) = E_+$, és minden $X \subseteq E$ halmazra, ha $f(X) = X$, akkor $E_- \subseteq X \subseteq E_+$ teljesül. (Ez úgy is megfogalmazható. hogy f-nek létezik tartalmazás tekintetében legkisebb és legnagyobb *fixpontja.*)

33. Az R reláció pontosan akkor ekvivalencia az E halmaz felett, ha $\mathrm{pr}_1 R = E$, $R = \overset{-1}{R}$ és $R \circ R = R$.

36. Ha E, F halmazok és $f : E \to F$ tetszőleges függvény, akkor létezik olyan G halmaz, és léteznek olyan $s : E \to G$, $i : G \to F$ függvények, hogy s *szürjekció*, i *injekció* és $f = i \circ s$. (Ezt a tényt úgy is megfogalmazhatjuk, hogy minden függvény előáll egy szürjekció és egy azt követő injekció kompozíciójaként.) Igaz-e, hogy minden függvény előáll egy injekció és egy azt követő szürjekció kompozíciójaként?

37. Ha R és S ekvivalenciák az E halmaz felett, akkor az $R \circ S$ reláció pontosan akkor ekvivalencia E felett, ha $R \circ S = S \circ R$ teljesül. Egy halmaz feletti ekvivalenciák tetszőleges nem üres rendszerének a *metszete* ekvivalencia az adott halmaz felett.

38. Legyenek R és S ekvivalenciák az E halmaz felett. Akkor és csak akkor létezik olyan T ekvivalencia az E halmaz felett, amelyre $R \subseteq T$ és $S \subseteq T$ teljesül, ha $R \circ S = S \circ R$. Ha $R \circ S = S \circ R$, akkor $R \circ S$ az a tartalmazás tekintetében legkisebb E feletti ekvivalencia, amelyre $R \subseteq T$ és $S \subseteq T$ teljesül.

39. Minden E halmazhoz létezik olyan X halmaz, hogy $X \subseteq E$ és $X \notin E$.

40. Legyenek E_1, E_2, F_1 és F_2 olyan halmazok, hogy E_1 kisebb-egyenlő számosságú F_1-nél és E_2 kisebb-egyenlő számosságú F_2-nél. Ha F_1 és F_2 mindketten legalább két elemű halmazok, akkor $E_1 \cup E_2$ kisebb-egyenlő számosságú az $F_1 \times F_2$ halmaznál.

(*Útmutatás.* Elegendő arra az esetre bizonyítani, amikor E_1 és E_2 diszjunktak. Legyenek $f_1 : E_1 \to F_1$ és $f_2 : E_2 \to F_2$ injekciók, és legyenek $a_1, b_1 \in F_1$, illetve $a_2, b_2 \in F_2$ olyanok, hogy $a_1 \neq b_1$ és $a_2 \neq b_2$. Legyen $f : E_1 \cup E_2 \to F_1 \times F_2$ az a függvény, amelyre $x_1 \in E_1$ esetén

$$f(x_1) = \begin{cases} (f_1(x_1), a_2) & \text{ha } f_1(x_1) \neq a_1 \\ (a_1, b_2) & \text{ha } f_1(x_1) = a_1 \end{cases}$$

továbbá $x_2 \in E_2$ esetén

$$f(x_2) = \begin{cases} (a_1, f_2(x_2)) & \text{ha } f_2(x_2) \neq b_2 \\ (b_1, b_2) & \text{ha } f_2(x_2) = b_2 \end{cases}.$$

Mutassuk meg, hogy f injekció, és "rajzoljuk le" ezt a függvényt!)

42. Az R reláció pontosan akkor rendezés az E halmaz felett, ha $R \cap \overset{-1}{R} = \mathrm{id}_E$ és $R \circ R = R$ teljesül.

43. Ha R rendezés az E halmaz felett és $F \subseteq E$, akkor az $R \cap (F \times F)$ reláció rendezés az F halmaz felett; ezt a rendezést R_F jelöli, és az R rendezés F-re vett *megszorításának* nevezzük. Ha $(E, \leq)$ rendezett halmaz és $F \subseteq E$, akkor egy $A \subseteq F$ halmazzal kapcsolatban beszélhetünk az A szuprémumáról az $(E, \leq)$ rendezett halmazban (amit $\sup_E A$ jelöl), valamint az A szuprémumáról az $(F, \leq_F)$ rendezett halmazban (amit $\sup_F A$ jelöl). Mutassuk meg, hogy ha $(E, \leq)$ rendezett halmaz, $F \subseteq E$ és $A \subseteq F$, akkor $\sup_E A$ és $\sup_F A$ létezése esetén $\sup_F A \leq \sup_F A$; továbbá, ha $\sup_E A$ létezik és eleme F-nek, akkor $\sup_F A$ is létezik és $\sup_F A = \sup_F A$. Azonban előfordul az, hogy $\sup_F A$ létezik, de $\sup_E A$ nem létezik, és az is lehetséges, hogy mindketten léteznek, de nem egyenlők (ekkor $\sup_E A \notin F$).

46. *Bebizonyítjuk* a kiválasztási axiómát! Legyen $(E_i)_{i \in I}$ olyan halmazrendszer, amelyre minden $i \in I$ esetén $E_i \neq \emptyset$. Minden $i \in I$ indexhez *kiválasztunk és rögzítünk* egy $x_i \in E_i$ elemet, ami lehetséges, hiszen $E_i \neq \emptyset$. Ekkor az $f := \{(i, x_i) | i \in I\}$ halmaz olyan függvény, hogy $\mathrm{Dom}(f) = I$ és minden $i \in I$ indexre $f(i) = x_i \in E_i$, vagyis $f \in \prod_{i \in I} E_i$, így $\prod_{i \in I} E_i \neq \emptyset$. Keressük meg a *hibát* ebben az érvelésben!

47. Ha f függvény, akkor az f *injektivitás-tartományának* nevezünk minden olyan

$E \subseteq \mathrm{Dom}(f)$ halmazt, amelyre $f|_E$ injekció. Mutassuk meg, hogy minden függvénynek létezik tartalmazás tekintetében *maximális* injektivitás-tartománya!

7. fejezet

A természetes számok halmaza

7.1. Végtelenségi axióma és a természetes számok halmaza

7.1.1. Definíció. *Ha E halmaz, akkor $E^+ := E \cup \{E\}$, és ezt a halmazt az E* **szukcesszorának** *nevezzük. Az M halmazt* **monotonnak** *nevezzük, ha*

$$(\emptyset \in M) \wedge (\forall x)((x \in M) \Rightarrow (x^+ \in M))$$

teljesül.

Végtelenségi axióma – *Létezik monoton halmaz.*

7.1.2. Tétel. *Létezik egyetlen olyan monoton halmaz, amely minden monoton halmaznak részhalmaza.*

Bizonyítás. A végtelenségi axióma alapján rögzítsünk egy M monoton halmazt, és jelölje $\mathscr{M}$ az M monoton részhalmazainak halmazát, vagyis

$$\mathscr{M} := \{X \subseteq M | (\emptyset \in X) \wedge (\forall x)((x \in X) \Rightarrow (x^+ \in X))\}.$$

Az $(X)_{X \in \mathscr{M}}$ rendszer indexhalmaza nem üres, mert $M \in \mathscr{M}$, így képezhető az $\mathbf{N} := \bigcap_{X \in \mathscr{M}} X$ metszethalmaz. Nyilvánvaló, hogy $\mathbf{N}$ is monoton halmaz és $\mathbf{N} \subseteq M$, vagyis $\mathbf{N} \in \mathscr{M}$. Ha N tetszőleges monoton halmaz, akkor $N \cap M \in \mathscr{M}$, ezért a definíció szerint $\mathbf{N} \subseteq N \cap M \subseteq N$, vagyis az $\mathbf{N}$ monoton halmaz minden monoton halmaznak részhalmaza.
Ha N és N' olyan monoton halmazok, amelyek minden monoton halmaznak részhalmazai, akkor $N \subseteq N'$ és $N' \subseteq N$, következésképpen a meghatározottsági axióma szerint $N = N'$. ■

7.1.3. Definíció. *A* **természetes számok halmazának** *nevezzük azt a monoton halmazt, amely minden monoton halmaznak részhalmaza, és ezt a halmazt az $\mathbb{N}$ szimbólummal jelöljük. Az $\mathbb{N}$ halmaz elemeit* **természetes számoknak** *nevezzük, továbbá: $0 := \emptyset$ és $\mathbb{N}^* := \{n \in \mathbb{N} | n \neq 0\}$, vagyis $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.*

Tehát a természetes számok halmaza a tartalmazás tekintetében legkisebb monoton halmaz. Látjuk, hogy ennek létezése pontosan azon múlik, hogy *létezik monoton halmaz*, tehát a végtelenségi axiómának az a szerepe, hogy lehetővé teszi a természetes számok bevezetését a halmazelméletben. Később, a halmazok végtelenségének definíciója (8.1.1.) után, látni fogjuk, hogy $\mathbb{N}$ végtelen halmaz (8.1.7.), tehát a végtelenségi axióma biztosítja végtelen halmaz létezését is: innen származik az axióma elnevezése.

Néhány nevezetes természetes szám definíciója és *szerkezete*:

$$\begin{aligned} 0 &:= \emptyset, \\ 1 &:= 0^+ = \{\emptyset\}, \\ 2 &:= 1^+ = \{\emptyset, \{\emptyset\}\}, \\ 3 &:= 2^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\ 4 &:= 3^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}, \end{aligned}$$

és így tovább. Vegyük észre, hogy ezek az objektumok a végtelenségi axióma *nélkül* is értelmezhetőek, hiszen a definíciójukban csak az üres halmaz és a szukcesszor fogalma szerepel! Azonban ahhoz, hogy az így előállítható objektumok *halmazáról*, vagyis az *összes természetes számok halmazáról* lehessen beszélni, szükségünk van a végtelenségi axiómára.

7.2. A teljes indukció és a végtelen leszállás tétele

A következő tételben a természetes számokra vonatkozó kijelentések bizonyításának legfontosabb elvéről lesz szó.

7.2.1. Tétel. (**A teljes indukció tétele**)

– *Ha $E \subseteq \mathbb{N}$ olyan halmaz, hogy $0 \in E$ és minden $n \in E$ elemre $n^+ \in E$ teljesül, akkor $E = \mathbb{N}$.* (**Halmazelméleti forma**)

– *Ha x olyan változó és $\mathscr{A}(x)$ olyan kijelentés, hogy $\mathscr{A}(0)$ tétel és*

$$(\forall x)(((x \in \mathbb{N}) \wedge \mathscr{A}(x)) \Rightarrow \mathscr{A}(x^+)) \tag{$*$}$$

is tétel, akkor $(\forall x)((x \in \mathbb{N}) \Rightarrow \mathscr{A}(x))$ is tétel. (**Logikai forma**)

Bizonyítás. Az első állításban az E-re vonatkozó feltétel éppen azt jelent, hogy E monoton részhalmaza $\mathbb{N}$-nek, így a $\mathbb{N}$ definíciója és a meghatározottsági axióma alapján $E = \mathbb{N}$ teljesül. A második állítás feltételei mellett az

$$E := \{x | (x \in \mathbb{N}) \wedge \mathscr{A}(x)\}$$

halmazra az első állítás feltételei teljesülnek, tehát $E = \mathbb{N}$, ami éppen azt jelenti, hogy $(\forall x)((x \in \mathbb{N}) \Rightarrow \mathscr{A}(x))$ teljesül. ■

Megjegyezzük, hogy az előző állításban szereplő $(*)$ kijelentést *indukciós hipotézisnek* nevezzük.

7.2.2. Tétel. (**A végtelen leszállás tétele**)

– *Ha $E \subseteq \mathbb{N}$ olyan halmaz, hogy $E \neq \emptyset$ és minden $n \in \mathbb{N}$ elemre: $n^+ \in E$ esetén $n \in E$ teljesül, akkor $0 \in E$.* (**Halmazelméleti forma**)

– *Ha x olyan változó és $\mathscr{A}(x)$ olyan kijelentés, hogy $(\exists x)((x \in \mathbb{N}) \wedge \mathscr{A}(x))$ tétel, valamint $(\forall x)(((x \in \mathbb{N}) \wedge \mathscr{A}(x^+)) \Rightarrow \mathscr{A}(x))$ is tétel, akkor $\mathscr{A}(0)$ is tétel.* (**Logikai forma**)

Bizonyítás. (I) A halmezelméleti formát indirekt bizonyítjuk, tehát feltesszük, hogy az E-re vonatkozó hipotézisek mellett $0 \notin E$. Ekkor $0 \in \mathbb{N} \setminus E$, továbbá a hipotézis szerint minden $n \in \mathbb{N}$ esetén, ha $n \in \mathbb{N} \setminus E$, akkor $n^+ \in \mathbb{N} \setminus E$. A teljes indukció halmazelméleti formáját alkalmazva az $\mathbb{N} \setminus E$ halmazra kapjuk, hogy $\mathbb{N} \setminus E = \mathbb{N}$, tehát $E \subseteq \mathbb{N}$ miatt $E = \emptyset$. Ez ellentmond az $E \neq \emptyset$ hipotézisnek.

(II) A logikai forma bizonyításához elegendő alkalmazni a halmazelméleti formát az

$$E := \{x|(x \in \mathbb{N}) \wedge \mathscr{A}(x)\}$$

halmazra. ■

Könnyen belátható, hogy a teljes indukció és a végtelen leszállás elve *ekvivalensek* egymással. Itt csak azt mutattuk meg, hogy az előbbiből következik az utóbbi.

Figyeljük meg, hogy az itt igazolt tételek teljesen függetlenek bármiféle $\mathbb{N}$ feletti rendezéstől! Bizonyításukban csak a természetes számok halmazának *definícióját* alkalmaztuk.

7.3. A természetes számok elemi tulajdonságai

A természetes számok definíciója nem kínál "belső" jellemzést a természetes számokra, vagyis nem adtunk meg olyan $\mathscr{N}(x)$ kijelentést, amely ekvivalens volna az $x \in \mathbb{N}$ kijelentéssel, tehát $\mathscr{N}(x)$ a természetes számok jellemzést adná. Azonban létezik ilyen kijelentés, de meglehetősen bonyolult szerkezetű (10.4.10.). De a természetes számok jellemzésének híján is megállapítható sok érdekes tény velük kapcsolatban, ami jól látható a következő állításokból. Ezek megfogalmazásához először bevezetünk egy fontos halmazelméleti fogalmat.

7.3.1. Definíció. *Azt mondjuk, hogy az E halmaz* **tranzitív**, *ha minden $x \in E$ elemre $x \subseteq E$ teljesül, vagyis E minden elemének minden eleme E-nek is eleme.*

7.3.2. Állítás.

a) $\mathbb{N}$ *tranzitív halmaz.*
b) *Minden természetes szám tranzitív halmaz.*
c) *Minden $n \in \mathbb{N}$ elemre $n \notin n$.*
d) *Minden $m, n \in \mathbb{N}$ elemre $(m \in n) \Leftrightarrow ((m \subseteq n) \wedge (m \neq n))$.*

Bizonyítás. a) Legyen $E := \{n \in \mathbb{N}|n \subseteq \mathbb{N}\}$. Triviális, hogy $0 \in E$, hiszen a definíció szerint $0 = \emptyset$. Ha $n \in E$, akkor $n \subseteq \mathbb{N}$ és $n \in \mathbb{N}$ miatt $\{n\} \subseteq \mathbb{N}$, így $n^+ := n \cup \{n\} \subseteq \mathbb{N}$, vagyis $n^+ \in E$. Ebből a teljes indukció elve alapján kapjuk, hogy $E = \mathbb{N}$, ami éppen azt jelent, hogy $\mathbb{N}$ tranzitív halmaz.

b) Legyen $E := \{n \in \mathbb{N}|(\forall k)((k \in n) \Rightarrow (k \subseteq n))\}$. Triviális, hogy $0 \in E$, különben létezne olyan $k \in 0$, hogy k nem részhalmaza 0-nak, holott 0-nak egyáltalán nincs eleme. Tegyük fel, hogy $n \in E$; megmutatjuk, hogy $n^+ \in E$. Ehhez legyen $k \in n^+$, tehát $k \in n$ vagy $k = n$. Ha $k \in n$, akkor $n \in E$ miatt $k \subseteq n$ és természetesen $n \subseteq n^+$, ezért $k \subseteq n^+$. Ha $k = n$, akkor a szukcesszor definíciója szerint $k \subseteq n^+$. Ezzel beláttuk, hogy $n \in E$ esetén $n^+ \in E$, tehát a teljes indukció elve alapján $E = \mathbb{N}$, ami éppen azt jelent, hogy minden természetes szám tranzitív halmaz.

c) Legyen $E := \{n \in \mathbb{N}|n \notin n\}$. Triviális, hogy $0 \in E$, különben $0 \in 0$ teljesülne, ami nem igaz, mert $0 = \emptyset$. Legyen $n \in E$, megmutatjuk, hogy ekkor $n^+ \in E$ is teljesül. Indirekt, tegyük fel, hogy $n^+ \notin E$, vagyis $n^+ \in n^+$. Ekkor a szukcesszor definíciója szerint $n^+ \in n$ vagy $n^+ = n$. Ha $n^+ \in n$, akkor $n \in n^+ \subseteq n$, hiszen b) szerint n tranzitív halmaz, ezért $n \in n$, ami viszont ellentmond annak, hogy $n \in E$. Ebből következik, hogy $n^+ = n$, tehát $n \in n$, ami ismét ellentmond az $n \in E$ hipotézisnek. Ezért $n^+ \in E$ szükségképpen teljesül, így a teljes indukció elve alapján $E = \mathbb{N}$, ami pontosan azt jelenti, hogy minden természetes szám nem eleme önmagának.

d) Ha $m, n \in \mathbb{N}$ és $m \in n$, akkor $m \subseteq n$, mert b) szerint n tranzitív halmaz, ugyanakkor $m \neq n$, különben $n \in n$ teljesülne, ami c) szerint lehetetlen. Ezért $m, n \in \mathbb{N}$ esetén az $(m \in n) \Rightarrow ((m \subseteq n) \wedge (m \neq n))$ következtetés helyes. A fordított implikáció bizonyításához legyen $E := \{n \in \mathbb{N} | (\forall m)(((m \subseteq n) \wedge (m \neq n)) \Rightarrow (m \in n))$. Azt kell igazolni, hogy $E = \mathbb{N}$.

Világos, hogy $0 \in E$, mert minden $m \in \mathbb{N}$ esetén az $(m \subseteq 0) \wedge (m \neq 0)$ kijelentés hamis, így az $((m \subseteq 0) \wedge (m \neq 0)) \Rightarrow (m \in 0)$ következtetés igaz (*a hamisból bármi következik*). Tegyük most fel, hogy $n \in E$ és legyen $m \in \mathbb{N}$ olyan, hogy $m \subseteq n^+$ és $m \neq n^+$; megmutatjuk, hogy $m \in n^+$, vagyis $n^+ \in E$.

Először azt igazoljuk, hogy a feltevések mellett $m \subseteq n$ teljesül. Ha nem így volna akkor létezne olyan $k \in m$, amelyre $k \notin n$. Ekkor $k \in m \subseteq n^+$, tehát $k \in n^+$, így $k \in n$ vagy $k = n$. De $k \notin n$, ezért szükségképpen $k = n$. Ebből kapjuk, hogy $n \in m$, tehát $\{n\} \subseteq m$, ugyanakkor $n \subseteq m$, mert b) szerint m tranzitív halmaz. Ezért $n^+ = n \cup \{n\} \subseteq m$, így $n^+ = m$ is teljesül, hiszen az m-re vonatkozó hipotézis szerint $m \subseteq n^+$. Ez a következmény viszont ellentmond a $m \neq n^+$ hipotézisnek, amivel igazoltuk, hogy $m \subseteq n$.

Ha $m = n$, akkor $m \in n^+$. Ha viszont $m \neq n$, akkor az előzőek szerint $(m \subseteq n) \wedge (m \neq n)$ teljesül, így $n \in E$ miatt $m \in n \subseteq n^+$, tehát $m \in n^+$. ■

7.3.3. Állítás. *Minden $m, n \in \mathbb{N}$ elemre teljesülnek a következő állítások:*

a) *$m \subseteq n$ ekvivalens azzal, hogy $m \in n$ vagy $m = n$,*

b) *$m \cap n \in \mathbb{N}$,*

c) *$m \subseteq n$ vagy $n \subseteq m$,*

d) *$(m \subseteq n) \Leftrightarrow (n \notin m)$,*

e) *$m \neq n$ ekvivalens azzal, hogy $m \in n$ vagy $n \in m$.*

Bizonyítás. a) Ha $m \subseteq n$ és $m \neq n$, akkor a 7.3.2. állítás d) pontja szerint $m \in n$. Megfordítva, ha $m \in n$, akkor $m \subseteq n$, mert a 7.3.2. állítás b) pontja szerint n tranzitív halmaz.

b) Legyen $m \in \mathbb{N}$ rögzítve és $E := \{n \in \mathbb{N} | m \cap n \in \mathbb{N}\}$. Triviális, hogy $m \cap 0 = 0 \in \mathbb{N}$, tehát $0 \in E$. Tegyük fel, hogy $n \in E$. A szukcesszor definíciója alapján

$$m \cap n^+ = m \cap (n \cup \{n\}) = (m \cap n) \cup (m \cap \{n\})$$

teljesül. Ha $n \in m$, akkor $\{n\} \subseteq m$ és $n \subseteq m$, mert m tranzitív halmaz, így $m \cap \{n\} = \{n\}$ és $m \cap n = n$, vagyis $m \cap n^+ = n \cup \{n\} = n^+ \in \mathbb{N}$. Ha $n \notin m$, akkor $m \cap \{n\} = \emptyset$, így az $n \in E$ hipotézis alapján $m \cap n^+ = m \cap n \in \mathbb{N}$ adódik. Ezért $m \cap n^+ \in \mathbb{N}$, vagyis $n^+ \in E$. A teljes indukció elve alapján $E = \mathbb{N}$, ami éppen azt jelenti, hogy adott $m \in \mathbb{N}$ esetén minden $n \in \mathbb{N}$ elemre $m \cap n \in \mathbb{N}$ teljesül. Ez *minden* $m \in \mathbb{N}$ elemre így van tehát (az általánosítás logikai szabálya szerint) minden $m, n \in \mathbb{N}$ elemre $m \cap n \in \mathbb{N}$ teljesül.

c) Az előzőek szerint $m \cap n \in \mathbb{N}$ és persze $m \cap n \subseteq m$ és $m \cap n \subseteq n$ is teljesül. Ha

$m \cap n \neq m$, akkor a 7.3.2. állítás d) pontja szerint $m \cap n \in m$. Hasonlóan kapjuk, hogy ha $m \cap n \neq n$, akkor $m \cap n \in n$. Tehát ha $m \cap n \neq m$ *és* $m \cap n \neq n$, akkor $m \cap n \in m$ *és* $m \cap n \in n$, így $m \cap n \in m \cap n$, ami ellentmond a 7.3.2. állítás c) pontjának. Ezért $m \cap n = m$ *vagy* $m \cap n = n$, ami éppen azt jelenti, hogy $m \subseteq n$ vagy $n \subseteq m$.

d) Ha $n \in m$, akkor a 7.3.2. állítás d) pontja szerint $n = m$ *vagy* n nem részhalmaza m-nek; ez utóbbi esetben a fentiek alapján $m \subseteq n$, így $(n \notin m) \Rightarrow (m \subseteq n)$ teljesül. Megfordítva, ha $m \subseteq n$, akkor $n \in m$ lehetetlen, különben $n \in n$ is teljesülne, ami ellentmond a 7.3.2. állítás c) pontjának; ezért $(m \subseteq n) \Rightarrow (n \notin m)$ is teljesül.

e) Ha $m \neq n$, akkor $(m \subseteq n) \wedge (m \neq n)$ vagy $(n \subseteq m) \wedge (n \neq m)$ teljesül, tehát az előző állítás d) pontja szerint $m \in n$ vagy $n \in m$ igaz. Megfordítva, akár $m \in n$, akár $n \in m$ teljesül, a 7.3.2. állítás d) pontja miatt $m \neq n$ is teljesül. ■

7.3.4. Tétel. (**Adott számtól indított teljes indukció**) *Legyen $m \in \mathbb{N}$ és E olyan halmaz, hogy $m \in E$, és minden $n \in \mathbb{N}$ esetén, ha $m \subseteq n$ és $n \in E$, akkor $n^+ \in E$. Ekkor minden $n \in \mathbb{N}$ esetén, ha $m \subseteq n$, akkor $n \in E$.*

Bizonyítás. Legyen $E' := m \cup E$. Megmutatjuk, hogy $\mathbb{N} \subseteq E'$.

Ha $0 = m$, akkor a hipotézis alapján $0 \in E$, tehát $0 \in E'$. Ha $m \neq 0$, akkor 7.3.2. miatt $0 \in m$, hiszen $0 := \emptyset \subseteq m$ teljesül, ezért ismét igaz, hogy $0 \in E'$. Tehát $0 \in E'$.

Tegyük fel, hogy $n \in E'$. Ekkor két eset lehetséges:

– ha $n \in m$, akkor az m halmaz tranzitivitása miatt (7.3.2. b) állítás) $n \subseteq m$, ezért $n^+ := n \cup \{n\} \subseteq m$; így $n^+ = m$ esetén $n^+ \in E \subseteq E'$, míg $n^+ \neq m$ esetén 7.3.2. d) miatt $n^+ \in m \subseteq E'$: vagyis $n^+ \in E'$;

– ha $n \notin m$, akkor $n \in E$ és 7.3.3. d) miatt $m \subseteq n$, tehát a hipotézis szerint $n^+ \in E \subseteq E'$, vagyis $n^+ \in E'$.

Ez azt jelenti, hogy E' monoton halmaz, tehát $\mathbb{N}$ definíciója szerint $\mathbb{N} \subseteq E'$. Ha $n \in \mathbb{N}$ és $m \subseteq n$, akkor 7.3.3. d) szerint $n \notin m$, tehát $n \in E'$ miatt $n \in E$, vagyis $\{n \in \mathbb{N} | m \subseteq n\} \subseteq E$. Ez pontosan azt jelenti, hogy minden $n \in \mathbb{N}$ esetén, ha $m \subseteq n$, akkor $n \in E$. ■

7.3.5. Állítás. *Ha $n \in \mathbb{N}$ és $x \subseteq n$ tranzitív halmaz, akkor $x \in \mathbb{N}$.*

Bizonyítás. Jelölje $\text{Trans}(x)$ a $(\forall y)((y \in x) \Rightarrow (y \subseteq x))$ kijelentést, tehát $\text{Trans}(x)$ azt jelenti, hogy x tranzitív halmaz. Legyen

$$E := \{n \in \mathbb{N} \mid (\forall x)((\text{Trans}(x) \wedge (x \subseteq n)) \Rightarrow (x \in \mathbb{N}))\}.$$

Azt kell igazolni, hogy $E = \mathbb{N}$.

Világos, hogy $0 \in E$, mert ha $x \subseteq 0 = \emptyset$, akkor $x = \emptyset$, vagyis $x = 0 \in \mathbb{N}$. Tegyük fel, hogy $n \in E$ és legyen $x \subseteq n^+$ tranzitív halmaz. Két eset lehetséges.

– Ha $n \notin x$, akkor $x \subseteq n$, ezért $n \in E$ miatt $x \in \mathbb{N}$.

– Ha $n \in x$, akkor x tranzitivitásából következik, hogy $n \subseteq x$, ezért $n^+ = n \cup \{n\} \subseteq x$, így $x = n^+ \in \mathbb{N}$.

Ezért a teljes indukció elve alapján $E = \mathbb{N}$. ■

7.3.6. Állítás.

a) *Minden $m, n \in \mathbb{N}$ esetén $m = n$ ekvivalens azzal, hogy $m^+ = n^+$.*

b) *Minden $n \in \mathbb{N}^*$ számhoz létezik egyetlen olyan $m \in \mathbb{N}$, amelyre $m^+ = n$.*

Bizonyítás. a) Ha $m^+ = n^+$, akkor $m \in m^+$ miatt $m \in n^+$, tehát $m \in n$ vagy $m = n$. Megmutatjuk, hogy $m \in n$ lehetetlen, tehát szükségképpen $m = n$. Ha ugyanis $m \in n$ teljesülne, akkor $n \in n^+ = m^+$ miatt $n \in m$ vagy $n = m$. Az első esetben $n \subseteq m$, mert m tranzitív halmaz, ezért $m \in m$, ami lehetetlen. A második esetben szintén $m \in m$, ami lehetetlen. Ezért $m^+ = n^+$ esetén szükségképpen $m = n$ teljesül.

b) Az egyértelműség a)-ból nyilvánvalóan következik. A létezés bizonyításához legyen $E := \{0\} \cup \{n \in \mathbb{N} | (n \neq 0) \wedge (\exists m)((m \in \mathbb{N}) \wedge (m^+ = n))\}$. A definíció alapján triviális, hogy $0 \in E$ és ha $n \in E$, akkor $n^+ \in E$, így a teljes indukció elve alapján $E = \mathbb{N}$, amit bizonyítani kellett. ■

7.3.7. Definíció. *Az $n \in \mathbb{N}^*$ szám* **predesszorának** *nevezzük és n^--szal jelöljük azt a természetes számot, amelyre $(n^-)^+ = n$ teljesül.*

7.4. Sorozatok, elemi rekurzió és iteráció

7.4.1. Definíció. Sorozatoknak *nevezzük a természetes számok halmazán értelmezett függvényeket. Ha E halmaz, akkor* E**-ben haladó sorozatoknak** *nevezzük azokat a sorozatokat, amelyek értékkészlete részhalmaza E-nek.*

7.4.2. Tétel. (**Az elemi rekurzív definíció tétele**) *Legyen E halmaz, $e \in E$ rögzített elem, és $g : \mathbb{N} \times E \to E$ tetszőleges függvény. Ekkor létezik egyetlen olyan E-ben haladó* $\mathbf{s}$ *sorozat, amelyre $\mathbf{s}(0) = e$ és minden $n \in \mathbb{N}$ számra $\mathbf{s}(n^+) = g(n, \mathbf{s}(n))$ teljesül.*

Bizonyítás. Először megmutatjuk, hogy minden $n \in \mathbb{N}$ számhoz *létezik egyetlen* olyan $f : n \to E$ függvény, amelyre teljesülnek a következők:

– ha $0 \in n$, akkor $f(0) = e$;
– minden $k \in n$ számra, ha $k^+ \in n$, akkor $f(k^+) = g(k, f(k))$.

Ehhez minden $n \in \mathbb{N}$ számra legyen S_n azon $f : n \to E$ függvények halmaza, amelyekre teljesülnek a fenti tulajdonságok. Megmutatjuk, hogy minden $n \in \mathbb{N}$ esetén S_n *egy elemű* halmaz; jelölje N azon $n \in \mathbb{N}$ számok halmazát, amelyekre S_n egy elemű halmaz. Nyilvánvaló, hogy $0 \in N$, mert $S_0 = \{\emptyset\}$. Tegyük fel, hogy $n \in N$ és legyen $\mathbf{s}_n$ az S_n halmaz egyetlen eleme. Legyen $f : n^+ \to E$ az a függvény, amelyre $k \in n$ esetén $f(k) := \mathbf{s}_n(k)$ és $f(n) := g(n^-, \mathbf{s}_n(n^-))$, ha $0 \in n$ (ha $0 \notin n$, akkor $n = 0$, és akkor $f = \emptyset$). A definícióból látszik, hogy $f \in S_{n^+}$. Ha $f' : n^+ \to E$ szintén olyan függvény, amelyre $f' \in S_{n^+}$, akkor világos, hogy $f'|_n \in S_n$, így $f'|_n = \mathbf{s}_n = f|_n$, vagyis $f' = f$ az n halmazon. Ugyanakkor, $0 \in n$ esetén

$$f'(n) = f'((n^-)^+) = g(n^-, f'(n^-)) = g(n^-, f(n^-)) =: f(n),$$

tehát $f' = f$. Ez azt jelenti, hogy $S_{n^+} = \{f\}$, vagyis $n^+ \in N$, így a teljes indukció elve alapján $N = \mathbb{N}$. Tehát minden $n \in \mathbb{N}$ esetén S_n egy elemű halmaz.

Világos, hogy minden $n \in \mathbb{N}$ esetén $S_n \subseteq \mathscr{F}_0(\mathbb{N}; E)$, ahol $\mathscr{F}_0(\mathbb{N}; E)$ jelöli az $\mathbb{N} \rightarrowtail E$ függvények halmazát. Ezért jól értelmezett az az $\mathbb{N}$-en értelmezett függvény, amely minden $n \in \mathbb{N}$ számhoz S_n-t rendeli. Valóban, ez a függvény egyenlő a

$$\{x | (\exists n)((n \in \mathbb{N}) \wedge (x = (n, S_n)))\}$$

halmazzal, és az előzőek szerint a $(\exists n)((n \in \mathbb{N}) \wedge (x = (n, S_n)))$ kijelentés kollektivizáló az x változóban, hiszen következik belőle az, hogy $x \in \mathbb{N} \times \mathscr{P}(\mathscr{F}_0(\mathbb{N}; E))$, így a részhalmaz axióma alkalmazható. Ilymódon tekinthetjük az $(S_n)_{n\in\mathbb{N}}$ rendszert.

Korábban láttuk, hogy egy elemű halmazok tetszőleges rendszerének a szorzata szintén egy elemű halmaz; legyen $(\mathbf{s}_n)_{n\in\mathbb{N}}$ az a halmaz, amelyre $\{(\mathbf{s}_n)_{n\in\mathbb{N}}\} = \prod_{n\in\mathbb{N}} S_n$ teljesül. Ekkor $(\mathbf{s}_n)_{n\in\mathbb{N}}$ az a függvény, amely az $\mathbb{N}$ halmazon értelmezett (tehát sorozat), továbbá, minden $n\in\mathbb{N}$ elemre $\mathbf{s}_n : n \to E$ az a függvény, amelyre teljesülnek a következők:

– ha $0 \in n$, akkor $\mathbf{s}_n(0) = e$;

– minden $k \in n$ számra, ha $k^+ \in n$, akkor $\mathbf{s}_n(k^+) = g(k, \mathbf{s}_n(k))$.

Ha $m, n \in \mathbb{N}$ és $m < n$, akkor $\mathbf{s}_n|_m \in S_m$, ezért $\mathbf{s}_n|_m = \mathbf{s}_m$, hiszen S_m egy elemű. Ezért létezik egyetlen olyan $\mathbf{s}$ függvény, amelyre

$$\mathrm{Dom}(\mathbf{s}) = \bigcup_{n\in\mathbb{N}} \mathrm{Dom}(\mathbf{s}_n) = \bigcup_{n\in\mathbb{N}} n = \mathbb{N},$$

és minden $n \in \mathbb{N}$ elemre $\mathbf{s}|_n = \mathbf{s}_n$, így $\mathbf{s}(0) = \mathbf{s}_1(0) = e$, továbbá $n \in \mathbb{N}$ esetén

$$\mathbf{s}(n^+) = \mathbf{s}_{(n^+)^+}(n^+) = g(n, \mathbf{s}_{(n^+)^+}(n)) = g(n, \mathbf{s}(n)),$$

tehát $\mathbf{s}$ olyan sorozat, amelynek a létezését állítottuk. ■

7.4.3. Definíció. *Ha E halmaz, $e \in E$ rögzített elem, és $g : \mathbb{N} \times E \to E$ függvény, akkor az e kezdőpont és g függvény által meghatározott* **elemi rekurzív sorozatnak** *nevezzük azt az E-ben haladó $\mathbf{s}$ sorozatot, amelyre $\mathbf{s}(0) = e$ és minden $n \in \mathbb{N}$ számra $\mathbf{s}(n^+) = g(n, \mathbf{s}(n))$.*

Gyakran előfordul, hogy az elemi rekurziónak csak egy speciális esetét alkalmazzuk: az *iterációt.*

7.4.4. Következmény. (**Az iterációs definíció tétele**) *Legyen E halmaz, $e \in E$ rögzített elem, és $f : E \to E$ tetszőleges függvény. Ekkor létezik egyetlen olyan E-ben haladó $\mathbf{s}$ sorozat, amelyre $\mathbf{s}(0) = e$ és minden $n \in \mathbb{N}$ számra $\mathbf{s}(n^+) = f(\mathbf{s}(n))$ teljesül.*

Bizonyítás. Elegendő az elemi rekurzív definíció tételét alkalmazni a E halmazra, az $e \in E$ kezdőpontra és a $g : \mathbb{N} \times E \to E;\quad (n, x) \mapsto f(x)$ függvényre. ■

7.4.5. Definíció. *Ha E halmaz, $e \in E$ rögzített elem, és $f : E \to E$ függvény, akkor az e kezdőpont és f függvény által meghatározott* **iterációs sorozatnak** *nevezzük azt az E-ben haladó $\mathbf{s}$ sorozatot, amelyre $\mathbf{s}(0) = e$ és minden $n \in \mathbb{N}$ számra $\mathbf{s}(n^+) = f(\mathbf{s}(n))$ teljesül.*

Könnyű példát adni olyan elemi rekurzióval értelmezhető sorozatokra, amelyek nem értelmezhetőek iterációval (**2**. Gyakorlat).

7.5. A rekurzív definíció tétele

7.5.1. Definíció. *Ha $\mathbf{s}$ sorozat, akkor minden $n \in \mathbb{N}$ esetén az $\mathbf{s}|_n$ leszűkített függvényt az* $\mathbf{s}$ **sorozat** n**-edik szeletének** *nevezzük. A 0-dik szeletet (ami nyilvánvalóan az üres függvény)* **triviális szeletnek** *nevezzük.*

A matematikában sokszor szükségünk van olyan sorozatok előállítására, amelyek rendelkeznek azzal a tulajdonsággal, hogy minden $n \in \mathbb{N}$ esetén a sorozat n helyen felvett értéke *egyértelműen* van meghatározva a sorozat n-edik szelete által. Vagyis olyan $\mathbf{s}$ sorozatot szeretnénk előállítani, amelyre minden $n \in \mathbb{N}$ esetén az $\mathbf{s}(n)$ érték egyértelműen kifejezhető az $\mathbf{s}|_n$ függvénnyel. Ez a konstrukció egészen általános feltételek mellett is lehetséges: erről szól az (általános) rekurzív definíció tétele. A pontos megfogalmazáshoz szükségünk lesz a következő halmazelméleti lemmára.

7.5.2. Lemma. *Minden E halmazhoz egyértelműen létezik az $(\mathscr{F}(n;E))_{n\in\mathbb{N}}$ függvény-halmaz-rendszer.*

Bizonyítás. Azt kell bizonyítani, hogy az

$$\mathbf{F} := \{z \mid (\exists n)(\ (n \in \mathbb{N}) \wedge (z = (n, \mathscr{F}(n;E)))\ )\}$$

halmaz jól értelmezett függvény. A $(\exists n)(\ (n \in \mathbb{N}) \wedge (z = (n, \mathscr{F}(n;E)))$ kijelentés kollektivizáló a z változóban, mert következik belőle, hogy $z \in \mathbb{N} \times \mathscr{P}(\mathscr{P}(\mathbb{N} \times E))$, így elég a részhalmaz-axiómára hivatkozni. Ezért az $\mathbf{F}$ halmaz jól értelmezett.

A definíció szerint, $z \in E$ esetén van olyan $n \in \mathbb{N}$, hogy $z = (n, \mathscr{F}(n;E))$, tehát z pár. Ez azt jelenti, hogy az $\mathbf{F}$ halmaz *reláció.*

Ha $(x,y),(x,y') \in \mathbf{F}$, akkor léteznek olyan $n, n' \in \mathbb{N}$ elemek, hogy $(x,y) = (n, \mathscr{F}(n;E))$ és $(x,y') = (n', \mathscr{F}(n';E))$. Ekkor $x = n$ és $x = n'$, tehát $n = n'$, amiből következik, hogy $y = \mathscr{F}(n;E) = \mathscr{F}(n';E) = y'$. Ez azt jelenti, hogy az $\mathbf{F}$ halmaz egyértelmű reláció, vagyis *függvény.*

Végül, ha $n \in \mathbb{N}$, akkor $(n, \mathscr{F}(n;E)) \in \mathbf{F}$, tehát $n \in \mathrm{pr}_1(\mathbf{F}) =: \mathrm{Dom}(\mathbf{F})$, így $\mathbb{N} \subseteq \mathrm{Dom}(\mathbf{F})$. Másfelől, ha $x \in \mathrm{Dom}(\mathbf{F})$, akkor van olyan y, hogy $(x,y) \in \mathbf{F}$, tehát létezik olyan $n \in \mathbb{N}$, amelyre $(x,y) = (n, \mathscr{F}(n;E))$, így $x = n \in \mathbb{N}$, vagyis $\mathrm{Dom}(\mathbf{F}) \subseteq \mathbb{N}$. Ez azt jelenti, hogy az $\mathbf{F}$ halmaz $\mathbb{N}$-en értelmezett függvény. ■

Megjegyezzük, hogy ha E nem üres halmaz, akkor az $(\mathscr{F}(n;E))_{n\in\mathbb{N}}$ függvényhalmaz-rendszer *diszjunkt*, mert $m, n \in \mathbb{N}$ esetén az $\mathscr{F}(m;E) \cap \mathscr{F}(n;E) \neq \emptyset$ feltételből következik olyan $\mathbf{s}'$ függvény létezése, hogy $\mathbf{s}' \in \mathscr{F}(m;E) \cap \mathscr{F}(n;E)$, következésképpen $m = \mathrm{Dom}(\mathbf{s}') = n$.

7.5.3. Tétel. (**A rekurzív definíció tétele**) *Legyen E halmaz és*

$$\mathbf{g} : \bigcup_{n\in\mathbb{N}} \mathscr{F}(n;E) \to E$$

tetszőleges függvény. Ekkor létezik egyetlen olyan $\mathbf{s} : \mathbb{N} \to E$ sorozat, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{s}(n) = \mathbf{g}(\mathbf{s}|_n)$ teljesül.

Bizonyítás. (I) Először teljes indukcióval megmutatjuk, hogy minden $n \in \mathbb{N}$ számhoz létezik egyetlen olyan $\mathbf{s} : n \to E$ függvény, amelyre minden $k \in n$ esetén $\mathbf{s}(k) = \mathbf{g}(\mathbf{s}|_k)$ teljesül. Ehhez legyen N az ilyen tulajdonságú természetes számok halmaza. Nyilvánvaló, hogy $0 \in N$; tegyük fel, hogy $n \in N$ és legyen $\mathbf{s}_n$ az az egyetlen $n \to E$ függvény, amelyre minden $k \in n$ esetén $\mathbf{s}_n(k) = \mathbf{g}(\mathbf{s}_n|_k)$ teljesül. Legyen $\mathbf{s} : n^+ \to E$ az a függvény, amelyre $k \in n$ esetén $\mathbf{s}(k) := \mathbf{s}_n(k)$ és $\mathbf{s}(n) := \mathbf{g}(\mathbf{s}_n)$. A definícióból látszik, hogy minden k természetes számra, ha $k \in n$ vagy $k = n$, akkor $\mathbf{s}|_k = \mathbf{s}_n|_k$. Világos, hogy minden $k \in n$ számra $\mathbf{s}(k) = \mathbf{s}_n(k) = \mathbf{g}(\mathbf{s}_n|_k) = \mathbf{g}(\mathbf{s}|_k)$ és $\mathbf{s}(n) = \mathbf{g}(\mathbf{s}_n) = \mathbf{g}(\mathbf{s}|_n)$.

Ez azt jelenti, hogy minden $k \in n^+$ elemre $\mathbf{s}(n) = \mathbf{g}(\mathbf{s}|_n)$. Ha $\mathbf{s}'$ szintén olyan $n^+ \to E$ függvény, amelyre minden $k \in n^+$ esetén $\mathbf{s}'(k) = \mathbf{g}(\mathbf{s}'|_k)$ teljesül, akkor ugyanez igaz minden $k \in n$ elemre, így az indukciós hipotézis alapján $\mathbf{s}'|_n = \mathbf{s}_n = \mathbf{s}|_n$. Ugyanakkor $\mathbf{s}'(n) = \mathbf{g}(\mathbf{s}'|_n) = \mathbf{g}(\mathbf{s}|_n) = \mathbf{s}(n)$, tehát $\mathbf{s}' = \mathbf{s}$. Ez azt jelenti, hogy $n^+ \in N$, tehát a teljes indukció elve alapján $N = \mathbb{N}$.

(II) Jelölje $\mathscr{A}$ a következő kijelentést:

$$(\exists n)(\exists \mathbf{s})(\ (x = (n, \mathbf{s})) \wedge (n \in \mathbb{N}) \wedge (\mathbf{s} \in \mathscr{F}(n; E)) \wedge ((\forall k)((k \in n) \Rightarrow (\mathbf{s}(k) = \mathbf{g}(\mathbf{s}|_k))))\ ).$$

Az $\mathscr{A}$ kijelentés kollektivizáló az x változóban, mert $\mathscr{A}$-ból következik, hogy $x \in \mathbb{N} \times \mathscr{P}(\mathbb{N} \times E)$, ezért elég a részhalmaz-axiómára hivatkozni. Legyen $\mathbf{S} := \{x|\mathscr{A}\}$. Az (I) alapján

$$\mathbf{S} : \mathbb{N} \to \bigcup_{n \in \mathbb{N}} \mathscr{F}(n; E)$$

az a függvény, amelyre minden $n \in \mathbb{N}$ esetén $\mathbf{S}(n)$ az az $n \to E$ függvény, amelyre minden $k \in n$ esetén $\mathbf{S}(n)(k) = \mathbf{g}(\mathbf{S}(n)|_k)$ teljesül. A zárójelek torlódásának elkerülése végett minden $n \in \mathbb{N}$ számra legyen $\mathbf{s}_n := \mathbf{S}(n)$, tehát $\mathbf{S}$ egyenlő az $(\mathbf{s}_n)_{n \in \mathbb{N}}$ rendszerrel. Ez azt jelenti, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{s}_n : n \to E$ az a függvény, amelyre minden $k \in n$ esetén $\mathbf{s}_n(k) = \mathbf{g}(\mathbf{s}_n|_k)$.

(III) Megmutatjuk, hogy $m, n \in \mathbb{N}$ és $m \subseteq n$ esetén $\mathbf{s}_n|_m = \mathbf{s}_m$. Valóban, az $\mathbf{s}_n|_m : m \to E$ leszűkített függvényre teljesül az, hogy minden $k \in m$ esetén $(\mathbf{s}_n|_m)(k) = \mathbf{s}_n(k) = \mathbf{g}(\mathbf{s}_n|_k) = \mathbf{g}((\mathbf{s}_n|_m)|_k)$, hiszen a leszűkítések tranzitivitása miatt $(\mathbf{s}_n|_m)|_k = \mathbf{s}_n|_k$. Ezért az (I) alapján $\mathbf{s}_n|_m = \mathbf{s}_m$.

Másfelől, bármely $m, n \in \mathbb{N}$ esetén $m \subseteq n$ vagy $n \subseteq m$ teljesül (7.3.3.), tehát minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}_m \subseteq \mathbf{s}_n$ vagy $\mathbf{s}_n \subseteq \mathbf{s}_m$. Ebből a függvények összeragasztásának tétele (6.2.10.) alapján kapjuk, hogy $\mathbf{s} := \bigcup_{n \in \mathbb{N}} \mathbf{s}_n$ olyan függvény, hogy $\mathrm{Dom}(\mathbf{s}) = \bigcup_{n \in \mathbb{N}} \mathrm{Dom}(\mathbf{s}_n) = \bigcup_{n \in \mathbb{N}} n = \mathbb{N}$, és $\mathrm{Im}(\mathbf{s}) = \bigcup_{n \in \mathbb{N}} \mathrm{Im}(\mathbf{s}_n) \subseteq E$, és minden $n \in \mathbb{N}$ esetén $\mathbf{s}_n \subseteq \mathbf{s}$. Ebből következik, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{s}(n) = \mathbf{s}_{n^+}(n) = \mathbf{g}(\mathbf{s}_{n^+}|_n) = \mathbf{g}((\mathbf{s}|_{n^+})|_n) = \mathbf{g}(\mathbf{s}|_n)$, vagyis $\mathbf{s}$ olyan E-ben haladó sorozat, amelynek az *egzisztenciáját* állítottuk.

(IV) Ha az $\mathbf{s}' : \mathbb{N} \to E$ sorozatra szintén teljesül az, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{s}'(n) = \mathbf{g}(\mathbf{s}'|_n)$, akkor minden $n \in \mathbb{N}$ számra $\mathbf{s}'|_n : n \to E$ olyan függvény, hogy minden $k \in n$ esetén $(\mathbf{s}'|_n)(k) = \mathbf{s}'(k) = \mathbf{g}(\mathbf{s}'|_k) = \mathbf{g}((\mathbf{s}'|_n)|_k)$, tehát $\mathbf{s}'|_n = \mathbf{S}(n) = \mathbf{s}_n = \mathbf{s}|_n$. Mivel pedig $\mathbb{N} = \bigcup_{n \in \mathbb{N}} n$, így ebből $\mathbf{s}' = \mathbf{s}$ következik, amivel $\mathbf{s}$ *unicitását* is igazoltuk. ■

7.5.4. Definíció. *Ha E halmaz, és*

$$\mathbf{g} : \bigcup_{n \in \mathbb{N}} \mathscr{F}(n; E) \to E$$

függvény, akkor a $\mathbf{g}$ függvény által meghatározott **rekurzív sorozatnak** *nevezzük azt az E-ben haladó $\mathbf{s}$ sorozatot, amelyre minden $n \in \mathbb{N}$ esetén $\mathbf{s}(n) = \mathbf{g}(\mathbf{s}|_n)$ teljesül.*

Vegyük észre, hogy az elemi rekurzív definíció tétele *következik* az imént bizonyított tételből. Legyen ugyanis E halmaz, $e \in E$ és $g : \mathbb{N} \times E \to E$ függvény, és értelmezzük azt a

$$\mathbf{g} : \bigcup_{n \in \mathbb{N}} \mathscr{F}(n; E) \to E$$

függvényt, amelyre $\mathbf{g}(\emptyset) := e$ és minden $n \in \mathbb{N}^*$, valamint $\mathbf{s}' \in \mathscr{F}(n;E)$ esetén $\mathbf{g}(\mathbf{s}') := g(n^-, \mathbf{s}'(n^-))$. Ekkor a $\mathbf{g}$ függvény által rekurzióval meghatározott $\mathbf{s}$ sorozat egyenlő a g függvény által elemi rekurzióval meghatározott sorozattal, hiszen

$$\mathbf{s}(0) = \mathbf{g}\left(\mathbf{s}|_0\right) = \mathbf{g}(\emptyset) := e,$$

és minden $n \in \mathbb{N}$ esetén

$$\mathbf{s}(n^+) = \mathbf{g}(\mathbf{s}|_{n^+}) = g((n^+)^-, \mathbf{s}|_{n^+}((n^+)^-)) = g(n, \mathbf{s}(n)).$$

7.6. A kiválasztási axiómával kombinált rekurzió tétele

A matematikában sokszor szükségünk van olyan sorozatok előállítására, amelyek *szeletei* előírt "tulajdonságokkal" rendelkeznek. Pontosabban: ha E halmaz és minden $n \in \mathbb{N}$ számra rögzítünk egy $F_n \subseteq \mathscr{F}(n;E)$ nem üres függvényhalmazt, akkor azt kérdezzük, hogy létezik-e olyan E-ben haladó $\mathbf{s}$ sorozat, amelyre minden $n \in \mathbb{N}$ esetén az $\mathbf{s}$ sorozat n-edik szelete eleme F_n-nek? Tehát ekkor a keresett $\mathbf{s}$ sorozat $n \in \mathbb{N}$ helyen felvett értéke nincs egyértelműen meghatározva az $\mathbf{s}|_n$ szelet által. A következő tétel elégséges, de nem szükséges feltételt ad ahhoz, hogy erre a kérdésre pozitív választ lehessen adni.

7.6.1. Tétel. (A kiválasztási axiómával kombinált rekurzió tétele) *Legyen E halmaz és $(F_n)_{n\in\mathbb{N}}$ olyan halmazrendszer, amelyre teljesül az, hogy minden $n \in \mathbb{N}$ esetén $F_n \subseteq \mathscr{F}(n;E)$ és $F_0 = \{\emptyset\}$. Tegyük fel, hogy*

$$(\forall n \in \mathbb{N})(\forall \mathbf{a} \in F_n)(\exists \mathbf{a}' \in F_{n^+}): \ \mathbf{a} = \mathbf{a}'|_n$$

teljesül. Ekkor létezik olyan $\mathbf{s}$ sorozat, amely az E halmazban halad, és minden $n \in \mathbb{N}$ esetén $\mathbf{s}|_n \in F_n$.

Bizonyítás. Ha $n \in \mathbb{N}$ és $\mathbf{a} \in F_n$, akkor az $\{\mathbf{a}' \in F_{n^+} |\ \mathbf{a} = \mathbf{a}'|_n\}$ halmaz a hipotézis alapján *nem üres*, ezért a kiválasztási axióma szerint minden $n \in \mathbb{N}$ számra

$$\prod_{\mathbf{a}\in F_n} \{\mathbf{a}' \in F_{n^+} |\ \mathbf{a} = \mathbf{a}'|_n\} \ \neq \ \emptyset.$$

Ismét a kiválasztási axióma alkalmazásával nyerjük, hogy

$$\prod_{n\in\mathbb{N}} \left(\prod_{\mathbf{a}\in F_n} \{\mathbf{a}' \in F_{n^+} |\ \mathbf{a} = \mathbf{a}'|_n\} \right) \ \neq \ \emptyset;$$

legyen f eleme ennek a szorzathalmaznak. Tehát f olyan függvény, amely az $\mathbb{N}$ halmazon értelmezett (vagyis sorozat), és minden $n \in \mathbb{N}$ esetén $f(n) : F_n \to F_{n^+}$ olyan függvény, hogy minden $\mathbf{a} \in F_n$ esetén az $f(n)(\mathbf{a})$ függvény leszűkítése n-re egyenlő $\mathbf{a}$-val.

Legyen most $\mathscr{E} := \bigcup_{n\in\mathbb{N}} F_n$. Ha $\mathbf{a} \in \mathscr{E}$, akkor van olyan $n \in \mathbb{N}$, hogy $\mathbf{a} \in F_n$, tehát $\mathbf{a} : n \to E$ függvény, így $\mathrm{Dom}(\mathbf{a}) = n \in \mathbb{N}$. Ezért értelmezhetjük a

$$g : \mathscr{E} \to \mathscr{E}; \quad \mathbf{a} \mapsto f(\mathrm{Dom}(\mathbf{a}))(\mathbf{a})$$

függvényt. Jelölje $\mathbf{e}$ az üres függvényt. Ekkor a hipotézis alapján $\mathbf{e} \in F_0$ az F_0 halmaz egyetlen eleme, így $\mathbf{e} \in \mathscr{E}$, tehát az iterációs tétel alapján tekinthetjük az $\mathbf{e} \in \mathscr{E}$ kezdőpont és a g függvény által meghatározott $\mathbf{S}$ iterációs sorozatot. Tehát $\mathbf{S}$ az a függvény, amelyre $\mathrm{Dom}(\mathbf{S}) = \mathbb{N}$ és $\mathrm{Im}(\mathbf{S}) \subseteq \mathscr{E}$, és $\mathbf{S}(0) = \mathbf{e} := \emptyset$, továbbá minden $n \in \mathbb{N}$ esetén $\mathbf{S}(n^+) = g(\mathbf{S}(n)) = f(\mathrm{Dom}(\mathbf{S}(n)))(\mathbf{S}(n))$ teljesül.

Teljes indukcióval könnyen belátható, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{S}(n) \in F_n$ teljesül. Valóban, a hipotézis szerint $\mathbf{S}(0) = \mathbf{e} \in F_0$, és ha $n \in \mathbb{N}$ olyan, hogy $\mathbf{S}(n) \in F_n$, akkor $\mathbf{S}(n) : n \to E$ függvény, tehát $\mathrm{Dom}(\mathbf{S}(n)) = n$, így

$$\mathbf{S}(n^+) = f(\mathrm{Dom}(\mathbf{S}(n)))(\mathbf{S}(n)) \in F_{(\mathrm{Dom}(\mathbf{S}(n)))^+} = F_{n^+}.$$

A definícióból következik, hogy minden $n \in \mathbb{N}$ esetén

$$\mathbf{S}(n^+)|_n = f(\mathrm{Dom}(\mathbf{S}(n)))(\mathbf{S}(n))|_n = f(n)(\mathbf{S}(n))|_n = \mathbf{S}(n),$$

vagyis $\mathbf{S}(n) = \mathbf{S}(n^+)|_n$. Ennek alkalmazásával teljes indukcióval bebizonyítjuk, hogy rögzített $n \in \mathbb{N}$ esetén, minden $m \in \mathbb{N}$ elemre, ha $n \subseteq m$, akkor $\mathbf{S}(m)|_n = \mathbf{S}(n)$, vagyis $\mathbf{S}(n) \subseteq \mathbf{S}(m)$. Ehhez legyen $N := n \cup \{m \in \mathbb{N} | (n \subseteq m) \wedge (\mathbf{S}(m)|_n = \mathbf{S}(n))\}$; azt kell igazolni, hogy $N = \mathbb{N}$.

Ha $0 \in n$, akkor $0 \in N$. Ha $0 \notin n$, akkor a 7.3.3. állítás szerint $n \subseteq 0 = \emptyset$, vagyis $n = 0$, így $N = \{m \in \mathbb{N} | \mathbf{S}(m)|_0 = \mathbf{S}(0)\}$, és világos, hogy $\mathbf{S}(0)|_0 = \emptyset = \mathbf{S}(0)$, vagyis $0 \in N$.

Tegyük fel, hogy $m \in N$. Ha $n \nsubseteq m$, akkor a 7.3.3. állítás szerint $m \in n$, tehát $m \in N$. Ha $n \subseteq m$ akkor a 7.3.3. állítás szerint $m \notin n$, így $m \in N$ miatt $\mathbf{S}(m)|_n = \mathbf{S}(n)$ teljesül. Ekkor $\mathbf{S}(m^+)|_n = (\mathbf{S}(m^+)|_m)|_n = \mathbf{S}(m)|_n = \mathbf{S}(n)$, vagyis $m^+ \in N$. Ezért a teljes indukció elve alapján $N = \mathbb{N}$.

A 7.3.3. állítás szerint minden $m \in \mathbb{N}$ esetén $m \subseteq n$ vagy $m \subseteq n$, ezért a függvények összeragasztásának tétele alapján az $\mathbf{s} := \bigcup_{n \in \mathbb{N}} \mathbf{S}(n)$ halmaz függvény. Ekkor $\mathrm{Dom}(\mathbf{s}) = \bigcup_{n \in \mathbb{N}} \mathrm{Dom}(\mathbf{S}(n)) = \bigcup_{n \in \mathbb{N}} n = \mathbb{N}$, és $\mathrm{Im}(\mathbf{s}) = \bigcup_{n \in \mathbb{N}} \mathrm{Im}(\mathbf{S}(n)) \subseteq E$, ezért $\mathbf{s}$ olyan E-ben haladó sorozat, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{S}(n) \subseteq \mathbf{s}$, tehát $\mathbf{s}|_n = \mathbf{S}(n) \in F_n$. ■

7.7. Műveletek a természetes számok halmaza felett

Most az iteráció néhány fontos, különös jelentőségű alkalmazását mutatjuk be.

7.7.1. Definíció. (**$\mathbb{N}$ feletti összeadás értelmezése**) *Minden $m \in \mathbb{N}$ esetén legyen s_m az m kezdőpont és az $\mathbb{N} \to \mathbb{N}$; $n \mapsto n^+$ függvény által meghatározott iterációs sorozat; tehát $s_m : \mathbb{N} \to \mathbb{N}$ az a függvény, amelyre $s_m(0) = m$ és minden $n \in \mathbb{N}$ esetén $s_m(n^+) = (s_m(n))^+$. Ekkor az*

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}; \quad (m, n) \mapsto m + n := s_m(n)$$

függvényt az $\mathbb{N}$ feletti **összeadásnak** *nevezzük.*

Tehát az $\mathbb{N}$ feletti összeadás olyan művelet, hogy minden $m, n \in \mathbb{N}$ számra

$$m + 0 = m;$$
$$m + n^+ = (m + n)^+$$

teljesül. Az $1 \in \mathbb{N}$ szám és a $+$ művelet definíciója alapján nyilvánvaló, hogy minden $n \in \mathbb{N}$ esetén $n + 1 = n + 0^+ = (n + 0)^+ = n^+$.

7.7.2. Állítás. *Az $\mathbb{N}$ feletti összeadás asszociatív, kommutatív és 0 a neutrális eleme.*

Bizonyítás. (I) Legyenek $m, n \in \mathbb{N}$ rögzítettek; teljes indukcióval igazoljuk, hogy minden $k \in \mathbb{N}$ esetén $(m+n)+k = m+(n+k)$ teljesül. Az összeadás értelmezése alapján $(m+n)+0 = m+n = m+(n+0)$, tehát az állítás igaz $k := 0$ esetén. Ha $k \in \mathbb{N}$ olyan, hogy $(m+n)+k = m+(n+k)$, akkor

$$(m+n)+k^+ = ((m+n)+k)^+ = (m+(n+k))^+ = m+(n+k)^+ = m+(n+k^+),$$

tehát az állítás k^+-ra is igaz, amivel a teljes indukciót végrehajtottuk. Ez azt jelenti, hogy minden $m, n \in \mathbb{N}$ esetén minden $k \in \mathbb{N}$ számra $(m+n)+k = m+(n+k)$ teljesül, vagyis az $\mathbb{N}$ feletti összeadás asszociatív.

(II) Megmutatjuk, hogy 0 az összeadás neutrális eleme. Ehhez n szerinti teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén $n+0 = 0+n = n$ teljesül. Ez $n := 0$-ra triviálisan igaz, és ha $n \in \mathbb{N}$ olyan, hogy $n+0 = 0+n = n$, akkor

$$0+n^+ = (0+n)^+ = n^+ = n^+ + 0.$$

(III) Most n szerinti teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén $n+1 = 1+n$ teljesül. Láttuk, hogy 0 az összeadás neutrális eleme, ezért $0+1 = 1 = 1+0$, így az állítás 0-ra igaz. Tegyük fel, hogy $n \in \mathbb{N}$ olyan, hogy $n+1 = 1+n$. Ekkor a definíciók és az előzőek szerint

$$1+n^+ = (1+n)^+ = (n+1)^+ = (n+1)+1 = n^+ + 1.$$

(IV) Legyen végül $m \in \mathbb{N}$ rögzített elem; teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén $m+n = n+m$ teljesül. Ez $n := 0$ esetén igaz, mert 0 az összeadás neutrális eleme. Ha $n \in \mathbb{N}$ olyan, hogy $m+n = n+m$, akkor az összeadás asszociativitását és (III)-t alkalmazva kapjuk, hogy

$$\begin{aligned} m+n^+ &= (m+n)^+ = (n+m)^+ = (n+m)+1 = \\ &= n+(m+1) = n+(1+m) = (n+1)+m = n^+ + m, \end{aligned}$$

amivel a teljes indukciót végrehajtottuk, ami azt jelenti, hogy az $\mathbb{N}$ feletti összeadás kommutatív. ■

7.7.3. Állítás. (**Az $\mathbb{N}$ feletti összeadás kancellativitása**) *Ha $m, n \in \mathbb{N}$, akkor a következő állítások ekvivalensek.*

(i) $m = n$.

(ii) *Minden $k \in \mathbb{N}$ esetén $m+k = n+k$.*

(iii) *Létezik olyan $k \in \mathbb{N}$, hogy $m+k = n+k$.*

Bizonyítás. (i)⇒(ii) és (ii)⇒(iii) triviális.

(iii)⇒(i) A hipotézis szerint az $E := \{k \in \mathbb{N} \mid m+k = n+k\}$ halmaz nem üres. Ha $k \in \mathbb{N}$ olyan, hogy $k^+ \in E$, akkor az $\mathbb{N}$ feletti összeadás definíciója szerint

$$(m+k)^+ = m+k^+ = n+k^+ = (n+k)^+,$$

ezért a 7.3.6. állítás a) pontja szerint $m+k = n+k$, vagyis $k \in E$. Ezért a végtelen leszállás elve alapján $0 \in E$, ami azt jelenti, hogy $m = m+0 = n+0 = n$. ■

7.7.4. Definíció. ($\mathbb{N}$ **feletti szorzás értelmezése**) *Minden* $m \in \mathbb{N}$ *esetén legyen* p_m *a* 0 *kezdőpont és az* $\mathbb{N} \to \mathbb{N}$; $n \mapsto n + m$ *függvény által meghatározott iterációs sorozat; tehát* $p_m : \mathbb{N} \to \mathbb{N}$ *az a függvény, amelyre* $p_m(0) = 0$ *és minden* $n \in \mathbb{N}$ *esetén* $p_m(n^+) = p_m(n) + m$. *Ekkor az*

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}; \quad (m, n) \mapsto m \cdot n := p_m(n)$$

függvényt az $\mathbb{N}$ *feletti* **szorzásnak** *nevezzük.*

Tehát az $\mathbb{N}$ feletti szorzás olyan művelet, hogy minden $m, n \in \mathbb{N}$ számra

$$m \cdot 0 = 0;$$
$$m \cdot n^+ = (m \cdot n) + m$$

teljesül.

7.7.5. Állítás. *Az* $\mathbb{N}$ *feletti szorzás asszociatív, kommutatív és* 1 *a neutrális eleme. Az* $\mathbb{N}$ *feletti szorzás disztributív az* $\mathbb{N}$ *feletti összeadásra nézve.*

Bizonyítás. (I) Először megmutatjuk, hogy 1 a szorzás neutrális eleme, vagyis minden $n \in \mathbb{N}$ esetén $n \cdot 1 = n = 1 \cdot n$ teljesül. A definíció szerint $1 \cdot 0 = 0$, ezért $0 \cdot 1 = 0 \cdot 0^+ = (0 \cdot 0) + 0 = 0 + 0 = 0 = 1 \cdot 0$, vagyis az állítás $n := 0$ esetén igaz. Tegyük fel, hogy $n \in \mathbb{N}$ olyan, hogy $n \cdot 1 = n = 1 \cdot n$ teljesül. Ekkor $1 \cdot n^+ = 1 \cdot n + 1 = n + 1 = n^+$, ugyanakkor $n^+ \cdot 1 = n^+ \cdot 0^+ = n^+ \cdot 0 + n^+ = 0 + n^+ = n^+$, vagyis $1 \cdot n^+ = n^+ = n^+ \cdot 1$, így az állítás n^+-ra is igaz. Tehát a teljes indukció elve alapján kapjuk, hogy 1 a szorzás neutrális eleme.

(II) Most igazoljuk, hogy a szorzás *balról* disztributív az összeadásra nézve. Ehhez legyen $k, m \in \mathbb{N}$ rögzített; teljes indukcióval megmutatjuk, hogy minden $n \in \mathbb{N}$ esetén $k \cdot (m + n) = (k \cdot m) + (k \cdot n)$. Ez igaz $n := 0$ esetén, mert

$$k \cdot (m + 0) = k \cdot m = (k \cdot m) + 0 = (k \cdot m) + (k \cdot 0).$$

Ha $n \in \mathbb{N}$ olyan, hogy $k \cdot (m + n) = (k \cdot m) + (k \cdot n)$, akkor az $\mathbb{N}$ feletti összeadás asszociativitását alkalmazva

$$k \cdot (m + n^+) = k \cdot (m + n)^+ = (k \cdot (m + n)) + k = ((k \cdot m) + (k \cdot n)) + k =$$
$$= (k \cdot m) + ((k \cdot n) + k) = (k \cdot m) + (k \cdot n^+),$$

tehát az állítás n^+-ra is igaz.

(III) Megmutatjuk, hogy a szorzás asszociatív. Ehhez legyen $k, m \in \mathbb{N}$ rögzített; teljes indukcióval megmutatjuk, hogy minden $n \in \mathbb{N}$ esetén $k \cdot (m \cdot n) = (k \cdot m) \cdot n$. Ez igaz $n := 0$ esetén, mert

$$k \cdot (m \cdot 0) = k \cdot 0 = 0 = (k \cdot m) \cdot 0.$$

Ha $n \in \mathbb{N}$ olyan, amelyre teljesül az egyenlőség, akkor kihasználva azt, hogy a szorzás balról disztributív az összeadásra nézve, és felhasználva azt, hogy 1 a szorzás neutrális eleme, kapjuk, hogy

$$k \cdot (m \cdot n^+) = k \cdot ((m \cdot n) + m) = (k \cdot (m \cdot n)) + (k \cdot m) =$$
$$= ((k \cdot m) \cdot n) + ((k \cdot m) \cdot 1) = (k \cdot m) \cdot (n + 1) = (k \cdot m) \cdot n^+$$

tehát az állítás n^+-ra is igaz.

(IV) Igazoljuk azt, hogy a szorzás *jobbról* disztributív az összeadásra nézve. Ehhez legyen $k, m \in \mathbb{N}$ rögzített; teljes indukcióval megmutatjuk, hogy minden $n \in \mathbb{N}$ esetén $(k+m) \cdot n = (k \cdot n) + (m \cdot n)$. Ez igaz $n := 0$ esetén, mert

$$(k+m) \cdot 0 = 0 = 0 + 0 = (k \cdot 0) + (m \cdot 0).$$

Ha $n \in \mathbb{N}$ olyan, amelyre teljesül az egyenlőség, akkor az összeadás asszociativitását és kommutativitását, valamint a szorzás összeadásra vonatkozó baloldali disztributivitását alkalmazva kapjuk, hogy

$$\begin{aligned}(k+m) \cdot n^+ &= ((k+m) \cdot n) + (k+m) = ((k \cdot n) + (m \cdot n)) + (k+m) = \\ &= (k \cdot n) + ((m \cdot n) + (k+m)) = (k \cdot n) + (((m \cdot n) + k) + m) = \\ &= (k \cdot n) + ((k + (m \cdot n)) + m) = (k \cdot n) + (k + ((m \cdot n) + m)) = \\ &= (k \cdot n) + (k + (m \cdot n^+)) = ((k \cdot n) + k) + (m \cdot n^+) = (k \cdot n^+) + (m \cdot n^+),\end{aligned}$$

tehát az állítás n^+-ra is igaz.

(V) Teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén $0 \cdot n = 0$ teljesül. Ez $n := 0$ esetén nyilvánvalóan igaz. Ha $n \in \mathbb{N}$ és $0 \cdot n = 0$, akkor $0 \cdot n^+ = (0 \cdot n) + 0 = 0 \cdot n = 0$, tehát az állítás n^+-ra is igaz.

(VI) Végül bebizonyítjuk, hogy a szorzás kommutatív. Ehhez legyen $m \in \mathbb{N}$ rögzített; n szerinti teljes indukcióval igazoljuk, hogy $m \cdot n = n \cdot m$. Ez igaz $n = 0$ esetén, mert az (V) alapján $m \cdot 0 = 0 = 0 \cdot m$ teljesül. Ha $n \in \mathbb{N}$ olyan, hogy $m \cdot n = n \cdot m$, akkor kihasználva a szorzás összeadásra vonatkozó jobboldali disztributivitását kapjuk, hogy

$$m \cdot n^+ = (m \cdot n) + m = (n \cdot m) + m = (n \cdot m) + (1 \cdot m) = (n+1) \cdot m = n^+ \cdot m,$$

tehát az állítás n^+-ra is igaz. ■

7.7.6. Állítás.

a) *Ha* $m, n \in \mathbb{N}$, *és* $m \neq 0$ *vagy* $n \neq 0$, *akkor* $m + n \neq 0$.

b) *Ha* $m, n \in \mathbb{N}$ *és* $m \neq 0$ *és* $n \neq 0$, *akkor* $m \cdot n \neq 0$.

c) *Ha* $m, n \in \mathbb{N}$ *és* $m \cdot n = 1$, *akkor* $m = 1$ *és* $n = 1$.

Bizonyítás. a) Az összeadás kommutativitása miatt elég azt igazolni, hogy ha $m, n \in \mathbb{N}$ és $n \neq 0$, akkor $m + n \neq 0$. Ez viszont nyilvánvalóan igaz, mert ha $n \neq 0$, akkor 7.3.6. b) alapján van olyan $k \in \mathbb{N}$, hogy $n = k^+$, ezért az összeadás definíciója szerint $m + n = m + k^+ = (m+k)^+ \neq \emptyset =: 0$, hiszen $m + k \in (m+k)^+$.

b) A szorzás kommutativitása miatt elég azt igazolni, hogy ha $m \in \mathbb{N}$ és $m \neq 0$, akkor minden $n \in \mathbb{N}^*$ esetén $m \cdot n \neq 0$. Ez viszont nyilvánvalóan igaz, mert $n \in \mathbb{N}$ és $n \neq 0$ esetén 7.3.6. b) alapján van olyan $k \in \mathbb{N}$, hogy $n = k^+$, ezért a szorzás definíciója szerint $m \cdot n = m \cdot k^+ = m \cdot k + m \neq 0$, hiszen $m \neq 0$, így elég az a) állításra hivatkozni.

c) Legyenek $m, n \in \mathbb{N}$ olyanok, hogy $m \cdot n = 1$. Ekkor a szorzás értelmezése és a szorzás kommutativitása miatt $m \neq 0$ és $n \neq 0$, így 7.3.6. b) alapján léteznek olyan $j, k \in \mathbb{N}$ elemek, hogy $m = j^+$ és $n = k^+$. A szorzás és összeadás definícióját alkalmazva kapjuk, hogy

$$0^+ = 1 = m \cdot n = m \cdot k^+ = m \cdot k + m = m \cdot k + j^+ = (m \cdot k + j)^+,$$

így 7.3.6. a) alapján $0 = m \cdot k + j$. Az a) állításból következik, hogy $m \cdot k = 0$ és $j = 0$. A b) állításból kapjuk, hogy $m = 0$ vagy $k = 0$. De $m \neq 0$, tehát $k = 0$. Ez azt jelenti, hogy $m = j^+ = 0^+ = 1$ és $n = k^+ = 0^+ = 1$. ■

Az előző állítás a) és b) részét a következő ekvivalens formában is alkalmazzuk.

a′) Ha $m, n \in \mathbb{N}$ és $m + n = 0$, akkor $m = 0$ *és* $n = 0$.

b′) Ha $m, n \in \mathbb{N}$ és $m \cdot n = 0$, akkor $m = 0$ *vagy* $n = 0$.

7.7.7. Állítás.

a) *Az $\mathbb{N}$ feletti összeadásra nézve csak a 0-nak létezik inverze.*

b) *Az $\mathbb{N}$ feletti szorzásra nézve csak az 1-nek létezik inverze.*

Bizonyítás. a) Ha az $m \in \mathbb{N}$ elemnek létezik inverze az $\mathbb{N}$ feletti összeadásra nézve, akkor van olyan $n \in \mathbb{N}$, hogy $m + n = 0$, ezért a 7.7.6. a) állítás alapján $m = 0$.

b) Ha az $m \in \mathbb{N}$ elemnek létezik inverze az $\mathbb{N}$ feletti szorzásra nézve, akkor van olyan $n \in \mathbb{N}$, hogy $m \cdot n = 1$, ezért a 7.7.6. c) állítás alapján $m = 1$. ■

7.7.8. Definíció. (**Az $\mathbb{N}$ feletti hatványozás értelmezése**) *Minden $m \in \mathbb{N}$ esetén legyen w_m az 1 kezdőpont és az $\mathbb{N} \to \mathbb{N}$; $n \mapsto n \cdot m$ függvény által meghatározott iterációs sorozat; tehát $w_m : \mathbb{N} \to \mathbb{N}$ az a függvény, amelyre $w_m(0) = 1$ és minden $n \in \mathbb{N}$ esetén $w_m(n^+) = w_m(n) \cdot m$. Ekkor az*

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad ; \quad (m, n) \mapsto m^n := w_m(n)$$

függvényt $\mathbb{N}$ feletti **hatványozásnak** *nevezzük.*

Tehát az $\mathbb{N}$ feletti hatványozás olyan művelet, hogy minden $m, n \in \mathbb{N}$ számra

$$m^0 = 1;$$

$$m^{n+1} = m^n \cdot m.$$

A definíció szerint $0^0 = 1$, valamint minden $m \in \mathbb{N}$ esetén $m^1 = m^{0+1} = m^0 \cdot m = 1 \cdot m = m$. Teljes indukcióval könnyen igazolható, hogy minden $n \in \mathbb{N}$ esetén $1^n = 1$, hiszen $1^0 = 1$ a definíció szerint teljesül, és ha $1^n = 1$ igaz, akkor $1^{n+1} = 1^n \cdot 1 = 1^1 = 1$.

A hatványozás *jelölésével* kapcsolatban van bizonyos kétértelműség. A 6.2.13. definícióban az áll, hogy ha E és F halmazok, akkor F^E jelöli az $E \to F$ függvények halmazát. Tehát, ha $m, n \in \mathbb{N}$, akkor az m^n szimbólum jelölheti az $n \to m$ függvények halmazát és az m természetes szám imént értelmezett n-edik hatványát is. Ez a két objektum *nem egyenlő*: ebből származik a jelölés kétértelműsége. Ennek feloldásához megállapodunk abban, hogy ha E és F halmazok, akkor az $E \to F$ függvények halmazát csak akkor jelöljük az F^E szimbólummal, ha ez nem vezet félreértésre, tehát inkább az egyértelmű $\mathscr{F}(E; F)$ jelölést használjuk.

Azonban tudnunk kell, hogy $m, n \in \mathbb{N}$ esetén a $\mathscr{F}(n; m)$ függvényhalmaz és az $m^n \in \mathbb{N}$ hatvány között létezik egy kitüntetett bijekció: erről szól majd a 8.1.21. állítás, amely szerint $\mathscr{F}(n; m)$ olyan véges halmaz, amelynek a számossága pontosan egyenlő az $m^n \in \mathbb{N}$ hatvánnyal.

7.7.9. Állítás.

a) *Ha $m \in \mathbb{N}$ és $m \neq 0$, akkor minden $n \in \mathbb{N}$ esetén $m^n \neq 0$.*

b) *Ha $m \in \mathbb{N}$ és $m \neq 1$, akkor minden $n \in \mathbb{N}^*$ esetén $m^n \neq 1$.*

Bizonyítás. a) Rögzített $m \in \mathbb{N}$, $m \neq 0$ szám mellett, n szerinti teljes indukcióval bizonyítunk. A definíció szerint $m^0 = 1 \neq 0$, tehát az állítás igaz, ha $n = 0$. Ha $n \in \mathbb{N}$ olyan, hogy $m^n \neq 0$, akkor $m \neq 0$ és 7.7.6. b) alapján $0 \neq m^n \cdot m = m^{n+1}$, tehát az állítás $n + 1$-re is igaz.

b) Ha $n \in \mathbb{N}^*$, akor van olyan $k \in \mathbb{N}$, hogy $n = k^+ = k+1$, tehát a hatványozás definíciója szerint $m^n = m^k \cdot m$, amiből $m \neq 1$ esetén 7.7.6. c) alapján $m^n \neq 1$ következik. ■

7.7.10. Állítás. (**A hatványozás azonosságai**) *Minden $k, m, n \in \mathbb{N}$ esetén*

$$k^{m+n} = k^m \cdot k^n,$$
$$k^{m \cdot n} = (k^m)^n,$$
$$(m \cdot n)^k = m^k \cdot n^k.$$

Bizonyítás. Rögzített k és m természetes számok esetében, n-szerinti teljes indukcióval igazoljuk, hogy $k^{m+n} = k^m \cdot k^n$. Ez igaz akkor, ha $n = 0$, mert $k^{m+0} = k^m = k^m \cdot 1 = k^m \cdot k^0$. Ha $n \in \mathbb{N}$ olyan, hogy $k^{m+n} = k^m \cdot k^n$, akkor az összeadás és hatványozás definíciója, az indukciós hipotézis alapján, valamint a szorzás asszociativitása folytán

$$k^{m+(n+1)} = k^{(m+n)+1} = k^{m+n} \cdot k = (k^m \cdot k^n) \cdot k = k^m \cdot (k^n \cdot k) = k^m \cdot k^{n+1},$$

tehát az állítás az $n + 1$ számra is teljesül.

Rögzített k és m természetes számok esetében, n-szerinti teljes indukcióval igazoljuk, hogy $k^{m \cdot n} = (k^m)^n$. Ez igaz akkor, ha $n = 0$, mert $k^{m \cdot 0} = k^0 = 1 = (k^m)^0$. Ha $n \in \mathbb{N}$ olyan, hogy $k^{m \cdot n} = (k^m)^n$, akkor a szorzás és hatványozás definíciója, az imént bizonyított összefüggés, valamint az indukciós hipotézis szerint

$$k^{m \cdot (n+1)} = k^{m \cdot n + m} = k^{m \cdot n} \cdot k^m = (k^m)^n \cdot k^m = (k^m)^{n+1},$$

tehát az állítás az $n + 1$ számra is teljesül.

Rögzített m és n természetes számok esetében, k-szerinti teljes indukcióval igazoljuk, hogy $(m \cdot n)^k = m^k \cdot n^k$. Ez igaz akkor, ha $k = 0$, mert $(m \cdot n)^0 = 1 = 1 \cdot 1 = m^0 \cdot n^0$. Ha $k \in \mathbb{N}$ olyan, hogy $(m \cdot n)^k = m^k \cdot n^k$, akkor a hatványozás definíciója, az induktív hipotézis, valamint a szorzás asszociativitása és kommutativitása miatt

$$(m \cdot n)^{k+1} = (m \cdot n)^k \cdot (m \cdot n) = (m^k \cdot n^k) \cdot (m \cdot n) = (m^k \cdot m) \cdot (n^k \cdot n) = m^{k+1} \cdot n^{k+1},$$

tehát az állítás a $k + 1$ számra is teljesül. ■

7.8. A természetes számok természetes rendezése

7.8.1. Lemma. *Minden $n \in \mathbb{N}$ esetén a*

$$\leq_n := \{(j, k) \in n \times n | (j \in k) \vee (j = k)\}$$

reláció jólrendezés az n halmaz felett.

Bizonyítás. Legyen $n \in \mathbb{N}$. A 7.3.3. a) állítás szerint $(j, k) \in n \times n$ esetén $j \leq_n k$ ekvivalens azzal, hogy $j \subseteq k$, ezért a $\leq_n$ reláció nyilvánvalóan rendezés az n halmaz felett. Ez a rendezés 7.3.3. c) alapján trichotóm, tehát $\leq_n$ lineáris rendezés n felett.

Azt kell még igazolni, hogy minden $n \in \mathbb{N}$ esetén minden $H \subseteq n$ nem üres halmaznak létezik legkisebb eleme a $\leq_n$ rendezés szerint. Ehhez jelölje E azon $n \in \mathbb{N}$ számok halmazát, amelyekre $\leq_n$ jólrendezés. Világos, hogy $0 \in E$, mert 0-nak nincs nem üres részhalmaza. Tegyük fel, hogy $n \in E$, és legyen $H \subseteq n^+$ nem üres halmaz; megmutatjuk, hogy H-nak létezik legkisebb eleme a $\leq_{n^+}$ rendezés szerint, ami azt jelenti, hogy $n^+ \in E$. Ha $H \cap n = \emptyset$, akkor $H \subseteq n^+$ és $H \neq \emptyset$ miatt $H = \{n\}$, így H-nak n a legkisebb eleme a $\leq_{n^+}$ rendezés szerint. Ezért feltehető, hogy $H \cap n \neq \emptyset$, tehát $H \cap n$ nem üres részhalmaza n-nek. Ekkor $n \in E$ miatt létezik $H \cap n$-nek legkisebb eleme a $\leq_n$ reláció szerint; legyen ez k. Ha k nem volna a H legkisebb eleme $\leq_{n^+}$ rendezés szerint, akkor létezne olyan $j \in n^+$, amelyre $j <_{n^+} k$ teljesülne. Ekkor $j \in k \in n$ miatt $j \in H \cap n$ és $j <_n k$, ami ellentmond annak, hogy k a $H \cap n$ legkisebb eleme $\leq_n$ szerint. Ezzel beláttuk, hogy $n \in E$ esetén $n^+ \in E$, így a teljes indukció elve alapján $E = \mathbb{N}$, vagyis minden $n \in \mathbb{N}$ elemre a $\leq_n$ reláció jólrendezés. ■

7.8.2. Tétel. (**A teljes indukció alternatívája**.) *Legyen E olyan halmaz, hogy minden $n \in \mathbb{N}$ esetén: ha $n \subseteq E$, akkor $n \in E$. Ekkor $\mathbb{N} \subseteq E$.*

Bizonyítás. Azt kell igazolni, hogy $\mathbb{N} \setminus E = \emptyset$. Ezt indirekt bizonyítjuk, tehát feltesszük, hogy $\mathbb{N} \setminus E \neq \emptyset$: legyen $n \in \mathbb{N} \setminus E$ rögzített elem. Ekkor $n \notin E$, tehát az E halmazra vonatkozó hipotézis alapján $n \not\subseteq E$, vagyis $n \setminus E$ nem üres részhalmaza n-nek. A $\leq_n$ reláció jólrendezés n felett, így vehetjük az $n \setminus E$ halmaz $\leq_n$ rendezés szerinti legkisebb elemét: legyen ez n_*. Ha $x \in n_*$, akkor $x \in n$, mert $n_* \in n$ és n tranzitivitása folytán $n_* \subseteq n$. Tehát minden $x \in n_*$ esetén $x <_n n_*$, így az n_* szám minimalitásából következik, hogy $x \in E$. Ez azt jelenti, hogy $n_* \subseteq E$, így az E halmazra vonatkozó hipotézis alapján $n_* \in E$, ami ellentmond annak, hogy $n_* \notin E$. ■

7.8.3. Tétel. *Az $\{(m,n) \in \mathbb{N} \times \mathbb{N} | (m \in n) \vee (m = n)\}$ reláció jólrendezés az $\mathbb{N}$ halmaz felett.*

Bizonyítás. Jelölje $\leq$ ezt a relációt, és minden $n \in \mathbb{N}$ esetén legyen $\leq_n$ a $\leq$ reláció megszorítása az $n \subseteq \mathbb{N}$ halmazra ($\mathbb{N}$ tranzitív halmaz!).

Először megjegyezzük, hogy az előzőek alapján a $\leq$ reláció egyenlő az $\subseteq$ relációval $\mathbb{N}$ felett, és minden $n \in \mathbb{N}$ esetén a $\leq_n$ reláció egyenlő a tartalmazás relációval az n halmaz felett. Ebből azonnal következik, hogy ezek a relációk *rendezések*, sőt *lineáris* rendezések, hiszen láttuk, hogy bármely két $j, k \in \mathbb{N}$ esetén $(j \subseteq k) \vee (k \subseteq j)$ teljesül.

Most megmutatjuk, hogy minden $n \in \mathbb{N}$ elemre a $\leq_n$ reláció jólrendezés, vagyis minden $H \subseteq n$ nem üres halmaznak létezik legkisebb eleme a $\leq_n$ rendezés szerint. Ehhez jelölje E azon $n \in \mathbb{N}$ számok halmazát, amelyekre $\leq_n$ jólrendezés. Világos, hogy $0 \in E$, mert 0-nak nincs nem üres részhalmaza. Tegyük fel, hogy $n \in E$, és legyen $H \subseteq n^+$ nem üres halmaz; megmutatjuk, hogy H-nak létezik legkisebb eleme a $\leq_{n^+}$ rendezés szerint, ami azt jelenti, hogy $n^+ \in E$. Ha $H \cap n = \emptyset$, akkor $H \subseteq n^+$ és $H \neq \emptyset$ miatt $H = \{n\}$, így H-nak n a legkisebb eleme a $\leq_{n^+}$ rendezés szerint. Ezért feltehető, hogy $H \cap n \neq \emptyset$, tehát $H \cap n$ nem üres részhalmaza n-nek. Ekkor $n \in E$ miatt létezik $H \cap n$-nek legkisebb eleme a $\leq_n$ reláció szerint; legyen ez k. Ha k nem volna a H legkisebb eleme $\leq_{n^+}$ rendezés szerint, akkor létezne olyan $j \in n^+$, amelyre $j <_{n^+} k$ teljesülne. Ekkor $j \in k \in n$ miatt $j \in H \cap n$ és $j <_n k$, ami ellentmond annak, hogy k a $H \cap n$ legkisebb eleme $\leq_n$ szerint. Ezzel beláttuk, hogy $n \in E$ esetén $n^+ \in E$, így a teljes indukció elve alapján $E = \mathbb{N}$, vagyis minden $n \in \mathbb{N}$ elemre a $\leq_n$ reláció jólrendezés.

Legyen most $H \subseteq \mathbb{N}$ tetszőleges nem üres halmaz, és legyen $m \in H$ rögzítve. Jelöljön n egy tetszőleges természetes számot, amelyre $m < n$ teljesül; például $n := m^+$ megfelelő, de nem szükséges ezt választani. Ekkor $m \in H \cap n$, vagyis $H \cap n$ nem üres részhalmaza

n-nek. A $\leq_n$ reláció jólrendezés, tehát $H \cap n$-nek létezik legkisebb eleme a $\leq_n$ rendezés szerint; legyen ez k. Ha k nem volna a H legkisebb eleme a $\leq$ rendezés szerint, akkor létezne olyan $j \in H$, amelyre $j < k$ teljesülne. Ekkor $j \in k \in n$ miatt $j \in H \cap n$ és $j <_n k$, ami ellentmond annak, hogy k a $H \cap n$ legkisebb eleme $\leq_n$ szerint. Ezért $\leq$ jólrendezés az $\mathbb{N}$ halmaz felett. ■

7.8.4. Definíció. *Az $\mathbb{N}$ halmaz feletti* **természetes rendezésnek** *nevezzük a*

$$\{(m, n) \in \mathbb{N} \times \mathbb{N} | (m \in n) \vee (m = n)\}$$

jólrendezést, és ezt a $\leq$ vagy $\leq_{\mathbb{N}}$ szimbólummal jelöljük.

Fontos az, hogy az előzőek szerint $m, n \in \mathbb{N}$ esetén:

$$m \leq n \Leftrightarrow m \subseteq n \Leftrightarrow (m \in n) \vee (m = n) \Leftrightarrow n \notin m.$$

Továbbá, ha $m, n \in \mathbb{N}$, akkor

$$m < n \Leftrightarrow (m \subseteq n) \wedge (m \neq n) \Leftrightarrow m \in n.$$

Ezeket az összefüggéseket a továbbiakban gyakran alkalmazzuk, külön hivatkozás nélkül.

7.8.5. Definíció. *Az $\mathbb{N} \to \mathbb{N}$ szigorúan monoton növő függvényeket* **indexsorozatoknak** *nevezzük. Az* $\mathbf{s}$ *sorozat* **részsorozatának** *nevezünk minden* $\mathbf{s} \circ \sigma$ *alakú függvényt, ahol $\sigma : \mathbb{N} \to \mathbb{N}$ szigorúan monoton növő függvény (vagyis σ indexsorozat). Az* $\mathbf{s}$ *sorozat* **átrendezésének** *nevezünk minden* $\mathbf{s} \circ \sigma$ *alakú függvényt, ahol $\sigma : \mathbb{N} \to \mathbb{N}$ bijekció.*

7.8.6. Állítás. *Ha $\sigma : \mathbb{N} \to \mathbb{N}$ szigorúan monoton növő függvény, akkor minden $n \in \mathbb{N}$ elemre $n \leq \sigma(n)$.*

Bizonyítás. Ha $E := \{n \in \mathbb{N} | n \leq \sigma(n)\}$, akkor nyilvánvalóan $0 \in E$, és ha $n \in E$, akkor $n < n^+$ és a σ szigorú monoton növése miatt $n \leq \sigma(n) < \sigma(n^+)$, ezért $n^+ \leq \sigma(n^+)$, vagyis $n^+ \in E$, így a teljes indukció elve alapján $E = \mathbb{N}$. ■

7.8.7. Állítás. *Ha $(E, \leq)$ rendezett halmaz, akkor az E halmazban haladó* $\mathbf{s}$ *sorozat pontosan akkor monoton növő (illetve fogyó), ha minden $n \in \mathbb{N}$ esetén $\mathbf{s}(n) \leq \mathbf{s}(n+1)$ (illetve $\mathbf{s}(n+1) \leq \mathbf{s}(n)$).*

Bizonyítás. Ha az $\mathbf{s}$ sorozat monoton növő (illetve fogyó), akkor minden $m, n \in \mathbb{N}$ esetén, ha $n \leq m$, akkor $\mathbf{s}(n) \leq \mathbf{s}(m)$ (illetve $\mathbf{s}(m) \leq \mathbf{s}(n)$), ezért $\mathbf{s}(n) \leq \mathbf{s}(n+1)$ (illetve $\mathbf{s}(n+1) \leq \mathbf{s}(n)$).

Megfordítva, tegyük fel, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{s}(n) \leq \mathbf{s}(n+1)$ (illetve $\mathbf{s}(n+1) \leq \mathbf{s}(n)$). Az $n \in \mathbb{N}$ rögzített természetes számtól indított teljes indukcióval igazoljuk, hogy minden $m \geq n$ természetes számra $\mathbf{s}(n) \leq \mathbf{s}(m)$ (illetve $\mathbf{s}(m) \leq \mathbf{s}(n)$).

Ha $m = n$, akkor a $\leq$ reláció E feletti reflexivitása miatt $\mathbf{s}(n) \leq \mathbf{s}(m)$ (illetve $\mathbf{s}(m) \leq \mathbf{s}(n)$). Ha $n \leq m$ és $\mathbf{s}(n) \leq \mathbf{s}(m)$ (illetve $\mathbf{s}(m) \leq \mathbf{s}(n)$), akkor a hipotézis szerint $\mathbf{s}(m) \leq \mathbf{s}(m+1)$ (illetve $\mathbf{s}(m+1) \leq \mathbf{s}(m)$), így az E feletti $\leq$ reláció tranzitivitása miatt $\mathbf{s}(n) \leq \mathbf{s}(m+1)$ (illetve $\mathbf{s}(m+1) \leq \mathbf{s}(n)$). Ezért minden $m \geq n$ természetes számra $\mathbf{s}(n) \leq \mathbf{s}(m)$ (illetve $\mathbf{s}(m) \leq \mathbf{s}(n)$). ■

7.8.8. Definíció. *Az* $\mathbf{s}$ *sorozatot* **stacionáriusnak** *nevezzük, ha létezik olyan $n \in \mathbb{N}$, hogy minden $k \in \mathbb{N}$ számra, $k > n$ esetén $\mathbf{s}(k) = \mathbf{s}(n)$. Ha* $\mathbf{s}$ *stacionárius sorozat, akkor az $\mathbb{N}$ halmaz jólrendezettsége miatt egyértelműen létezik olyan legkisebb $n \in \mathbb{N}$, hogy minden $k \in \mathbb{N}$ számra, $k > n$ esetén $\mathbf{s}(k) = \mathbf{s}(n)$; ekkor az $\mathbf{s}(n)$ elemet az* $\mathbf{s}$ *sorozat* **stacionárius értékének** *nevezzük.*

7.9. A műveletek kapcsolata a rendezéssel

7.9.1. Állítás. *Minden $m, n \in \mathbb{N}$ számra az $m \leq n$ és $m^+ \leq n^+$ kijelentések ekvivalensek.*

Bizonyítás. Legyenek $m, n \in \mathbb{N}$ olyanok, hogy $m \leq n$, vagyis $m \subseteq n$. Ekkor $n \subseteq n^+$ miatt $m \subseteq n^+$ teljesül. Továbbá, ha $m = n$, akkor $n \in n^+$ miatt $m \in n^+$. Ha pedig $m \in n$, akkor ismét $n \subseteq n^+$ alapján $m \in n^+$. Tehát $m \in n^+$ is igaz, így $m^+ = m \cup \{m\} \subseteq n^+$ is teljesül, vagyis $m^+ \leq n^+$.

Megfordítva, ha $m^+ \leq n^+$, akkor $m \in m^+ \subseteq n^+$, tehát $m \in n$ vagy $m = n$, vagyis $m \leq n$. ■

A természetes számok halmazán adott természetes rendezés tulajdonságait gyakran alkalmazzuk a műveletekkel kapcsolatos állítások bizonyításában. Erre ad példát a következő állítás.

7.9.2. Állítás. (**Az $\mathbb{N}$ feletti rendezés kapcsolata az összeadással**) *Ha $m, n \in \mathbb{N}$, akkor a következő állítások ekvivalensek.*

(i) $m \leq n$.

(ii) *Minden $k \in \mathbb{N}$ esetén $m + k \leq n + k$.*

(iii) *Létezik olyan $k \in \mathbb{N}$, hogy $m + k \leq n + k$.*

Bizonyítás. (i)⇒(ii) Rögzített $m, n \in \mathbb{N}$, $m \leq n$ számokra, k-szerinti teljes indukcióval igazoljuk, hogy minden $k \in \mathbb{N}$ esetén $m + k \leq n + k$. Ha $k = 0$, akkor $m + k = m + 0 = m \leq n = n + 0 = n + k$, tehát az állítás igaz. Ha $k \in \mathbb{N}$ olyan, hogy $m + k \leq n + k$, akkor az összeadás iteratív definíciója és az előző állítás alapján $m + k^+ = (m + k)^+ \leq (n + k)^+ = n + k^+$. Ezzel megmutattuk, hogy minden $m, n, k \in \mathbb{N}$ esetén, ha $m \leq n$, akkor $m + k \leq n + k$.

(ii)⇒(iii) Triviális.

(iii)⇒(i) A hipotézis szerint az $E := \{k \in \mathbb{N} \mid m + k \leq n + k\}$ halmaz nem üres, és ha $k \in \mathbb{N}$ olyan, hogy $k^+ \in E$, akkor $(m + k)^+ = m + k^+ \leq n + k^+ = (m + k)^+$, így 7.9.1. szerint $m + k \leq n + k$, vagyis $k \in E$. Ezért a végtelen leszállás tétele (7.2.2.) alapján $0 \in E$, ami azt jelenti, hogy $m + 0 \leq n + 0 = n$. ■

7.9.3. Következmény. (**Az egyenlőtlenségek összedásának szabálya**) *Ha $m, n \in \mathbb{N}$ és $m', n' \in \mathbb{N}$ olyan számok, amelyekre $m \leq n$ és $m' \leq n'$, akkor $m + m' \leq n + n'$.*

Bizonyítás. A 7.9.2. állítás és az $\mathbb{N}$ feletti összeadás kommutativitása szerint

$$m + m' \leq n + m' = m' + n \leq n' + n = n + n'. \blacksquare$$

7.9.4. Állítás. *Minden $m, n \in \mathbb{N}$ esetén a következő állítások ekvivalensek.*

(i) $m \leq n$.

(ii) *Létezik egyetlen olyan $k \in \mathbb{N}$, hogy $m + k = n$.*

(iii) *Létezik olyan $k \in \mathbb{N}$, hogy $m + k = n$.*

Bizonyítás. (i)⇒(ii) A összeadás kancellativitása (7.7.3.) miatt a $k \in \mathbb{N}$ szám egyértelműsége nyilvánvaló, hiszen ha $k, k' \in \mathbb{N}$ olyanok, hogy $m + k = n = m + k'$, akkor $k = k'$.

Legyen $m \in \mathbb{N}$ rögzítve. Ekkor m-től indított teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén, ha $m \leq n$, akkor létezik olyan $k \in \mathbb{N}$, hogy $m + k = n$.

Az állítás igaz, ha $n = m$, hiszen ekkor $k := 0 \in \mathbb{N}$ olyan, hogy $m + k = m + 0 = m = n$. Ha $n \in \mathbb{N}$, $m \leq n$ és $k \in \mathbb{N}$ olyan, hogy $m + k = n$, akkor az összeadás értelmezése alapján $m + k^+ = (m + k)^+ = n^+$, vagyis n^+-hoz a $k^+ \in \mathbb{N}$ szám olyan lesz, amelyre $m + k^+ = n^+$.

(ii)⇒(iii) Triviális.

(iii)⇒(i) Rögzített $m \in \mathbb{N}$ esetén, teljes indukcióval igazoljuk, hogy minden $k \in \mathbb{N}$ számra $m \leq m+k$. (Ebből nyilvánvalóan kapjuk, hogy (iii)⇒(i) igaz.) Valóban, ha $k = 0$, akkor $m = m + k$, tehát $m \leq m + k$. Ha $k \in \mathbb{N}$ olyan, hogy $m \leq m + k$, akkor az összeadás definíciója alapján $m \leq m + k \leq (m + k)^+ = m + k^+$, tehát $m \leq m + k^+$. ■

7.9.5. Állítás. (**Az $\mathbb{N}$ feletti rendezés kapcsolata a szorzással**) *Ha $m, n \in \mathbb{N}$, akkor a következő állítások ekvivalensek.*

(i) $m \leq n$.

(ii) *Minden $k \in \mathbb{N}$ esetén $m \cdot k \leq n \cdot k$.*

(iii) *Létezik olyan $k \in \mathbb{N}^*$, hogy $m \cdot k \leq n \cdot k$.*

Bizonyítás. (i)⇒(ii) Rögzített $m, n \in \mathbb{N}$, $m \leq n$ számokra, k-szerinti teljes indukcióval igazoljuk, hogy minden $k \in \mathbb{N}$ esetén $m \cdot k \leq n \cdot k$. Ha $k = 0$, akkor $m \cdot k = m \cdot 0 = 0 = n \cdot 0 = n \cdot k$, tehát az állítás igaz. Ha $k \in \mathbb{N}$ olyan, hogy $m \cdot k \leq n \cdot k$, akkor a szorzás definícióját és a 7.9.2. állítást kétszer alkalmazva kapjuk, hogy $m \cdot k^+ = m \cdot k + m \leq n \cdot k + m \leq n \cdot k + n = n \cdot k^+$, tehát az állítás igaz k^+-ra. (Itt a 7.9.2. állítást először úgy alkalmaztuk, hogy $m \cdot k \leq n \cdot k$ miatt $m \cdot k + m \leq n \cdot k + m$, majd úgy, hogy $m \leq n$ miatt $n \cdot k + m \leq n \cdot k + n$.)

(ii)⇒(iii) triviális.

(iii)⇒(i) A hipotézis szerint a $\{k \in \mathbb{N}^* \mid m \cdot k \leq n \cdot k\}$ halmaz nem üres, ezért létezik ennek legkisebb eleme az $\mathbb{N}$ feletti természetes rendezés szerint: jelölje ezt k_*. Ha $k_* = 1$, akkor $m = m \cdot 1 \leq n \cdot 1 = n$, ezért elég azt igazolni, hogy $k_* \neq 1$ lehetetlen.

Indirekt, tegyük fel, hogy $k_* \neq 1$. A definíció szerint $k_* \neq 0$, így 7.3.6. b) alapján van olyan $j \in \mathbb{N}$, hogy $k_* = j^+$, és ekkor $j \neq 0$, mivel $k_* \neq 1$. Ez azt jelenti, hogy $j < k_*$ és $j \in \mathbb{N}^*$, tehát k_* minimalitási tulajdonsága folytán $j \notin \{k \in \mathbb{N}^* \mid m \cdot k \leq n \cdot k\}$, vagyis $m \cdot j \not\leq n \cdot j$, azaz $n \cdot j < m \cdot j$.

A 7.9.4. állítás szerint vehetünk olyan $k \in \mathbb{N}$ számot, hogy $n \cdot j + k = m \cdot j$, és természetesen $k \neq 0$. Ehhez az egyenlőséghez hozzáadva n-t, és kihasználva az $\mathbb{N}$ feletti összeadás asszociativitását és kommutativitását kapjuk, hogy $n \cdot j + n + k = m \cdot j + n$, tehát $k_* = j^+$ és az $\mathbb{N}$ feletti szorzás definíciója, $m \cdot k_* \leq n \cdot k_*$, valamint 7.9.2. alapján

$$m \cdot k_* + k \leq n \cdot k_* + k = n \cdot j^+ + k = n \cdot j + n + k = m \cdot j + n.$$

Ugyanakkor, $k_* = j^+$ és az $\mathbb{N}$ feletti szorzás definíciója szerint

$$m \cdot k_* + k = m \cdot j^+ + k = m \cdot j + m + k,$$

tehát azt kapjuk, hogy $m \cdot j + m + k \leq m \cdot j + n$. Ebből 7.9.2. alkalmazásával nyerjük, hogy $m + k \leq n$. Ebből a 7.9.4. állítás alapján $m \leq n$ adódik, így az (igazolt) (i)⇒(ii) következtetés szerint $m \cdot j \leq n \cdot j$, ami ellentmond annak, hogy $n \cdot j < m \cdot j$. ■

7.9.6. Következmény. (**Az egyenlőtlenségek szorzásának szabálya**) *Ha $m, n \in \mathbb{N}$ és $m', n' \in \mathbb{N}$ olyan számok, amelyekre $m \leq n$ és $m' \leq n'$, akkor $m \cdot m' \leq n \cdot n'$.*

Bizonyítás. A 7.9.5. állítás és az $\mathbb{N}$ feletti szorzás kommutativitása szerint $m \cdot m' \leq n \cdot m' = m' \cdot n \leq m' \cdot n' = n' \cdot m'$. ■

7.9.7. Definíció. *Ha $m, n \in \mathbb{N}$ és $m \leq n$, akkor $n \dot{-} m$ jelöli azt a természetes számot, amelyre $m + (n \dot{-} m) = n$, és az $n \dot{-} m \in \mathbb{N}$ elemet az n és m természetes számok* **különbségének** *nevezzük.*

7.9.8. Állítás. (**Az $\mathbb{N}$ feletti szorzás kancellativitása**) *Ha $m, n \in \mathbb{N}$, akkor a következő állítások ekvivalensek.*

(i) $m = n$.

(ii) *Minden $k \in \mathbb{N}$ esetén $m \cdot k = n \cdot k$.*

(iii) *Létezik olyan $k \in \mathbb{N}^*$, hogy $m \cdot k = n \cdot k$.*

Bizonyítás. (i)⇒(ii) és (ii)⇒(iii) triviális.

(iii)⇒(i) Ha $k \in \mathbb{N}^*$ olyan, hogy $m \cdot k = n \cdot k$, akkor $m \cdot k \leq n \cdot k$ és $n \cdot k \leq m \cdot k$, ezért 7.9.5. alapján $m \leq n$ és $n \leq m$, tehát $m = n$. ■

7.9.9. Állítás. (**Az $\mathbb{N}$ feletti rendezés kapcsolata a hatványozással**) *Ha $m, n \in \mathbb{N}$, akkor a következő állítások ekvivalensek.*

(i) $m \leq n$.

(ii) *Minden $k \in \mathbb{N}$ esetén $m^k \leq n^k$.*

(iii) *Létezik olyan $k \in \mathbb{N}^*$, hogy $m^k \leq n^k$.*

Bizonyítás. (i)⇒(ii) Rögzített $m, n \in \mathbb{N}$, $m \leq n$ számokra, k-szerinti teljes indukcióval igazoljuk, hogy minden $k \in \mathbb{N}$ esetén $m^k \leq n^k$. Ha $k = 0$, akkor $m^k = m^0 = 1 = n^0 = n^k$, tehát az állítás igaz. Ha $k \in \mathbb{N}$ olyan, hogy $m^k \leq n^k$, akkor a hatványozás definícióját és a 7.9.5. állítást kétszer alkalmazva kapjuk, hogy $m^{k^+} = m^k \cdot m \leq n^k \cdot m \leq n^k \cdot n = n^{k^+}$, tehát az állítás igaz k^+-ra. (Itt a 7.9.5. állítást először úgy alkalmaztuk, hogy $m^k \leq n^k$ miatt $m^k \cdot m \leq n^k \cdot m$, majd úgy, hogy $m \leq n$ miatt $n^k \cdot m \leq n^k \cdot n$.)

(ii)⇒(iii) triviális.

(iii)⇒(i) A hipotézis szerint a $\{k \in \mathbb{N}^* \mid m^k \leq n^k\}$ halmaz nem üres, ezért létezik ennek legkisebb eleme az $\mathbb{N}$ feletti természetes rendezés szerint: jelölje ezt k_*. Ha $k_* = 1$, akkor $m = m^1 \leq n^1 = n$, ezért elég azt igazolni, hogy $k_* \neq 1$ lehetetlen.

Indirekt, tegyük fel, hogy $k_* \neq 1$. A definíció szerint $k_* \neq 0$, így 7.3.6. b) alapján van olyan $j \in \mathbb{N}$, hogy $k_* = j^+$, és ekkor $j \neq 0$, mivel $k_* \neq 1$. Ez azt jelenti, hogy $j < k_*$ és $j \in \mathbb{N}^*$, tehát k_* minimalitási tulajdonsága folytán $j \notin \{k \in \mathbb{N}^* \mid m^k \leq n^k\}$, vagyis $m^j \not\leq n^j$, azaz $n^j < m^j$.

Ekkor $n^j \leq m^j$ és $m^{k_*} \leq n^{k_*}$, így kétszer alkalmazva a 7.9.5. állítást és a hatványozás definícióját kapjuk, hogy

$$n^j \cdot m \leq m^j \cdot m = m^{j^+} = m^{k_*} \leq n^{k_*} = n^{j^+} = n^j \cdot n,$$

amiből ismét 7.9.5. alapján $m \leq n$ következik, hiszen $n^j \in \mathbb{N}^*$. Ezért az (igazolt) (i)⇒(ii) következtetés szerint $m^j \leq n^j$, ami ellentmond annak, hogy $n^j < m^j$. ■

7.9.10. Következmény. (**A egyenlőtlenségek hatványozásának szabálya**) *Ha $m, n \in \mathbb{N}$ és $p, q \in \mathbb{N}$ olyan számok, amelyekre $m \leq n$ és $p \leq q$, akkor $m^p \leq n^q$.*

Bizonyítás. Az $p \leq q$ feltétel és 7.9.4. alapján vehetünk olyan $k \in \mathbb{N}$ számot, amelyre $p + k = q$. Világos, hogy $1 \leq n^k$, így 7.9.5. és a hatványozás azonosságai miatt $n^p = n^p \cdot 1 \leq n^p \cdot n^k = n^{p+k} = n^q$, tehát az $m \leq n$ egyenlőtlenségből 7.9.9. alkalmazásával kapjuk, hogy $m^p \leq n^p \leq n^q$. ■

7.9.11. Állítás. (**Az $\mathbb{N}$ feletti hatványozás kancellativitása**) *Ha $m, n \in \mathbb{N}$, akkor a következő állítások ekvivalensek.*

(i) $m = n$.

(ii) *Minden $k \in \mathbb{N}$ esetén $m^k = n^k$.*

(iii) *Létezik olyan $k \in \mathbb{N}^*$, hogy $m^k = n^k$.*

Bizonyítás. (i)⇒(ii) és (ii)⇒(iii) triviális.

(iii)⇒(i) Ha $k \in \mathbb{N}^*$ olyan, hogy $m^k = n^k$, akkor $m^k \leq n^k$ és $n^k \leq m^k$ miatt, 7.9.9. alapján $m \leq n$ és $n \leq m$, tehát $m = n$. ■

7.10. Műveletekkel kapcsolatos szigorú egyenlőtlenségek

7.10.1. Lemma. *Minden $m, n \in \mathbb{N}$ számra az $m < n$ és $m^+ < n^+$ kijelentések ekvivalensek.*

Bizonyítás. Tegyük fel, hogy $m < n$. Ekkor $m \leq n$, tehát 7.9.1. alapján $m^+ \leq n^+$, ugyanakkor 7.3.6. szerint az $m^+ = n^+$ egyenlőségből $m = n$ következne, holott $m \neq n$. Ezért $m < n$ esetén $m^+ < n^+$.

Megfordítva, ha $m^+ < n^+$, akkor $m^+ \leq n^+$, tehát ismét 7.9.1. alapján $m \leq n$, és természetesen $m \neq n$, így $m < n$. ■

7.10.2. Állítás. *Ha $m, n \in \mathbb{N}$ és $m < n$, akkor minden $k \in \mathbb{N}$ esetén $m + k < n + k$, és ha $k \neq 0$, akkor $m \cdot k < n \cdot k$.*

Bizonyítás. Ha $m, n \in \mathbb{N}$ és $m < n$, akkor $m \leq n$, tehát 7.9.2. alapján $m + k \leq n + k$, és az összeadás kancellativitása (7.7.3.) és $m \neq n$ miatt $m + k = n + k$ lehetetlen, tehát $m + k < n + k$.

Ha $m, n \in \mathbb{N}$ és $m < n$, akkor $m \leq n$, tehát 7.9.5. alapján minden $k \in \mathbb{N}$ esetén $m \cdot k \leq n \cdot k$, és a szorzás kancellativitása (7.9.8.) miatt $k \neq 0$ esetén $m \cdot k = n \cdot k$ lehetetlen, mert ebből $m = n$ következne. ■

7.10.3. Állítás. *Ha $m, n \in \mathbb{N}$ és $k \in \mathbb{N}$ olyanok, hogy $m + k < n + k$, akkor $m < n$.*

Bizonyítás. Valóban, ha $n \leq m$ teljesülne, akkor 7.9.2. alapján $n + k \leq m + k$ is igaz volna. ■

7.11. Oszthatóság és prímszámok

7.11.1. Definíció. *Ha $m, n \in \mathbb{N}$, akkor azt mondjuk, hogy m* **osztója** *n-nek, vagy n* **többszöröse** *m-nek, vagy n* **osztható** *m-mel, ha létezik olyan $q \in \mathbb{N}$, hogy $m \cdot q = n$,* *és ezt a kijelentést az $m \mid n$ szimbólummal jelöljük. A $\neg(m \mid n)$ kijelentést az $m \nmid n$ szimbólummal rövidítjük. Az*

$$\{ (m,n) \in \mathbb{N} \times \mathbb{N} \mid m \mid n \}$$

halmazt $\mathbb{N}$ feletti **oszthatóság-relációnak** *nevezzük.*

7.11.2. Állítás. *Ha $m, n \in \mathbb{N}$, és m osztója n-nek, és $m \neq 0$, akkor egyértelműen létezik olyan $q \in \mathbb{N}$, hogy $m \cdot q = n$.*

Bizonyítás. Ha $q, q' \in \mathbb{N}$ olyanok, hogy $m \cdot q = n = m \cdot q'$, akkor az $\mathbb{N}$ feletti szorzás kancellativitása (7.9.8.) és $m \neq 0$ miatt $q = q'$. ■

7.11.3. Definíció. *Ha $m, n \in \mathbb{N}$, és m osztója n-nek, és $m \neq 0$, akkor $\frac{n}{m}$ jelöli azt a természetes számot, amelyre $m \cdot \left(\frac{n}{m}\right) = n$, teljesül, és ezt az $\frac{n}{m} \in \mathbb{N}$ elemet az n és m természetes számok* **hányadosának** *nevezzük.*

7.11.4. Állítás. *Legyenek $m, n, k \in \mathbb{N}$.*

a) *Ha k osztója m-nek is és n-nek is, akkor k osztója $m + n$-nek, és $k \neq 0$ esetén*

$$\frac{m}{k} + \frac{n}{k} = \frac{m+n}{k}.$$

b) *Ha k osztója n-nek, akkor $k \cdot m$ osztója $n \cdot m$-nek, és $k \neq 0 \neq m$ esetén*

$$\frac{n \cdot m}{k \cdot m} = \frac{n}{k}.$$

Bizonyítás. a) Legyenek $p, q \in \mathbb{N}$ olyanok, hogy $k \cdot p = m$ és $k \cdot q = n$. Ekkor az $\mathbb{N}$ feletti szorzás $\mathbb{N}$ feletti összeadásra vonatkozó disztributivitása folytán $k \cdot (p + q) = (k \cdot p) + (k \cdot q) = m + n$, tehát k osztója $m + n$-nek, és látható, hogy ha $k \neq 0$, akkor

$$\frac{m}{k} + \frac{n}{k} = p + q = \frac{m+n}{k}.$$

b) Ha $p \in \mathbb{N}$ olyan, hogy $k \cdot p = n$, akkor az $\mathbb{N}$ feletti szorzás kommutativitása és asszociativitása miatt $(k \cdot m) \cdot p = (k \cdot p) \cdot m = n \cdot m$, tehát $k \cdot m$ osztója $n \cdot m$-nek, és látható, hogy $k \neq 0 \neq m$ esetén

$$\frac{n \cdot m}{k \cdot m} = p = \frac{n}{k}. \blacksquare$$

7.11.5. Állítás. *Az $\mathbb{N}$ feletti oszthatóság-reláció rendezés $\mathbb{N}$ felett.*

Bizonyítás. Minden $n \in \mathbb{N}$ esetén $n \cdot 1 = n$, ezért $n \mid n$, vagyis az $\mathbb{N}$ feletti oszthatóság-reláció reflexív $\mathbb{N}$ felett.

Legyenek $m, n \in \mathbb{N}$ olyanok, hogy $m \mid n$ és $n \mid m$. Vegyünk olyan $q, q' \in \mathbb{N}$ számokat, amelyekre $m \cdot q = n$ és $n \cdot q' = m$. Ha $m = 0$, akkor $n = 0 \cdot q = 0$, tehát $m = n$. Ha $m \neq 0$, akkor $m \cdot (q \cdot q') = m = m \cdot 1$ és a szorzás kancellativitása (7.9.8.) alapján $q \cdot q' = 1$. Ebből 7.7.6. c) alkalmazásával $q = 1$ adódik, tehát $m = n$. Ez azt jelenti, hogy az $\mathbb{N}$ feletti oszthatóság-reláció antiszimmetrikus.

Legyenek $m, n, k \in \mathbb{N}$ olyanok, hogy $m \mid n$ és $n \mid k$. Vegyünk olyan $q, q' \in \mathbb{N}$ számokat, amelyekre $m \cdot q = n$ és $n \cdot q' = k$. Ekkor $m \cdot (q \cdot q') = k$, tehát $m \mid k$. Ez azt jelenti, hogy az $\mathbb{N}$ feletti oszthatóság-reláció tranzitív. ■

Könnyen látható, hogy az $\mathbb{N}$ feletti oszthatóság-reláció *nem lineáris* rendezés, vagyis léteznek olyan $m, n \in \mathbb{N}$ számok, hogy az $m \mid n$ és $n \mid m$ állítások közül egyik sem teljesül. Az is nyilvánvaló, hogy minden $n \in \mathbb{N}$ esetén $1 \mid n$ és $n \mid n$, vagyis minden természetes számnak osztója 1 és önmaga. Különösen érdekesek azok a természetes számok, amelyeknek a multiplikatív neutrális elemen és önmagukon kívül nincs más osztója.

Nyilvánvaló, hogy ha $n \in \mathbb{N}^*$ és $m \in \mathbb{N}$ olyan, hogy $m \mid n$, akkor $m \leq n$, hiszen van olyan $q \in \mathbb{N}$, amelyre $m \cdot q = n$ és természetesen $1 \leq q$, így 7.9.5. alapján $m = m \cdot 1 \leq m \cdot q = n$.

7.11.6. Definíció. *Azt mondjuk, hogy a $p \in \mathbb{N}$ elem* **prímszám**, *ha $p \geq 2$ és p-nek 1-en és p-n kívül nincs más osztója. A prímszámok halmazát $\mathbb{P}$ jelöli, tehát*

$$\mathbb{P} := \{\ p \in \mathbb{N} \mid (p \geq 2) \wedge (\forall m \in \mathbb{N})(\ (m \mid p) \Rightarrow ((m = 1) \vee (m = p))\ )\ \}.$$

7.11.7. Állítás. *Minden $n \in \mathbb{N}$ esetén, ha $n \geq 2$, akkor van olyan $p \in \mathbb{P}$, hogy $p \mid n$ (vagyis minden 2-nél nagyobb-egyenlő természetes számnak létezik prímosztója).*

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy az

$$E := \{\ n \in \mathbb{N} \mid (n \geq 2) \wedge \neg(\exists p \in \mathbb{P})\ p \mid n\ \}$$

halmaz nem üres. Az $\mathbb{N}$ feletti természetes rendezés jólrendezés (7.8.3.), így E-nek létezik legkisebb eleme: legyen ez n_*. Világos, hogy $n_* \notin \mathbb{P}$, tehát létezik olyan $k \in \mathbb{N}$, hogy $k \mid n_*$ és $2 \leq k < n_*$. Az n_* szám minimalitási tulajdonsága miatt $k \notin E$, így k-hoz vehetünk olyan $p \in \mathbb{P}$ számot, amelyre $p \mid k$. Ekkor $p \mid n_*$, tehát $n_* \notin E$, ami ellentmond annak, hogy $n_* \in E$. ■

7.11.8. Tétel. (**Euklidészi maradékos osztás**) *Minden $m \in \mathbb{N}$ és $n \in \mathbb{N}^*$ esetén egyértelműen léteznek olyan $q, r \in \mathbb{N}$ számok, hogy $m = q \cdot n + r$ és $r < n$.*

Bizonyítás. (I) Először megmutatjuk, hogy minden $m \in \mathbb{N}$ és $n \in \mathbb{N}^*$ esetén létezik olyan $p \in \mathbb{N}^*$, hogy $m < p \cdot n$. Ezt könnyen beláthatjuk rögzített $n \in \mathbb{N}^*$ mellett, m-szerinti teljes indukcióval. Valóban, ha $m = 0$, akkor $p := 1$ olyan, hogy $m = 0 < n = p \cdot n$. Tegyük fel, hogy az $m \in \mathbb{N}$ természetes számhoz $p \in \mathbb{N}^*$ olyan, amelyre $m < p \cdot n$. Ekkor $m^+ = m + 1 < p \cdot n + 1 \leq p \cdot n + n = (p + 1) \cdot n$.

(II) Az egzisztencia bizonyításához legyenek $m \in \mathbb{N}$ és $n \in \mathbb{N}^*$. Ekkor (I) alapján $\{p \in \mathbb{N}^* | m < p \cdot n\} \neq \emptyset$ és $\mathbb{N}$ felett a természetes rendezés jólrendezés (7.8.3.). Jelölje p_* a $\{p \in \mathbb{N}^* | m < p \cdot n\}$ halmaz legkisebb elemét. Ekkor $p_* \in \mathbb{N}^*$, így létezik p_*-nak predesszora: legyen $q \in \mathbb{N}$ az a szám, amelyre $q^+ = p_*$. Két eset lehetséges:

– Ha $q = 0$, akkor $p_* = 1$, tehát $m < p_* \cdot n = n$, így $q := 0$ és $r := m$ olyan természetes számok, hogy $m = q \cdot n + r$ és $r < n$.

– Ha $q > 0$, akkor $q \in \mathbb{N}^*$ és $q < p_*$, így a p_* minimalitása miatt $q \cdot n \leq m$, tehát létezik olyan $r \in \mathbb{N}$, amelyre $m = q \cdot n + r$ teljesül (7.9.4.). Ugyanakkor

$$q \cdot n + r = m < p_* \cdot n = (q + 1) \cdot n = q \cdot n + n,$$

ezért $r < n$ (7.10.3.).

(III) Az unicitás bizonyításához legyenek $m \in \mathbb{N}$ és $n \in \mathbb{N}^*$, és vegyünk olyan $q, q', r, r' \in \mathbb{N}$ számokat, amelyekre $m = q \cdot n + r$ és $r < n$, valamint $m = q' \cdot n + r'$

és $r' < n$.

Tegyük fel, hogy $q < q'$, tehát van olyan $k \in \mathbb{N}$, hogy $q + k = q'$ és $k \neq 0$. Ekkor

$$q \cdot n + r = m = q' \cdot n + r' = (q + k) \cdot n + r' = q \cdot n + (k \cdot n + r'),$$

tehát az összeadás kancellativitása miatt $r = k \cdot n + r'$. Mivel $1 \leq k$, így 7.9.2. alapján $n = 1 \cdot n \leq k \cdot n \leq k \cdot n + r' = r$, vagyis $n \leq r$, ami ellentmond annak, hogy $r < n$. Ebből következik, hogy $q' \leq q$.

Ha azt tesszük fel, hogy $q' < q$, akkor az előző bekezdésben leírt gondolatmenetet követve azt kapjuk, hogy $n \leq r'$, ami ellentmond annak, hogy $r' < n$. Ebből következik, hogy $q \leq q'$.

Ezért $q = q'$, így $q \cdot n = q' \cdot n$, amiből $q \cdot n + r = q' \cdot n + r'$ és az összeadás kancellativitása folytán $r = r'$ is következik. ■

7.11.9. Lemma. *Ha $a, b, c \in \mathbb{N}$, valamint $c > 0$, $c \mid a$ és $c \mid (a + b)$, akkor $c \mid b$.*

Bizonyítás. Legyenek $m, n \in \mathbb{N}$ olyanok, hogy $a = m \cdot c$ és $a + b = n \cdot c$. Ekkor $m \cdot c = a \leq a + b = n \cdot c$, ezért $c \in \mathbb{N}^*$ és 7.9.5. alapján $m \leq n$, tehát van olyan $k \in \mathbb{N}$, hogy $m + k = n$ (7.9.4.). Ezért az $\mathbb{N}$ feletti szorzás összeadásra vonatkozó disztributivitását alkalmazva

$$m \cdot c + b = a + b = n \cdot c = (m + k) \cdot c = m \cdot c + k \cdot c,$$

így az összeadás kancellativitása (7.7.3.) folytán $b = k \cdot c$, tehát $c \mid b$. ■

7.11.10. Lemma. *Ha $p \in \mathbb{P}$ és $a, b \in \mathbb{N}$ olyanok, hogy $0 < a < p$ és $0 < b < p$, akkor p nem osztója az $a \cdot b$ szorzatnak.*

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy $p \in \mathbb{P}$ és $a, b \in \mathbb{N}$ olyanok, hogy $0 < a < p$, $0 < b < p$ és $p \mid a \cdot b$. Ekkor $\{b\,' \in \mathbb{N} | (0 < b\,' < p) \wedge (p \mid a \cdot b\,')\}$ nem üres részhalmaza $\mathbb{N}$-nek, és az $\mathbb{N}$ feletti természetes rendezés jólrendezés (7.8.3.), így jól értelmezett a

$$b_* := \min\{b\,' \in \mathbb{N} | (0 < b\,' < p) \wedge (p \mid a \cdot b\,')\}$$

szám. Ekkor $b_* > 0$, tehát 7.11.8. alapján léteznek olyan $q, r \in \mathbb{N}$ számok, hogy $p = q \cdot b_* + r$ és $r < b_*$. Világos, hogy $b_* > 1$, mert $b_* = 1$ esetén $p \mid a$ teljesülne, ami $a < p$ miatt lehetetlen. Ezért $r > 0$, különben $p = q \cdot b_*$ teljesülne, vagyis $b_* \mid p$, ami ellentmond annak, hogy p prímszám. Ugyanakkor $r < b_* < p$, tehát $0 < r < p$. Az $\mathbb{N}$ feletti szorzás összeadásra vonatkozó disztributivitását alkalmazva, valamint felhasználva az $\mathbb{N}$ feletti szorzás asszociativitását és kommutativitását kapjuk, hogy

$$a \cdot p = a \cdot (q \cdot b_* + r) = a \cdot (q \cdot b_*) + a \cdot r = q \cdot (a \cdot b_*) + a \cdot r.$$

A definíció szerint $p \mid a \cdot b_*$, ezért $p \mid q \cdot (a \cdot b_*)$. Továbbá $p \mid a \cdot p$ triviálisan igaz, ezért 7.11.9. alapján $p \mid a \cdot r$. Ez azt jelenti, hogy $r \in \{b\,' \in \mathbb{N} | (0 < b\,' < p) \wedge (p \mid a \cdot b\,')\}$, így a b_* szám minimalitási tulajdonsága miatt $b_* \leq r$, ami természetesen ellentmond annak, hogy $r < b_*$. ■

7.11.11. Lemma. (Euklidész-lemma) *Ha $p \in \mathbb{P}$ és $a, b \in \mathbb{N}$ olyanok, hogy $p \mid a \cdot b$, akkor $p \mid a$ vagy $p \mid b$.*

Bizonyítás. A 7.11.8. tétel kétszeri alkalmazásával vehetünk olyan $m, n, r, s \in \mathbb{N}$ számokat, amelyekre $a = m \cdot p + r$ és $r < p$, valamint $b = n \cdot p + s$ és $s < p$. Az $\mathbb{N}$ feletti összeadás és szorzás tulajdonságait alkalmazva kapjuk, hogy

$$a \cdot b = (m \cdot p + r) \cdot (n \cdot p + s) = (m \cdot n) \cdot p^2 + (m \cdot s + r \cdot n) \cdot p + r \cdot s.$$

Világos, hogy $p \mid ((m \cdot n) \cdot p^2 + (m \cdot s + r \cdot n) \cdot p)$, és a hipotézis alapján $p \mid a \cdot b$, így a 7.11.9. lemma szerint $p \mid r \cdot s$. Ha $r > 0$ és $s > 0$, akkor $r < p$ és $s < p$ miatt, az 7.11.10. lemmából arra következtethetünk, hogy p nem osztója az $r \cdot s$ szorzatnak. Ezért $r = 0$, és akkor $p \mid a$, vagy $s = 0$, és akkor $p \mid b$. ■

7.11.12. Következmény. *Ha $p, q \in \mathbb{P}$ és $p \neq q$, akkor minden $n \in \mathbb{N}^*$ esetén $p \nmid q^n$.*

Bizonyítás. 1-től indított, n szerinti teljes indukcióval bizonyítunk. Mivel $q \in \mathbb{P}$, $p \neq 1$ és $p \neq q$, így $p \nmid q = q^1$, tehát az állítás igaz $n = 1$ esetén. Ha az állítás igaz az $n \in \mathbb{N}^*$ számra, akkor $p \nmid q^n$ és $p \nmid q$, így $p \in \mathbb{P}$ és 7.11.11. szerint $p \nmid q^n \cdot q = q^{n+1}$, tehát az állítás $n + 1$-re is igaz. ■

7.11.13. Tétel. *Ha $p \in \mathbb{N}$ olyan szám, hogy $p \geq 2$, akkor*

$$p \in \mathbb{P} \quad \Leftrightarrow \quad (\forall a \in \mathbb{N})(\forall b \in \mathbb{N}) : (\ p \mid (a \cdot b) \ \Rightarrow \ ((p \mid a) \vee (p \mid b))\ ).$$

Bizonyítás. Az Euklidész-lemma (7.11.11.) szerint a $\Rightarrow$ következtetés teljesül. Ha $p \notin \mathbb{P}$, akkor léteznek olyan $a, b \in \mathbb{N}$, hogy $p = a \cdot b$, valamint $0 < a < p$ és $0 < b < p$. Ekkor természetesen $p \mid a \cdot b$ és p sem a-nak, sem b-nek nem osztója, így a $\Leftarrow$ következtetés is helyes. ■

7.12. Egész számok

7.12.1. Állítás. *Az $\mathbb{N} \times \mathbb{N}$ halmazon bevezetjük a következő relációt:*

$$R := \{((m, n), (m', n')) \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \mid m + n' = m' + n\}.$$

Ekkor R ekvivalencia az $\mathbb{N} \times \mathbb{N}$ halmaz felett.

Bizonyítás. Az R reláció nyilvánvalóan reflexív $\mathbb{N} \times \mathbb{N}$ felett, és szimmetrikus is, mert ha $(m, n) \in \mathbb{N} \times \mathbb{N}$ és $(m', n') \in \mathbb{N} \times \mathbb{N}$, akkor $((m, n), (m', n')) \in R$ esetén $m + n' = m' + n$ tehát az egyenlőség szimmetrikussága miatt $m' + n = m + n'$, ami azt jelenti, hogy $((m', n'), (m, n)) \in R$.

Az R reláció tranzitivitásának bizonyításához legyenek $(m, n), (m', n'), (m'', n'') \in \mathbb{N} \times \mathbb{N}$ olyanok, hogy $((m, n), (m', n')) \in R$ és $((m', n'), (m'', n'')) \in R$. Ekkor $m + n' = m' + n$ és $m' + n'' = m'' + n'$, amiből összeadással kapjuk, hogy $(m + n') + (m' + n'') = (m' + n) + (m'' + n')$. Az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása miatt $(m+n')+(m'+n'') = (m+n'')+(n'+m')$ és $(m'+n)+(m''+n') = (m''+n)+(n'+m')$, tehát $(m+n'')+(n'+m') = (m''+n)+(n'+m')$. Ebből az $\mathbb{N}$ feletti összeadás kancellativitása (7.7.3.) alapján $m + n'' = m'' + n$ adódik, tehát $((m, n), (m'', n'')) \in R$. ■

7.12.2. Definíció. *Ha R jelöli az $\{((m, n), (m', n')) \in (\mathbb{N}\times\mathbb{N})\times(\mathbb{N}\times\mathbb{N}) \mid m+n' = m'+n\}$ ekvivalenciát $\mathbb{N} \times \mathbb{N}$ felett, akkor*

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/R$$

és a $\mathbb{Z}$ faktorhalmazt az **egész számok halmazának** *nevezzük, és $\mathbb{Z}$ elemei az* **egész számok**. *Minden $(m,n) \in \mathbb{N} \times \mathbb{N}$ esetén az (m,n) pár R szerinti ekvivalencia-osztályát $m-n$ jelöli, vagyis*

$$m - n \ := \ \{(m',n') \in \mathbb{N} \times \mathbb{N} \mid m + n' = m' + n\}.$$

Továbbá, a

$$\mathrm{J}_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}; \quad n \mapsto n - 0$$

leképezést az $\mathbb{N}$ és $\mathbb{Z}$ halmazok közötti **kanonikus leképezésnek** *nevezzük.*

Nyilvánvaló, hogy $(m,n) \in \mathbb{N} \times \mathbb{N}$ és $(m',n') \in \mathbb{N} \times \mathbb{N}$ esetén

$$m - n = m' - n' \quad \Leftrightarrow \quad m + n' = m' + n,$$

továbbá, a $\mathrm{J}_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ leképezés injekció, mert $m, n \in \mathbb{N}$ és $m - 0 = n - 0$ esetén $m = m + 0 = n + 0 = n$.

7.12.3. Állítás.

a) *Létezik egyetlen olyan $\perp : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ művelet, amelyre teljesül az, hogy minden $(m,n) \in \mathbb{N} \times \mathbb{N}$ és $(p,q) \in \mathbb{N} \times \mathbb{N}$ esetén*

$$(m-n) \perp (p-q) = (m+p) - (n+q).$$

b) *Létezik egyetlen olyan $\top : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ művelet, amelyre teljesül az, hogy minden $(m,n) \in \mathbb{N} \times \mathbb{N}$ és $(p,q) \in \mathbb{N} \times \mathbb{N}$ esetén*

$$(m-n) \top (p-q) = (m \cdot p + n \cdot q) - (m \cdot q + n \cdot p).$$

c) *A $\mathrm{J}_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ kanonikus leképezésre teljesül az, hogy minden $m, n \in \mathbb{N}$ esetén*

$$\mathrm{J}_{\mathbb{N}}(m+n) = \mathrm{J}_{\mathbb{N}}(m) \perp \mathrm{J}_{\mathbb{N}}(n), \quad \mathrm{J}_{\mathbb{N}}(m \cdot n) = \mathrm{J}_{\mathbb{N}}(m) \top \mathrm{J}_{\mathbb{N}}(n).$$

Bizonyítás. Megállapodunk, hogy az egész számok halmazának definíciójában bevezetett R ekvivalenciát az $\approx$ szimbólummal jelöljük és az infix jelölést alkalmazzuk.

a) Az előírt tulajdonságú $\perp : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ függvény egyértelmű létezésének bizonyításához azt szükséges és elégséges igazolni, hogy $(m,n), (m',n'), (p,q), (p',q') \in \mathbb{N} \times \mathbb{N}$ esetén teljesül az, hogy ha $(m,n) \approx (m',n')$ és $(p,q) \approx (p',q')$, akkor $(m+p, n+q) \approx (m'+p', n'+q')$. Ez viszont nyilvánvalóan igaz, mert a hipotézis szerint $m + n' = m' + n$ és $p + q' = p' + q$, ezért $(m+n') + (p+q') = (m'+n) + (p'+q)$, így az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása alapján $(m+p) + (n'+q') = (m'+p') + (n+q)$, vagyis $(m+p, n+q) \approx (m'+p', n'+q')$.

b) Az előírt tulajdonságú $\top : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ függvény egyértelmű létezésének bizonyításához azt szükséges és elégséges igazolni, hogy $(m,n), (m',n'), (p,q), (p',q') \in \mathbb{N} \times \mathbb{N}$ esetén teljesül az, hogy ha $(m,n) \approx (m',n')$ és $(p,q) \approx (p',q')$, akkor $(m \cdot p + n \cdot q, m \cdot q + n \cdot p) \approx (m' \cdot p' + n' \cdot q', m' \cdot q' + n' \cdot p')$. Ennek bizonyításához felhasználjuk azt, hogy a hipotézis szerint $m + n' = m' + n$ és $p + q' = p' + q$, és azt kell igazolni, hogy

$$A := (m \cdot p + n \cdot q) + (m' \cdot q' + n' \cdot p') = (m' \cdot p' + n' \cdot q') + (m \cdot q + n \cdot p) =: B.$$

Az A-hoz hozzáadva az $m \cdot q'$ számot, és felhasználva az $m + n' = m' + n$, $p + q' = p' + q$ hipotéziseket, valamint az $\mathbb{N}$ feletti szorzás össszeadásra vonatkozó disztributivitását és az

$\mathbb{N}$ feletti összeadás asszociativitását és kommutativitását, a következő egyenlőség-láncot kapjuk:

$$\begin{gathered}A+m\cdot q'=m\cdot(p+q')+n\cdot q+m'\cdot q'+n'\cdot p'=\\=m\cdot(p'+q)+n\cdot q+m'\cdot q'+n'\cdot p'=m\cdot p'+m\cdot q+n\cdot q+m'\cdot q'+n'\cdot p'=\\=(m+n')\cdot p'+m\cdot q+n\cdot q+m'\cdot q'=(m'+n)\cdot p'+m\cdot q+n\cdot q+m'\cdot q'=\\=m'\cdot p'+n\cdot p'+m\cdot q+n\cdot q+m'\cdot q'=m'\cdot p'+n\cdot(p'+q)+m\cdot q+m'\cdot q'=\\=m'\cdot p'+n\cdot(p+q')+m\cdot q+m'\cdot q'=m'\cdot p'+n\cdot p+n\cdot q'+m\cdot q+m'\cdot q'=\\=m'\cdot p'+n\cdot p+(n+m')\cdot q'+m\cdot q=m'\cdot p'+n\cdot p+(n'+m)\cdot q'+m\cdot q=\\=m'\cdot p'+n\cdot p+n'\cdot q'+m\cdot q'+m\cdot q=B+m\cdot q'.\end{gathered}$$

Ebből az $\mathbb{N}$ feletti összeadás kancellativitása (7.7.3.) alapján kapjuk, hogy $A=B$.

c) Legyenek $m,n\in\mathbb{N}$. Ekkor $(m,0)\in \mathrm{J}_{\mathbb{N}}(m)$ és $(n,0)\in \mathrm{J}_{\mathbb{N}}(n)$, ezért $(m+n,0)=(m+n,0+0)\in \mathrm{J}_{\mathbb{N}}(m)\perp \mathrm{J}_{\mathbb{N}}(n)$, tehát $\mathrm{J}_{\mathbb{N}}(m)\perp \mathrm{J}_{\mathbb{N}}(n)=\mathrm{J}_{\mathbb{N}}(m+n)$. Továbbá, $(m\cdot n,0)=(m\cdot n+0\cdot 0, m\cdot 0+n\cdot 0)\in \mathrm{J}_{\mathbb{N}}(m)\top \mathrm{J}_{\mathbb{N}}(n)$, tehát $\mathrm{J}_{\mathbb{N}}(m)\top \mathrm{J}_{\mathbb{N}}(n)=\mathrm{J}_{\mathbb{N}}(m\cdot n)$. ■

7.12.4. Definíció. *A* 7.12.3. *állítás* a) *pontjában értelmezett $\mathbb{Z}$ feletti $\perp$ műveletet a $+$ szimbólummal, és a* 7.12.3. *állítás* b) *pontjában értelmezett $\mathbb{Z}$ feletti $\top$ műveletet a $\cdot$ szimbólummal jelöljük, továbbá a $+$ műveletet $\mathbb{Z}$ feletti* **összszeadásnak** *és a $\cdot$ műveletet $\mathbb{Z}$ feletti* **szorzásnak** *nevezzük.*

Tehát a $\mathbb{Z}$ feletti $+$ és $\cdot$ műveletekre teljesül az, hogy minden $(m,n),(p,q)\in\mathbb{N}\times\mathbb{N}$ esetén

$$\begin{gathered}(m-n)+(p-q)=(m+p)-(n+q),\\(m-n)\cdot(p-q)=(m\cdot p+n\cdot q)-(m\cdot q+n\cdot p).\end{gathered}$$

Megjegyezzük még, hogy azért nem vezetnek félreértésre a $\mathbb{Z}$ feletti műveletek jelölésére alkalmazott $+$ és $\cdot$ szimbólumok, mert a műveletek operandusainak típusából mindig kiderül, hogy természetes számok, vagy egész számok közötti össszeadásról, vagy szorzásról van szó.

7.12.5. Állítás. (**A $\mathbb{Z}$ feletti műveletek tulajdonságai**)

a) *A $\mathbb{Z}$ feletti összeadás asszociatív, neutrális-elemes, iverzelemes és kommutatív (tehát kommutatív csoportművelet).*

b) *A $\mathbb{Z}$ feletti szorzás asszociatív, neutrális-elemes és kommutatív.*

c) *A $\mathbb{Z}$ feletti szorzás disztributív a $\mathbb{Z}$ feletti összeadásra nézve.*

d) *A $\mathbb{Z}$ feletti szorzás zérusosztómentes, vagyis minden $a,b\in\mathbb{Z}$ esetén, ha $a\cdot b=\mathbf{0}$, akkor $a=\mathbf{0}$, vagy $b=\mathbf{0}$ (ahol $\mathbf{0}$ jelöli az összeadás szerinti neutrális elemet).*

e) *A $\mathbb{Z}$ feletti szorzás szerint csak $\mathbf{1}$ és $-\mathbf{1}$ invertálható (ahol $\mathbf{1}$ jelöli a szorzás szerinti neutrális elemet).*

Bizonyítás. a) Ha $a,b,c\in\mathbb{Z}$ és $(m,n),(p,q),(r,s)\in\mathbb{N}\times\mathbb{N}$ olyanok, hogy $a=m-n$, $b=p-q$ és $c=r-s$, akkor az $\mathbb{N}$ feletti összeadás asszociativitása miatt

$$\begin{gathered}(a+b)+c=((m+p)-(n+q))+(r-s)=((m+p)+r)-((n+q)+s)=\\=(m+(p+r))-(n+(q+s))=(m-n)+((p+r)-(q+s))=a+(b+c),\end{gathered}$$

tehát a $\mathbb{Z}$ feletti összeadás asszociatív.

Ha $a, b \in \mathbb{Z}$ és $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$ olyanok, hogy $a = m - n$ és $b = p - q$, akkor az $\mathbb{N}$ feletti összeadás kommutativitása miatt

$$a+b = (m-n)+(p-q) = (m+p)-(n+q) = (p+m)-(q+n) = (p-q)+(m-n) = b+a,$$

tehát a $\mathbb{Z}$ feletti összeadás kommutatív.

Legyen $\mathbf{0} := 0 - 0$. Ha $a \in \mathbb{Z}$ és $(m, n) \in \mathbb{N} \times \mathbb{N}$ olyan, hogy $a = m - n$, akkor

$$a + \mathbf{0} = (m - n) + (0 - 0) = (m + 0) - (n + 0) = m - n = a,$$

ezért $\mathbf{0}$ a $\mathbb{Z}$ feletti összeadás neutrális eleme. Nyilvánvaló, hogy minden $k \in \mathbb{N}$ esetén $\mathbf{0} = k - k$, mert $k + 0 = 0 + k$.

Legyen $a \in \mathbb{Z}$ és $(m, n) \in \mathbb{N} \times \mathbb{N}$ olyan, hogy $a = m - n$. Ekkor

$$a + (n - m) = (m - n) + (n - m) = (m + n) - (m + n) = \mathbf{0},$$

ami azt jelenti, hogy $n - m$ az a-nak inverze a $\mathbb{Z}$ feletti összeadás szerint.

b) Ha $a, b, c \in \mathbb{Z}$ és $(m, n), (p, q), (r, s) \in \mathbb{N} \times \mathbb{N}$ olyanok, hogy $a = m - n$, $b = p - q$ és $c = r - s$, akkor az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása, az $\mathbb{N}$ feletti szorzás asszociativitása, valamint az $\mathbb{N}$ feletti szorzás $\mathbb{N}$ feletti összedásra vonatkozó disztributivitása miatt

$$\begin{aligned}
(a \cdot b) \cdot c &= ((m - n) \cdot (p - q)) \cdot (r - s) = ((m \cdot p + n \cdot q) - (m \cdot q + n \cdot p)) \cdot (r - s) = \\
&= ((m \cdot p + n \cdot q) \cdot r + (m \cdot q + n \cdot p) \cdot s) - ((m \cdot p + n \cdot q) \cdot s + (m \cdot q + n \cdot p) \cdot r) = \\
&= (m \cdot p \cdot r + n \cdot q \cdot r + m \cdot q \cdot s + n \cdot p \cdot s) - (m \cdot p \cdot s + n \cdot q \cdot s + m \cdot q \cdot r + n \cdot p \cdot r) = \\
&= (m \cdot (p \cdot r + q \cdot s) + n \cdot (q \cdot r + p \cdot s)) - (m \cdot (p \cdot s + q \cdot r) + n \cdot (q \cdot s + p \cdot r)) = \\
&= (m - n) \cdot ((p \cdot r + q \cdot s) - (q \cdot r + p \cdot s)) = (m - n) \cdot ((p - q) \cdot (r - s)) = a \cdot (b \cdot c),
\end{aligned}$$

tehát a $\mathbb{Z}$ feletti szorzás asszociatív.

Ha $a, b \in \mathbb{Z}$ és $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$ olyanok, hogy $a = m - n$ és $b = p - q$, akkor az $\mathbb{N}$ feletti szorzás és összeadás kommutativitása miatt

$$\begin{aligned}
a \cdot b &= (m - n) \cdot (p - q) = (m \cdot p + n \cdot q) - (m \cdot q + n \cdot p) = \\
&= (p \cdot m + q \cdot n) - (q \cdot m + p \cdot n) = (p \cdot m + q \cdot n) - (p \cdot n + q \cdot m) = \\
&= (p - q) \cdot (m - n) = b \cdot a,
\end{aligned}$$

tehát a $\mathbb{Z}$ feletti szorzás kommutatív.

Legyen $\mathbf{1} := 1 - 0$. Ha $a \in \mathbb{Z}$ és $(m, n) \in \mathbb{N} \times \mathbb{N}$ olyan, hogy $a = m - n$, akkor

$$a \cdot \mathbf{1} = (m - n) \cdot (1 - 0) = (m \cdot 1 + n \cdot 0) - (m \cdot 0 + n \cdot 1) = m - n = a,$$

ezért $\mathbf{1}$ a $\mathbb{Z}$ feletti szorzás neutrális eleme. Nyilvánvaló, hogy minden $k \in \mathbb{N}$ esetén $\mathbf{1} = (k + 1) - k$, mert $(k + 1) + 0 = 1 + k$.

c) Ha $a, b, c \in \mathbb{Z}$ és $(m, n), (p, q), (r, s) \in \mathbb{N} \times \mathbb{N}$ olyanok, hogy $a = m - n$, $b = p - q$ és $c = r - s$, akkor az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása, az $\mathbb{N}$ feletti szorzás asszociativitása, valamint az $\mathbb{N}$ feletti szorzás összedásra vonatkozó disztributivitása miatt

$$\begin{aligned}
(a + b) \cdot c &= ((m - n) + (p - q)) \cdot (r - s) = ((m + p) - (n + q)) \cdot (r - s) = \\
&= ((m + p) \cdot r + (n + q) \cdot s) - ((m + p) \cdot s + (n + q) \cdot r) = \\
&= (m \cdot r + p \cdot r + n \cdot s + q \cdot s) - (m \cdot s + p \cdot s + n \cdot r + q \cdot r) = \\
&= ((m \cdot r + n \cdot s) + (p \cdot r + q \cdot s)) - ((m \cdot s + n \cdot r) + (p \cdot s + q \cdot r)) = \\
&= ((m \cdot r + n \cdot s) - (m \cdot s + n \cdot r)) + ((p \cdot r + q \cdot s) - (p \cdot s + q \cdot r)) = \\
&= (m - n) \cdot (r - s) + (p - q) \cdot (r - s) = a \cdot c + b \cdot c,
\end{aligned}$$

tehát a $\mathbb{Z}$ feletti szorzás disztributív a $\mathbb{Z}$ feletti össszeadásra nézve.

d) A $\mathbb{Z}$ feletti szorzás zérusosztómentességének bizonyításához elég azt megmutatni, hogy ha $a, b \in \mathbb{Z}$, valamint $a \cdot b = \mathbf{0}$ és $a \neq \mathbf{0}$, akkor $b = \mathbf{0}$ (2.5.7.). Ehhez legyenek $(m,n),(p,q) \in \mathbb{N} \times \mathbb{N}$ olyanok, hogy $a = m - n$ és $b = p - q$, továbbá tegyük fel, hogy

$$\mathbf{0} = a \cdot b = (m-n) \cdot (p-q) = (m \cdot p + n \cdot q) - (m \cdot q + n \cdot p),$$

tehát $m \cdot p + n \cdot q = m \cdot q + n \cdot p$, és $\mathbf{0} \neq a = m - n$. Ekkor $m \neq n$, tehát két eset lehetséges.

– Ha $m < n$, akkor vehetünk olyan $j \in \mathbb{N}$ elemet, hogy $j \neq 0$ és $m + j = n$ (7.9.4.). Ebből az $\mathbb{N}$ feletti szorzás összeadásra vonatkozó disztributivitása, valamint az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása miatt

$$\begin{aligned} m \cdot p + m \cdot q + j \cdot q = m \cdot p + (m+j) \cdot q = m \cdot p + n \cdot q = m \cdot q + n \cdot p = \\ = m \cdot q + (m+j) \cdot p = m \cdot q + m \cdot p + j \cdot p = m \cdot p + m \cdot q + j \cdot p, \end{aligned}$$

amiből az $\mathbb{N}$ feletti összeadás kancellativitása (7.7.3.) alapján $j \cdot q = j \cdot p$, így a $\mathbb{N}$ feletti szorzás kancellativitása (7.9.8.) és $j \neq 0$ miatt $q = p$.

– Ha $m > n$, akkor vehetünk olyan $k \in \mathbb{N}$ elemet, hogy $k \neq 0$ és $m = k + n$ (7.9.4.). Ebből az $\mathbb{N}$ feletti szorzás összeadásra vonatkozó disztributivitása, valamint az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása miatt következik, hogy

$$\begin{aligned} k \cdot p + n \cdot p + n \cdot q = (k+n) \cdot p + n \cdot q = m \cdot p + n \cdot q = m \cdot q + n \cdot p \\ = (k+n) \cdot q + n \cdot p = k \cdot q + n \cdot q + n \cdot p = k \cdot q + n \cdot p + n \cdot q, \end{aligned}$$

amiből az $\mathbb{N}$ feletti összeadás kancellativitása (7.7.3.) alapján $k \cdot p = k \cdot q$, így a $\mathbb{N}$ feletti szorzás kancellativitása (7.9.8.) és $k \neq 0$ miatt $p = q$.

Mindkét esetben azt kapjuk, hogy $b = p - q = p - p = \mathbf{0}$.

e) Legyenek $a, a' \in \mathbb{Z}$ olyanok, hogy $a \cdot a' = \mathbf{1} = 1 - 0$. Megmutatjuk, hogy ekkor vagy $a = a' = \mathbf{1}$, vagy $a = a' = -\mathbf{1}$. Ehhez legyenek $m, n, m', n' \in \mathbb{N}$ olyanok, hogy $a = m - n$ és $a' = m' - n'$. Tehát az a hipotézis, hogy

$$1 - 0 = \mathbf{1} = a \cdot a' = (m-n) \cdot (m'-n') = (m \cdot m' + n \cdot n') - (m \cdot n' + n \cdot m'),$$

ami ekvivalens azzal, hogy

$$1 + m \cdot n' + n \cdot m' = m \cdot m' + n \cdot n'.$$

Először megjegyezzük, hogy minden $x \in \mathbb{Z}$ esetén $\mathbf{0} \cdot x = \mathbf{0}$, hiszen $\mathbf{0} = 0 - 0$, ezért minden $p, q \in \mathbb{N}$ esetén $\mathbf{0} \cdot (p - q) = (0 \cdot p + 0 \cdot q) - (0 \cdot q + 0 \cdot p) = 0 - 0 = \mathbf{0}$. Ebből, és az $a \cdot a' = \mathbf{1} \neq \mathbf{0}$ egyenlőségből következik, hogy $a \neq \mathbf{0}$ és $a' \neq \mathbf{0}$, vagyis $m \neq n$ és $m' \neq n'$. Ekkor két eset lehetséges: $m > n$ vagy $m < n$.

– Tegyük fel, hogy $m > n$. Ekkor van olyan $k \in \mathbb{N}$, hogy $k \neq 0$ és $m = n + k$, ezért a hipotézis alapján

$$1 + n \cdot n' + k \cdot n' + n \cdot m' = n \cdot m' + k \cdot m' + n \cdot n'.$$

Az $\mathbb{N}$ feletti összeadás kancellativitása (7.7.3.) alapján ebből következik, hogy $1 + k \cdot n' = k \cdot m'$. Ha $m' \leq n'$ teljesülne, akkor $k \cdot n' < 1 + k \cdot n' = k \cdot m' \leq k \cdot n'$ lenne, ami lehetetlen, ezért $n' < m'$, így létezik olyan $k' \in \mathbb{N}$, hogy $k' \neq 0$ és $m' = n' + k'$. Ekkor

$$1 + k \cdot n' = k \cdot m' = k \cdot (n' + k') = k \cdot n' + k \cdot k',$$

amiből ismét az $\mathbb{N}$ feletti összeadás kancellativitása szerint $1 = k \cdot k'$ következik. Ezért 7.7.6. c) alapján $k = 1 = k'$, így $m = n + 1$ és $m' = n' + 1$, tehát $a = m - n = (n + 1) - n = 1 - 0 = \mathbf{1}$ és $a' = m' - n' = (n' + 1) - n' = 1 - 0 = \mathbf{1}$.

– Tegyük fel, hogy $m < n$. Ekkor van olyan $k \in \mathbb{N}$, hogy $k \neq 0$ és $m + k = n$, ezért a hipotézis alapján

$$1 + m \cdot n' + m \cdot m' + k \cdot m' = m \cdot m' + m \cdot n' + k \cdot n'.$$

Az $\mathbb{N}$ feletti összeadás kancellativitása (7.7.3.) alapján ebből következik, hogy $1+k\cdot m' = k \cdot n'$. Ha $m' \geq n'$ teljesülne, akkor $k \cdot m' < 1 + k \cdot m' = k \cdot n' \leq k \cdot m'$, mi lehetlen, ezért $m' < n'$, így létezik olyan $k' \in \mathbb{N}$, hogy $k' \neq 0$ és $m' + k' = n'$. Ekkor

$$1 + k \cdot m' = k \cdot n' = k \cdot (m' + k') = k \cdot m' + k \cdot k',$$

amiből ismét az $\mathbb{N}$ feletti összeadás kancellativitása szerint $1 = k \cdot k'$ következik. Ezért 7.7.6. c) alapján $k = 1 = k'$, így $n = m + 1$ és $n' = m' + 1$, tehát $a = m - n = m - (m + 1) = 0 - 1 = -\mathbf{1}$, és $a' = m' - n' = m' - (m' + 1) = 0 - 1 = -\mathbf{1}$.

Végül megjegyezzük, hogy $\mathbf{1}$ természetesen invertálható a $\mathbb{Z}$ szorzása szerint, továbbá

$$(-\mathbf{1}) \cdot (-\mathbf{1}) = (0 - 1) \cdot (0 - 1) = (0 \cdot 0 + 1 \cdot 1) - (0 \cdot 1 + 1 \cdot 0) = 1 - 0 = \mathbf{1},$$

ezért $-\mathbf{1}$ is invertálható a $\mathbb{Z}$ szorzása szerint, és $(-\mathbf{1})^{-1} = -\mathbf{1}$. ■

Megállapodunk abban, hogy a továbbiakban minden $a \in \mathbb{Z}$ esetén $-a$ jelöli az a elem inverzét a $\mathbb{Z}$ feletti összeadás szerint, továbbá a

$$\mathbb{Z}^* := \mathbb{Z} \setminus \{\mathbf{0}\}$$

jelölést alkalmazzuk.

7.12.6. Állítás. (**A $\mathbb{Z}$ feletti összeadás és szorzás kancellativitása**)

a) *Ha $a, b, c \in \mathbb{Z}$, akkor $a + c = b + c$ esetén $a = b$.*

b) *Ha $a, b, c \in \mathbb{Z}$ és $c \neq \mathbf{0}$, akkor $a \cdot c = b \cdot c$ esetén $a = b$.*

Bizonyítás. a) Az $a + c = b + c$ egyenlőség mindkét oldalához jobbról hozzáadva a $-c$ additív inverzet, és felhasználva a $\mathbb{Z}$ feletti összeadás asszociativitását kapjuk, hogy

$$a = a+\mathbf{0} = a+(c+(-c)) = (a+c)+(-c) = (b+c)+(-c) = b+(c+(-c)) = b+\mathbf{0} = b.$$

b) Először megjegyezzük, hogy minden $x \in \mathbb{Z}$ esetén $\mathbf{0} \cdot x = \mathbf{0}$, mert a $\mathbb{Z}$ feletti szorzás $\mathbb{Z}$ feletti összeadásra vonatkozó disztributivitása folytán

$$\mathbf{0} \cdot x + \mathbf{0} \cdot x = (\mathbf{0} + \mathbf{0}) \cdot x = \mathbf{0} \cdot x,$$

amiből a $\mathbb{Z}$ feletti összeadás asszociativitása miatt következik, hogy

$$\mathbf{0}\cdot x = \mathbf{0}\cdot x+\mathbf{0} = \mathbf{0}\cdot x+(\mathbf{0}\cdot x+(-(\mathbf{0}\cdot x))) = (\mathbf{0}\cdot x+\mathbf{0}\cdot x)+(-(\mathbf{0}\cdot x)) = \mathbf{0}\cdot x+(-(\mathbf{0}\cdot x)) = \mathbf{0}.$$

Ebből következik, hogy $x, y \in \mathbb{Z}$ esetén $(-x) \cdot y = -(x \cdot y)$, mert a $\mathbb{Z}$ feletti szorzás $\mathbb{Z}$ feletti összeadásra vonatkozó disztributivitása folytán

$$(x \cdot y) + ((-x) \cdot y) = (x + (-x)) \cdot y = \mathbf{0} \cdot y = \mathbf{0} = (x \cdot y) + (-(x \cdot y)),$$

tehát az a) állítás alapján $(-x) \cdot y = -(x \cdot y)$.

Ha $a, b, c \in \mathbb{Z}$, $c \neq \mathbf{0}$ és $a \cdot c = b \cdot c$, akkor a $\mathbb{Z}$ feletti szorzás $\mathbb{Z}$ feletti összeadásra vonatkozó disztributivitása és $-(b \cdot c) = (-b) \cdot c$ folytán

$$\mathbf{0} = (b \cdot c) + (-(b \cdot c)) = (a \cdot c) + (-(b \cdot c)) = (a \cdot c) + ((-b) \cdot c) = (a + (-b)) \cdot c.$$

A $\mathbb{Z}$ feletti szorzás zérusosztómentessége (7.12.5. d) állítás) és $c \neq \mathbf{0}$ miatt ebből $a + (-b) = \mathbf{0}$ következik, ezért a $\mathbb{Z}$ feletti összeadás asszociativitásának alkalmazásával kapjuk az

$$a = a + \mathbf{0} = a + ((-b) + b) = (a + (-b)) + b = \mathbf{0} + b = b$$

egyenlőségeket. ■

7.12.7. Állítás. *Minden $a \in \mathbb{Z}$ esetén léteznek olyan $m, n \in \mathbb{N}$, hogy $a = \mathrm{J}_{\mathbb{N}}(m) + (-\mathrm{J}_{\mathbb{N}}(n))$.*

Bizonyítás. Ha $a \in \mathbb{Z}$, akkor létezik olyan $(m, n) \in \mathbb{N} \times \mathbb{N}$, hogy $a = m - n$, és ekkor

$$\mathrm{J}_{\mathbb{N}}(m) + (-\mathrm{J}_{\mathbb{N}}(n)) = (m - 0) + (-(n - 0)) = (m - 0) + (0 - n) = m - n = a. \blacksquare$$

Most rendezést fogunk bevezetni az egész számok halmazán. Ehhez szükségünk lesz a következő lemmára.

7.12.8. Lemma. *Ha $(m, n), (m', n'), (p, q), (p', q') \in \mathbb{N} \times \mathbb{N}$, $m - n = m' - n'$, $p - q = p' - q'$ és $m + q \leq p + n$, akkor $m' + q' \leq p' + n'$. Ha $a, b \in \mathbb{Z}$, akkor*

$$(\forall (m, n) \in a)(\forall (p, q) \in b)\ (m + q \leq p + n) \ \Leftrightarrow\ (\exists (m, n) \in a)(\exists (p, q) \in b)\ (m + q \leq p + n)$$

teljesül.

Bizonyítás. Nyilvánvaló, hogy a második kijelentés ekvivalens az elsővel. Az első kijelentés bizonyításához tegyük fel, hogy $m + n' = m' + n$, $p + q' = p' + q$ és $m + q \leq p + n$. Ekkor felhasználva az $\mathbb{N}$ feletti összeadás asszociativitását és kommutativitását, valamint a 7.9.2. állítást kapjuk, hogy

$$\begin{aligned}(m' + q') + (n + q) &= (m' + n) + q' + q = (n' + m) + q' + q = (m + q) + n' + q' \leq \\ &\leq (p + n) + n' + q' = (p + q') + n + n' = (p' + q) + n + n' = (p' + n') + (n + q).\end{aligned}$$

Ebből ismét a 7.9.2. állítás alapján kapjuk, hogy $m' + q' \leq p' + n'$. ■

7.12.9. Állítás. *A $\mathbb{Z}$ halmazon értelmezzük a következő relációt*

$$T := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid (\exists (m, n) \in a)(\exists (p, q) \in b)\ (m + q \leq p + n)\}$$

Ekkor T lineáris rendezés $\mathbb{Z}$ felett, és minden $m, n \in \mathbb{N}$ számra

$$m \leq n \ \Leftrightarrow\ (\mathrm{J}_{\mathbb{N}}(m), \mathrm{J}_{\mathbb{N}}(n)) \in T.$$

Bizonyítás. Ha $a \in \mathbb{Z}$, akkor van olyan $(m, n) \in \mathbb{N} \times \mathbb{N}$, hogy $a = m - n$, és ekkor az $\mathbb{N}$ feletti természetes rendezés reflexivitása miatt $m + n \leq m + n$, ami definíció szerint azt jelenti, hogy $(a, a) \in T$. Tehát a T reláció reflexív $\mathbb{Z}$ felett.

Legyenek $a, b \in \mathbb{Z}$ és tegyük fel, hogy $(a, b) \in T$ és $(b, a) \in T$. Ekkor léteznek olyan $(m, n) \in a$, $(p, q) \in b$, $(p', q') \in b$ és $(m', n') \in a$ elemek, hogy $m + q \leq p + n$ és $p' + n' \leq m' + q'$. Ugyanakkor $m + n' = m' + n$ és $p + q' = p' + q$ is teljesül. Ezért az

$\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása, valamint 7.9.2. alapján kapjuk, hogy

$$(m+q')+p = m+(q'+p) = m+(p'+q) = (m+q)+p' \leq (p+n)+p' = (n+p')+p$$

tehát 7.9.2. szerint $m+q' \leq n+p'$. Ismét a 7.9.2. állítást alkalmazva ebből

$$(m'+q')+n = (m'+n)+q' = (m+n')+q' = (m+q')+n' \leq (n+p')+n' = (p'+n')+n$$

adódik, tehát ismét 7.9.2. szerint $m'+q' \leq p'+n'$. Ugyanakkor $p'+n' \leq m'+q'$ is igaz, tehát az $\mathbb{N}$ feletti természetes rendezés antiszimmetrikussága folytán $m'+q' = p'+n'$. Ez azt jelenti, hogy $a = m'-n' = p'-q' = b$. Tehát a T reláció antiszimmetrikus.

Legyenek $a, b, c \in \mathbb{Z}$ olyanok, hogy $(a,b) \in T$ és $(b,c) \in T$. Ekkor vehetünk olyan $(m,n) \in a$, $(p,q) \in b$, $(p',q') \in b$ és $(r,s) \in c$ elemeket, hogy $m+q \leq p+n$ és $p'+s \leq r+q'$. Összeadva ezeket az egyenlőtlenségeket (7.9.3.) és felhasználva az $\mathbb{N}$ feletti összeadás asszociativitását és kommutativitását kapjuk, hogy

$$(m+s)+(p+q') = (m+s)+(p'+q) = (m+q)+(p'+s) \leq (p+n)+(r+q') = (r+n)+(p+q'),$$

tehát 7.9.2. szerint $m+s \leq r+n$, ami azt jelenti, hogy $(a,c) \in T$. Tehát a T reláció tranzitív.

Legyenek $a, b \in \mathbb{Z}$, és vegyünk $(m,n) \in a$ és $(p,q) \in b$ elemeket. Ekkor az $\mathbb{N}$ feletti természetes rendezés linearitása szerint $m+q \leq p+n$ vagy $p+n \leq m+q$ teljesül. Az első esetben $(a,b) \in T$, a másodikban $(b,a) \in T$. Ezzel bebizonyítottuk, hogy T lineáris rendezés $\mathbb{Z}$ felett.

Legyenek $m, n \in \mathbb{N}$. Ha $m \leq n$, akkor $m+0 = m \leq n = n+0$ miatt $(\mathrm{J}_{\mathbb{N}}(m), \mathrm{J}_{\mathbb{N}}(n)) = (m-0, n-0) \in T$. Megfordítva, ha $(\mathrm{J}_{\mathbb{Z}}(m), \mathrm{J}_{\mathbb{Z}}(n)) \in T$, akkor $(n,0) \in \mathrm{J}_{\mathbb{Z}}(n)$ és $(m,0) \in \mathrm{J}_{\mathbb{Z}}(m)$ miatt a 7.12.8. lemma szerint $m+0 \leq n+0$, tehát $m \leq n$. ■

7.12.10. Definíció. *A* 7.12.9. *állításban értelmezett $\mathbb{Z}$ feletti T lineáris rendezést a $\leq$ vagy $\leq_{\mathbb{Z}}$ szimbólummal jelöljük és $\mathbb{Z}$ feletti* (*természetes*) **rendezésnek** *nevezzük. Továbbá, a*

$$\mathbb{Z}_+ := \{a \in \mathbb{Z} \mid \mathbf{0} \leq a\},$$
$$\mathbb{Z}_+^* := \{a \in \mathbb{Z} \mid \mathbf{0} < a\}$$

jelöléseket alkalmazzuk.

Tehát a definíció szerint, ha $m, n, p, q \in \mathbb{N}$, akkor

$$m-n \leq p-q \quad \Leftrightarrow \quad m+q \leq p+n,$$
$$m-0 \leq p-0 \quad \Leftrightarrow \quad m \leq p$$

teljesül. Továbbá, ha $m, n \in \mathbb{N}$, akkor

$$\mathbf{0} \leq m-n \Leftrightarrow 0-0 \leq m-n \Leftrightarrow 0+n \leq m+0 \Leftrightarrow n \leq m.$$

7.12.11. Állítás. (**A $\mathbb{Z}$ feletti összeadás kapcsolata a rendezéssel**) *Minden $a, b \in \mathbb{Z}$ esetén a következő állítások ekvivalensek.*

(i) $a \leq b$.

(ii) *Minden $c \in \mathbb{Z}$ esetén $a+c \leq b+c$.*

(iii) *Létezik olyan $c \in \mathbb{Z}$, hogy $a+c \leq b+c$.*

Bizonyítás. Legyenek $a, b \in \mathbb{Z}$, valamint $(m, n) \in a$ és $(p, q) \in b$.

(i)$\Rightarrow$(ii) Legyen $c \in \mathbb{Z}$ és $(r, s) \in c$. Az $a \leq b$ hipotézis szerint $m + q \leq p + n$, ezért az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása, valamint 7.9.2. miatt

$$(m + r) + (q + s) = (m + q) + (r + s) \leq (p + n) + (r + s) = (p + r) + (n + s),$$

ami azt jelenti, hogy

$$a + c = (m - n) + (r - s) = (m + r) - (n + s) \leq (p + r) - (q + s) = (p - q) + (r - s) = b + c.$$

(ii)$\Rightarrow$(iii) Triviális.

(iii)$\Rightarrow$(i) Legyen $c \in \mathbb{Z}$, $(r, s) \in c$, és tegyük fel, hogy $a + c \leq b + c$. Ekkor $(m - n) + (r - s) \leq (p - q) + (r - s)$, tehát a $\mathbb{Z}$ feletti összeadás definíciója szerint $(m + r) - (n + s)) \leq (p + r) - (q + s)$, ami a $\mathbb{Z}$ feletti rendezés definíciója alapján azt jelenti, hogy $(m + r) + (q + s) \leq (p + r) + (n + s))$. Felhasználva az $\mathbb{N}$ feletti összeadás asszociativitását és kommutativitását, ebből kapjuk, hogy $(m + q) + (r + s) \leq (p + n) + (r + s)$, amiből 7.9.2. alapján következik, hogy $m + q \leq p + n$, vagyis $a = m - n \leq p - q = b$. ■

7.12.12. Következmény. *Minden $a, b \in \mathbb{Z}$ esetén*

$$a \leq b \quad \Leftrightarrow \quad -b \leq -a.$$

Bizonyítás. Tegyük fel, hogy $a \leq b$. Ekkor 7.12.11. a) szerint $\mathbf{0} = a + (-a) \leq b + (-a)$. Ebből a $\mathbb{Z}$ feletti összeadás asszociativitása és kommutativitása, valamint 7.12.11. a) alapján kapjuk, hogy

$$-b = \mathbf{0} + (-b) \leq (b + (-a)) + (-b) = (b + (-b)) + (-a) = \mathbf{0} + (-a) = -a.$$

Ez azt jelenti, hogy minden $a, b \in \mathbb{Z}$ esetén, ha $a \leq b$, akkor $-b \leq -a$. Ha $a, b \in \mathbb{Z}$ és $-b \leq -a$, akkor ezt a szabályt alkalmazva a $-b$ és $-a$ egész számokra kapjuk, hogy $a = -(-a) \leq -(-b) = b$. ■

7.12.13. Állítás. (**A $\mathbb{Z}$ feletti szorzás kapcsolata a rendezéssel**) *Minden $a, b \in \mathbb{Z}$ esetén a következő állítások ekvivalensek.*

(i) $a \leq b$.

(ii) *Minden $c \in \mathbb{Z}_+$ esetén $a \cdot c \leq b \cdot c$.*

(iii) *Létezik olyan $c \in \mathbb{Z}_+^*$, hogy $a \cdot c \leq b \cdot c$.*

Bizonyítás. Legyenek $a, b \in \mathbb{Z}$ olyanok, hogy $a \leq b$, és vegyünk $(m, n) \in a$ és $(p, q) \in b$ elemeket.

(i)$\Rightarrow$(ii) Legyen $c \in \mathbb{Z}_+$ és $(r, s) \in c$. A hipotézis szerint $m + q \leq p + n$, így a 7.9.4. állítás alapján vehetünk olyan $k \in \mathbb{N}$ számot, amelyre $(m + q) + k = p + n$. Tudjuk, hogy

$$a \cdot c = (m - n) \cdot (r - s) = (m \cdot r + n \cdot s) - (m \cdot s + n \cdot r),$$
$$b \cdot c = (p - q) \cdot (r - s) = (p \cdot r + q \cdot s) - (p \cdot s + q \cdot r),$$

ezért az $a \cdot c \leq b \cdot c$ egyenlőtlenség azzal ekvivalens, hogy

$$(m \cdot r + n \cdot s) + (p \cdot s + q \cdot r) \leq (p \cdot r + q \cdot s) + (m \cdot s + n \cdot r).$$

Az $\mathbb{N}$ feletti szorzás $\mathbb{N}$ feletti összeadására vonatkozó disztributivitása, valamint az $\mathbb{N}$ feletti összeadás asszociativitása és kommutativitása miatt

$$(m \cdot r + n \cdot s) + (p \cdot s + q \cdot r) = (m + q) \cdot r + (p + n) \cdot s =$$
$$= (m + q) \cdot r + ((m + q) + k) \cdot s = (m + q) \cdot (r + s) + k \cdot s,$$

ugyanakkor

$$(p \cdot r + q \cdot s) + (m \cdot s + n \cdot r) = (p + n) \cdot r + (m + q) \cdot s =$$
$$= ((m + q) + k) \cdot r + (m + q) \cdot s = (m + q) \cdot (r + s) + k \cdot r.$$

A $\mathbf{0} \leq c = r - s$ feltételből, vagyis az $s \leq r$ egyenlőtlenségből 7.9.5. alapján kapjuk, hogy $k \cdot s \leq k \cdot r$, tehát ismét a 7.9.2. állítás alkalmazásával $(m + q) \cdot (r + s) + k \cdot s \leq (m + q) \cdot (r + s) + k \cdot r$ adódik, vagyis

$$(m \cdot r + n \cdot s) + (p \cdot s + q \cdot r) \leq (p \cdot r + q \cdot s) + (m \cdot s + n \cdot r),$$

amit bizonyítani kellett.

(ii)$\Rightarrow$(iii) Triviális.

(iii)$\Rightarrow$(i) Legyen $c \in \mathbb{Z}_+^*$, $(r, s) \in c$, és tegyük fel, hogy $a \cdot c \leq b \cdot c$. Ekkor

$$(m \cdot r + n \cdot s) - (m \cdot s + n \cdot r) = (m - n) \cdot (r - s) = a \cdot c \leq$$
$$\leq b \cdot c = (p - q) \cdot (r - s) = (p \cdot r + q \cdot s) - (p \cdot s + q \cdot r$$

ami a $\mathbb{Z}$ feletti rendezés definíciója szerint azt jelenti, hogy

$$(m \cdot r + n \cdot s) + (p \cdot s + q \cdot r) \leq (p \cdot r + q \cdot s) + (m \cdot s + n \cdot r).$$

Az $\mathbb{N}$ feletti összeadás aszzociativitását és kommutativitását alkalmazva ez azzal ekvivalens, hogy

$$(m + q) \cdot r + (n + p) \cdot s \leq (p + n) \cdot r + (m + q) \cdot s.$$

A $\mathbf{0} < c = r - s$ feltételből, vagyis az $s < r$ egyenlőtlenségből 7.9.4. alapján kapjuk, hogy létezik olyan $k \in \mathbb{N}^*$, hogy $s + k = r$. Az r szám helyére beírva az $s + k$ összeget, és kihasználva az $\mathbb{N}$ feletti szorzás $\mathbb{N}$ feletti összeadásra vonatkozó disztributivitását, valamint az $\mathbb{N}$ feletti összeadás asszociativitását és kommutativitását kapjuk, hogy

$$((m + q) + (n + p)) \cdot s + (m + q) \cdot k = (m + q) \cdot (s + k) + (n + p) \cdot s =$$
$$= (m + q) \cdot r + (n + p) \cdot s \leq\leq (p + n) \cdot r + (m + q) \cdot s =$$
$$= (p + n) \cdot (s + k) + (m + q) \cdot s = ((p + n) + (m + q)) \cdot s + (p + n) \cdot k.$$

Ebből a 7.9.2. állítás alapján kapjuk, hogy $(m + q) \cdot k \leq (p + n) \cdot k$, és ebből $k \in \mathbb{N}^*$ miatt, 7.9.5. alkalmazásával nyerjük, hogy $m + q \leq p + n$, vagyis $a = m - n \leq p - q = b$, amit bizonyítani kellett. ■

7.13. Gyakorlatok

1. Mutassuk meg, hogy az iterációs definíció tétele (7.4.4.) olyan speciális esete az elemi rekurzív definíció tételének (7.4.2.), amely *ekvivalens* ez utóbbival.

(*Útmutatás.* Tegyük fel, hogy az iterációs definíció tétele igaz, és legyen E halmaz, $e \in E$, valamint $g : \mathbb{N} \times E \to E$ függvény. Értelmezzük az

$$f : \mathbb{N} \times E \to \mathbb{N} \times E; \quad (n, x) \mapsto (n^+, g(n, x))$$

függvényt, és jelölje $\tilde{\mathbf{s}}$ az f függvény és a $(0, e)$ kezdőpont által iterációval meghatározott $\mathbb{N} \times E$-ben haladó sorozatot. Teljes indukcióval könnyen igazolható, hogy minden $n \in \mathbb{N}$ esetén $\mathrm{pr}_1(\tilde{\mathbf{s}}(n)) = n$ és $\mathrm{pr}_2(\tilde{\mathbf{s}}(n^+)) = g(n, \mathrm{pr}_2(\tilde{\mathbf{s}}(n)))$, ezért az $\mathbf{s} := \mathrm{pr}_2 \circ \tilde{\mathbf{s}}$ függvény megegyezik a g függvény és az e kezdőpont által elemi rekurzióval meghatározott E-ben haladó sorozattal.)

2. (**Fibonacci-sorozatok**) Legyen $(a, b) \in \mathbb{N} \times \mathbb{N}$ tetszőleges pár, és értelmezzük a

$$\mathbf{g} : \bigcup_{n \in \mathbb{N}} \mathscr{F}(n; \mathbb{N}) \to \mathbb{N}$$

függvényt a következőképpen:

– Legyen $\mathbf{g}(\emptyset) := a$, és minden $\mathbf{s}' \in \mathscr{F}(1; \mathbb{N})$ esetén $\mathbf{g}(\mathbf{s}') := b$.

– Minden $n \in \mathbb{N}$ esetén, ha $n \neq 0$ és $n \neq 1$, valamint $\mathbf{s}' \in \mathscr{F}(n; \mathbb{N})$, akkor legyen $\mathbf{g}(\mathbf{s}') := \mathbf{s}'(n^-) + \mathbf{s}'((n^-)^-)$.

Ekkor a $\mathbf{g}$ függvény által rekurzióval meghatározott $\mathbf{s}$ sorozat olyan, hogy

$$\mathbf{s}(0) = \mathbf{g}(\mathbf{s}|_0) = \mathbf{g}(\emptyset) := a,$$
$$\mathbf{s}(1) = \mathbf{g}(\mathbf{s}|_1) := b,$$

továbbá, minden $n \in \mathbb{N}$ esetén, ha $n \neq 0$ és $n \neq 1$, akkor

$$\mathbf{s}(n) = \mathbf{g}(\mathbf{s}|_n) = (\mathbf{s}|_n)(n^-) + (\mathbf{s}|_n)((n^-)^-) = \mathbf{s}(n^-) + \mathbf{s}((n^-)^-).$$

Ezt az $\mathbf{s}$ sorozatot (a, b)-kezdeti feltételű **Fibonacci-sorozatnak** nevezzük. Mutassuk meg, hogy ha $a \in \mathbb{N}^*$, akkor az (a, a) kezdeti feltételű Fibonacci-sorozat nem értelmezhető iterációval, de értelmezhető egyszerű rekurzióval.

8. fejezet

Véges halmazok és véges műveletek

8.1. Véges halmaz számossága

8.1.1. Definíció. *Azt mondjuk, hogy a E halmaz*

- **véges***, ha létezik olyan $n \in \mathbb{N}$, hogy E és n ekvipotensek;*
- **végtelen***, ha nem véges, vagyis minden $n \in \mathbb{N}$ számra E és n nem ekvipotensek.*

A definíció alapján nyilvánvaló, hogy véges (illetve végtelen) halmazzal ekvipotens halmaz szükségképpen véges (illetve végtelen) halmaz.

A véges halmazok *számosságának* bevezetéséhez szükséges a következő állítás.

8.1.2. Állítás. *Ha $n \in \mathbb{N}$, akkor nem létezik olyan $H \subseteq n$ halmaz, amelyre $H \neq n$ és H ekvipotens n-nel.* (*Tehát egyetlen természetes szám sem ekvipotens egyetlen valódi részhalmazával sem.*)

Bizonyítás. Teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén, minden $H \subseteq n$ halmazra, ha $H \neq n$, akkor H nem ekvipotens n-nel. Ez igaz az $n := 0$ számra, mert a $0 = \emptyset$ halmaznak nincs nem üres részhalmaza. Legyen $n \in \mathbb{N}$ olyan, hogy minden $H \subseteq n$ halmazra, ha $H \neq n$, akkor H nem ekvipotens n-nel. Azt kell igazolni, hogy minden $H \subseteq n^+$ halmazra, ha $H \neq n^+$, akkor H nem ekvipotens n^+-szal.

Indirekt tegyük fel, hogy $H \subseteq n^+$ olyan, hogy $H \neq n^+$, de H ekvipotens n^+-szal; ebből ellentmondásra fogunk jutni. Ehhez jelöljön f egy $n^+ \to H$ bijekciót!

(I) Először tegyük fel, hogy $n \notin H$; ekkor a $H \subseteq n^+$ feltevés szerint $H \subseteq n$ teljesül. Ha $k \in n$, akkor $k \neq n$, így az f injektivitása folytán $f(k) \neq f(n)$, vagyis $f(k) \in H \setminus \{f(n)\}$. Ekkor az $f|_n : n \to H \setminus \{f(n)\}$ függvény injektív (mert injekció leszűkítése injekció), továbbá szürjektív is, mert $m \in H \setminus \{f(n)\}$ esetén az f szürjektivitása következtében van olyan $k \in n^+$, hogy $f(k) = m$; ekkor $k = n$ lehetetlen, különben $f(n) = f(k) = m \in H \setminus \{f(n)\}$, ami lehetetlen; ezért $k \in n$, így $f|_n(k) = f(k) = m$. Természetesen $H \setminus \{f(n)\}$ valódi részhalmaza H-nak, hiszen $f(n) \in H$. Tehát $H \setminus \{f(n)\}$ olyan valódi részhalmaza n-nek, amely az $f|_n$ függvény által ekvipotens n-nel. Ez ellentmond az indukciós hipotézisnek, tehát az $n \notin H$ feltevés helytelen.

(II) Tegyük fel, hogy $n \in H$. Ekkor $H \setminus \{n\}$ valódi részhalmaza n-nek, különben $H = (H \setminus \{n\}) \cup \{n\} = n \cup \{n\} = n^+$, holott $H \neq n^+$.

Két eset lehetséges: $f(n) = n$ vagy $f(n) \neq n$.

Ha $f(n) = n$, akkor $k \in n$ esetén $k \neq n$, így az f injektivitása folytán $f(k) \neq f(n) = n$, vagyis $f(k) \in H \setminus \{n\}$. Ekkor az $f|_n : n \to H \setminus \{n\}$ függvény bijekció az n és $H \setminus \{n\}$

halmazok között. Valóban, az $f|_n$ függvény injektív, és ráképez $H \setminus \{n\}$-re, hiszen ha $m \in H \setminus \{n\}$, akkor az f szürjektivitása folytán létezik olyan $k \in n^+$, hogy $f(k) = m$; ekkor $k \neq n$, különben $n = f(n) = f(k) = m$ teljesülne, holott $m \neq n$, így $k \in n$, tehát $f|_n(k) = f(k) = m$. Azonban az indukciós hipotézis szerint nem létezhet bijekció n és $H \setminus \{n\}$ között.

Az előző ellentmondás azt mutatja, hogy szükségképpen $f(n) \neq n$ teljesül. Ugyanakkor $n \in H = \mathrm{Im}(f)$, ezért létezik (egyetlen) olyan $k \in n^+$, amelyre $f(k) = n$. Ekkor $k \neq n$, különben $n = f(k) = f(n)$ teljesülne, holott a hipotézis szerint $f(n) \neq n$. Ezért $k \in n$ teljesül. Minden $j \in n$ számra, ha $j \neq k$, akkor $f(j) \neq f(k) = n$, vagyis $f(j) \in H \setminus \{n\}$. Továbbá, az $f(n) \neq n$ feltevés alapján $f(n) \in H \setminus \{n\}$ is teljesül. Legyen most $f' : n \to H \setminus \{n\}$ az a függvény, amelyre minden $j \in n$ esetén

$$f'(j) = \begin{cases} f(j) & \text{, ha } j \neq k \\ f(n) & \text{, ha } j = k \end{cases}$$

teljesül. Nyilvánvaló, hogy f' bijekció az n és $H \setminus \{n\}$ halmazok között, és $H \setminus \{n\}$ valódi részhalmaza n-nek. Ez ellentmond az indukciós hipotézisnek.

Ebből az következik, hogy minden $H \subseteq n^+$ halmazra, ha $H \neq n^+$, akkor H nem ekvipotens n^+-szal, amivel a teljes indukciót végrehajtottuk. ■

8.1.3. Következmény. *Véges halmaz nem ekvipotens egyetlen valódi részhalmazával sem.*

Bizonyítás. Legyen E véges halmaz, és $n \in \mathbb{N}$ olyan, hogy E ekvipotens n-nel. Legyen $f : E \to n$ bijekció, és vegyünk egy $H \subseteq E$ halmazt, amelyre $H \neq E$. Ekkor $f\langle H \rangle \subseteq n$ olyan halmaz, hogy $f\langle H \rangle \neq n$, így 8.1.2. alapján $f\langle H \rangle$ nem ekvipotens n-nel, így E-vel sem ekvipotens. Világos, hogy az $f|_H$ leszűkített függvény bijekció H és $f\langle H \rangle$ között, ezért H és $f\langle H \rangle$ ekvipotensek. Ebből következik, hogy H nem ekvipotens E-vel. ■

8.1.4. Tétel. *Minden E véges halmazhoz egyértelműen létezik olyan $n \in \mathbb{N}$, amelyre E ekvipotens n-nel.*

Bizonyítás. Legyenek $m, n \in \mathbb{N}$ olyanok, hogy m és n ekvipotensek E-vel; ekkor m és n ekvipotensek. Ha $m \neq n$, akkor m valódi részhalmaza n-nek (amellyel n ekvipotens), vagy n valódi részhalmaza m-nek (amellyel m ekvipotens). A 8.1.2. állítás szerint mindkét eset lehetetlen, ezért $m = n$. ■

8.1.5. Definíció. *Az E véges halmaz* **számosságának** *nevezzük azt az egyértelműen meghatározott $n \in \mathbb{N}$ természetes számot, amelyre teljesül az, hogy E ekvipotens n-nel; ezt az n számot a $\mathrm{Card}(E)$ szimbólummal jelöljük.*

A definíció szerint minden $n \in \mathbb{N}$ esetén $\mathrm{Card}(n) = n$, hiszen n ekvipotens n-nel. Speciálisan: $\mathrm{Card}(\emptyset) = 0$ is teljesül. Továbbá, minden $\mathfrak{a}$ halmazra, $\mathrm{Card}(\{\mathfrak{a}\}) = 1$, mert az $\{\mathfrak{a}\}$ és $\{\emptyset\}$ halmazok közötti egyetlen függvény nyilvánvalóan bijekció, és $1 = \{\emptyset\}$. Továbbá, minden $\mathfrak{a}$ és $\mathfrak{b}$ halmazra, ha $\mathfrak{a} \neq \mathfrak{b}$, akkor $\mathrm{Card}(\{\mathfrak{a}, \mathfrak{b}\}) = 2$, mert az

$$f : \{\mathfrak{a}, \mathfrak{b}\} \to \{\emptyset, \{\emptyset\}\} \quad x \mapsto \begin{cases} \emptyset & \text{, ha } x = \mathfrak{a}; \\ \{\emptyset\} & \text{, ha } x = \mathfrak{b} \end{cases}$$

függvény nyilvánvalóan bijekció, és $2 = \{\emptyset, \{\emptyset\}\}$.

A következő tétel megvilágítja a véges halmazokra bevezetett Card *számosságoperáció* alaptulajdonságát.

8.1.6. Tétel. *Az E és F véges halmazok akkor és csak akkor ekvipotensek, ha* $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Bizonyítás. Ha E és F ekvipotensek, akkor F ekvipotens $\mathrm{Card}(F)$-fel (definíció szerint), és F ekvipotens $\mathrm{Card}(E)$-vel is, mert F ekvipotens E-vel, hiszen az ekvipotencia szimmetrikus (6.5.2. b) pont), továbbá E ekvipotens $\mathrm{Card}(E)$-vel, és az ekvipotencia tranzitív (6.5.2. c) pont). Ezért 8.1.4. alapján $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Megfordítva, a definíció szerint E ekvipotens $\mathrm{Card}(E)$-vel, és $\mathrm{Card}(F)$ ekvipotens F-fel, ezért $\mathrm{Card}(E) = \mathrm{Card}(F)$ esetén E ekvipotens F-fel, hiszen az ekvipotencia tranzitív (6.5.2. c) pont). ■

8.1.7. Tétel. *Az* $\mathbb{N}$ *halmaz végtelen és* $\mathbb{N} \notin \mathbb{N}$.

Bizonyítás. Létezik $\mathbb{N}$-nek olyan valódi részhalmaza, amely $\mathbb{N}$-nel ekvipotens. Például az $\mathbb{N} \to \mathbb{N}$; $n \mapsto n^+$ leképezés injekció és az értékkészlete egyenlő $\mathbb{N}^*$-gal, így $\mathbb{N}$ és $\mathbb{N}^*$ ekvipotensek. Ezért 8.1.3. szerint $\mathbb{N}$ nem lehet véges halmaz. Ha $\mathbb{N} \in \mathbb{N}$ teljesülne, akkor $\mathbb{N}$ ekvipotens volna egy természetes számmal, tehát $\mathbb{N}$ véges volna. Ebből következik, hogy $\mathbb{N} \notin \mathbb{N}$. ■

Az előző tétel szerint *létezik* végtelen halmaz, és látható, hogy végtelen halmaz létezése a végtelenségi axiómából következik. Ez indokolja a "végtelenségi" axióma elnevezést.

8.1.8. Állítás. *Ha E véges halmaz és $H \subseteq E$, akkor H is véges és* $\mathrm{Card}(H) \leq \mathrm{Card}(E)$. *Minden olyan halmaz végtelen, amely tartalmaz végtelen részhalmazt.*

Bizonyítás. A második állítás következik az elsőből. Az első bizonyításához először azt mutatjuk meg, hogy az

$$N := \{n \in \mathbb{N} | (\forall H \subseteq n)(\exists m \in \mathbb{N})((m \leq n) \wedge (m \text{ és } H \text{ ekvipotensek}))\}$$

halmaz egyenlő $\mathbb{N}$-nel. Világos, hogy $0 \in N$. Tegyük fel, hogy $n \in N$; megmutatjuk, hogy ekkor $n^+ \in N$. Ehhez legyen $H \subseteq n^+$ tetszőleges; olyan $m \in \mathbb{N}$ számot keresünk, amely ekvipotens H-val és amelyre $m \leq n^+$ teljesül. Ha $n \notin H$, akkor $H \subseteq n$, így az $n \in N$ hipotézis alapján van olyan $m \in \mathbb{N}$, amely ekvipotens H-val és amelyre $m \leq n$ teljesül, tehát $m \leq n^+$ is igaz. Ezért tegyük fel, hogy $n \in H$; ekkor $H \setminus \{n\} \subseteq n$, tehát az $n \in N$ hipotézis alapján van olyan $m \in \mathbb{N}$, amely ekvipotens $H \setminus \{n\}$-nel és amelyre $m \leq n$ teljesül. Legyen $f : m \to H \setminus \{n\}$ tetszőleges bijekció, és jelölje f' azt a függvényt, amely az m^+ halmazon értelmezett, f-nek kiterjesztése, és olyan, hogy $f'(m) := n$. Ekkor $f' : m^+ \to H$ bijekció és $m^+ \leq n^+$. Ez azt jelenti, hogy $n^+ \in N$ is igaz, így a teljes indukció elve alapján $N = \mathbb{N}$.
Legyen most E véges halmaz és $H \subseteq E$ tetszőleges halmaz. Ekkor E ekvipotens a $\mathrm{Card}(E) \in \mathbb{N}$ számmal; legyen $f : E \to \mathrm{Card}(E)$ tetszőleges bijekció. Ekkor az $f|_H$ függvény bijekció H és az $f\langle H\rangle \subseteq \mathrm{Card}(E)$ halmaz között. Az előzőek szerint van olyan $m \in \mathbb{N}$, amely ekvipotens $f\langle H\rangle$-val és amelyre $m \leq \mathrm{Card}(E)$ teljesül. Ekkor H és m ekvipotensek, tehát H véges és $\mathrm{Card}(H) = m \leq \mathrm{Card}(E)$. ■

8.1.9. Következmény. *Minden $E \subseteq \mathbb{N}$ véges halmazhoz létezik olyan $n \in \mathbb{N}$, hogy minden $k \in E$ esetén $k \leq n$ (vagyis E felülről korlátos* $\mathbb{N}$*-ben).*

Bizonyítás. Legyen $E \subseteq \mathbb{N}$ olyan halmaz, hogy

$$(\forall n \in \mathbb{N})(\exists k \in E) : k > n.$$

Megmutatjuk, hogy ekkor E végtelen halmaz. Valóban, minden $n \in \mathbb{N}$ esetén $\{k \in E | k > n\} \neq \emptyset$, és az $\mathbb{N}$ feletti természetes rendezés jólrendezés, ezért jól értelmezett az

$$f : \mathbb{N} \to \mathbb{N}; \quad n \mapsto \min(\{k \in E | k > n\})$$

függvény. A feltétel alapján nyilvánvaló, hogy az E halmaz nem üres. Legyen $e \in E$ rögzített elem, és jelölje σ az e kezdőpont és f függvény által meghatározott, $\mathbb{N}$-ben haladó iterációs sorozatot. Ekkor $n \in \mathbb{N}$ esetén $\sigma(n+1) = f(\mathbf{s}(n)) \in \{k \in E | k > \sigma(n)\}$, tehát $\sigma(n+1) \in E$ és $\sigma(n+1) > \sigma(n)$, vagyis $\sigma : \mathbb{N} \to \mathbb{N}$ szigorúan monoton növő sorozat, és $\operatorname{Im}(\sigma) \subseteq E$. A σ függvény bijekció $\mathbb{N}$ és $\operatorname{Im}(\sigma)$ közöt, így 8.1.7. alapján $\operatorname{Im}(\sigma)$ végtelen részhalmaza E-nek. Ezért 8.1.8.-ból kapjuk, hogy E végtelen halmaz. ■

8.1.10. Lemma. *Ha E véges halmaz és $\mathfrak{a}$ halmaz, akkor $E \cup \{\mathfrak{a}\}$ véges halmaz, és $\mathfrak{a} \notin E$ esetén*

$$\operatorname{Card}(E \cup \{\mathfrak{a}\}) = \operatorname{Card}(E) + 1.$$

Bizonyítás. Tegyük fel, hogy $\mathfrak{a} \notin E$. Legyen $n \in \mathbb{N}$ olyan, hogy E és n ekvipotensek, és rögzítsünk egy $f : E \to n$ bijekciót. Ekkor $\operatorname{Card}(E) = n$, és az

$$E \cup \{\mathfrak{a}\} \to n^+; \quad x \mapsto \begin{cases} f(x) & , \text{ha } x \in E; \\ n & , \text{ha } x = \mathfrak{a} \end{cases}$$

leképezés nyilvánvalóan bijekció, ezért $E \cup \{\mathfrak{a}\}$ véges halmaz és $\operatorname{Card}(E \cup \{\mathfrak{a}\}) = n^+ = \operatorname{Card}(E) + 1$. ■

A lemmából következik, hogy ha E véges halmaz és $\mathfrak{a} \in E$, akkor $\operatorname{Card}(E) = \operatorname{Card}(E \setminus \{\mathfrak{a}\}) + 1$, mert $E = (E \setminus \{\mathfrak{a}\}) \cup \{\mathfrak{a}\}$ és $\mathfrak{a} \notin E \setminus \{\mathfrak{a}\}$.

8.1.11. Állítás. *Ha f függvény, akkor minden $E \subseteq \operatorname{Dom}(f)$ véges halmazra $f\langle E\rangle$ véges halmaz és $\operatorname{Card}(f\langle E\rangle) \leq \operatorname{Card}(E)$, továbbá $\operatorname{Card}(f\langle E\rangle) = \operatorname{Card}(E)$ pontosan akkor teljesül, ha f injektív az E halmazon.*

Bizonyítás. Rögzített f függvény esetén az E halmaz számossága szerinti teljes indukcióval bizonyítunk.

Ha $E \subseteq \operatorname{Dom}(f)$ olyan véges halmaz, hogy $\operatorname{Card}(E) = 0$, akkor $E = \emptyset$, ezért $f\langle E\rangle = \emptyset$, tehát $f\langle E\rangle$ véges és $\operatorname{Card}(f\langle E\rangle) = 0 = \operatorname{Card}(E)$.

Legyen $n \in \mathbb{N}$ olyan, hogy az állítás igaz minden olyan $E \subseteq \operatorname{Dom}(f)$ véges halmazra, amelyre $\operatorname{Card}(E) = n$. Legyen $E \subseteq \operatorname{Dom}(f)$ olyan véges halmaz, amelyre $\operatorname{Card}(E) = n+1$, és rögzítsünk egy $x_* \in E$ elemet. Ekkor $E \setminus \{x_*\} \subseteq \operatorname{Dom}(f)$ véges halmaz és $\operatorname{Card}(E \setminus \{x_*\}) = n$, így az indukciós hipotézis alapján $f\langle E \setminus \{x_*\}\rangle$ véges halmaz és $\operatorname{Card}(f\langle E \setminus \{x_*\}\rangle) \leq n$, valamint $\operatorname{Card}(f\langle E \setminus \{x_*\}\rangle) = n$ pontosan akkor teljesül, ha f injektív az $E \setminus \{x_*\}$ halmazon. Nyilvánvaló, hogy

$$f\langle E\rangle = f\langle (E \setminus \{x_*\}) \cup \{x_*\}\rangle = f\langle E \setminus \{x_*\}\rangle \cup \{f(x_*)\},$$

ezért 8.1.10. alapján $f\langle E\rangle$ véges halmaz, és

– ha $f(x_*) \in f\langle E \setminus \{x_*\}\rangle$, akkor $f\langle E\rangle = f\langle E \setminus \{x_*\}\rangle$, tehát

$$\operatorname{Card}(f\langle E\rangle) = \operatorname{Card}(f\langle E \setminus \{x_*\}\rangle) \leq n < n+1 = \operatorname{Card}(E),$$

– ha $f(x_*) \notin f\langle E \setminus \{x_*\}\rangle$, akkor

$$\operatorname{Card}(f\langle E\rangle) = \operatorname{Card}(f\langle E \setminus \{x_*\}\rangle) + 1 \leq n+1 = \operatorname{Card}(E).$$

Ha f injektív az E halmazon, akkor az $E \setminus \{x_*\}$ halmazon is injektív, ezért az indukciós hipotézis alapján $\mathrm{Card}(f\langle E \setminus \{x_*\}\rangle) = n$, ugyanakkor $f(x_*) \in f\langle E \setminus \{x_*\}\rangle$, így $\mathrm{Card}(f\langle E\rangle) = n + 1 = \mathrm{Card}(E)$.

Ha f nem injektív az E halmazon, akkor

– $f(x_*) \in f\langle E \setminus \{x_*\}\rangle$ esetén $\mathrm{Card}(f\langle E\rangle) \leq n < n + 1 = \mathrm{Card}(E)$,

– $f(x_*) \notin f\langle E \setminus \{x_*\}\rangle$ esetén f szükségképpen nem injektív az $E \setminus \{x_*\}$ halmazon, így az indukciós hipotézis alapján $\mathrm{Card}(f\langle E \setminus \{x_*\}\rangle) < n$, következésképpen $\mathrm{Card}(f\langle E\rangle) = \mathrm{Card}(f\langle E \setminus \{x_*\}\rangle) + 1 < n + 1 = \mathrm{Card}(E)$.

Tehát $\mathrm{Card}(f\langle E\rangle) = \mathrm{Card}(E)$ pontosan akkor teljesül, ha f injektív az E halmazon. ■

8.1.12. Állítás. *Ha E és F véges halmazok, akkor $E \cup F$ is véges, és*

$$\mathrm{Card}(E \cup F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(E) + \mathrm{Card}(F).$$

Bizonyítás. Rögzítve az E véges halmazt, az F véges halmaz számossága szerinti teljes indukcióval bizonyítunk, tehát azt mutatjuk meg, hogy minden $n \in \mathbb{N}$ számra és minden F véges halmazra, ha $\mathrm{Card}(F) = n$, akkor $E \cup F$ véges halmaz és fennáll a $\mathrm{Card}(E \cup F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(E) + \mathrm{Card}(F)$ egyenlőség.

Ha $n = 0$ és F olyan véges halmaz, hogy $\mathrm{Card}(F) = 0$, akkor $F = \emptyset$, ezért $E \cup F = E$ véges halmaz és $E \cap F = \emptyset$, így a bizonyítandó egyenlőség triviálisan teljesül.

Legyen $n \in \mathbb{N}$ olyan, amelyre teljesül az állítás, és vegyünk egy F véges halmazt, amelyre $\mathrm{Card}(F) = n^+$. Azt kell megmutatni, hogy $E \cup F$ véges halmaz és teljesül a $\mathrm{Card}(E \cup F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(E) + \mathrm{Card}(F)$ egyenlőség.

Legyen $f : n^+ \to F$ bijekció. Ekkor az $f|_n$ leszűkített függvény bijekció az n és az $F' := F \setminus \{f(n)\}$ halmazok között, így az indukciós hipotézist alkalmazva az F' halmazra kapjuk, hogy $E \cup F'$ véges halmaz, és

$$\mathrm{Card}(E \cup F') + \mathrm{Card}(E \cap F') = \mathrm{Card}(E) + \mathrm{Card}(F') = \mathrm{Card}(E) + n.$$

Mindkét oldalhoz hozzáadva 1-et kapjuk, hogy

$$\mathrm{Card}(E \cup F') + \mathrm{Card}(E \cap F') + 1 = \mathrm{Card}(E) + n^+ = \mathrm{Card}(E) + \mathrm{Card}(F).$$

Nyilvánvaló, hogy $E \cap F' := E \cap (F \setminus \{f(n)\}) = (E \cap F) \setminus \{f(n)\}$.

Tegyük fel, hogy $f(n) \in E$. Ekkor $f(n) \in E \cap F$, így $E \cup F = E \cup F'$, tehát $E \cup F$ véges halmaz, és $\mathrm{Card}(E \cup F) = \mathrm{Card}(E \cup F')$. Továbbá, az 8.1.10. lemma után álló megjegyzés szerint $\mathrm{Card}(E \cap F) = \mathrm{Card}((E \cap F) \setminus \{f(n)\}) + 1 = \mathrm{Card}(E \cap F') + 1$, tehát fennáll az $\mathrm{Card}(E \cup F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(E) + \mathrm{Card}(F)$ egyenlőség.

Tegyük fel, hogy $f(n) \notin E$. Ekkor $E \cap F = E \cap F'$ és $E \cup F = (E \cup F') \cup \{f(n)\}$. Mivel $f(n) \notin E \cup F'$, így 8.1.10. szerint $E \cup F$ véges halmaz és $\mathrm{Card}(E \cup F) = \mathrm{Card}(E \cup F') + 1$, tehát fennáll az $\mathrm{Card}(E \cup F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(E) + \mathrm{Card}(F)$ egyenlőség.

Ezzel megmutattuk, hogy $E \cup F$ véges halmaz, és $\mathrm{Card}(E \cup F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(E) + \mathrm{Card}(F)$, amivel az állítást igazoltuk. ■

8.1.13. Következmény. *Ha $(E_i)_{i \in I}$ olyan halmazrendszer, hogy I véges és minden $i \in I$ esetén E_i véges, akkor $\bigcup_{i \in I} E_i$ is véges halmaz. (Vagyis véges sok véges halmaz uniója véges.)*

Bizonyítás. Az állítást az I halmaz számossága szerinti teljes indukcióval igazoljuk. Ha $\mathrm{Card}(I) = 0$, akkor $I = \emptyset$, ezért $\bigcup_{i\in I} E_i = \emptyset$ is véges halmaz. Legyen $n \in \mathbb{N}$ olyan, hogy az állítás igaz minden olyan I esetén, amelyre $\mathrm{Card}(I) = n$.

Legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy I véges, $\mathrm{Card}(I) = n + 1$, és minden $i \in I$ esetén E_i véges halmaz. Legyen $i_* \in I$ rögzített elem és $I_* := I \setminus \{i_*\}$. Ekkor

$$\bigcup_{i\in I} E_i = \bigcup_{i\in I_*\cup\{i_*\}} E_i = \Big(\bigcup_{i\in I_*} E_i\Big) \cup E_{i_*},$$

és mivel $\mathrm{Card}(I_*) = n$, így az indukciós hipotézis alapján $\bigcup_{i\in I_*} E_i$ véges halmaz, tehát a 8.1.12. állítást alkalmazva az $E := \bigcup_{i\in I_*} E_i$ és $F := E_{i_*}$ véges halmazokra kapjuk, hogy $\bigcup_{i\in I} E_i$ véges halmaz. ■

8.1.14. Következmény. *Ha E és F diszjunkt véges halmazok, akkor $E \cup F$ is véges, és*

$$\mathrm{Card}(E \cup F) = \mathrm{Card}(E) + \mathrm{Card}(F).$$

Bizonyítás. Világos, hogy $\mathrm{Card}(E \cap F) = \mathrm{Card}(\emptyset) = 0$, így az állítás azonnal következik 8.1.12.-ből. ■

8.1.15. Következmény. *Ha E véges halmaz és $H \subseteq E$, akkor*

$$\mathrm{Card}(E \setminus H) = \mathrm{Card}(E) \dot{-} \mathrm{Card}(H),$$

és $\mathrm{Card}(H) = \mathrm{Card}(E)$ *esetén* $H = E$.

Bizonyítás. Világos, hogy $E = H \cup (E \setminus H)$, továbbá a H és $E \setminus H$ halmazok végesek és diszjunktak, így 8.1.14. alapján $\mathrm{Card}(E) = \mathrm{Card}(H) + \mathrm{Card}(E \setminus H)$. Továbbá, $\mathrm{Card}(H) \le \mathrm{Card}(E)$ (8.1.8.), így az $\mathbb{N}$-ben értelmezett különbség definíciója (7.9.7.) szerint $\mathrm{Card}(E \setminus H) = \mathrm{Card}(E) \dot{-} \mathrm{Card}(H)$.

Ebből következik, hogy $\mathrm{Card}(H) = \mathrm{Card}(E)$ esetén $\mathrm{Card}(E \setminus H) = 0$, tehát $E \setminus H = \emptyset$, következésképpen $E = H \cup (E \setminus H) = H$. ■

8.1.16. Tétel. *Ha E és F olyan véges halmazok, hogy* $\mathrm{Card}(E) = \mathrm{Card}(F)$*, akkor minden $f : E \to F$ függvényre a következő állítások ekvivalensek.*

(i) *Az f függvény bijekció.*

(ii) *Az f függvény injekció.*

(iii) *Az f függvény szürjekció.*

Bizonyítás. (i)⇒(ii) Triviális.

(ii)⇒(iii) Tegyük fel, hogy f injekció. Ekkor E és $\mathrm{Im}(f)$ ekvipotens halmazok, tehát $\mathrm{Card}(E) = \mathrm{Card}(\mathrm{Im}(f))$. A 8.1.15. állítás szerint $\mathrm{Card}(F \setminus \mathrm{Im}(f)) = \mathrm{Card}(F) \dot{-} \mathrm{Card}(\mathrm{Im}(f))$, tehát $\mathrm{Card}(E) = \mathrm{Card}(F)$ miatt $F \setminus \mathrm{Im}(f) = \emptyset$, vagyis $\mathrm{Im}(f) = F$, azaz f szürjektív.

(iii)⇒(i) Tegyük fel, hogy f szürjekció. Ekkor vehetjük f-nek egy $g : F \to E$ jobbinverzét (6.8.1.). Ekkor g injekció, tehát F és $\mathrm{Im}(g)$ ekvipotens halmazok, így $\mathrm{Card}(F) =$

$\mathrm{Card}(\mathrm{Im}(g))$. A 8.1.15. állítás szerint $\mathrm{Card}(E \setminus \mathrm{Im}(g)) = \mathrm{Card}(E) \dot{-} \mathrm{Card}(\mathrm{Im}(g))$, tehát $\mathrm{Card}(E) = \mathrm{Card}(F)$ miatt $E \setminus \mathrm{Im}(g) = \emptyset$, vagyis $\mathrm{Im}(g) = E$, azaz g szürjektív. Ez azt jelenti, hogy $g : F \to E$ bijekció, tehát az $f \circ g = \mathrm{id}_F$ függvény-egyenlőséget jobbról komponálva g^{-1}-gyel kapjuk, hogy $f = g^{-1}$, tehát $f : E \to F$ bijekció. ■

8.1.17. Állítás. *Ha E és F véges halmazok, akkor $E \times F$ is véges, és*

$$\mathrm{Card}(E \times F) = \mathrm{Card}(E) \cdot \mathrm{Card}(F).$$

Bizonyítás. Rögzítve az E véges halmazt, az F véges halmaz számossága szerinti teljes indukcióval bizonyítunk, tehát azt mutatjuk meg, hogy minden $n \in \mathbb{N}$ számra és minden F véges halmazra, ha $\mathrm{Card}(F) = n$, akkor $E \times F$ véges halmaz és fennáll a $\mathrm{Card}(E \times F) = \mathrm{Card}(E) \cdot \mathrm{Card}(F)$ egyenlőség.

Ha $n = 0$ és F olyan véges halmaz, hogy $\mathrm{Card}(F) = n$, akkor $F = \emptyset$, ezért $E \times F = \emptyset$ véges halmaz, és a bizonyítandó egyenlőség triviálisan teljesül.

Legyen $n \in \mathbb{N}$ olyan, amelyre teljesül az állítás, és vegyünk egy F véges halmazt, amelyre $\mathrm{Card}(F) = n^+$. Azt kell megmutatni, hogy $E \times F$ véges halmaz és teljesül a $\mathrm{Card}(E \times F) = \mathrm{Card}(E) \cdot \mathrm{Card}(F)$ egyenlőség.

Legyen $f : n^+ \to F$ bijekció. Ekkor az $f|_n$ leszűkített függvény bijekció az n és az $F' := F \setminus \{f(n)\}$ halmazok között, így az indukciós hipotézist alkalmazva az F' halmazra kapjuk, hogy $E \times F'$ véges halmaz, és

$$\mathrm{Card}(E \times F') = \mathrm{Card}(E) \cdot \mathrm{Card}(F') = \mathrm{Card}(E) \cdot n.$$

Nyilvánvaló, hogy

$$E \times F = (E \times F') \cup (E \times \{f(n)\}),$$

és itt a jobb oldalon diszjunkt halmazok állnak. Az $E \to E \times \{f(n)\}$; $x \mapsto (x, f(n))$ leképezés bijekció, ezért $E \times \{f(n)\}$ véges halmaz és $\mathrm{Card}(E \times \{f(n)\}) = \mathrm{Card}(E)$. Most alkalmazzuk a 8.1.14. állítást az $E \times F'$ és $E \times \{f(n)\}$ diszjunkt véges halmazokra. Azt kapjuk, hogy $E \times F$ véges és

$$\begin{aligned} \mathrm{Card}(E \times F) &= \mathrm{Card}(E \times F') + \mathrm{Card}(E \times \{f(n)\}) = \\ &= \mathrm{Card}(E) \cdot n + \mathrm{Card}(E) = \mathrm{Card}(E) \cdot n^+ = \mathrm{Card}(E) \cdot \mathrm{Card}(F), \end{aligned}$$

ahol felhasználtuk a természetes számok szorzásának iteratív definícióját. ■

8.1.18. Következmény. *Ha $(E_i)_{i \in I}$ olyan halmazrendszer, hogy I véges halmaz, és minden $i \in I$ esetén E_i véges, akkor $\prod_{i \in I} E_i$ is véges halmaz. (Vagyis véges sok véges halmaz szorzata véges.)*

Bizonyítás. Az I halmaz számossága szerinti teljes indukcióval bizonyítunk.

Ha $\mathrm{Card}(I) = 0$, akkor $I = \emptyset$, így a szorzathalmaz definíciója alapján $\prod_{i \in I} E_i = \{\emptyset\}$ véges halmaz.

Tegyük fel, hogy $n \in \mathbb{N}$ olyan, hogy az állítás igaz minden olyan I esetén, amelyre $\mathrm{Card}(I) = n$.

Legyen I olyan véges indexhalmaz, hogy $\mathrm{Card}(I) = n + 1$. Rögzítsünk egy $i_* \in I$ elemet és legyen $I_* := I \setminus \{i_*\}$. Ekkor a

$$\prod_{i \in I} E_i \to \Big(\prod_{i \in I_*} E_i\Big) \times E_{i_*}; \quad f \mapsto (f|_{I_*}, f(i_*))$$

leképezés bijekció, és $\mathrm{Card}(I_*) = n$ miatt az indukciós hipotézis szerint $\prod_{i \in I_*} E_i$ véges halmaz, tehát 8.1.17. alapján a $\left(\prod_{i \in I_*} E_i\right) \times E_{i_*}$ szorzathalmaz véges. Ezért az ezzel ekvipotens $\prod_{i \in I} E_i$ szorzathalmaz is véges. ■

8.1.19. Állítás. *Ha $(E_i)_{i \in I}$ olyan halmazrendszer, hogy I véges halmaz és minden $i \in I$ esetén $E_i \neq \emptyset$, akkor $\prod_{i \in I} E_i \neq \emptyset$.*

Bizonyítás. Az I halmaz számossága szerinti teljes indukcióval bizonyítunk.

Ha $\mathrm{Card}(I) = 0$, akkor $I = \emptyset$, így a szorzathalmaz definíciója alapján $\prod_{i \in I} E_i = \{\emptyset\} \neq \emptyset$.

Tegyük fel, hogy $n \in \mathbb{N}$ olyan, hogy az állítás igaz minden olyan I esetén, amelyre $\mathrm{Card}(I) = n$.

Legyen I olyan véges indexhalmaz, hogy $\mathrm{Card}(I) = n + 1$. Rögzítsünk egy $i_* \in I$ elemet és legyen $I_* := I \setminus \{i_*\}$. Ekkor a

$$\prod_{i \in I} E_i \to \left(\prod_{i \in I_*} E_i\right) \times E_{i_*}; \quad f \mapsto (f|_{I_*}, f(i_*))$$

leképezés bijekció, és $\mathrm{Card}(I_*) = n$ miatt az indukciós hipotézis alapján $\prod_{i \in I_*} E_i \neq \emptyset$, tehát $E_{i_*} \neq \emptyset$ következtében a $\left(\prod_{i \in I_*} E_i\right) \times E_{i_*}$ szorzathalmaz sem üres. Ezért az ezzel ekvipotens $\prod_{i \in I} E_i$ szorzathalmaz sem üres. ■

8.1.20. Állítás. *Legyen $(E_i)_{i \in I}$ olyan halmazrendszer, hogy minden $i, j \in I$ esetén $E_i \subseteq E_j$ vagy $E_j \subseteq E_i$.*

a) *Minden $J \subseteq I$ nem üres véges halmazhoz van olyan $i \in I$, hogy $\bigcup_{j \in J} E_j \subseteq E_i$.*

b) *Minden $X \subseteq \bigcup_{i \in I} E_i$ nem üres véges halmazhoz van olyan $i \in I$, hogy $X \subseteq E_i$.*

Bizonyítás. a) A $J \subseteq I$ nem üres véges halmaz számossága szerinti teljes indukcióval bizonyítunk.

Ha $\mathrm{Card}(J) = 1$, akkor $j_* \in J$ esetén $i := j_* \in I$ olyan index, hogy $\bigcup_{j \in J} E_j = E_{j_*} = E_i$, tehát az állítás igaz.

Legyen $n \in \mathbb{N}^*$ olyan természetes szám, hogy az állítás igaz minden olyan $J \subseteq I$ véges halmazra, amelyre $\mathrm{Card}(J) = n$. Rögzítsünk egy $J \subseteq I$ véges halmazt, amelyre $\mathrm{Card}(J) = n^+$ és legyen $j_* \in J$. Ekkor $\mathrm{Card}(J \setminus \{j_*\}) = n$, így az indukciós hipotézis alapján van olyan $i_* \in I$, amelyre $\bigcup_{j \in J \setminus \{j_*\}} E_j \subseteq E_{i_*}$. Az $(E_i)_{i \in I}$ halmazrendszerre vonatkozó hipotézis alapján $E_{i_*} \subseteq E_{j_*}$ vagy $E_{j_*} \subseteq E_{i_*}$. Legyen $i := j_*$, ha $E_{i_*} \subseteq E_{j_*}$, és $i := i_*$, ha $E_{j_*} \subseteq E_{i_*}$. Ekkor $E_{j_*} \cup E_{i_*} \subseteq L_i$, következésképpen

$$\bigcup_{j \in J} E_j = E_{j_*} \cup \Big(\bigcup_{j \in J \setminus \{j_*\}} E_j\Big) \subseteq E_{j_*} \cup E_{i_*} \subseteq E_i,$$

tehát az állítás igaz n^+-ra.

b) Az a) állítás alapján elég azt igazolni, hogy létezik olyan $I_* \subseteq I$ véges halmaz, amelyre $X \subseteq \bigcup\limits_{i \in I_*} E_i$. Ehhez tekintsük az

$$X \to \mathscr{P}(I); \quad x \mapsto \{i \in I | x \in E_i\}$$

függvényt. Mivel $X \subseteq \bigcup\limits_{i \in I} E_i$, így minden $x \in X$ esetén $\{i \in I | x \in E_i\} \neq \emptyset$, következésképpen $\prod\limits_{x \in X} \{i \in I | x \in E_i\} \neq \emptyset$. (Ehhez még a kiválasztási axiómára sincs szükség, mert X véges, így elég a 8.1.19. állításra hivatkozni.) Legyen $\iota \in \prod\limits_{x \in X} \{i \in I | x \in E_i\}$. Ekkor $\iota : X \to I$ olyan függvény, hogy minden $x \in X$ esetén $x \in E_{\iota(x)}$, tehát $X \subseteq \bigcup\limits_{i \in \mathrm{Im}(\iota)} E_i$, így az $I_* := \mathrm{Im}(\iota) \subseteq I$ véges halmaz (8.1.11.) eleget tesz a követelménynek. ■

8.1.21. Állítás. *Ha E és F véges halmazok, akkor az $E \to F$ függvények $\mathscr{F}(E; F)$ halmaza véges, és*

$$\mathrm{Card}(\mathscr{F}(E; F)) = (\mathrm{Card}(F))^{\mathrm{Card}(E)}.$$

Bizonyítás. Rögzítve az F véges halmazt, az E véges halmaz számossága szerinti teljes indukcióval bizonyítunk, tehát azt mutatjuk meg, hogy minden $n \in \mathbb{N}$ számra és minden E véges halmazra, ha $\mathrm{Card}(E) = n$, akkor $\mathscr{F}(E; F)$ véges halmaz, és $\mathrm{Card}(\mathscr{F}(E; F)) = (\mathrm{Card}(F))^{\mathrm{Card}(E)}$.

Ha $n = 0$, akkor a hatványozás értelmezése alapján $(\mathrm{Card}(F))^{\mathrm{Card}(E)} = (\mathrm{Card}(F))^0 = 1$. Ugyanakkor, $\mathscr{F}(E; F) = \mathscr{F}(\emptyset; F) = \{\emptyset\}$, tehát $\mathscr{F}(E; F)$ véges halmaz, és fennállnak a $\mathrm{Card}(\mathscr{F}(E; F)) = 1 = (\mathrm{Card}(F))^{\mathrm{Card}(E)}$ egyenlőségek.

Legyen $n \in \mathbb{N}$ olyan, amelyre teljesül az állítás, és vegyünk egy E véges halmazt, amelyre $\mathrm{Card}(E) = n^+$. Azt kell megmutatni, hogy $\mathscr{F}(E; F)$ véges halmaz, és $\mathrm{Card}(\mathscr{F}(E; F)) = (\mathrm{Card}(F))^{\mathrm{Card}(E)}$.

Legyen $f : n^+ \to E$ bijekció. Ekkor az $f|_n$ leszűkített függvény bijekció az n és az $E' := E \setminus \{f(n)\}$ halmazok között, így az indukciós hipotézist alkalmazva az E' halmazra kapjuk, hogy $\mathscr{F}(E'; F)$ véges halmaz, és

$$\mathrm{Card}(\mathscr{F}(E'; F)) = (\mathrm{Card}(F))^{\mathrm{Card}(E')}.$$

Nyilvánvaló, hogy az

$$\mathscr{F}(E; F) \to \mathscr{F}(E'; F) \times F; \quad g \mapsto (g|_{E'}, g(f(n)))$$

leképezés bijekció, és 8.1.17. alapján $\mathscr{F}(E'; F) \times F$ véges halmaz, valamint

$$\mathrm{Card}(\mathscr{F}(E'; F) \times F) = \mathrm{Card}(\mathscr{F}(E'; F)) \cdot \mathrm{Card}(F) =$$
$$= (\mathrm{Card}(F))^{\mathrm{Card}(E')} \cdot \mathrm{Card}(F) = (\mathrm{Card}(F))^{\mathrm{Card}(E')+1} = (\mathrm{Card}(F))^{\mathrm{Card}(E)},$$

ahol felhasználtuk a természetes számok hatványozásának iteratív definícióját. Ezért $\mathscr{F}(E; F)$ véges halmaz, és

$$\mathrm{Card}(\mathscr{F}(E; F)) = \mathrm{Card}(\mathscr{F}(E'; F) \times F) = (\mathrm{Card}(F))^{\mathrm{Card}(E)}. \blacksquare$$

Az előző állítás megvilágítja azt, hogy ha E és F halmazok, akkor miért jelöljük az $\mathscr{F}(E;F)$ függvényhalmazt F^E-vel. Ugyanis, ha E és F véges halmazok, akkor ezzel a jelöléssel, 8.1.21. alapján írhatjuk, hogy

$$\mathrm{Card}(F^E) = \mathrm{Card}(F)^{\mathrm{Card}(E)}.$$

8.1.22. Következmény. *Ha E véges halmaz, akkor a $\mathscr{P}(E)$ hatványhalmaz is véges, és*

$$\mathrm{Card}(\mathscr{P}(E)) = 2^{\mathrm{Card}(E)}.$$

Bizonyítás. Tudjuk, hogy $2 := \{0,1\}$, és a

$$\mathscr{P}(E) \to \mathscr{F}(E;2); \quad H \mapsto \chi_H$$

leképezés bijekció (még akkor is, ha E nem véges), ezért az állítás azonnal következik a 8.1.21. állításból. ■

8.2. Rendezett véges halmazok

8.2.1. Állítás. *Minden véges halmaz felett létezik lineáris rendezés.*

Bizonyítás. Ha E véges halmaz és $n \in \mathbb{N}$ olyan természetes szám, hogy E és n ekvipotensek, akkor véve egy $f : E \to n$ bijekciót, az $f_*(\leq_n)$ reláció lineáris rendezés E felett (6.10.4. és 6.10.5.). ■

8.2.2. Állítás. *Legyen $(E, \leq)$ rendezett halmaz. Ekkor E minden nem üres véges részhalmazának létezik $\leq$ szerint minimális és létezik $\leq$ szerint maximális eleme.*

Bizonyítás. Az $X \subseteq E$ nem üres véges halmaz számossága szerinti teljes indukcióval bizonyítunk. Ha $\mathrm{Card}(X) = 1$, akkor az állítás nyilvánvaló. Legyen $n \in \mathbb{N}^*$ olyan, hogy az állítás az E minden n számosságú részhalmazára igaz, és legyen $X \subseteq E$ olyan véges halmaz, hogy $\mathrm{Card}(X) = n+1$. Rögzítsünk egy $x_* \in X$ elemet és legyen $X_* := X \setminus \{x_*\}$. Ekkor $X_* \subseteq E$ olyan véges halmaz, hogy $\mathrm{Card}(X_*) = n$, így az indukciós hipotézis miatt léteznek olyan $\underline{x}, \overline{x} \in X_*$ elemek, hogy $\underline{x}$ minimális és $\overline{x}$ maximális eleme X_*-nak.

Ha $\underline{x}$ és x_* nem összehasonlíthatóak a $\leq$ rendezés szerint, akkor minden $x \in X$ elemre: $x \leq \underline{x}$ esetén $x \neq x_*$, tehát $x \in X_*$, így $x = \underline{x}$, tehát $\underline{x}$ minimális eleme X-nek. Ha $\underline{x}$ és x_* összehasonlíthatóak a $\leq$ rendezés szerint, akkor két eset lehetséges.

– Ha $\underline{x} \leq x_*$, akkor $x \in X_*$ és $x \leq \underline{x}$ esetén $\underline{x} = x$, míg $x_* \leq \underline{x}$ esetén a $\leq$ reláció antiszimmetrikussága folytán $\underline{x} = x_*$, tehát $\underline{x}$ minimális eleme X-nek.

– Ha $x_* \leq \underline{x}$, akkor $x \in X_*$ és $x \leq x_*$ esetén $x \leq \underline{x}$, így $\underline{x} = x$, tehát $x_* \leq x$, vagyis a $\leq$ reláció antiszimmetrikussága folytán $x = x_*$, ezért x_* minimális eleme X-nek.

Ha $\overline{x}$ és x_* nem összehasonlíthatóak a $\leq$ rendezés szerint, akkor minden $x \in X$ elemre: $\overline{x} \leq x$ esetén $x \neq x_*$, tehát $x \in X_*$, így $x = \overline{x}$, tehát $\overline{x}$ maximális eleme X-nek. Ha $\overline{x}$ és x_* összehasonlíthatóak a $\leq$ rendezés szerint, akkor két eset lehetséges.

– Ha $x_* \leq \overline{x}$, akkor $x \in X_*$ és $\overline{x} \leq x$ esetén $\overline{x} = x$, míg $\overline{x} \leq x_*$ esetén a $\leq$ reláció antiszimmetrikussága folytán $\overline{x} = x_*$, tehát $\overline{x}$ maximális eleme X-nek.

– Ha $\overline{x} \leq x_*$, akkor $x \in X_*$ és $x_* \leq x$ esetén $\overline{x} \leq x$, így $\overline{x} = x$, tehát $x \leq x_*$, vagyis a $\leq$ reláció antiszimmetrikussága folytán $x = x_*$, ezért x_* maximális eleme X-nek. ■

8.2.3. Állítás. *Ha $(E, \leq)$ lineárisan rendezett halmaz és E véges, akkor $(E, \leq)$ jólrendezett halmaz, és E minden nem üres részhalmazának létezik legnagyobb eleme.*

Bizonyítás. Az állítást az E halmaz számossága szerinti teljes indukcióval bizonyítjuk. Ha $\mathrm{Card}(E) = 0$ vagy $\mathrm{Card}(E) = 1$, akkor az állítás nyilvánvalóan igaz. Legyen $n \in \mathbb{N}$ olyan, hogy az állítás igaz minden olyan véges lineárisan rendezett halmazra, amelynek alaphalmaza n számosságú, és rögzítsünk egy olyan $(E, \leq)$ véges lineárisan rendezett halmazt, amelyre és $\mathrm{Card}(E) = n + 1$. Legyen továbbá $X \subseteq E$ nem üres halmaz.

Legyen $\mathfrak{a} \in X$ rögzített elem, és képezzük az $E' := E \setminus \{\mathfrak{a}\}$ és $X' := X \setminus \{\mathfrak{a}\}$ halmazokat, továbbá jelölje $\leq'$ a $\leq$ rendezés megszorítását E'-re. Ha $X' = \emptyset$, akkor $X = \{\mathfrak{a}\}$, tehát $\mathfrak{a} = \min_{\leq}(X) = \max_{\leq}(X)$. Tegyük fel, hogy $X' \neq \emptyset$. Ekkor $(E', \leq')$ véges lineárisan rendezett halmaz, és $\mathrm{Card}\,(E') = n$, és $X' \subseteq E'$ nem üres halmaz, így indukciós hipotézist alkalmazva $(E', \leq')$-re és X'-re kapjuk olyan $x'_-, x'_+ \in X'$ elemek létezését, amelyekre minden $x \in X'$ esetén $x'_- \leq' x \leq' x'_+$, tehát $x'_- \leq x \leq x'_+$. Az $\mathfrak{a}$ és x'_- elemek összehasonlíthatók a $\leq$ rendezés szerint, és az $\mathfrak{a}$ és x'_+ elemek is összehasonlíthatók a $\leq$ rendezés szerint: itt használjuk ki azt, hogy a $\leq$ rendezés lineáris E felett. Legyen $x_- := \min_{\leq}(\mathfrak{a}, x'_-)$ és $x_+ := \max_{\leq}(\mathfrak{a}, x'_+)$. Világos, hogy ekkor minden $x \in X$ esetén $x_- \leq x \leq x_+$, vagyis $x_- = \min_{\leq}(X)$ és $x_+ = \max_{\leq}(X)$. ■

8.2.4. Állítás. *Ha $(E, \leq)$ lineárisan rendezett halmaz, E véges, és $n := \mathrm{Card}(E)$, akkor minden $f : n \to E$ bijekcióhoz létezik egyetlen olyan $\sigma : n \to n$ bijekció, amelyre az $f \circ \sigma : n \to E$ függvény szigorúan monoton növő a $\leq_n$ és $\leq$ rendezések szerint (vagy ami ugyanaz, $f \circ \sigma$ izomorfizmus az $(n, \leq_n)$ és $(E, \leq)$ jólrendezett halmazok között).*

Bizonyítás. Az állításban szereplő egyértelműség 6.13.10. nyilvánvaló következménye, mert az előző állítás szerint $(n, \leq_n)$ és $(E, \leq)$ jólrendezett halmazok.

Az állítást az E halmaz számossága szerinti teljes indukcióval bizonyítjuk. Ha $\mathrm{Card}(E) = 0$ vagy $\mathrm{Card}(E) = 1$, akkor az állítás nyilvánvalóan igaz. Legyen $n \in \mathbb{N}$ olyan, hogy az állítás igaz minden olyan véges lineárisan rendezett halmazra, amelynek alaphalmaza n számosságú, és rögzítsünk egy olyan $(E, \leq)$ véges lineárisan rendezett halmazt, amelyre és $\mathrm{Card}(E) = n + 1$ és legyen $f : n + 1 \to E$ tetszőleges bijekció.

Az előző állítás alapján vehetjük azt az $m \in n + 1$ elemet, amelyre $f(m) = \max(E)$. Vezessük be a $\tau : n + 1 \to n + 1$ bijekciót úgy, hogy

– ha $m \in n$, akkor $\tau(m) := n$ és $\tau(n) := m$ és minden $i \in n + 1$ esetén, ha $i \neq m$ és $i \neq n$, akkor $\tau(i) := i$ (tehát τ az m és n elemeket felcserélő *transzpozíciója* az $n + 1$ halmaznak);

– ha $m = n$, akkor $\tau := \mathrm{id}_{n+1}$.

Ekkor az $(f \circ \tau)|_n$ függvény bijekció az n és $E \setminus \{\max(E)\}$ halmaz között, mert ezek a halmazok ekvipotens véges halmazok, és az $(f \circ \tau)|_n$ függvény injekció, hiszen injekciók kompozíciója, és az a függvény az $E \setminus \{\max(E)\}$ halmazba érkezik, mert

– ha $m \in n$, akkor $(f \circ \tau)|_n(m) = f(n) \neq f(m) = \max(E)$, hiszen f injektív és $m \neq n$, továbbá minden $i \in n$ esetén, ha $i \neq m$, akkor $\tau(i) = i$, hiszen $i \neq n$ is teljesül, így $(f \circ \tau)|_n(i) = f(i) \neq f(m) = \max(E)$, mert f injektív;

– ha $m = n$, akkor minden $i \in n$ esetén $(f \circ \tau)|_n(i) = f|_n(i) = f(i) \neq f(n) = f(m) = \max(E)$, mert f injektív.

Tehát az $E \setminus \{\max(E)\}$ halmaz a $\leq$ rendezés $\leq'$-vel jelölt megszorításával ellátva véges lineárisan rendezett halmaz, és $\mathrm{Card}\,(E \setminus \{\max(E)\}) = n$, és $(f \circ \tau)|_n : n \to E \setminus \{\max(E)\}$ bijekció. Ezért az indukciós hipotézis alapján vehetünk olyan $\sigma' : n \to n$ bijekciót, amelyre a $(f \circ \tau)|_n \circ \sigma' : n \to E \setminus \{\max(E)\}$ leképezés szigorúan monoton növő a $\leq_n$ és $\leq'$ rendezések szerint.

Vezessük be a következő függvényt:

$$\sigma : n+1 \to n+1; \quad i \mapsto \begin{cases} \tau(\sigma'(i)) & , \text{ha } i \in n, \\ m & , \text{ha } i = n. \end{cases}$$

Megmutatjuk, hogy a σ függvény bijekció. Ez triviális akkor, ha $m = n$, ezért feltehető, hogy $m \in n$. Legyenek $i, j \in n+1$ olyanok, hogy $i \neq j$. Ha $i, j \in n$, akkor σ definícója szerint $\sigma(i) = \tau(\sigma'(i)) \neq \tau(\sigma'(j)) = \sigma(j)$, mert $\tau \circ \sigma'$ injekció. Ha $i \in n$ és $j = n$, akkor σ definíciója szerint $\sigma(i) = \tau(\sigma'(i)) \neq \tau(n) = m = \sigma(n) = \sigma(j)$, hiszen τ injekció és $\sigma'(i) \in n$, tehát $\sigma'(i) \neq n$. Hasonlóan, $j \in n$ és $i = n$ esetén $\sigma(i) \neq \sigma(j)$.

Végül, az $f \circ \sigma : n+1 \to E$ függvény szigorúan monoton növő a $\leq_n$ és $\leq$ rendezések szerint. Ennek bizonyításához legyenek $i, j \in n+1$ olyanok, hogy $i < j$. Ha $j < n$, akkor $i, j \in n$ és $i <_n j$, így az $(f \circ \tau)|_n \circ \sigma'$ függvény szigorú monoton növése és σ definíciója szerint

$$(f \circ \sigma)(i) = \left((f \circ \tau)|_n \circ \sigma'\right)(i) < \left((f \circ \tau)|_n \circ \sigma'\right)(j) = (f \circ \sigma)(j).$$

Ha $j = n$, akkor σ definíciója szerint

$$(f \circ \sigma)(i) \leq \max(E) = f(m) = f(\sigma(n)) = (f \circ \sigma)(j),$$

és mivel $f \circ \sigma$ injekció és $i \neq j$, így $(f \circ \sigma)(i) < (f \circ \sigma)(j)$. ∎

8.2.5. Következmény. *Ha $(E, \leq)$ lineárisan rendezett halmaz, E véges, és $n := \mathrm{Card}(E)$, akkor létezik egyetlen olyan $f : n \to E$ függvény, amely szigorúan monoton növő a $\leq_n$ és $\leq$ rendezések szerint, (vagy ami ugyanaz, f izomorfizmus az $(n, \leq_n)$ és $(E, \leq)$ jólrendezett halmazok között).*

Bizonyítás. A 8.2.4. állítás szerint létezik olyan $n \to E$ függvény, amely szigorúan monoton növő a $\leq_n$ és $\leq$ rendezések szerint. Ha f és f' ilyen függvények, akkor $f^{-1} \circ f' : n \to n$ szigorúan monoton növő függvény, ezért 6.13.11. alapján $f^{-1} \circ f' = \mathrm{id}_n$, tehát $f = f'$. ∎

8.2.6. Állítás. *Legyen $(E, \leq)$ rendezett halmaz, és $f : E \to E$ olyan szürjekció, amelyre minden $x \in E$ esetén $f(x) \leq x$. Ha $f \neq \mathrm{id}_E$, akkor létezik olyan E-ben haladó szigorúan monoton növő $(x_n)_{n \in \mathbb{N}}$ sorozat, amelyre minden $n \in \mathbb{N}$ esetén $f(x_n) < x_n$.*

Bizonyítás. Legyen $X := \{x \in E | f(x) < x\}$, amelyre feltettük, hogy nem üres. A kiválasztási axiómával kombinált rekurzió-tételt alkalmazva megmutatjuk, hogy létezik olyan X-ben haladó $(x_n)_{n \in \mathbb{N}}$ sorozat, amelyre minden $n \in \mathbb{N}$ esetén $f(x_{n+1}) = x_n$.

Ehhez azt kell igazolni, hogy minden $n \in \mathbb{N}$ számra, ha $(x_k)_{k \in n}$ olyan X-ben haladó rendszer, hogy minden $k \in n$ számra, $k+1 < n$ esetén $f(x_{k+1}) = x_k$, akkor van olyan $x_n \in X$, hogy minden $k \in n+1$ számra, $k+1 < n+1$ esetén $f(x_{k+1}) = x_k$.

A hipotézis szerint $X \neq \emptyset$, és ha $x_0 \in X$, akkor az $(x_k)_{k \in 1}$ (egy tagú) rendszer logikailag triviálisan olyan, hogy minden $k \in 0$ számra, $k+1 < 0$ esetén $f(x_{k+1}) = x_k$.

Legyen most $n \in \mathbb{N}^*$ és $(x_k)_{k \in n}$ olyan X-ben haladó rendszer, hogy minden $k \in n$ számra, $k+1 < n$ esetén $f(x_{k+1}) = x_k$. Ekkor $x_{n-1} \in X$, tehát $f(x_{n-1}) < x_{n-1}$, továbbá f szürjektivitása folytán van olyan $x \in E$, hogy $f(x) = x_{n-1}$. Világos, hogy ekkor $f(x) < x$, vagyis $f(x) \neq x$, különben $x_{n-1} = f(x) = x$, vagyis $x_{n-1} = x$ teljesülne, amiből következne, hogy $x_{n-1} = f(x) = f(x_{n-1}) < x_{n-1}$, ami lehetetlen. Tehát $x \in X$, így az $x_n := x$ definícióval olyan $(x_k)_{k\in n+1}$ rendszert kapunk, amely X-ben halad, és amelyre minden $k \in n+1$ számra, $k+1 < n+1$ esetén $f(x_{k+1}) = x_k$.

Rögzítsünk olyan X-ben haladó $(x_n)_{n\in\mathbb{N}}$ sorozatot, amelyre minden $n \in \mathbb{N}$ esetén $f(x_{n+1}) = x_n$. Ekkor minden $n \in \mathbb{N}$ esetén $x_n = f(x_{n+1}) < x_{n+1}$, tehát az X-ben haladó $(x_n)_{n\in\mathbb{N}}$ sorozat szigorúan monoton növő. ■

8.2.7. Következmény. *Ha $(E, \leq)$ rendezett halmaz, és E véges, és $f : E \to E$ olyan szürjekció, amelyre minden $x \in E$ esetén $f(x) \leq x$, akkor $f = \mathrm{id}_E$.* ■

8.3. Rendezett véges műveletek

8.3.1. Definíció. *Az $(S, \top)$ párt* **magmának** *nevezzük, ha $\top$ művelet az S halmaz felett.*

A legelemibb nem triviális példák magmákra az $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$ és $(\mathbb{Z}, \cdot)$ párok. Ezek mind *neutrális-elemes, kommutatív és asszociatív* magmák. Később bevezetjük a *testeket*, és látni fogjuk, hogy ha $(K, +, \cdot)$ test, akkor $(K, +)$ és $(K, \cdot)$ szintén neutrális-elemes, kommutatív és asszociatív magmák. Az asszociatív magmákat *félcsoportoknak* nevezzük.

Megállapodunk abban, hogy $m, n \in \mathbb{N}$ esetén az

$$[\![m, n]\!] := \{k \in \mathbb{N} \mid m \leq k \leq n\}$$

jelölést alkalmazzuk.

8.3.2. Tétel. *Ha $(S, \top)$ magma, akkor létezik egyetlen olyan*

$$(G_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathscr{F}(\mathscr{F}([\![0, n]\!]; S); S)$$

sorozat, hogy $G_0 : \mathscr{F}(\{0\}; S) \to S$ az a függvény, amelyre minden $f \in \mathscr{F}(\{0\}; S)$ esetén $G_0(f) := f(0)$, továbbá minden $n \in \mathbb{N}$ és $f \in \mathscr{F}([\![0, n+1]\!]; S)$ esetén

$$G_{n+1}(f) = G_n(f|_{[\![0,n]\!]}) \top f(n+1).$$

Bizonyítás. (*Egzisztencia.*) Értelmezzük a következő halmazt:

$$E := \bigcup_{n\in\mathbb{N}} (\{n\} \times \mathscr{F}(\mathscr{F}([\![0, n]\!]; S); S)),$$

továbbá azt az $F : E \to E$ függvényt, amelyre minden $(n, g) \in E$ esetén

$$F(n, g) := (n+1, f \mapsto g(f|_{[\![0,n]\!]}) \top f(n+1)).$$

Legyen $e := (0, f \mapsto f(0))$, amely egy konkrét eleme az $\{0\} \times \mathscr{F}(\mathscr{F}(\{0\}; S); S)$ halmaznak, vagyis $e \in E$. Jelölje $(\widetilde{G}_n)_{n\in\mathbb{N}}$ az e kezdőpont és az $F : E \to E$ függvény által meghatározott E-ben haladó iterációs sorozatot. Tehát minden $n \in \mathbb{N}$ esetén $\widetilde{G}_n \in E$ és $\widetilde{G}_0 = e$, valamint minden $n \in \mathbb{N}$ esetén $\widetilde{G}_{n+1} = F(\widetilde{G}_n)$. Minden $n \in \mathbb{N}$ esetén legyen

$$G_n := \mathrm{pr}_2(\widetilde{G}_n).$$

Megmutatjuk, hogy a $(G_n)_{n\in\mathbb{N}}$ sorozat eleget tesz a követelményeknek.

Ehhez először teljes indukcióval belátjuk, hogy minden $n \in \mathbb{N}$ esetén $\mathrm{pr}_1(\widetilde{G}_n) = n$. Valóban, ez igaz, ha $n = 0$, mert a definíciók szerint $\widetilde{G}_0 = e = (0, f \mapsto f(0))$, tehát $\mathrm{pr}_1(\widetilde{G}_0) = 0$. Ha az $n \in \mathbb{N}$ számra $\mathrm{pr}_1(\widetilde{G}_n) = n$ teljesül, akkor az iterációs definíció szerint

$$\mathrm{pr}_1(\widetilde{G}_{n+1}) = \mathrm{pr}_1(F(\widetilde{G}_n)) = n + 1,$$

mert az F definíciója szerint triviális, hogy $(n, g) \in E$ esetén $\mathrm{pr}_1(F(n, g)) = n + 1$, és az indukciós hipotézis alapján $\widetilde{G}_n$ első komponense egyenlő n-nel.

Ebből látszik, hogy minden $n \in \mathbb{N}$ esetén $\widetilde{G}_n = (\mathrm{pr}_1(\widetilde{G}_n), G_n) = (n, G_n) \in E$, tehát $G_n \in \mathscr{F}(\mathscr{F}([\![0, n]\!]; S); S)$, vagyis $(G_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathscr{F}(\mathscr{F}([\![0, n]\!]; S); S)$.

A definíció szerint

$$G_0 = \mathrm{pr}_2(\widetilde{G}_0) = \mathrm{pr}_2(e) = (f \mapsto f(0)).$$

Ha $n \in \mathbb{N}$ tetszőleges, akkor az iterációs definíció alapján

$$G_{n+1} = \mathrm{pr}_2(\widetilde{G}_{n+1}) = \mathrm{pr}_2(F(\widetilde{G}_n)) = \mathrm{pr}_2(F(n, G_n)),$$

vagyis az F függvény értelmezése szerint minden $f \in \mathscr{F}([\![0, n + 1]\!]; S)$ esetén

$$G_{n+1}(f) = G_n(f|_{[\![0,n]\!]}) \top f(n + 1).$$

(*Unicitás.*) Tegyük fel, hogy $(G_n)_{n\in\mathbb{N}}, (G'_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathscr{F}(\mathscr{F}([\![0, n]\!]; S); S)$ olyanok, hogy mindkettőre teljesülnek az előírt tulajdonságok. Ekkor $0 \in \{k \in \mathbb{N} | G_k = G'_k\}$, mert G_0 és G'_0 mindketten egyenlőek a konkrét $\mathscr{F}(\{0\}; S) \to S;\ f \mapsto f(0)$ függvénnyel. Ha $n \in \{k \in \mathbb{N} | G_k = G'_k\}$, azaz $G_n = G'_n$, akkor minden $f \in \mathscr{F}([\![0, n + 1]\!]; S)$ esetén

$$G_{n+1}(f) = G_n(f|_{[\![0,n]\!]}) \top f(n + 1) = G'_n(f|_{[\![0,n]\!]}) \top f(n + 1) = G'_{n+1}(f),$$

vagyis $n + 1 \in \{k \in \mathbb{N} | G_k = G'_k\}$. Ebből a teljes indukció halmazelméleti formáját alkalmazva következik, hogy minden $n \in \mathbb{N}$ esetén $G_n = G'_n$. ■

8.3.3. Definíció. *Legyen* $(S, \top)$ *magma, és* $(G_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathscr{F}(\mathscr{F}([\![0, n]\!]; S); S)$ *az a sorozat, amelyre* $G_0 : \mathscr{F}(\{0\}; S) \to S$ *az a függvény, amelyre minden* $f \in \mathscr{F}(\{0\}; S)$ *esetén* $G_0(f) := f(0)$*, továbbá minden* $n \in \mathbb{N}$ *és* $f \in \mathscr{F}([\![0, n + 1]\!]; S)$ *esetén* $G_{n+1}(f) = G_n(f|_{[\![0,n]\!]}) \top f(n + 1)$*. Ha* $m, n \in \mathbb{N}$ *olyanok, hogy* $m \leq n$*, és* f *olyan függvény, hogy* $[\![m, n]\!] \subseteq \mathrm{Dom}(f)$ *és* $f\langle[\![m, n]\!]\rangle \subseteq S$*, akkor*

$$\mathop{\top}_{k=m}^{n} f(k) := G_{n-m}(f'),$$

ahol $f' : [\![0, n - m]\!] \to S$ *az a függvény, amelyre minden* $k \in [\![0, n - m]\!]$ *esetén* $f'(k) := f(k + m)$*.*

Speciálisan, ha $m = 0$, akkor a definíció feltételei mellett

$$\mathop{\top}_{k=0}^{n} f(k) := G_n(f|_{[\![0,n]\!]}).$$

8.3.4. Állítás. *Legyen* $(S, \top)$ *magma. Ha* $m, n \in \mathbb{N}$ *olyanok, hogy* $m \leq n$*, és* f *olyan függvény, hogy* $[\![m, n]\!] \subseteq \mathrm{Dom}(f)$ *és* $f\langle[\![m, n]\!]\rangle \subseteq S$*, akkor minden* $q \in \mathbb{N}$ *esetén*

$$\mathop{\top}_{k=m}^{n} f(k) = \mathop{\top}_{k=m+q}^{n+q} f(k - q).$$

Bizonyítás. Legyen $(G_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathscr{F}(\mathscr{F}([\![0,n]\!];S);S)$ az a sorozat, amelyre $G_0 : \mathscr{F}(\{0\};S) \to S$ az a függvény, amelyre minden $g \in \mathscr{F}(\{0\};S)$ esetén $G_0(g) := g(0)$, továbbá minden $n \in \mathbb{N}$ és $g \in \mathscr{F}([\![0,n+1]\!];S)$ esetén $G_{n+1}(g) = G_n\left(g|_{[\![0,n]\!]}\right) \top g(n+1)$. A definíció szerint

$$\mathop{\top}_{k=m}^{n} f(k) = G_{n-m}(f'),$$

ahol $f' : [\![0,n-m]\!] \to S$ az a függvény, amelyre minden $k \in [\![0,n-m]\!]$ esetén $f'(k) := f(k+m)$. Továbbá, ha bevezetjük a

$$g : [\![m+q,n+q]\!] \to S; \quad k \mapsto f(k-q)$$

leképezést, akkor a definíció szerint

$$\mathop{\top}_{k=m+q}^{n+q} f(k-q) = \mathop{\top}_{k=m+q}^{n+q} g(k) = G_{(n+q)-(m+q)}(g') = G_{n-m}(g'),$$

ahol $g' : [\![0,(n+q)-(m+q)]\!] \to S$ az a függvény, amelyre minden $k \in [\![0,(n+q)-(m+q)]\!]$ esetén $g'(k) := g(k+m+q)$. Ekkor $\mathrm{Dom}(g') = \mathrm{Dom}(f')$ és minden $k \in [\![0,n-m]\!]$ esetén $g'(k) := g(k+m+q) = f((k+m+q)-q) = f(k+m) = f'(k)$. Tehát $g' = f'$, ezért

$$\mathop{\top}_{k=m}^{n} f(k) = G_{n-m}(f') = G_{n-m}(g') = \mathop{\top}_{k=m+q}^{n+q} f(k-q),$$

amit bizonyítani kellett. ■

8.3.5. Állítás. *Legyen $(S,\top)$ magma.*

a) *Ha $m \in \mathbb{N}$ és f olyan függvény, hogy $m \in \mathrm{Dom}(f)$ és $f(m) \in S$, akkor*

$$\mathop{\top}_{k=m}^{m} f(k) = f(m).$$

b) *Ha $m,n \in \mathbb{N}$ olyan számok, hogy $m \leq n$, akkor minden f függvényre, $[\![m,n+1]\!] \subseteq \mathrm{Dom}(f)$ és $f\langle[\![m,n+1]\!]\rangle \subseteq S$ esetén*

$$\mathop{\top}_{k=m}^{n+1} f(k) = \left(\mathop{\top}_{k=m}^{n} f(k)\right) \top f(n+1).$$

c) *Ha $m,n \in \mathbb{N}$ olyan számok, hogy $m \leq n$, továbbá f,g olyan függvények, hogy $[\![m,n]\!] \subseteq \mathrm{Dom}(f) \cap \mathrm{Dom}(g)$, valamint $f\langle[\![m,n]\!]\rangle \subseteq S$ és $f = g$ az $[\![m,n]\!]$ halmazon, akkor*

$$\mathop{\top}_{k=m}^{n} f(k) = \mathop{\top}_{k=m}^{n} g(k).$$

d) *Legyenek $m,m' \in \mathbb{N}$, valamint g,g' olyan függvények, hogy $[\![0,m]\!] \subseteq \mathrm{Dom}(g)$, $g\langle[\![0,m]\!]\rangle \subseteq S$, $[\![0,m']\!] \subseteq \mathrm{Dom}(g')$, $g'\langle[\![0,m']\!]\rangle \subseteq S$. Értelmezzük a következő függvényt:*

$$f : [\![0,m+m'+1]\!] \to S; \quad i \mapsto \begin{cases} g(i) & \text{, ha } 0 \leq i \leq m; \\ g'(i-(m+1)) & \text{, ha } m+1 \leq i \leq m+m'+1. \end{cases}$$

Ha a $\top$ művelet asszociatív, akkor

$$\left(\mathop{\top}_{j=0}^{m} g(j)\right) \top \left(\mathop{\top}_{k=0}^{m'} g'(k)\right) = \mathop{\top}_{i=0}^{m+m'+1} f(i).$$

e) *Legyen $n \in \mathbb{N}^*$ és f olyan függyvény, hogy $[\![0,n]\!] \subseteq \mathrm{Dom}(f)$ és $f\langle[\![0,n]\!]\rangle \subseteq S$. Ha a $\top$ művelet asszociatív, akkor minden $m \leq n$ természetes számra*

– *ha $m < n$, akkor*

$$\left(\mathop{\top}_{j=0}^{m} f(j)\right) \top \Big(\mathop{\top}_{k=m+1}^{n} f(k)\Big) = \mathop{\top}_{i=0}^{n} f(i),$$

– *ha $0 < m$, akkor*

$$\left(\mathop{\top}_{j=0}^{m-1} f(j)\right) \top \Big(\mathop{\top}_{k=m}^{n} f(k)\Big) = \mathop{\top}_{i=0}^{n} f(i),$$

– *ha $0 < m < n$, akkor*

$$\left(\mathop{\top}_{j=0}^{m-1} f(j)\right) \top f(m) \top \Big(\mathop{\top}_{k=m+1}^{n} f(k)\Big) = \mathop{\top}_{i=0}^{n} f(i).$$

Bizonyítás. Jelölje $(G_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathscr{F}(\mathscr{F}([\![0,n]\!];S);S)$ azt a sorozatot, amelyre $G_0 : \mathscr{F}(\{0\};S) \to S$ az a függvény, amelyre minden $f \in \mathscr{F}(\{0\};S)$ esetén $G_0(f) := f(0)$, és minden $n \in \mathbb{N}$ és $f \in \mathscr{F}([\![0,n+1]\!];S)$ esetén $G_{n+1}(f) = G_n(f|_{[\![0,n]\!]}) \top f(n+1)$.

a) A definíció szerint $\mathop{\top}_{k=m}^{m} f(k) = G_0(f')$, ahol $f' : \{0\} \to S$ az a függvény, amelyre $f'(0) = f(0+m) = f(m)$. Ezért G_0 értelmezése alapján $G_0(f') = f'(0) = f(m)$, tehát $\mathop{\top}_{k=m}^{m} f(k) = f(m)$.

b) Értelmezzük a következő függvényeket:

$$f' : [\![0, n-m]\!] \to S; \quad k \mapsto f(k+m),$$
$$f'' : [\![0, (n+1)-m]\!] \to S; \quad k \mapsto f(k+m).$$

Világos, hogy $f''|_{[\![0,n-m]\!]} = f'$, és a definíció szerint

$$\mathop{\top}_{k=m}^{n} f(k) := G_{n-m}(f'),$$
$$\mathop{\top}_{k=m}^{n+1} f(k) := G_{(n+1)-m}(f''),$$

amiből következik, hogy

$$G_{(n+1)-m}(f'') = G_{(n-m)+1}(f'') = G_{n-m}(f''|_{[\![0,n-m]\!]}) \top f''((n-m)+1) =$$
$$= G_{n-m}(f') \top f(n+1) = \Big(\mathop{\top}_{k=m}^{n} f(n)\Big) \top f(n+1).$$

c) A hipotézis szerint az

$$f' : [\![0, n-m]\!] \to S; \quad k \mapsto f(k+m)$$
$$g' : [\![0, n-m]\!] \to S; \quad k \mapsto g(k+m)$$

függvények egyenlőek, hiszen $k \in [\![0, n-m]\!]$ esetén $k + m \in [\![m, n]\!] \subseteq \{k \in \mathrm{Dom}(f) \cap \mathrm{Dom}(g) | f(k) = g(k)\}$. Ezért a definíció szerint

$$\mathop{\top}_{k=m}^{n} f(k) := G_{n-m}(f') = G_{n-m}(g') = \mathop{\top}_{k=m}^{n} g(k).$$

d) Az állítást m' szerinti teljes indukcióval bizonyítjuk.

Ha $m' = 0$, akkor az a) és c) állítás, valamint az f függvény definíciója szerint

$$\Big(\mathop{\top}_{j=0}^{m} g(j)\Big)\top\Big(\mathop{\top}_{k=0}^{m'} g'(k)\Big) = \Big(\mathop{\top}_{j=0}^{m} g(j)\Big)\top g'(0) =$$
$$= \Big(\mathop{\top}_{j=0}^{m} f(j)\Big)\top f(m+1) = \mathop{\top}_{i=0}^{m+1} f(i) = \mathop{\top}_{i=0}^{m+m'+1} f(i),$$

tehát az állítás igaz.

Legyen $m' \in \mathbb{N}$ olyan szám, amelyre az állítás igaz, és g mellett legyen g' olyan függvény, hogy $[\![0, m'+1]\!] \subseteq \mathrm{Dom}(g')$ és $g'\langle[\![0, m'+1]\!]\rangle \subseteq S$, valamint értelmezzük azt az $f : [\![0, m+(m'+1)+1]\!] \to S$ függvényt, amelyre minden $i \in [\![0, m+(m'+1)+1]\!]$ esetén

$$f(i) := \begin{cases} g(i) & \text{, ha } 0 \le i \le m; \\ g'(i-(m+1)) & \text{,ha } m+1 \le i \le m+(m'+1)+1. \end{cases}$$

Ekkor $f' := f|_{[\![0,m+m'+1]\!]}$ az a függvény, amelyre minden $i \in [\![0, m+m'+1]\!]$ esetén

$$f'(i) = \begin{cases} g(i) & \text{, ha } 0 \le i \le m; \\ g'(i-(m+1)) & \text{, ha } m+1 \le i \le m+m'+1, \end{cases}$$

ezért az indukciós hipotézis és a c) állítás szerint

$$\Big(\mathop{\top}_{j=0}^{m} g(j)\Big)\top\Big(\mathop{\top}_{k=0}^{m'} g'(k)\Big) = \mathop{\top}_{i=0}^{m+m'+1} f(i).$$

Ebből a b) állítás kétszeri alkalmazásával és a $\top$ művelet asszociativitásának felhasználásával nyerjük, hogy

$$\Big(\mathop{\top}_{j=0}^{m} g(j)\Big)\top\Big(\mathop{\top}_{k=0}^{m'+1} g'(k)\Big) = \Big(\mathop{\top}_{j=0}^{m} g(j)\Big)\top\Big(\Big(\mathop{\top}_{k=0}^{m'} g'(k)\Big)\top g'(m'+1)\Big) =$$
$$= \Big(\Big(\mathop{\top}_{j=0}^{m} g(j)\Big)\top\Big(\mathop{\top}_{k=0}^{m'} g'(k)\Big)\Big)\top g'(m'+1) = \Big(\mathop{\top}_{i=0}^{m+m'+1} f(i)\Big)\top g'(m'+1) =$$
$$= \Big(\mathop{\top}_{i=0}^{m+m'+1} f(i)\Big)\top f(m+(m'+1)+1) = \mathop{\top}_{i=0}^{m+(m'+1)+1} f(i),$$

ahol felhasználtuk azt, hogy az f függvény értelmezése alapján $f(m+(m'+1)+1) = g'(m'+1)$.

e) Tegyük fel, hogy $m < n$, és legyen $m' := n-m-1 \in \mathbb{N}$ számot. Vezessük be a $g := f|_{[\![0,m]\!]}$ és a

$$g' : [\![0, m']\!] \to S; \quad k \mapsto f(m+k+1)$$

függvényeket. Ekkor $m+m'+1 = n$ és d) alapján

$$\Big(\mathop{\top}_{j=0}^{m} g(j)\Big)\top\Big(\mathop{\top}_{k=0}^{n-m-1} g'(k)\Big) = \mathop{\top}_{i=0}^{n} \widetilde{f}(i). \tag{1}$$

teljesül, ahol $\widetilde{f} : [\![0, n]\!] \to \S$ az a függvény, amelyre minden $i \in [\![0, n]\!]$ esetén

$$\widetilde{f}(i) := \begin{cases} g(i) & \text{, ha } 0 \le i \le m; \\ g'(i-(m+1)) & \text{, ha } m+1 \le i \le n. \end{cases}$$

Ha $i \in [\![0,m]\!]$, akkor g definíciója szerint $\widetilde{f}(i) = g(i) = f(i)$. Ha $i \in [\![m+1,n]\!]$, akkor g' definíciója szerint $\widetilde{f}(i) = g'(i-(m+1)) = f(m+i-(m+1)+1) = f(i)$. Ez azt jelenti, hogy $\widetilde{f} = f|_{[\![0,n]\!]}$, ezért a c) állításból következik, hogy

$$\mathop{\top}_{i=0}^{n} \widetilde{f}(i) = \mathop{\top}_{i=0}^{n} f(i). \tag{2}$$

Ugyanakkor g definíciója szerint

$$\mathop{\top}_{j=0}^{m} g(j) = \mathop{\top}_{j=0}^{m} f(j), \tag{3}$$

és g' definíciójából, valamint a 8.3.4. állításból következik, hogy

$$\mathop{\top}_{k=0}^{n-m-1} g'(k) = \mathop{\top}_{k=0}^{n-m-1} f(m+k+1) = \mathop{\top}_{k=m+1}^{n} f(k). \tag{4}$$

Az (1), (2), (3) és (4) egyenlőségek alapján

$$\left(\mathop{\top}_{j=0}^{m} f(j)\right) \top \left(\mathop{\top}_{k=m+1}^{n} f(k)\right) = \mathop{\top}_{i=0}^{n} f(i).$$

Tegyük fel, hogy $0 < m$. Vezessük be a $g := f|_{[\![0,m-1]\!]}$ és

$$g' : [\![0,n-m]\!] \to S; \quad k \mapsto f(m+k)$$

függvényeket. Ekkor d) alapján

$$\left(\mathop{\top}_{j=0}^{m-1} g(j)\right) \top \left(\mathop{\top}_{k=0}^{n-m} g'(k)\right) = \mathop{\top}_{i=0}^{n} \widetilde{f}(i). \tag{5}$$

teljesül, ahol $\widetilde{f} : [\![0,n]\!] \to S$ az a függvény, amelyre minden $i \in [\![0,n]\!]$ esetén

$$\widetilde{f}(i) := \begin{cases} g(i) & \text{, ha } 0 \leq i \leq m-1; \\ g'(i-m) & \text{, ha } m \leq i \leq n. \end{cases}$$

Ha $i \in [\![0,m-1]\!]$, akkor g definíciója szerint $\widetilde{f}(i) = g(i) = f(i)$. Ha $i \in [\![m,n]\!]$, akkor g' definíciója szerint $\widetilde{f}(i) = g'(i-m)) = f(m+i-m) = f(i)$. Ez azt jelenti, hogy $\widetilde{f} = f|_{[\![0,n]\!]}$, ezért a c) állításból következik, hogy

$$\mathop{\top}_{i=0}^{n} \widetilde{f}(i) = \mathop{\top}_{i=0}^{n} f(i). \tag{6}$$

Ugyanakkor g definíciója szerint

$$\mathop{\top}_{j=0}^{m-1} g(j) = \mathop{\top}_{j=0}^{m-1} f(j), \tag{7}$$

és g' definíciójából, valamint a 8.3.4. állításból következik, hogy

$$\mathop{\top}_{k=0}^{n-m} g'(k) = \mathop{\top}_{k=0}^{n-m} f(m+k) = \mathop{\top}_{k=m}^{n} f(k). \tag{8}$$

Az (5), (6), (7) és (8) egyenlőségek alapján

$$\Big(\mathop{\top}_{j=0}^{m-1} f(j)\Big)\top\Big(\mathop{\top}_{k=m}^{n} f(k)\Big) = \mathop{\top}_{i=0}^{n} f(i).$$

Végül, ha $0 < m < n$, akkor $m < n$, tehát fennáll a

$$\Big(\mathop{\top}_{j=0}^{m} f(j)\Big)\top\Big(\mathop{\top}_{k=m+1}^{n} f(k)\Big) = \mathop{\top}_{i=0}^{n} f(i)$$

egyenlőség, ugyanakkor a b) állítás szerint

$$\mathop{\top}_{j=0}^{m} f(j) = \Big(\mathop{\top}_{j=0}^{m-1} f(j)\Big)\top f(m),$$

amit behelyettesítve az előző egyenlőségbe kapjuk a bizonyítandó

$$\Big(\mathop{\top}_{j=0}^{m-1} f(j)\Big)\top f(m)\top\Big(\mathop{\top}_{k=m+1}^{n} f(k)\Big) = \mathop{\top}_{i=0}^{n} f(i)$$

formulát. ■

Tehát, ha $(S,\top)$ magma, $m\in\mathbb{N}$ és f olyan függvény, hogy $[\![m,m+3]\!]\subseteq \mathrm{Dom}(f)$ és $f\langle[\![m,m+3]\!]\rangle\subseteq S$, akkor

$$\mathop{\top}_{k=m}^{m} f(k) = f(m),$$
$$\mathop{\top}_{k=m}^{m+1} f(k) = f(m)\top f(m+1),$$
$$\mathop{\top}_{k=m}^{m+2} f(k) = (f(m)\top f(m+1))\top f(m+2),$$
$$\mathop{\top}_{k=m}^{m+3} f(k) = ((f(m)\top f(m+1))\top f(m+2))\top f(m+3).$$

Természetesen, ha a $\top$ művelet asszociatív, akkor itt a jobb oldalon a zárójelezés tetszőleges lehet, de ha $\top$ nem kommutatív, akkor az $f(k)$ elemek sorrendje még ekkor is lényeges.

Most egy olyan alternatív módszerről lesz szó, amelynek alkalmazásával szintén értelmezhetnénk a rendezett véges műveleteket tetszőleges magma esetében.

8.3.6. Állítás. *Legyen $(S,\top)$ magma és $\mathbf{s}:\mathbb{N}\to S$ függvény. Ekkor létezik egyetlen olyan $\mathbf{s}':\mathbb{N}\to S$ függvény, amelyre teljesülnek a következők:*

$$\mathbf{s}'(0) = \mathbf{s}(0)$$
$$(\forall\, n\in\mathbb{N}):\ \mathbf{s}'(n+1) = \mathbf{s}'(n)\top\mathbf{s}(n+1).$$

Bizonyítás. Értelmezzük a

$$g:\mathbb{N}\times S\to S;\quad (n,x)\mapsto x\top\mathbf{s}(n+1)$$

függvényt. A keresett $\mathbf{s}':\mathbb{N}\to S$ sorozat éppen az $\mathbf{s}(0)$ kezdőpont és a g függvény által meghatározott elemi rekurzív sorozat, tehát ennek egyértelmű létezése azonnal következik az elemi rekurzív definíció tételéből (7.4.2.). ■

8.3.7. Definíció. *Ha* $(S, \top)$ *magma és* $\mathbf{s} : \mathbb{N} \to S$ *függvény, akkor* $\top\mathbf{s}$ *jelöli azt az* $\mathbb{N} \to S$ *függvényt (vagyis* S*-ben haladó sorozatot), amelyre teljesülnek a következők:*

$$(\top\mathbf{s})(0) = \mathbf{s}(0)$$
$$(\forall\, n \in \mathbb{N}): \ (\top\mathbf{s})(n+1) = (\top\mathbf{s})(n)\top\mathbf{s}(n+1).$$

8.3.8. Állítás. *Legyen* $(S, \top)$ *magma és* $\mathfrak{e}$ *olyan halmaz, hogy* $\mathfrak{e} \notin S$*. Vezessük be az* $\widetilde{S} := S \cup \{\mathfrak{e}\}$ *halmazt és értelmezzük a*

$$\widetilde{\top} : \widetilde{S} \times \widetilde{S} \to \widetilde{S}$$

műveletet úgy, hogy $\widetilde{\top}|_{S\times S} := \top$ *és minden* $s \in \widetilde{S}$ *esetén* $s\widetilde{\top}\mathfrak{e} := s =: \mathfrak{e}\widetilde{\top}s$*. Ekkor* $(\widetilde{S}, \widetilde{\top})$ *olyan neutrális-elemes magma, amelynek* $\mathfrak{e}$ *a neutrális eleme.*

Bizonyítás. Triviális. ■

8.3.9. Állítás. *Legyen* $(S, \top)$ *magma, és* $m, n \in \mathbb{N}$ *olyan számok, hogy* $m \le n$*, valamint legyen* f *olyan függvény, hogy* $[\![m, n]\!] \subseteq \mathrm{Dom}(f)$ *és* $f\langle[\![m, n]\!]\rangle \subseteq S$*. Legyen* $\mathfrak{e}$ *olyan halmaz, hogy* $\mathfrak{e} \notin S$*. Vezessük be az* $\widetilde{S} := S \cup \{\mathfrak{e}\}$ *halmazt és értelmezzük a*

$$\widetilde{\top} : \widetilde{S} \times \widetilde{S} \to \widetilde{S}$$

műveletet úgy, hogy $\widetilde{\top}|_{S\times S} := \top$ *és minden* $s \in \widetilde{S}$ *esetén* $s\widetilde{\top}\mathfrak{e} := s =: \mathfrak{e}\widetilde{\top}s$*. Jelölje* $\left(f|_{[\![m,n]\!]}\right)^\circ : \mathbb{N} \to \widetilde{S}$ *azt a sorozatot, amelyre minden* $k \in \mathbb{N}$ *esetén*

$$\left(f|_{[\![m,n]\!]}\right)^\circ(k) := \begin{cases} f(k) & ,\ ha\ k \in [\![m, n]\!], \\ \mathfrak{e} & ,\ ha\ k \notin [\![m, n]\!], \end{cases}$$

tehát $\left(f|_{[\![m,n]\!]}\right)^\circ$ *az* $f|_{[\![m,n]\!]}$ *függvény* $\mathfrak{e}$*-vel vett kiterjesztése* $[\![m, n]\!]$*-ről* $\mathbb{N}$*-re. Ekkor a* $\widetilde{\top}\left(f|_{[\![m,n]\!]}\right)^\circ$ *sorozat stacionárius, és a stacionárius értéke egyenlő a*

$$\mathop{\top}_{k=m}^{n} f(k) \in S$$

elemmel.

Bizonyítás. Meg fogjuk mutatni, hogy minden $k \in \mathbb{N}$ esetén

$$(\widetilde{\top}\left(f|_{[\![m,n]\!]}\right)^\circ)(k) = \begin{cases} \mathfrak{e} & \text{, ha } k < m, \\ \mathop{\top}\limits_{j=m}^{k} f(j) & \text{, ha } m \le k \le n, \\ \mathop{\top}\limits_{j=m}^{n} f(j) & \text{, ha } k > n, \end{cases}$$

amiből azonnal következik az állítás. Ehhez vezessük be az $\mathbf{s} := \left(f|_{[\![m,n]\!]}\right)^\circ$ jelölést.

(I) Először igazoljuk, hogy minden $k < m$ természetes számra $(\widetilde{\top}\mathbf{s})(k) = \mathfrak{e}$. Indirekt, tegyük fel, hogy az $E := \{k \in \mathbb{N} | (k < m) \wedge ((\widetilde{\top}\mathbf{s})(k) \neq \mathfrak{e})\}$ halmaz nem üres, tehát létezik ennek legkisebb eleme: legyen ez k_*. Ha $k_* = 0$ lenne, akkor $0 \in E$ miatt $0 < m$, tehát $0 \notin [\![m, n]\!]$, így $\mathbf{s}(0) = \mathfrak{e}$, ugyanakkor $(\widetilde{\top}\mathbf{s})(0) = \mathbf{s}(0)$, vagyis $(\widetilde{\top}\mathbf{s})(0) = \mathfrak{e}$, ami ellentmond annak, hogy $0 = k_* \in E$. Ezért $k_* > 0$, tehát a k_* szám minimalitási tulajdonsága miatt $(\widetilde{\top}\mathbf{s})(k_* - 1) = \mathfrak{e}$. Ekkor viszont

$$\mathfrak{e} \neq (\widetilde{\top}\mathbf{s})(k_*) = (\widetilde{\top}\mathbf{s})((k_* - 1) + 1) = (\widetilde{\top}\mathbf{s})(k_* - 1)\widetilde{\top}\mathbf{s}(k_*) = \mathfrak{e}\widetilde{\top}\mathbf{s}(k_*) = \mathbf{s}(k_*),$$

vagyis $\mathbf{s}(k_*) \neq \mathfrak{e}$, ami ellentmond annak, hogy $k_* < m$ miatt $k_* \notin [\![m, n]\!]$, következésképpen $\mathbf{s}(k_*) = \mathfrak{e}$.

(II) Megmutatjuk, hogy minden $k \in [\![m, n]\!]$ esetén $(\widetilde{\top}\mathbf{s})(k) = \mathop{\top}\limits_{j=m}^{k} f(j)$. Ehhez legyen $E := \left\{k \in [\![m, n]\!] \;\middle|\; (\widetilde{\top}\mathbf{s})(k) \neq \mathop{\top}\limits_{j=m}^{k} f(j)\right\}$, és indirekt tegyük fel, hogy $E \neq \emptyset$. Legyen k_* az E halmaz legkisebb eleme.

A definíció szerint $(\widetilde{\top}\mathbf{s})(0) = \mathbf{s}(0)$, tehát ha $m = 0$, akkor $\mathop{\top}\limits_{j=0}^{0} f(j) = f(0) = \mathbf{s}(0)$ miatt $(\widetilde{\top}\mathbf{s})(0) = \mathop{\top}\limits_{j=0}^{0} f(j)$, vagyis $m \notin E$. Ezért $k_* = m = 0$ lehetetlen.

Ha $m > 0$, akkor (I) alapján $(\widetilde{\top}\mathbf{s})(m - 1) = \mathfrak{e}$, ezért 8.3.5. a) alapján

$$(\widetilde{\top}\mathbf{s})(m) = (\widetilde{\top}\mathbf{s})((m-1)+1) = (\widetilde{\top}\mathbf{s})(m-1)\widetilde{\top}\mathbf{s}(m) = \mathfrak{e}\widetilde{\top}\mathbf{s}(m) = \mathbf{s}(m) = f(m) = \mathop{\top}\limits_{j=m}^{m} f(j),$$

így $k_* \in E$ miatt $k_* = m > 0$ lehetetlen.

Tehát $k_* > m$, így $k_* - 1 \in [\![m, n]\!]$, ezért a k_* szám minimalitási tulajdonsága miatt $(\widetilde{\top}\mathbf{s})(k_* - 1) = \mathop{\top}\limits_{j=m}^{k_*-1} f(j)$. Ebből 8.3.5. b) alapján következik, hogy

$$(\widetilde{\top}\mathbf{s})(k_*) = (\widetilde{\top}\mathbf{s})(k_* - 1)\widetilde{\top}\mathbf{s}(k_*) = \left(\mathop{\top}\limits_{j=m}^{k_*-1} f(j)\right)\widetilde{\top}\mathbf{s}(k_*) = \left(\mathop{\top}\limits_{j=m}^{k_*-1} f(j)\right)\top f(k_*) = \mathop{\top}\limits_{j=m}^{k_*} f(j),$$

ami ellentmond annak, hogy $k_* \in E$.

(III) A (II) állítás alapján $(\widetilde{\top}\mathbf{s})(n) = \mathop{\top}\limits_{j=m}^{n} f(j)$, ezért utoljára elég azt igazolni, hogy minden $k \geq n + 1$ természetes számra $(\widetilde{\top}\mathbf{s})(k) = (\widetilde{\top}\mathbf{s})(n)$. Ezt az $n + 1$ számtól indított k szerinti teljes indukcióval fogjuk belátni.

Világos, hogy $n + 1 \notin [\![m, n]\!]$ miatt $\mathbf{s}(n + 1) = \mathfrak{e}$, ezért

$$(\widetilde{\top}\mathbf{s})(n + 1) = (\widetilde{\top}\mathbf{s})(n)\widetilde{\top}\mathbf{s}(n + 1) = (\widetilde{\top}\mathbf{s})(n)\widetilde{\top}\mathfrak{e} = (\widetilde{\top}\mathbf{s})(n),$$

tehát az állítás igaz az $n + 1$ számra.

Legyen $k \geq n + 1$ olyan természetes szám, amelyre $(\widetilde{\top}\mathbf{s})(k) = (\widetilde{\top}\mathbf{s})(n)$. Mivel $k + 1 \notin [\![m, n]\!]$, így $\mathbf{s}(k + 1) = \mathfrak{e}$, következésképpen

$$(\widetilde{\top}\mathbf{s})(k + 1) = (\widetilde{\top}\mathbf{s})(k)\widetilde{\top}\mathbf{s}(k + 1) = (\widetilde{\top}\mathbf{s})(k)\widetilde{\top}\mathfrak{e} = (\widetilde{\top}\mathbf{s})(k) = (\widetilde{\top}\mathbf{s})(n),$$

tehát az egyenlőség a $k + 1$ számra is igaz. ■

8.4. A felcserélési formula

8.4.1. Lemma. *Legyen* $(S,\top)$ *kommutatív asszociatív magma. Ha* $n\in\mathbb{N}$ *és* g,h *olyan függvények, hogy* $[\![0,n]\!]\subseteq \mathrm{Dom}(g)\cap\mathrm{Dom}(h)$*, valamint* $g\langle[\![0,n]\!]\rangle\subseteq S$ *és* $h\langle[\![0,n]\!]\rangle\subseteq S$*, akkor*

$$\Big(\mathop{\top}_{j=0}^{n} g(j)\Big)\top\Big(\mathop{\top}_{j=0}^{n} h(j)\Big)=\mathop{\top}_{j=0}^{n}(g(j)\top h(j)).$$

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk.

Ha $n=0$, akkor 8.3.5. a) kétszeri alkalmazásával kapjuk, hogy

$$\Big(\mathop{\top}_{j=0}^{0} g(j)\Big)\top\Big(\mathop{\top}_{j=0}^{0} h(j)\Big)=g(0)\top h(0)=\mathop{\top}_{j=0}^{0}(g(j)\top h(j)),$$

tehát az állítás igaz.

Legyen $n\in\mathbb{N}$ olyan, amelyre az állítás igaz, és vegyünk olyan g és h függvényeket, amelyekre $[\![0,n+1]\!]\subseteq\mathrm{Dom}(g)\cap\mathrm{Dom}(h)$, valamint $g\langle[\![0,n+1]\!]\rangle\subseteq S$ és $h\langle[\![0,n+1]\!]\rangle\subseteq S$. Ekkor

$$\Big(\mathop{\top}_{j=0}^{n+1} g(j)\Big)\top\Big(\mathop{\top}_{j=0}^{n+1} h(j)\Big)\overset{(1)}{=}\Big(\Big(\mathop{\top}_{j=0}^{n} g(j)\Big)\top g(n+1)\Big)\top\Big(\Big(\mathop{\top}_{j=0}^{n} h(j)\Big)\top h(n+1)\Big)\overset{(2)}{=}$$
$$\overset{(2)}{=}\Big(\Big(\mathop{\top}_{j=0}^{n} g(j)\Big)\top\Big(\mathop{\top}_{j=0}^{n} h(j)\Big)\Big)\top\Big(g(n+1)\top h(n+1)\Big)\overset{(3)}{=}$$
$$\overset{(3)}{=}\Big(\mathop{\top}_{j=0}^{n}(g(j)\top h(j))\Big)\top\Big(g(n+1)\top h(n+1)\Big)\overset{(4)}{=}\mathop{\top}_{j=0}^{n+1}(g(j)\top h(j)),$$

ahol

- az $\overset{(1)}{=}$ egyenlőségnél a 8.3.5. b) állítást alkalmazzuk;
- a $\overset{(2)}{=}$ egyenlőségnél felhasználjuk a $\top$ művelet asszociativitását és kommutativitását;
- a $\overset{(3)}{=}$ egyenlőségnél az indukciós hipotézisre hivatkozunk;
- a $\overset{(4)}{=}$ egyenlőségnél ismét a 8.3.5. b) állítást alkalmazzuk. ■

8.4.2. Állítás. *Legyen* $(S,\top)$ *kommutatív asszociatív magma,* $n\in\mathbb{N}$ *és* $(f_k)_{k\in[\![0,n]\!]}$ *olyan rendszer, hogy minden* $k\in[\![0,n]\!]$ *esetén* $f_k:[\![0,k]\!]\to S$ *függvény. Ekkor*

$$\mathop{\top}_{k=0}^{n}\Big(\mathop{\top}_{j=0}^{k} f_k(j)\Big)=\mathop{\top}_{j=0}^{n}\Big(\mathop{\top}_{k=j}^{n} f_k(j)\Big).$$

(**Felcserélési formula.**)

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk.

Ha $n=0$, akkor 8.3.5. a) négyszeri alkalmazásával kapjuk, hogy

$$\mathop{\top}_{k=0}^{0}\Big(\mathop{\top}_{j=0}^{k} f_k(j)\Big)=\mathop{\top}_{j=0}^{0} f_0(j)=f_0(0)=\mathop{\top}_{k=0}^{0} f_k(0)=\mathop{\top}_{j=0}^{0}\Big(\mathop{\top}_{k=j}^{0} f_k(j)\Big),$$

adódik, tehát az állítás igaz.

Legyen $n \in \mathbb{N}$ olyan, amelyre az állítás igaz, és vegyünk olyan $(f_k)_{k \in [\![0,n+1]\!]}$ rendszert, hogy minden $k \in [\![0, n+1]\!]$ esetén $f_k : [\![0,k]\!] \to S$ függvény. Ekkor

$$\begin{aligned}
&\mathop{\top}_{k=0}^{n+1}\Big(\mathop{\top}_{j=0}^{k} f_k(j)\Big) \overset{(1)}{=} \Big(\mathop{\top}_{k=0}^{n}\Big(\mathop{\top}_{j=0}^{k} f_k(j)\Big)\Big)\top\Big(\mathop{\top}_{j=0}^{n+1} f_{n+1}(j)\Big) \overset{(2)}{=} \\
&\overset{(2)}{=} \Big(\mathop{\top}_{j=0}^{n}\Big(\mathop{\top}_{k=j}^{n} f_k(j)\Big)\Big)\top\Big(\Big(\mathop{\top}_{j=0}^{n} f_{n+1}(j)\Big)\top f_{n+1}(n+1)\Big) \overset{(3)}{=} \\
&\overset{(3)}{=} \Big(\Big(\mathop{\top}_{j=0}^{n}\Big(\mathop{\top}_{k=j}^{n} f_k(j)\Big)\Big)\top\Big(\mathop{\top}_{j=0}^{n} f_{n+1}(j)\Big)\Big)\top f_{n+1}(n+1) \overset{(4)}{=} \\
&\overset{(4)}{=} \Big(\mathop{\top}_{j=0}^{n}\Big(\Big(\mathop{\top}_{k=j}^{n} f_k(j)\Big)\top f_{n+1}(j)\Big)\Big)\top f_{n+1}(n+1) \overset{(5)}{=} \\
&\overset{(5)}{=} \Big(\mathop{\top}_{j=0}^{n}\Big(\mathop{\top}_{k=j}^{n+1} f_k(j)\Big)\Big)\top f_{n+1}(n+1) \overset{(6)}{=} \mathop{\top}_{j=0}^{n+1}\Big(\mathop{\top}_{k=j}^{n+1} f_k(j)\Big),
\end{aligned}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.3.5. b) állítást alkalmazzuk a

$$[\![0, n+1]\!] \to S; \quad k \mapsto \mathop{\top}_{j=0}^{k} f_k(j)$$

függvényre;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználjuk az indukciós hipotézist az $(f_k)_{k \in [\![0,n]\!]}$ függvényrendszerre, és ismét alkalmazzuk a 8.3.5. b) állítást, ezúttal az f_{n+1} függvényre;

– a $\overset{(3)}{=}$ egyenlőségnél a $\top$ művelet asszociativitását alkalmazzuk;

– a $\overset{(4)}{=}$ egyenlőségnél felhasználjuk az előző lemmát a

$$g : [\![0, n]\!] \to S; \quad j \mapsto \mathop{\top}_{k=j}^{n} f_k(j),$$
$$h : [\![0, n]\!] \to S; \quad j \mapsto f_{n+1}(j),$$

függvényekre;

– az $\overset{(5)}{=}$ egyenlőségnél ismét a 8.3.5. b) állításra hivatkozunk, amelyet minden $j \in [\![0, n]\!]$ esetén a

$$[\![j, n+1]\!] \to S; \quad k \mapsto f_k(j)$$

függvényre alkalmazunk;

– a $\overset{(6)}{=}$ egyenlőségnél a 8.3.5. a) és b) állítását alkalmazzuk a

$$[\![0, n+1]\!] \to S; \quad j \mapsto \mathop{\top}_{k=j}^{n+1} f_k(j)$$

függvényre. ■

8.5. Véges műveletek

8.5.1. Lemma. *Legyen* $(S, \top)$ *asszociatív magma,* $n \in \mathbb{N}$ *és* $f : [\![0, n]\!] \to S$ *olyan függvény, hogy az* $\mathrm{Im}(f)$ *halmaz a* $\top$ *művelet szerint kommutatív. Ekkor minden* $\sigma : [\![0, n]\!] \to [\![0, n]\!]$ *bijekcióra*

$$\mathop{\top}_{k=0}^{n} (f \circ \sigma)(k) = \mathop{\top}_{k=0}^{n} f(k).$$

Bizonyítás. Jelölje $\mathscr{A}(n)$ a következő kijelentést:

"$n \in \mathbb{N}$ és minden $f : [\![0, n]\!] \to S$ függvényre, ha az $\mathrm{Im}(f)$ halmaz a $\top$ művelet szerint kommutatív, akkor minden $\sigma : [\![0, n]\!] \to [\![0, n]\!]$ bijekcióra

$$\mathop{\top}_{k=0}^{n} (f \circ \sigma)(k) = \mathop{\top}_{k=0}^{n} f(k)$$

teljesül."

Teljes indukcióval bebizonyítjuk, hogy $(\forall\, n \in \mathbb{N})\ \mathscr{A}(n)$ igaz.

Mivel $[\![0, 0]\!] = \{0\}$, így egyetlen $\{0\} \to \{0\}$ bijekció (sőt függvény) létezik: az $\{0\}$ halmaz identikus függvénye, tehát $\mathscr{A}(0)$ triviálisan igaz.

Mivel $[\![0, 1]\!] = \{0, 1\}$, így egyetlen nem identikus $\sigma : \{0, 1\} \to \{0, 1\}$ bijekció létezik: az, amelyre $\sigma(0) = 1$ és $\sigma(1) = 0$. Tehát, ha $f : [\![0, 1]\!] \to S$ olyan függvény, hogy az $\mathrm{Im}(f)$ halmaz a $\top$ művelet szerint kommutatív, akkor

$$\mathop{\top}_{k=0}^{1} (f \circ \sigma)(k) = f(\sigma(0)) \top f(\sigma(1)) = f(1) \top f(0) = f(0) \top f(1) = \mathop{\top}_{k=0}^{1} f(k).$$

Ez azt jelenti, hogy $\mathscr{A}(1)$ is igaz.

Tegyük fel, hogy $n \geq 1$ olyan természetes szám, amelyre $\mathscr{A}(n)$ igaz. Jelölje $\mathbf{S}$ azon $\sigma : [\![0, n+1]\!] \to [\![0, n+1]\!]$ bijekciók halmazát, amelyekre teljesül az, hogy minden $f : [\![0, n+1]\!] \to S$ függvényre, ha $\mathrm{Im}(f)$ a $\top$ művelet szerint kommutatív halmaz, akkor

$$\mathop{\top}_{k=0}^{n+1} (f \circ \sigma)(k) = \mathop{\top}_{k=0}^{n+1} f(k).$$

Az $\mathscr{A}(n+1)$ állítás bizonyításához azt kell igazolni, hogy $\mathbf{S}$ *egyenlő* az összes $[\![0, n+1]\!] \to [\![0, n+1]\!]$ bijekciók halmazával. Ehhez először néhány megállapítást teszünk az $\mathbf{S}$ halmazzal kapcsolatban.

(I) Ha $\sigma, \sigma' \in \mathbf{S}$, akkor $\sigma \circ \sigma' \in \mathbf{S}$. Valóban, ha $f : [\![0, n+1]\!] \to S$ olyan függvény, hogy $\mathrm{Im}(f)$ a $\top$ művelet szerint kommutatív halmaz, akkor $f \circ \sigma : [\![0, n+1]\!] \to S$ olyan függvény, hogy $\mathrm{Im}(f \circ \sigma) = \mathrm{Im}(f)$, vagyis $\mathrm{Im}(f \circ \sigma)$ is kommutatív halmaz S-ben a $\top$ művelet szerint, ezért $\sigma, \sigma' \in \mathbf{S}$ alapján

$$\mathop{\top}_{k=0}^{n+1} ((f \circ \sigma) \circ \sigma')(k) = \mathop{\top}_{k=0}^{n+1} (f \circ \sigma)(k) = \mathop{\top}_{k=0}^{n+1} f(k),$$

vagyis $\sigma \circ \sigma' \in \mathbf{S}$.

(II) Legyen $\sigma : [\![0, n+1]\!] \to [\![0, n+1]\!]$ olyan bijekció, hogy $\sigma(n+1) = n+1$. Megmutatjuk, hogy $\sigma \in \mathbf{S}$. Ehhez rögzítsünk egy olyan $f : [\![0, n+1]\!] \to S$ függvényt, hogy az $\mathrm{Im}(f)$

halmaz a $\top$ művelet szerint kommutatív. Nyilvánvaló, hogy $\sigma|_{[\![0,n]\!]} : [\![0,n]\!] \to [\![0,n]\!]$ bijekció, és $f|_{[\![0,n]\!]} : [\![0,n]\!] \to S$ olyan függvény, hogy $\mathrm{Im}\left(f|_{[\![0,n]\!]}\right) \subseteq \mathrm{Im}(f)$, tehát az $\mathrm{Im}\left(f|_{[\![0,n]\!]}\right)$ halmaz a $\top$ művelet szerint szintén kommutatív. Ezért $\mathscr{A}(n)$ alapján

$$\mathop{\top}_{k=0}^{n}(f\circ\sigma)(k) = \mathop{\top}_{k=0}^{n}\left(\left(f|_{[\![0,n]\!]}\right)\circ\left(\sigma|_{[\![0,n]\!]}\right)\right)(k) = \mathop{\top}_{k=0}^{n}\left(f|_{[\![0,n]\!]}\right)(k) = \mathop{\top}_{k=0}^{n} f(k).$$

Ebből következik, hogy

$$\mathop{\top}_{k=0}^{n+1}(f\circ\sigma)(k) = \Big(\mathop{\top}_{k=0}^{n}(f\circ\sigma)(k)\Big)\top(f\circ\sigma)(n+1) = \Big(\mathop{\top}_{k=0}^{n} f(k)\Big)\top f(n+1) = \mathop{\top}_{k=0}^{n+1} f(k),$$

tehát $\sigma \in \mathbf{S}$.

(III) Legyen $\sigma_*{:}[\![0,n{+}1]\!]{\to}[\![0,n{+}1]\!]$ az a bijekció, amelyre $\sigma_*(n) := n{+}1$, és $\sigma_*(n{+}1) := n$, és minden $k < n$ természetes számra $\sigma_*(k) := k$. Megmutatjuk, hogy $\sigma_* \in \mathbf{S}$. Ehhez rögzítsünk egy olyan $f : [\![0,n+1]\!] \to S$ függvényt, hogy az $\mathrm{Im}(f)$ halmaz a $\top$ művelet szerint kommutatív. Ekkor

$$\mathop{\top}_{k=0}^{n+1}(f\circ\sigma_*)(k) = \Big(\mathop{\top}_{k=0}^{n}(f\circ\sigma_*)(k)\Big)\top(f\circ\sigma_*)(n+1) =$$
$$= \bigg(\Big(\mathop{\top}_{k=0}^{n-1}(f\circ\sigma_*)(k)\Big)\top(f\circ\sigma_*)(n)\bigg)\top(f\circ\sigma_*)(n+1) = \bigg(\Big(\mathop{\top}_{k=0}^{n-1} f(k)\Big)\top f(n+1)\bigg)\top f(n).$$

A $\top$ művelet asszociativitása és az $\mathrm{Im}(f)$ halmaz $\top$ szerinti kommutativitása miatt

$$\bigg(\Big(\mathop{\top}_{k=0}^{n-1} f(k)\Big)\top f(n+1)\bigg)\top f(n) = \Big(\mathop{\top}_{k=0}^{n-1} f(k)\Big)\top(f(n+1)\top f(n)) =$$
$$= \Big(\mathop{\top}_{k=0}^{n-1} f(k)\Big)\top(f(n)\top f(n+1)) = \bigg(\Big(\mathop{\top}_{k=0}^{n-1} f(k)\Big)\top f(n)\bigg)\top f(n+1) =$$
$$= \Big(\mathop{\top}_{k=0}^{n} f(k)\Big)\top f(n+1) = \mathop{\top}_{k=0}^{n+1} f(k).$$

Ebből következik, hogy $\sigma_* \in \mathbf{S}$.

Ezután könnyen belátható, hogy minden $[\![0,n+1]\!] \to [\![0,n+1]\!]$ bijekció eleme $\mathbf{S}$-nek. Legyen ugyanis $\sigma : [\![0,n+1]\!] \to [\![0,n+1]\!]$ tetszőleges bijekció. Ha $\sigma(n+1) = n+1$, akkor (II) alapján $\sigma \in \mathbf{S}$. Tegyük fel, hogy $\sigma(n+1) \neq n+1$. Jelölje σ_1 azt az $[\![0,n{+}1]\!] \to [\![0,n{+}1]\!]$ bijekciót, amelyre $\sigma_1(n) := \sigma(n{+}1)$, és $\sigma_1(\sigma(n{+}1)) := n$, és minden $k \in [\![0,n+1]\!]$ esetén, ha $k \neq \sigma(n+1)$ és $k \neq n$, akkor $\sigma_1(k) := k$. (Megjegyezzük, hogy $\sigma(n+1) = n$ lehetséges, és ekkor σ_1 nyilvánvalóan egyenlő a $[\![0,n+1]\!]$ halmaz identikus függvényével.) Világos, hogy $\sigma_1(n{+}1) = n{+}1$, hiszen $n{+}1 \neq \sigma(n{+}1)$ és $n{+}1 \neq n$, ezért (II) alapján $\sigma_1 \in \mathbf{S}$. Legyen $\sigma_2 := \sigma_* \circ (\sigma_1 \circ \sigma)$. Ekkor $\sigma_2 : [\![0,n+1]\!] \to [\![0,n+1]\!]$ olyan bijekció, amelyre nyilvánvalóan $\sigma_2(n+1) = n+1$, így (II) alapján $\sigma_2 \in \mathbf{S}$. Ugyanakkor $\sigma = \sigma_1^{-1} \circ (\sigma_*^{-1} \circ \sigma_2)$, ezért a nyilvánvaló $\sigma_1^{-1} = \sigma_1$ és $\sigma_*^{-1} = \sigma_*$ összefüggések alapján $\sigma = \sigma_1 \circ (\sigma_* \circ \sigma_2)$. Ebből (III) és (I) alkalmazásával kapjuk, hogy $\sigma \in \mathbf{S}$. ■

8.5.2. Állítás. *Legyen $(S,\top)$ asszociatív magma, I nem üres véges halmaz, és f olyan S-be érkező függvény, hogy $I \subseteq \mathrm{Dom}(f)$ és az $f\langle I\rangle$ halmaz a $\top$ művelet szerint kommutatív. Ha $\tau, \tau' : [\![0, \mathrm{Card}(I)-1]\!] \to I$ tetszőleges bijekciók, akkor*

$$\mathop{\top}_{k=0}^{\mathrm{Card}(I)-1}(f\circ\tau)(k) = \mathop{\top}_{k=0}^{\mathrm{Card}(I)-1}(f\circ\tau')(k).$$

Bizonyítás. A 8.5.1. lemmát alkalmazzuk a $\tau^{-1}\circ\tau' : [\![0,\mathrm{Card}(I)-1]\!] \to [\![0,\mathrm{Card}(I)-1]\!]$ bijekcióra és az $f\circ\tau : [\![0,\mathrm{Card}(I)-1]\!] \to S$ függvényre, amelynek értékkészlete egyenlő $f\langle I\rangle$-vel, vagyis a $\top$ művelet szerint kommutatív halmaz. Azt kapjuk, hogy

$$\mathop{\top}_{k=0}^{\mathrm{Card}(I)-1}(f\circ\tau')(k) = \mathop{\top}_{k=0}^{\mathrm{Card}(I)-1}\big((f\circ\tau)\circ(\tau^{-1}\circ\tau')\big)(k) = \mathop{\top}_{k=0}^{\mathrm{Card}(I)-1}(f\circ\tau)(k).\ \blacksquare$$

8.5.3. Definíció. *Legyen $(S,\top)$ asszociatív magma, I nem üres véges halmaz, és f olyan függvény, hogy $I\subseteq \mathrm{Dom}(f)$ és $f\langle I\rangle\subseteq S$ a $\top$ művelet szerint kommutatív halmaz, vagyis minden $i,j\in I$ esetén $f(i)\top f(j)=f(j)\top f(i)$. Ekkor*

$$\mathop{\top}_{i\in I} f(i) := \mathop{\top}_{k=0}^{\mathrm{Card}(I)-1}(f\circ\tau)(k),$$

ahol $\tau : [\![0,\mathrm{Card}(I)-1]\!]\to I$ tetszőleges bijekció.

8.5.4. Állítás. *Legyen $(S,\top)$ asszociatív magma.*

a) *Ha f olyan függvény, hogy $\beta\in\mathrm{Dom}(f)$ és $f(\beta)\in S$, akkor*

$$\mathop{\top}_{i\in\{\beta\}} f(i) = f(\beta).$$

b) *Ha I nem üres véges halmaz, β olyan halmaz, hogy $\beta\notin I$, és f olyan függvény, hogy $I\cup\{\beta\}\subseteq\mathrm{Dom}(f)$ és $f\langle I\cup\{\beta\}\rangle\subseteq S$ a $\top$ művelet szerint kommutatív halmaz, akkor*

$$\mathop{\top}_{i\in I\cup\{\beta\}} f(i) = \Big(\mathop{\top}_{i\in I} f(i)\Big)\top f(\beta).$$

Bizonyítás. a) Ha $\tau : \{0\}\to\{\beta\}$ függvény, akkor τ bijekció, és $\tau(0)=\beta$, valamint

$$\mathop{\top}_{i\in\{\beta\}} f(i) = \mathop{\top}_{k=0}^{0}(f\circ\tau)(k) = (f\circ\tau)(0) = f(\beta)$$

teljesül 8.3.5. a) miatt.

b) Legyen $n:=\mathrm{Card}(I)$, és vegyünk egy tetszőleges $\tau : [\![0,n-1]\!]\to I$ bijekciót, továbbá jelöle $\tau_\beta : [\![0,n]\!]\to I\cup\{\beta\}$ azt a függvényt, amely τ-nak kiterjesztése és $\tau_\beta(n):=\beta$. Ekkor τ_β bijekció $[\![0,n]\!]$ és $I\cup\{\beta\}$ között, így a definíció, valamint 8.3.5. c) és b) szerint

$$\mathop{\top}_{i\in I\cup\{\beta\}} f(i) = \mathop{\top}_{k=0}^{n}(f\circ\tau_\beta)(k) = \Big(\mathop{\top}_{k=0}^{n-1}(f\circ\tau_\beta)(k)\Big)\top(f\circ\tau_\beta)(n) =$$
$$= \Big(\mathop{\top}_{k=0}^{n-1}(f\circ\tau)(k)\Big)\top f(\beta) = \Big(\mathop{\top}_{i\in I} f(i)\Big)\top f(\beta).\ \blacksquare$$

8.5.5. Következmény. *Legyen $(S,\top)$ asszociatív magma. Legyenek A és B olyan nem üres véges halmazok, hogy $A\cap B=\emptyset$. Ha f olyan függvény, hogy $A\cup B\subseteq\mathrm{Dom}(f)$ és $f\langle A\cup B\rangle\subseteq S$ a $\top$ művelet szerint kommutatív halmaz, akkor*

$$\mathop{\top}_{i\in A\cup B} f(i) = \Big(\mathop{\top}_{i\in A} f(i)\Big)\top\Big(\mathop{\top}_{i\in B} f(i)\Big).$$

Bizonyítás. A B halmaz számossága szerinti teljes indukcióval bizonyítunk.

A $\mathrm{Card}(B) = 1$ eset azonnal következik a 8.5.4. a) és b) állításból. Tegyük fel, hogy $m \in \mathbb{N}^*$ olyan, hogy az állítás minden olyan B véges halmazra teljesül, amely nem metszi A-t és $\mathrm{Card}(B) = m$.

Legyen B olyan véges halmaz, hogy $\mathrm{Card}(B) = m + 1$ és $A \cap B = \emptyset$. Legyen $\beta_* \in B$ rögzített elem és $B_* = B \setminus \{\beta_*\}$. Ekkor

$$\begin{aligned}\mathop{\top}_{i\in A\cup B} f(i) &= \mathop{\top}_{i\in(A\cup B_*)\cup\{\beta_*\}} f(i) \overset{(1)}{=} \Big(\mathop{\top}_{i\in A\cup B_*} f(i)\Big)\top f(\beta_*) \overset{(2)}{=}\\ &\overset{(2)}{=} \Big(\Big(\mathop{\top}_{i\in A} f(i)\Big)\top\Big(\mathop{\top}_{i\in B_*} f(i)\Big)\Big)\top f(\beta_*) \overset{(3)}{=} \Big(\mathop{\top}_{i\in A} f(i)\Big)\top\Big(\Big(\mathop{\top}_{i\in B_*} f(i)\Big)\top f(\beta_*)\Big) \overset{(4)}{=}\\ &\overset{(4)}{=} \Big(\mathop{\top}_{i\in A} f(i)\Big)\top\Big(\mathop{\top}_{i\in B_*\cup\{\beta_*\}} f(i)\Big) = \Big(\mathop{\top}_{i\in A} f(i)\Big)\top\Big(\mathop{\top}_{i\in B} f(i)\Big),\end{aligned}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználjuk a 8.5.4. b) állítást;

– a $\overset{(2)}{=}$ egyenlőségnél az indukciós hipotézist alkalmazzuk a B_* halmazra, amely m számosságú;

– a $\overset{(3)}{=}$ egyenlőségnél a $\top$ művelet asszociativitását alkalmazzuk, végül

– a $\overset{(4)}{=}$ egyenlőségnél ismét a 8.5.4. b) állításra hivatkozunk. ■

8.5.6. Következmény. *Legyen $(S, \top)$ asszociatív magma, és legyenek $s, t \in S$ olyan elemek, hogy $s\top t = t\top s$. Ha $I = \{\alpha, \beta\}$ két elemű halmaz és $f : I \to S$ az a függvény, amelyre $f(\alpha) := s$ és $f(\beta) = t$, akkor*

$$\mathop{\top}_{i\in I} f(i) = s\top t.$$

Bizonyítás. Alkalmazhatjuk a 8.5.5. állítást az $A := \{\alpha\}$ és $B := \{\beta\}$ diszjunkt halmazokra kapjuk, hogy

$$\mathop{\top}_{i\in I} f(i) = \Big(\mathop{\top}_{i\in\{\alpha\}} f(i)\Big)\top\Big(\mathop{\top}_{i\in\{\beta\}} f(i)\Big) = f(\alpha)\top f(\beta) = s\top t,$$

ahol az utolsó előtti egyenlőségnél felhasználtuk a 8.5.4. a) állítást. ■

8.5.7. Következmény. *Legyen $(S, \top)$ asszociatív magma és $H \subseteq S$ a $\top$ művelet szerint kommutatív halmaz. A következő állítások ekvivalensek.*

(i) *Minden H-ban haladó $(s_i)_{i\in I}$ nem üres véges rendszerre $\mathop{\top}_{i\in I} s_i \in H$.*

(ii) *$H\top H \subseteq H$ (vagyis minden $s, t \in H$ esetén $s\top t \in H$).*

Bizonyítás. (i)⇒(ii) Legyen $s, t \in H$, és vezessük be azt az $(x_i)_{i\in\{0,1\}}$ rendszert, amelyre $x_0 := s$ és $x_1 := t$. Ekkor 8.5.6. és (i) alapján fennáll a $s\top t = \mathop{\top}_{i\in\{0,1\}} x_i \in H$ egyenlőség, tehát (ii) teljesül.

(ii)⇒(i) Az I indexhalmaz számossága szerinti teljes indukcióval igazoljuk, hogy (ii) teljesülése esetén minden H-ban haladó $(s_i)_{i\in I}$ nem üres véges rendszerre $\mathop{\top}_{i\in I} s_i \in H$.

Ha $(s_i)_{i\in I}$ olyan H-ban haladó rendszer, hogy $\mathrm{Card}(I)=1$, akkor van olyan β halmaz, hogy $I=\{\beta\}$, ezért 8.5.5. a) szerint $\top_{i\in I} s_i = \top_{i\in\{\beta\}} s_i = s_\beta \in H$, tehát az állítás igaz, ha $\mathrm{Card}(I)=1$.

Legyen $n\in\mathbb{N}^*$, és tegyük fel, hogy az állítás igaz minden olyan H-ban haladó rendszerre, amelynek indexhalmaza n számosságú. Legyen $(s_i)_{i\in I}$ olyan H-ban haladó véges rendszer, hogy $\mathrm{Card}(I)=n{+}1$. Rögzítsünk egy $\beta\in I$ elemet és legyen $J:=I\backslash\{\beta\}$. Ekkor

$$\top_{i\in I} s_i = \top_{i\in J\cup\{\beta\}} s_i \overset{(1)}{=} \Big(\top_{i\in J} s_i\Big)\top s_\beta \overset{(2)}{\in} H\top H \overset{(3)}{\subseteq} H,$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.5.4. b) állítást alkalmaztuk;

– a $\overset{(2)}{\in}$ összefüggésnél kihasználtuk, hogy $\mathrm{Card}(J)=n$, így az indukciós hipotézis szerint $\top_{i\in J} s_i \in H$;

– a $\overset{(3)}{\subseteq}$ összefüggésnél a (ii) hipotézist alkalmaztuk. ■

8.5.8. Következmény. *Legyen $(S,\top)$ asszociatív magma, I nem üres véges halmaz és f olyan függvény, hogy $I\subseteq \mathrm{Dom}(f)$ és $\mathrm{Im}(f)\subseteq S$ a $\top$ művelet szerint kommutatív halmaz. Ha $s\in S$ olyan, hogy minden $i\in I$ esetén $s\top f(i)=f(i)\top s$, akkor minden $J\subseteq I$ nem üres halmazra*

$$s\top\Big(\top_{i\in J} f(i)\Big) = \Big(\top_{i\in J} f(i)\Big)\top s.$$

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy a

$$\mathscr{J} := \left\{\, J\subseteq I \;\middle|\; (J\neq\emptyset)\wedge\left(s\top\Big(\top_{i\in J} f(i)\Big)\neq\Big(\top_{i\in J} f(i)\Big)\top s\right)\,\right\}$$

halmaz nem üres. Tekintsük a

$$\mathscr{J}\to\mathbb{N}^*;\quad J\mapsto \mathrm{Card}(J)$$

függvényt, amelynek értékkészlete nem üres részhalmaza $\mathbb{N}^*$-nak, tehát $\mathbb{N}$ természetes jólrendezettsége miatt létezik ennek legkisebb eleme; legyen ez az n szám. Vegyünk olyan $J\in\mathscr{J}$ halmazt, hogy $\mathrm{Card}(J)=n$, és legyen $i_*\in J$ rögzített elem.

Ha $J=\{i_*\}$, akkor 8.5.4. a) és $s\top f(i_*)=f(i_*)\top s$ alapján

$$s\top\Big(\top_{i\in J} f(i)\Big) = s\top f(i_*) = f(i_*)\top s = \Big(\top_{i\in J} f(i)\Big)\top s,$$

ami lehetetlen, mert $J\in\mathscr{J}$. Ezért $J_*:=J\setminus\{i_*\}\neq\emptyset$, így írható, hogy:

$$s\top\Big(\top_{i\in J} f(i)\Big) \overset{(1)}{=} s\top\Big(\Big(\top_{i\in J_*} f(i)\Big)\top f(i_*)\Big) \overset{(2)}{=} \Big(s\top\Big(\top_{i\in J_*} f(i)\Big)\Big)\top f(i_*) \overset{(3)}{=}$$
$$\overset{(3)}{=} \Big(\Big(\top_{i\in J_*} f(i)\Big)\top s\Big)\top f(i_*) \overset{(4)}{=} \Big(\top_{i\in J_*} f(i)\Big)\top(s\top f(i_*)) \overset{(5)}{=}$$
$$\overset{(5)}{=} \Big(\top_{i\in J_*} f(i)\Big)\top(f(i_*)\top s) \overset{(6)}{=} \Big(\Big(\top_{i\in J_*} f(i)\Big)\top f(i_*)\Big)\top s \overset{(7)}{=} \Big(\top_{i\in J} f(i)\Big)\top s,$$

ahol

– az $\overset{(1)}{=}$ és $\overset{(7)}{=}$ egyenlőségnél a 8.5.4. b) állítás alkalmaztuk;

– a $\overset{(2)}{=}$, $\overset{(4)}{=}$ és $\overset{(6)}{=}$ egyenlőségeknél a $\top$ művelet asszociativitását alkalmaztuk;

– a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk azt, hogy $J_* \subseteq I$ olyan nem üres halmaz, amelyre $\mathrm{Card}(J_*) = n-1$, így az n szám definciója szerint $J_* \notin \mathscr{J}$, vagyis

$$s\top\Big(\mathop{\top}_{i\in J_*} f(i)\Big) = \Big(\mathop{\top}_{i\in J_*} f(i)\Big)\top s;$$

– az $\overset{(5)}{=}$ egyenlőségnél ismét az $s\top f(i_*) = f(i_*)\top s$ egyenlőségre hivatkoztunk.

Tehát azt kaptuk, hogy $s\top\Big(\mathop{\top}_{i\in J} f(i)\Big) = \Big(\mathop{\top}_{i\in J} f(i)\Big)\top s$, vagyis $J \notin \mathscr{J}$, holott $J \in \mathscr{J}$. Ez az ellentmondás az állítást igazolja. ■

8.5.9. Következmény. *Legyen $(S,\top)$ asszociatív magma, I nem üres véges halmaz és f, g olyan függvények, hogy $I \subseteq \mathrm{Dom}(f)\cap\mathrm{Dom}(g)$ és $\mathrm{Im}(f)\cup\mathrm{Im}(g) \subseteq S$ a $\top$ művelet szerint kommutatív halmaz. Ekkor az $\{f(i)\top g(i) | i \in I\}$ halmaz a $\top$ művelet szerint kommutatív és*

$$\mathop{\top}_{i\in I}(f(i)\top g(i)) = \Big(\mathop{\top}_{i\in I} f(i)\Big)\top\Big(\mathop{\top}_{i\in I} g(i)\Big).$$

Bizonyítás. Az $\mathrm{Im}(f)\cup\mathrm{Im}(g)$ halmaz $\top$ művelet szerint kommutativitását és a $\top$ művelet asszociativitását alkalmazva kapjuk, hogy minden $i, j \in I$ esetén

$$\begin{aligned}
&(f(i)\top g(i))\top(f(j)\top g(j)) = (f(i)\top(g(i)\top f(j)))\top g(j) \overset{(*)}{=} (f(i)\top(f(j)\top g(i)))\top g(j) =\\
&= ((f(i)\top f(j))\top g(i))\top g(j) \overset{(*)}{=} ((f(j)\top f(i))\top g(i))\top g(j) = (f(j)\top(f(i)\top g(i)))\top g(j) =\\
&= f(j)\top((f(i)\top g(i))\top g(j)) = f(j)\top(f(i)\top(g(i)\top g(j))) \overset{(*)}{=} f(j)\top(f(i)\top(g(j)\top g(i))) =\\
&= f(j)\top((f(i)\top g(j))\top g(i)) \overset{(*)}{=} f(j)\top((g(j)\top f(i))\top g(i)) = (f(j)\top(g(j)\top f(i)))\top g(i) =\\
&= (f(j)\top g(j))\top f(i))\top g(i) = (f(j)\top g(j))\top(f(i)\top g(i)),
\end{aligned}$$

ahol a $\overset{(*)}{=}$ egyenlőségeknél az $\mathrm{Im}(f)\cup\mathrm{Im}(g)$ halmaz $\top$ művelet szerint kommutativitását, míg a többi egyenlőségnél a $\top$ művelet asszociativitását alkalmaztuk.

Ezután az I halmaz számossága szerinti teljes indukcióval igazoljuk az egyenlőséget.

Ha $\mathrm{Card}(I) = 1$ és $i_* \in I$, akkor 8.5.4. a) alapján

$$\mathop{\top}_{i\in I}(f(i)\top g(i)) = f(i_*)\top g(i_*) = \Big(\mathop{\top}_{i\in I} f(i)\Big)\top\Big(\mathop{\top}_{i\in I} g(i)\Big).$$

Legyen $n \in \mathbb{N}^*$ olyan természetes szám, hogy az állítás igaz minden olyan I indexhalmaz esetében, amelyre $\mathrm{Card}(I) = n$. Legyen I olyan véges halmaz, hogy $\mathrm{Card}(I) = n+1$, és legyenek f, g olyan függvények, hogy $I \subseteq \mathrm{Dom}(f)\cap\mathrm{Dom}(g)$ és $\mathrm{Im}(f)\cup\mathrm{Im}(g) \subseteq S$ a $\top$ művelet szerint kommutatív halmaz. Legyen $i_* \in I$ rögzített elem és $I_* := I \setminus \{i_*\}$.

Ekkor

$$\begin{aligned}
\top_{i\in I}(f(i)\top g(i)) &\overset{(1)}{=} \Big(\top_{i\in I_*}(f(i)\top g(i))\Big)\top(f(i_*)\top g(i_*)) \overset{(2)}{=} \\
&\overset{(2)}{=} \Big(\Big(\top_{i\in I_*} f(i)\Big)\top\Big(\top_{i\in I_*} g(i)\Big)\Big)\top(f(i_*)\top g(i_*)) \overset{(3)}{=} \\
&\overset{(3)}{=} \Big(\Big(\Big(\top_{i\in I_*} f(i)\Big)\top\Big(\top_{i\in I_*} g(i)\Big)\Big)\top f(i_*)\Big)\top g(i_*) \overset{(4)}{=} \\
&\overset{(4)}{=} \Big(\Big(\top_{i\in I_*} f(i)\Big)\top\Big(\Big(\top_{i\in I_*} g(i)\Big)\top f(i_*)\Big)\Big)\top g(i_*) \overset{(5)}{=} \\
&\overset{(5)}{=} \Big(\Big(\top_{i\in I_*} f(i)\Big)\top\Big(f(i_*)\top\Big(\top_{i\in I_*} g(i)\Big)\Big)\Big)\top g(i_*) \overset{(6)}{=} \\
&\overset{(6)}{=} \Big(\Big(\Big(\top_{i\in I_*} f(i)\Big)\top f(i_*)\Big)\top\Big(\top_{i\in I_*} g(i)\Big)\Big)\top g(i_*) \overset{(7)}{=} \\
&\overset{(7)}{=} \Big(\Big(\top_{i\in I} f(i)\Big)\top\Big(\top_{i\in I_*} g(i)\Big)\Big)\top g(i_*) \overset{(8)}{=} \\
&\overset{(8)}{=} \Big(\top_{i\in I} f(i)\Big)\top\Big(\Big(\top_{i\in I_*} g(i)\Big)\top g(i_*)\Big) \overset{(9)}{=} \Big(\top_{i\in I} f(i)\Big)\top\Big(\top_{i\in I} g(i)\Big),
\end{aligned}$$

ahol

– az $\overset{(1)}{=}$, $\overset{(7)}{=}$ és $\overset{(9)}{=}$ egyenlőségeknél a 8.5.5. b) állítást alkalmaztuk, rendre az

$$I \to S; \quad i \mapsto f(i)\top g(i),$$

az f, és a g függvényekre;

– az $\overset{(2)}{=}$ egyenlőségnél felhasználtuk azt, hogy $0 < \mathrm{Card}(I_*) = n-1 < n$, tehát az indukciós hipotézis alapján

$$\top_{i\in I_*}(f(i)\top g(i)) = \Big(\top_{i\in I_*} f(i)\Big)\top\Big(\top_{i\in I_*} g(i)\Big);$$

– a $\overset{(3)}{=}$, $\overset{(4)}{=}$, $\overset{(6)}{=}$ és $\overset{(8)}{=}$ egyenlőségeknél a $\top$ művelet asszociativitását alkalmaztuk;

– az $\overset{(5)}{=}$ egyenlőségnél a 8.5.8. állítást alkalmaztuk az $s := f(i_*)$, valamint $f := g$ szereposztással. ■

8.6. A véges műveletek általános kommutativitása

8.6.1. Tétel. (**A véges műveletek általános kommutativitása**) *Legyen* $(S,\top)$ *asszociatív magma,* I *és* J *nem üres véges halmazok, valamint* $\sigma : J \to I$ *tetszőleges bijekció. Ha* f *olyan függvény, hogy* $I \subseteq \mathrm{Dom}(f)$ *és* $f\langle I\rangle \subseteq S$ *a* $\top$ *művelet szerint kommutatív halmaz, akkor*

$$\top_{i\in I} f(i) = \top_{j\in J}(f\circ\sigma)(j).$$

Bizonyítás. Legyen $n := \mathrm{Card}(I)-1$, ami természetesen egyenlő a $\mathrm{Card}(J)-1$ számmal. Legyenek $\tau_I : [\![0,n]\!] \to I$ és $\tau_J : [\![0,n]\!] \to J$ bijekciók. Ekkor $\tau_J^{-1}\circ\sigma^{-1}\circ\tau_I : [\![0,n]\!] \to [\![0,n]\!]$

bijekció, ezért a definíció és 8.5.1. alapján

$$\top_{i\in I} f(i) := \top_{k=0}^{n}(f\circ\tau_I)(k) = \top_{k=0}^{n}\left((f\circ\sigma\circ\tau_J)\circ(\tau_J^{-1}\circ\sigma^{-1}\circ\tau_I)\right)(k) =$$
$$= \top_{k=0}^{n}(f\circ\sigma\circ\tau_J)(k) =: \top_{j\in J}(f\circ\sigma)(j),$$

hiszen $f\circ\sigma\circ\tau_J : [\![0,n]\!] \to S$ olyan függvény, amelyre $\mathrm{Im}\,(f\circ\sigma\circ\tau_J) = f\langle I\rangle$, vagyis $\mathrm{Im}\,(f\circ\sigma\circ\tau_J)$ a $\top$ művelet szerint kommutatív részhalmaza S-nek. ■

8.7. A véges műveletek általános asszociativitása

8.7.1. Tétel. (**A véges műveletek általános asszociativitása I.**) *Legyen* $(S,\top)$ *asszociatív magma. Legyen* I *nem üres véges halmaz és* $(I_j)_{j\in J}$ *olyan diszjunkt halmazrendszer, hogy* $I = \bigcup_{j\in J} I_j$ *és minden* $j\in J$ *indexre* $I_j \neq \emptyset$ *(tehát* $(I_j)_{j\in J}$ *az* I *halmaz partíciója). Ekkor* J *is nem üres véges halmaz, és ha* f *olyan függvény, hogy* $I\subseteq \mathrm{Dom}(f)$ *és* $f\langle I\rangle \subseteq S$ *a* $\top$ *művelet szerint kommutatív, akkor a*

$$J\to S;\quad j\mapsto \top_{i\in I_j} f(i)$$

függvény értékkészlete a $\top$ *művelet szerint kommutatív részhalmaza* S*-nek és*

$$\top_{i\in I} f(i) = \top_{j\in J}\Big(\top_{i\in I_j} f(i)\Big).$$

Bizonyítás. Ha $j, j' \in J$ és $j\neq j'$, akkor az I_j és $I_{j'}$ indexhalmazok diszjunktak, ezért 8.5.5. alapján

$$\Big(\top_{i\in I_j} f(i)\Big)\top\Big(\top_{i\in I_{j'}} f(i)\Big) = \top_{i\in I_j\cup I_{j'}} f(i) =$$
$$= \top_{i\in I_{j'}\cup I_j} f(i) = \Big(\top_{i\in I_{j'}} f(i)\Big)\top\Big(\top_{i\in I_j} f(i)\Big),$$

tehát a

$$J\to S;\quad j\mapsto \top_{i\in I_j} f(i)$$

függvény értékkészlete a $\top$ művelet szerint kommutatív részhalmaza S-nek.

Az egyenlőséget a J halmaz számossága szerinti teljes indukcióval bizonyítjuk. Világos, hogy $J\neq\emptyset$, különben I üres volna. Továbbá a J halmaz véges, mert a kiválasztási axióma szerint vehetünk egy $\sigma\in\prod_{j\in J} I_j$ kiválasztó függvényt, és ekkor az $(I_j)_{j\in J}$ halmazrendszer diszjunktsága miatt a $\sigma : J\to I$ függvény injekció, így J kisebb-egyenlő számosságú I-nél. (Sőt itt a kiválasztási axióma helyett hivatkozhatunk az 8.1.19. állításra is, hiszen J véges halmaz.)

Ha $\mathrm{Card}(J) = 1$, akkor az állítás 8.5.4. a) alapján igaz, míg $\mathrm{Card}(J) = 2$ esetén az állítás ekvivalens a 8.5.5. lemmával. Tegyük fel, hogy $m\geq 2$ olyan természetes szám, amelyre az állítás igaz, ha $\mathrm{Card}(J) = m$.

Legyen J olyan véges halmaz, hogy $\mathrm{Card}(J) = m+1$. Rögzítsünk egy $j_* \in J$ elemet, és legyenek $J_* := J \setminus \{j_*\}$, valamint $I_* := \bigcup_{j \in J_*} I_j$, tehát $I = I_* \cup I_{j_*}$. Továbbá, vezessük be a

$$g : J \to S; \quad j \mapsto \top_{i \in I_j} f(i)$$

függvényt. Ekkor

$$\begin{aligned}\top_{i\in I} f(i) &= \top_{i\in I_*\cup I_{j_*}} f(i) \overset{(1)}{=} \Big(\top_{i\in I_*} f(i)\Big)\top\Big(\top_{i\in I_{j_*}} f(i)\Big) \overset{(2)}{=} \\ &\overset{(2)}{=} \Big(\top_{j\in J_*}\Big(\top_{i\in I_j} f(i)\Big)\top\Big(\top_{i\in I_{j_*}} f(i)\Big) \overset{(3)}{=} \Big(\top_{j\in J_*} g(j)\Big)\top g(j_*) \overset{(4)}{=} \\ &\overset{(4)}{=} \top_{j\in J_*\cup\{j_*\}} g(j) = \top_{j\in J}\Big(\top_{i\in I_j} f(i)\Big),\end{aligned}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél ismét a 8.5.5. lemmát használjuk az $A := I_*$ és $B := I_{j_*}$ választással;

– a $\overset{(2)}{=}$ egyenlőségnél az indukciós hipotézist alkalmazzuk a J_* halmazra, amely m számosságú;

– a $\overset{(3)}{=}$ egyenlőségnél a g függvény definícióját alkalmazzuk;

– a $\overset{(4)}{=}$ egyenlőségnél a g függvény definíciójára és újra a 8.5.5. lemmára hivatkozunk, az $A := J_*$ és $B := \{j_*\}$ választással. ■

8.7.2. Következmény. *Legyen $(S, \top)$ kommutatív asszociatív magma. Ha I és J nem üres véges halmazok, valamint f olyan függvény, hogy $I \times J \subseteq \mathrm{Dom}(f)$ és $\mathrm{Im}(f) \subseteq S$, akkor*

$$\top_{i\in I}\Big(\top_{j\in J} f(i,j)\Big) = \top_{(i,j)\in I\times J} f(i,j) = \top_{j\in J}\Big(\top_{i\in I} f(i,j)\Big).$$

Bizonyítás. Az $(\{i\} \times J)_{i\in I}$ rendszer partíciója az $I \times J$ nem üres véges halmaznak, ezért a $\top$ művelet általános asszociativitása (8.7.1.) alapján

$$\top_{(i,j)\in I\times J} f(i,j) = \top_{i\in I}\Big(\top_{x\in\{i\}\times J} f(x)\Big) = \top_{i\in I}\Big(\top_{j\in J} f(i,j)\Big),$$

ahol az utolsó egyenlőségnél a $\top$ művelet általános kommutativitását (8.6.1.) alkalmazzuk minden $i \in I$ esetén a $J \to \{i\} \times J;\ j \mapsto (i,j)$ bijekcióra.

Az $(I \times \{j\})_{j\in J}$ rendszer partíciója az $I \times J$ nem üres véges halmaznak, ezért a $\top$ művelet általános asszociativitása (8.7.1.) alapján

$$\top_{(i,j)\in I\times J} f(i,j) = \top_{j\in J}\Big(\top_{x\in I\times\{j\}} f(x)\Big) = \top_{j\in J}\Big(\top_{i\in I} f(i,j)\Big),$$

ahol az utolsó egyenlőségnél a $\top$ művelet általános kommutativitását (8.6.1.) alkalmazzuk minden $j \in J$ esetén az $I \to I \times \{j\};\ i \mapsto (i,j)$ bijekcióra. ■

A 8.7.1. tételben az $(I_j)_{j\in J}$ halmazrendszer az I halmaz *partíciója* volt, és az

f függvény definíciós tartománya tartalmazta I-t. Azonban sokszor előfordul, hogy az $(I_j)_{j\in J}$ halmazrendszer *nem diszjunkt*, és az f függvény helyett egy olyan $(f_j)_{j\in J}$ függvényrendszer áll a rendelkezésünkre, amelyre minden $j \in J$ esetén $I_j \subseteq \mathrm{Dom}(f_j)$, és az f_j függvények még csak össze sem ragaszthatók, mert létezhetnek olyan $j, j' \in J$ indexek, amelyekre $f_j \neq f_{j'}$ a $\mathrm{Dom}(f_j) \cap \mathrm{Dom}(f_{j'})$ halmazon. Ilyen esetre vonatkozik az általános asszociativitás tételének következő formája, amelyet azonban csak olyan asszociatív magmára fogalmazunk meg, amely *neutrális elemes* és *kommutatív.*

8.7.3. Tétel. (**A véges műveletek általános asszociativitása II.**) *Legyen* $(S, \top)$ *neutrális elemes, kommutatív és asszociatív magma. Legyen* J *nem üres véges halmaz és* $(I_j)_{j\in J}$ *olyan halmazrendszer, hogy minden* $j \in J$ *indexre* I_j *nem üres és véges. Legyen* $(f_j)_{j\in J}$ *olyan függvényrendszer, hogy minden* $j \in J$ *esetén* $I_j \subseteq \mathrm{Dom}(f_j)$ *és* $f_j\langle I_j\rangle \subseteq S$. *Legyen* $I := \bigcup_{j\in J} I_j$ *és minden* $i \in I$ *esetén* $J_i := \{j \in J | i \in I_j\}$. *Ekkor*

$$\mathop{\top}_{j\in J}\Big(\mathop{\top}_{i\in I_j} f_j(i)\Big) = \mathop{\top}_{i\in I}\Big(\mathop{\top}_{j\in J_i} f_j(i)\Big).$$

Bizonyítás. Jelölje e az $(S, \top)$ magma neutrális elemét. Először megjegyezzük, hogy ha f függvény, és $I \subseteq \mathrm{Dom}(f)$ nem üres véges halmaz, és minden $i \in I$ esetén $f(i) := e$, akkor $\mathop{\top}_{i\in I} f(i) = e$. Ez az állítás triviálisan igazolható az I halmaz számossága szerinti teljes indukcióval. (És még az is kiderül, hogy e-re elég azt megkövetelni, hogy *jobboldali neutrális elem* legyen a $\top$ művelet szerint.)

Áttérve az állítás bizonyítására, vezessük be a

$$f : I \times J \to S; \quad (i, j) \mapsto \begin{cases} f_j(i) & , \text{ha } i \in I_j \\ e & , \text{ha } i \notin I_j \end{cases}$$

függvényt. Ekkor 8.7.2. alkalmazásával kapjuk, hogy

$$\mathop{\top}_{j\in J}\Big(\mathop{\top}_{i\in I} f(i,j)\Big) = \mathop{\top}_{i\in I}\Big(\mathop{\top}_{j\in J} f(i,j)\Big).$$

Legyen $j \in J$. Ha $I_j \neq I$, akkor 8.5.5. alapján

$$\mathop{\top}_{i\in I} f(i,j) = \Big(\mathop{\top}_{i\in I_j} f(i,j)\Big) \top \Big(\mathop{\top}_{i\in I\setminus I_j} f(i,j)\Big),$$

és $i \in I_j$ esetén $f(i,j) = f_j(i)$, míg $i \in I \setminus I_j$ esetén $f(i,j) = e$, tehát

$$\mathop{\top}_{i\in I_j} f(i,j) = \mathop{\top}_{i\in I_j} f_j(i), \qquad \mathop{\top}_{i\in I\setminus I_j} f(i,j) = e,$$

amiből következik, hogy

$$\mathop{\top}_{i\in I} f(i,j) = \Big(\mathop{\top}_{i\in I_j} f_j(i)\Big) \top e = \mathop{\top}_{i\in I_j} f_j(i).$$

Ez azt jelenti, hogy minden $j \in J$ esetén

$$\mathop{\top}_{i\in I} f(i,j) = \mathop{\top}_{i\in I_j} f_j(i),$$

hiszen ezt most igazoltuk $I_j \neq I$ esetén, és ha $I_j = I$, akkor ez triviálisan igaz.

Legyen $i \in I$. Ha $J \neq J_i = \{j \in J | i \in I_j\}$, akkor 8.5.5. alapján

$$\top_{j\in J} f(i,j) = \Big(\top_{j\in J_i} f(i,j)\Big)\top\Big(\top_{j\in J\setminus J_i} f(i,j)\Big),$$

és $j \in J_i$ esetén $i \in I_j$, tehát $f(i,j) = f_j(i)$, míg $j \in J \setminus J_i$ esetén $i \notin J_i$, tehát $f(i,j) = e$, ezért

$$\top_{j\in J_i} f(i,j) = \top_{j\in J_i} f_j(i), \qquad \top_{j\in J\setminus J_i} f(i,j) = e,$$

amiből következik, hogy

$$\top_{j\in J} f(i,j) = \Big(\top_{j\in J_i} f_j(i)\Big)\top e = \top_{j\in J_i} f_j(i).$$

Ez azt jelenti, hogy minden $i \in I$ esetén

$$\top_{j\in J} f(i,j) = \top_{j\in J_i} f_j(i),$$

hiszen ezt most igazoltuk $J_i \neq J$ esetén, és ha $J_i = J$, akkor ez triviálisan igaz.

Ezzel megmutattuk, hogy

$$\top_{j\in J}\Big(\top_{i\in I_j} f_j(i)\Big) = \top_{j\in J}\Big(\top_{i\in I} f(i,j)\Big) = \top_{i\in I}\Big(\top_{j\in J} f(i,j)\Big) = \top_{i\in I}\Big(\top_{j\in J_i} f_j(i)\Big). \blacksquare$$

8.8. A véges műveletek általános disztributivitása

8.8.1. Állítás. *Legyenek $(S, \perp)$ és $(S', \perp')$ kommutatív és asszociatív magmák, valamint $\pi : S \to S'$ olyan függvény, hogy minden $s, t \in S$ esetén $\pi(s \perp t) = \pi(s) \perp' \pi(t)$. Ekkor minden J nem üres véges halmazra és $g : J \to S$ függvényre*

$$\pi\Big(\perp_{j\in J} g(j)\Big) = \perp'_{j\in J} \pi(g(j)).$$

Bizonyítás. A J halmaz számossága szerinti teljes indukcióval bizonyítunk.

Ha $\mathrm{Card}(J) = 1$ és $j_* \in J$, akkor kétszer alkalmazva a 8.3.5. a) állítást kapjuk, hogy

$$\pi\Big(\perp_{j\in J} g(j)\Big) = \pi\Big(\perp_{j\in\{j_*\}} g(j)\Big) = \pi(g(j_*)) = \perp'_{j\in\{j_*\}} \pi(g(j)) = \perp'_{j\in J} \pi(g(j)),$$

tehát az állítás igaz.

Tegyük fel, hogy $n \in \mathbb{N}^*$ olyan, hogy az állítás igaz minden J indexhalmazra, amelyre $\mathrm{Card}(J) = n$.

Legyen J olyan véges indexhalmaz, hogy $\mathrm{Card}(J) = n + 1$, és rögzítsünk egy $j_* \in J$ elemet, továbbá legyen $J_* := J \setminus \{j_*\}$. Ekkor

$$\pi\Big(\perp_{j\in J} g(j)\Big) = \pi\Big(\perp_{j\in J_*\cup\{j_*\}} g(j)\Big) \overset{(1)}{=} \pi\Big(\Big(\perp_{j\in J_*} g(j)\Big)\perp g(j_*)\Big) \overset{(2)}{=}$$

$$\overset{(2)}{=} \pi\Big(\perp_{j\in J_*} g(j)\Big)\perp'\pi\left(g(j_*)\right) \overset{(3)}{=} \Big(\perp'_{j\in J_*} \pi(g(j))\Big)\perp'\pi\left(g(j_*)\right) \overset{(4)}{=}$$

$$\overset{(4)}{=} \perp'_{j\in J_*\cup\{j_*\}} \pi(g(j)) = \perp'_{j\in J} \pi(g(j)),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.5.4. b) állítást alkalmazzuk;

– a $\overset{(2)}{=}$ egyenlőségnél π függvény $\bot$ és $\bot'$ műveletekkel való kapcsolatát használjuk;

– a $\overset{(3)}{=}$ egyenlőségnél az indukciós hipotézisre hivatkozunk;

– a $\overset{(4)}{=}$ egyenlőségnél ismét a 8.5.4. b) állítást alkalmazzuk. ■

8.8.2. Következmény. *Legyen S halmaz, és legyenek $\top$, $\bot$ olyan asszociatív műveletek S felett, hogy $\top$ disztributív $\bot$-ra nézve. Tegyük fel, hogy a $\bot$ művelet kommutatív. Ha J nem üres véges halmaz, $g : J \to S$ függvény és $s \in S$, akkor*

$$s\top\Big(\mathop{\bot}_{j\in J} g(j)\Big) = \mathop{\bot}_{j\in J}(s\top g(j)),$$
$$\Big(\mathop{\bot}_{j\in J} g(j)\Big)\top s = \mathop{\bot}_{j\in J}(g(j)\top s).$$

Bizonyítás. Elegendő a 8.8.1. állítást alkalmazni az $(S', \bot') := (S, \bot)$ választással, úgy, hogy π helyére az $S \to S;\ s' \mapsto s\top s'$ és az $S \to S;\ s' \mapsto s'\top s$ leképezéseket helyettesítjük. Ezekre a π függvényekre a megkövetelt egyenlőség azért teljesül, mert a $\top$ művelet disztributív $\bot$-ra nézve. ■

8.8.3. Tétel. (**A véges műveletek általános disztributivitása.**) *Legyen S halmaz, és legyenek $\top$, $\bot$ olyan kommutatív és asszociatív műveletek S felett, hogy $\top$ disztributív $\bot$-ra nézve. Legyen I nem üres véges halmaz, $(J_i)_{i\in I}$ nem üres véges halmazok rendszere, és $(f_i)_{i\in I}$ olyan függvényrendszer, hogy minden $i \in I$ esetén $J_i \subseteq \mathrm{Dom}(f_i)$ és $\mathrm{Im}(f_j) \subseteq S$. Ekkor a $J := \prod_{i\in I} J_i$ nem üres és véges halmazra fennáll a*

$$\mathop{\top}_{i\in I}\Big(\mathop{\bot}_{j\in J_i} f_i(j)\Big) = \mathop{\bot}_{\sigma\in J}\Big(\mathop{\top}_{i\in I} f_i(\sigma(i))\Big)$$

egyenlőség.

Bizonyítás. Az I halmaz számossága szerinti teljes indukcióval bizonyítunk.

Tegyük fel, hogy $\mathrm{Card}(I) = 1$ és $i_* \in I$. Vezessük be azt a $\tau : J_{i_*} \to J$ leképezést, amelyre minden $j \in J_{i_*}$ esetén $\tau(j)(i_*) := j$. Nyilvánvaló, hogy τ bijekció. Ekkor

$$\mathop{\bot}_{\sigma\in J}\Big(\mathop{\top}_{i\in I} f_i(\sigma(i))\Big) = \mathop{\bot}_{\sigma\in J}\Big(\mathop{\top}_{i\in\{i_*\}} f_i(\sigma(i))\Big) \overset{(1)}{=} \mathop{\bot}_{\sigma\in J} f_{i_*}(\sigma(i_*)) \overset{(2)}{=}$$
$$\overset{(2)}{=} \mathop{\bot}_{j\in J_{i_*}} f_{i_*}(\tau(j)(i_*)) = \mathop{\bot}_{j\in J_{i_*}} f_{i_*}(j) \overset{(3)}{=} \mathop{\top}_{i\in\{i_*\}}\Big(\mathop{\bot}_{j\in J_i} f_i(j)\Big) = \mathop{\top}_{i\in I}\Big(\mathop{\bot}_{j\in J_i} f_i(j)\Big),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.5.4. a) állítást alkalmazzuk minden $\sigma \in J$ esetén az $I \to S;\ i \mapsto f_i(\sigma(i))$ függvényre és a $\top$ műveletre;

– a $\overset{(2)}{=}$ egyenlőségnél a $\bot$ művelet általános kommutativitását alkalmazzuk az $J \to S;\ \sigma \mapsto f_{i_*}(\sigma(i_*))$ függvényre és a $\tau : J_{i_*} \to J$ bijekcióra (8.6.1.);

– a $\overset{(3)}{=}$ egyenlőségnél ismét a 8.5.4. a) állítást alkalmazzuk a $I \to S;\ i \mapsto \mathop{\bot}_{j\in J_i} f_i(j)$

függvényre és a $\top$ műveletre.

Tegyük fel, hogy $n \in \mathbb{N}^*$ olyan, hogy az állítás igaz minden olyan I indexhalmaz esetén, amelyre $\mathrm{Card}(I) = n$.

Legyen I olyan indexhalmaz, hogy $\mathrm{Card}(I) = n + 1$. Rögzítsünk egy $i_* \in I$ elemet, és legyen $I_* := I \setminus \{i_*\}$, valamint $J_* := \prod_{i \in I_*} J_i$. Vezessük be azt a

$$\tau : J_* \times J_{i_*} \to J$$

függvényt, amelyre minden $(\sigma_*, j) \in J_* \times J_{i_*}$ esetén $\tau(\sigma_*, j) \in J$ az a rendszer, amelyre minden $i \in I$ esetén

$$\tau(\sigma_*, j)(i) := \begin{cases} \sigma_*(i) & \text{, ha } i \in I_*, \\ j & \text{, ha } i = i_*. \end{cases}$$

Könnyen látható, hogy a τ függvény bijekció $J_* \times J_{i_*}$ és J között, amelynek inverze a

$$\tau^{-1} : J \to J_* \times J_{i_*}; \quad \sigma \mapsto (\sigma|_{I_*}, \sigma(i_*))$$

leképezés. Ekkor

$$\begin{aligned}
&\bot_{\sigma \in J} \Big(\top_{i \in I} f_i(\sigma(i)) \Big) \overset{(1)}{=} \bot_{(\sigma_*, j) \in J_* \times J_{i_*}} \Big(\top_{i \in I} f_i(\tau(\sigma_*, j)(i)) \Big) \overset{(2)}{=} \\
&\overset{(2)}{=} \bot_{(\sigma_*, j) \in J_* \times J_{i_*}} \Big(\Big(\top_{i \in I_*} f_i(\tau(\sigma_*, j)(i)) \Big) \top f_{i_*}(\tau(\sigma_*, j)(i_*)) \Big) \overset{(3)}{=} \\
&\overset{(3)}{=} \bot_{(\sigma_*, j) \in J_* \times J_{i_*}} \Big(\Big(\top_{i \in I_*} f_i(\sigma_*(i)) \Big) \top f_{i_*}(j) \Big) \overset{(4)}{=} \bot_{\sigma_* \in J_*} \Big(\bot_{j \in J_{i_*}} \Big(\Big(\top_{i \in I_*} f_i(\sigma_*(i)) \Big) \top f_{i_*}(j) \Big) \Big) \overset{(5)}{=} \\
&\overset{(5)}{=} \bot_{\sigma_* \in J_*} \Big(\Big(\top_{i \in I_*} f_i(\sigma_*(i)) \Big) \top \Big(\bot_{j \in J_{i_*}} f_{i_*}(j) \Big) \Big) \overset{(6)}{=} \Big(\bot_{\sigma_* \in J_*} \Big(\top_{i \in I_*} f_i(\sigma_*(i)) \Big) \Big) \top \Big(\bot_{j \in J_{i_*}} f_{i_*}(j) \Big) \overset{(7)}{=} \\
&\overset{(7)}{=} \Big(\top_{i \in I_*} \Big(\bot_{j \in J_i} f_i(j) \Big) \Big) \top \Big(\bot_{j \in J_{i_*}} f_{i_*}(j) \Big) \overset{(8)}{=} \top_{i \in I_* \cup \{i_*\}} \Big(\bot_{j \in J_i} f_i(j) \Big) = \top_{i \in I} \Big(\bot_{j \in J_i} f_i(j) \Big),
\end{aligned}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a $\bot$ művelet általános kommutativitását alkalmazzuk az $J \to S;\ \sigma \mapsto \top_{i \in I} f_i(\sigma(i))$ függvényre és a $\tau : J_* \times J_{i_*} \to J$ bijekcióra (8.6.1.);

– a $\overset{(2)}{=}$ egyenlőségnél a 8.5.4. b) állítást alkalmazzuk minden $(\sigma_*, j) \in J_* \times J_{i_*}$ esetén az $I \to S;\ i \mapsto f_i(\tau(\sigma_*, j)(i))$ függvényre és a $\top$ műveletre;

– a $\overset{(3)}{=}$ egyenlőségnél felhasználuk a τ bijekció definícióját;

– a $\overset{(4)}{=}$ egyenlőségnél a 8.7.2. állításra hivatkozunk;

– az $\overset{(5)}{=}$ egyenlőségnél a 8.8.2. állítást alkalmazzuk, a $g := f_{i_*}$ függvényre és minden $\sigma_* \in J_*$ esetén az $s := \top_{i \in I_*} f_i(\sigma_*(i))$ elemre;

– a $\overset{(6)}{=}$ egyenlőségnél ismét a 8.8.2. állítást alkalmazzuk, de ezúttal a $g : J_* \to S;\ \sigma_* \mapsto \top_{i \in I_*} f_i(\sigma_*(i))$ függvényre és az $s := \bot_{j \in J_{i_*}} f_{i_*}(j)$ elemre;

– a $\overset{(7)}{=}$ egyenlőségnél felhasználjuk az indukciós hipotézist az I_* indexhalmazra, amelyre $\mathrm{Card}(I_*) = n$;

– a $\overset{(8)}{=}$ egyenlőségnél újra a 8.5.4. b) állításra hivatkozunk. ∎

9. fejezet

A véges műveletek halmazelméleti és elemi aritmetikai alkalmazásai

A természetes számok halmaza felett a $+$ (összeadás) és $\cdot$ (szorzás) műveletek kommutatívak és asszociatívak. Megállapodunk abban, hogy ha $m, n \in \mathbb{N}$, $m \leq n$ és f olyan függvény, hogy $[\![m, n]\!] \subseteq \mathrm{Dom}(f)$ és $f\langle[\![m, n]\!]\rangle \subseteq \mathbb{N}$, akkor a

$$\sum_{k=m}^{n} f(k) := \mathop{+}\limits_{k=m}^{n} f(k)$$

$$\prod_{k=m}^{n} f(k) := \mathop{\cdot}\limits_{k=m}^{n} f(k)$$

definíciókat, illetve jelöléseket alkalmazzuk. Továbbá, ha I nem üres véges halmaz és f olyan függvény, hogy $I \subseteq \mathrm{Dom}(f)$ és $f\langle I\rangle \subseteq \mathbb{N}$, akkor a

$$\sum_{i\in I} f(i) := \mathop{+}\limits_{i\in I} f(i)$$

$$\prod_{i\in I} f(i) := \mathop{\cdot}\limits_{i\in I} f(i)$$

definíciókat, illetve jelöléseket alkalmazzuk.

9.1. Természetes számok véges rendszerének összege és szorzata

9.1.1. Állítás. *Legyen I nem üres véges halmaz és f olyan függvény, hogy $I \subseteq \mathrm{Dom}(f)$ és $f\langle I\rangle \subseteq \mathbb{N}$. Ha $n \in \mathbb{N}$ olyan, hogy minden $i \in I$ esetén $f(i) = n$, akkor*

$$\sum_{i\in I} f(i) = n \cdot \mathrm{Card}(I),$$

$$\prod_{i\in I} f(i) = n^{\mathrm{Card}(I)}.$$

Bizonyítás. Az I halmaz számossága szerinti teljes indukcióval bizonyítunk.

Ha $\mathrm{Card}(I) = 1$ és $i_* \in I$, akkor 8.5.4. a) alapján

$$\sum_{i\in I} f(i) = f(i_*) = n = n \cdot 1 = n \cdot \mathrm{Card}(I),$$

$$\prod_{i\in I} f(i) = f(i_*) = n = n^1 = n^{\mathrm{Card}(I)}.$$

Legyen $m \in \mathbb{N}^*$ olyan, hogy az állítás igaz minden olyan I véges halmazra, amelyre $\mathrm{Card}(I) = m$.

Tegyük fel, hogy I olyan véges halmaz, hogy $\mathrm{Card}(I) = m + 1$. Legyen $i_* \in I$ rögzített elem és $I_* := I \setminus \{i_*\}$. Ekkor $\mathrm{Card}(I_*) = m$, tehát az indukciós hipotézis alapján

$$\sum_{i \in I_*} f(i) = n \cdot \mathrm{Card}(I_*) = n \cdot m,$$
$$\prod_{i \in I_*} f(i) = n^{\mathrm{Card}(I_*)} = n^m,$$

amiből az $\mathbb{N}$ feletti műveletek értelmezése és 8.5.4. b) alkalmazásával következik, hogy

$$\sum_{i \in I} f(i) = \Big(\sum_{i \in I_*} f(i)\Big) + f(i_*) = n \cdot m + n = n \cdot (m+1) = n \cdot \mathrm{Card}(I),$$
$$\prod_{i \in I} f(i) = \Big(\prod_{i \in I_*} f(i)\Big) \cdot f(i_*) = n^m \cdot n = n^{m+1} = n^{\mathrm{Card}(I)}. \blacksquare$$

9.1.2. Állítás. *Ha I nem üres véges halmaz és f olyan függvény, hogy $I \subseteq \mathrm{Dom}(f)$ és $f\langle I \rangle \subseteq \mathbb{N}$, akkor*

$$\sum_{i \in I} f(i) = \sum_{j \in f\langle I \rangle} j \cdot \mathrm{Card}(I \cap \overset{-1}{f}\langle\{j\}\rangle)$$
$$\prod_{i \in I} f(i) = \prod_{j \in f\langle I \rangle} j^{\mathrm{Card}(I \cap \overset{-1}{f}\langle\{j\}\rangle)}.$$

Bizonyítás. Az $\Big(I \cap \overset{-1}{f}\langle\{j\}\rangle\Big)_{j \in f\langle I \rangle}$ halmazrendszer partíciója az I halmaznak, ezért az $\mathbb{N}$ feletti összeadás általános asszociativitása és 9.1.1. miatt

$$\sum_{i \in I} f(i) = \sum_{j \in f\langle I \rangle} \Big(\sum_{i \in I \cap \overset{-1}{f}\langle\{j\}\rangle} f(i)\Big) = \sum_{j \in f\langle I \rangle} j \cdot \mathrm{Card}(I \cap \overset{-1}{f}\langle\{j\}\rangle),$$

továbbá az $\mathbb{N}$ feletti szorzás általános asszociativitása és 9.1.1. miatt

$$\prod_{i \in I} f(i) = \prod_{j \in f\langle I \rangle} \Big(\prod_{i \in I \cap \overset{-1}{f}\langle\{j\}\rangle} f(i)\Big) = \prod_{j \in f\langle I \rangle} j^{\mathrm{Card}(I \cap \overset{-1}{f}\langle\{j\}\rangle)}$$

teljesül. $\blacksquare$

9.1.3. Állítás. *Legyen I nem üres véges halmaz, $(J_i)_{i \in I}$ nem üres véges halmazok rendszere, és $(f_i)_{i \in I}$ olyan függvényrendszer, hogy minden $i \in I$ esetén $J_i \subseteq \mathrm{Dom}(f_i)$ és $f_i\langle J_i \rangle \subseteq \mathbb{N}$. Ekkor a $J := \prod_{i \in I} J_i$ nem üres véges halmazra fennáll a*

$$\prod_{i \in I} \Big(\sum_{j \in J_i} f_i(j) \Big) = \sum_{\sigma \in J} \Big(\prod_{i \in I} f_i(\sigma(i)) \Big)$$

egyenlőség.

Bizonyítás. A 8.8.3. tétel nyilvánvaló következménye, az $S := \mathbb{N}$, $\top := \cdot$, és $\perp := +$ választással. $\blacksquare$

9.1.4. Állítás. *Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy I nem üres véges halmaz és minden $i \in I$ esetén E_i is véges, akkor az $\bigcup_{i\in I} E_i$ és $\prod_{i\in I} E_i$ halmazok is végesek, és fennállnak a*

$$\mathrm{Card}\Big(\bigcup_{i\in I} E_i\Big) \le \sum_{i\in I} \mathrm{Card}(E_i),$$
$$\mathrm{Card}\Big(\prod_{i\in I} E_i\Big) = \mathrm{P}_{i\in I} \mathrm{Card}(E_i)$$

összefüggések. Ha az $(E_i)_{i\in I}$ halmazrendszer diszjunkt, akkor

$$\mathrm{Card}\Big(\bigcup_{i\in I} E_i\Big) = \sum_{i\in I} \mathrm{Card}(E_i).$$

Bizonyítás. Az $\bigcup_{i\in I} E_i$ és $\prod_{i\in I} E_i$ halmazok végességét a 8.1.13. és 8.1.18. állításokban már igazoltuk, ezért itt csak a számosságokra vonatkozó összefüggéseket kell bizonyítani.

(I) A halmazunió számosságára vonatkozó formulákat az I halmaz számossága szerinti teljes indukcióval bizonyítjuk.

Ha $\mathrm{Card}(I) = 1$ és $\beta \in I$, akkor $I = \{\beta\}$ és $\bigcup_{i\in I} E_i = E_\beta$, ezért 8.5.4. a) alapján

$$\mathrm{Card}\Big(\bigcup_{i\in I} E_i\Big) = \mathrm{Card}(E_\beta) = \sum_{i\in\{\beta\}} \mathrm{Card}(E_i) = \sum_{i\in I} \mathrm{Card}(E_i).$$

Legyen $n \in \mathbb{N}^*$ olyan, hogy a halmazunió számosságára vonatkozó formulák igazak minden olyan I véges halmaz esetén, amelyre $\mathrm{Card}(I) = n$.

Legyen I olyan véges halmaz, hogy $\mathrm{Card}(I) = n + 1$. Rögzítsünk egy $i_* \in I$ elemet, és értelmezzük az $I_* := I \setminus \{i_*\}$ halmazt. Ekkor

$$\mathrm{Card}\Big(\bigcup_{i\in I} E_i\Big) = \mathrm{Card}\Big(\Big(\bigcup_{i\in I} E_i\Big) \cup E_{i_*}\Big) \overset{(1)}{\le} \mathrm{Card}\Big(\bigcup_{i\in I} E_{i_*}\Big) + \mathrm{Card}(E_{i_*}) \overset{(2)}{\le}$$
$$\overset{(2)}{\le} \sum_{i\in I_*} \mathrm{Card}(E_i) + \mathrm{Card}(E_{i_*}) \overset{(3)}{=} \sum_{i\in I_*\cup\{i_*\}} \mathrm{Card}(E_i) = \sum_{i\in I} \mathrm{Card}(E_i),$$

ahol

– az $\overset{(1)}{\le}$ egyenlőtlenségnél a 8.1.12. állítást alkalmazzuk az $E := \bigcup_{i\in I} E_{i_*}$ és $F := E_{i_*}$ választással;

– a $\overset{(2)}{\le}$ egyenlőtlenségnél felhasználjuk az indukciós hipotézist az I_* indexhalmazra, amelyre $\mathrm{Card}(I_*) = n$;

– a $\overset{(3)}{=}$ egyenlőségnél a 8.5.4. b) állításra hivatkozunk, amit az $(\mathbb{N}, +)$ félcsoportra alkalmazunk.

Ha az $(E_i)_{i\in I}$ halmazrendszer *diszjunkt*, akkor itt az $\overset{(1)}{\le}$ egyenlőtlenség helyett egyenlőség áll 8.1.14. miatt, és a $\overset{(2)}{\le}$ egyenlőtlenség helyett is egyenlőség van, a diszjunkt rendszerre vonatkozó indukciós hipotézis alapján, ezért ekkor

$$\mathrm{Card}\Big(\bigcup_{i\in I} E_i\Big) = \sum_{i\in I} \mathrm{Card}(E_i).$$

(II) A halmazszorzat számosságára vonatkozó formulát az I halmaz számossága szerinti teljes indukcióval bizonyítjuk.

Ha $\mathrm{Card}(I) = 1$ és $\beta \in I$, akkor $I = \{\beta\}$ és a

$$\prod_{i\in I} E_i \to E_\beta; \quad f \mapsto f(\beta),$$

leképezés bijekció, ezért 8.5.4. a) alapján

$$\mathrm{Card}\Big(\prod_{i\in I} E_i\Big) = \mathrm{Card}(E_\beta) = \mathop{\mathrm{P}}_{i\in\{\beta\}} \mathrm{Card}(E_i) = \mathop{\mathrm{P}}_{i\in I} \mathrm{Card}(E_i).$$

Legyen $n \in \mathbb{N}^*$ olyan, hogy a halmazszorzat számosságára vonatkozó formula igaz minden olyan I véges halmaz esetén, amelyre $\mathrm{Card}(I) = n$.

Legyen I olyan véges halmaz, hogy $\mathrm{Card}(I) = n + 1$. Rögzítsünk egy $i_* \in I$ elemet, és értelmezzük az $I_* := I \setminus \{i_*\}$ halmazt. Ekkor a

$$\prod_{i\in I} E_i \to \Big(\prod_{i\in I_*} E_i\Big) \times E_{i_*}; \quad f \mapsto (f|_{I_*}, f(i_*))$$

leképezés bijekció, ezért

$$\mathrm{Card}\Big(\prod_{i\in I} E_i\Big) = \mathrm{Card}\Big(\Big(\prod_{i\in I_*} E_i\Big) \times E_{i_*}\Big) \overset{(1)}{=} \mathrm{Card}\Big(\prod_{i\in I_*} E_i\Big) \cdot \mathrm{Card}\,(E_{i_*}) \overset{(2)}{=}$$

$$\overset{(2)}{=} \Big(\mathop{\mathrm{P}}_{i\in I_*} \mathrm{Card}(E_i)\Big) \cdot \mathrm{Card}\,(E_{i_*}) \overset{(3)}{=} \mathop{\mathrm{P}}_{i\in I_*\cup\{i_*\}} \mathrm{Card}(E_i) = \mathop{\mathrm{P}}_{i\in I} \mathrm{Card}(E_i),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.1.17. állítást alkalmazzuk az $E := \prod_{i\in I} E_{i_*}$ és $F := E_{i_*}$ választással;

– az $\overset{(2)}{=}$ egyenlőségnél felhasználjuk az indukciós hipotézist az I_* indexhalmazra, amelyre $\mathrm{Card}(I_*) = n$;

– az $\overset{(3)}{=}$ egyenlőségnél a 8.5.4. b) állításra hivatkozunk, amit az $(\mathbb{N}, \cdot)$ félcsoportra alkalmazunk. ■

9.1.5. Állítás. *Minden $n \in \mathbb{N}^*$ számra és véges halmazok minden $(E_i)_{i\in n}$ rendszerére:*

$$\mathrm{Card}\Big(\bigcup_{i\in n} E_i\Big) = \sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;n)} \mathrm{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big) \qquad (*)$$

teljesül, ahol minden $k \le n$ természetes számra $\mathscr{M}(k;n)$ a $k \to n$ szigorúan monoton növő függvények halmaza.

Bizonyítás. A $(*)$ egyenlőséget n szerinti teljes indukcióval igazoljuk. Ez az egyenlőség $n = 1$ esetén triviális, valamint $n = 2$ esetén minden E_0 és E_1 véges halmazra

$$\sum_{k=1}^{2} (-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;2)} \mathrm{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big) =$$

$$= \sum_{\sigma\in\mathscr{M}(1;2)} \mathrm{Card}\Big(\bigcap_{i\in 1} E_{\sigma(i)}\Big) - \sum_{\sigma\in\mathscr{M}(2;2)} \mathrm{Card}\Big(\bigcap_{i\in 2} E_{\sigma(i)}\Big) =$$

$$= \mathrm{Card}(E_0) + \mathrm{Card}(E_1) - \mathrm{Card}(E_0 \cap E_1) = \mathrm{Card}(E_0 \cup E_1),$$

ahol az utolsó egyenlőségnél felhasználtuk a 8.1.12. állításban igazolt formulát.

Tegyük fel, hogy $n \in \mathbb{N}^*$ olyan szám, hogy a $(*)$ egyenlőség teljesül véges halmazok minden $(E_i)_{i\in n}$ rendszerére. Vegyük véges halmazoknak egy tetszőleges $(E_i)_{i\in n+1}$ rendszerét. Ekkor

$$\operatorname{Card}\Big(\bigcup_{i\in n+1} E_i\Big) = \operatorname{Card}\Big(\Big(\bigcup_{i\in n} E_i\Big) \cup E_n\Big) \overset{(1)}{=}$$
$$= \operatorname{Card}\Big(\bigcup_{i\in n} E_i\Big) + \operatorname{Card}(E_n) - \operatorname{Card}\Big(\Big(\bigcup_{i\in n} E_i\Big) \cap E_n\Big) \overset{(2)}{=}$$
$$\overset{(2)}{=} \sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;n)} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big) + \operatorname{Card}(E_n) - \operatorname{Card}\Big(\bigcup_{i\in n}(E_i \cap E_n)\Big) \overset{(3)}{=}$$
$$\overset{(3)}{=} \sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;n)} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big) + \operatorname{Card}(E_n) -$$
$$-\sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;n)} \operatorname{Card}\Big(\bigcap_{i\in k} (E_{\sigma(i)} \cap E_n)\Big)\Big),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.1.12. állítást alkalmaztuk az $E := \bigcup_{i\in n} E_i$ és $F := E_n$ választással;

– a $\overset{(2)}{=}$ egyenlőségnél az indukciós hipotézist alkalmaztuk az $(E_i)_{i\in n}$ halmazrendszerre;

– a $\overset{(3)}{=}$ egyenlőségnél szintén az indukciós hipotézist alkalmaztuk az $(E_i \cap E_n)_{i\in n}$ halmazrendszerre.

Nyilvánvaló, hogy minden $1 \leq k \leq n$ természetes számra

$$\mathscr{M}(k;n) = \{\sigma \in \mathscr{M}(k;n+1) | n \notin \operatorname{Im}(\sigma)\},$$

továbbá világos, hogy a

$$\{\sigma' \in \mathscr{M}(k+1;n+1) | \sigma'(k) = n\} \to \mathscr{M}(k;n); \quad \sigma' \mapsto \sigma'|_k$$

leképezés bijekció. Ezekből kapjuk, hogy

$$\sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;n)} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big) = \sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\substack{\sigma\in\mathscr{M}(k;n+1)\\ n\notin\operatorname{Im}(\sigma)}} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big),$$

valamint

$$\sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;n)} \operatorname{Card}\Big(\bigcap_{i\in k} (E_{\sigma(i)} \cap E_n)\Big)\Big) =$$
$$= \sum_{k=1}^{n} (-1)^{k-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(k+1;n+1)\\ \sigma'(k)=n}} \operatorname{Card}\Big(\bigcap_{i\in k+1} E_{\sigma'(i)}\Big)\Big) =$$
$$= \sum_{j=2}^{n+1} (-1)^{j}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ \sigma'(j-1)=n}} \operatorname{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big) = -\sum_{j=2}^{n+1} (-1)^{j-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ \sigma'(j-1)=n}} \operatorname{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big).$$

Ez azt jelenti, hogy

$$\mathrm{Card}\Big(\bigcup_{i\in n+1} E_i\Big) = \sum_{k=1}^{n}(-1)^{k-1}\Big(\sum_{\substack{\sigma\in\mathscr{M}(k;n+1)\\ n\notin\mathrm{Im}(\sigma)}} \mathrm{Card}\Big(\bigcap_{i\in k} E_{\sigma'(i)}\Big)\Big)+$$
$$+\mathrm{Card}(E_n) + \sum_{j=2}^{n+1}(-1)^{j-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ \sigma'(j-1)=n}} \mathrm{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big).$$

Továbbá, nyilvánvaló, hogy

$$\mathrm{Card}(E_n) = \sum_{\substack{\sigma'\in\mathscr{M}(1;n+1)\\ \sigma'(0)=n}} \mathrm{Card}\Big(\bigcap_{i\in 1} E_{\sigma'(i)}\Big),$$

valamint minden $2 \leq j \leq n+1$ természetes számra

$$\{\sigma' \in \mathscr{M}(j;n+1) | \sigma'(j-1) = n\} = \{\sigma' \in \mathscr{M}(j;n+1) | n \in \mathrm{Im}(\sigma')\},$$

következésképpen

$$\sum_{j=2}^{n+1}(-1)^{j-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ \sigma'(j-1)=n}} \mathrm{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big) = \sum_{j=2}^{n+1}(-1)^{j-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ n\in\mathrm{Im}(\sigma')}} \mathrm{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big),$$

vagyis

$$\mathrm{Card}(E_n) + \sum_{j=2}^{n+1}(-1)^{j-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ \sigma'(j-1)=n}} \mathrm{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big) =$$
$$= \sum_{j=1}^{n+1}(-1)^{j-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ n\in\mathrm{Im}(\sigma')}} \mathrm{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big).$$

Most figyelembe vesszük, hogy

$$\sum_{k=1}^{n}(-1)^{k-1}\Big(\sum_{\substack{\sigma\in\mathscr{M}(k;n+1)\\ n\notin\mathrm{Im}(\sigma)}} \mathrm{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big) = \sum_{k=1}^{n+1}(-1)^{k-1}\Big(\sum_{\substack{\sigma\in\mathscr{M}(k;n+1)\\ n\notin\mathrm{Im}(\sigma)}} \mathrm{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big),$$

hiszen $k = n+1$ esetén $\mathscr{M}(k; n+1)$ egyetlen eleme id_{n+1}, és természetesen $n \in \mathrm{Im}(\mathrm{id}_{n+1})$, így a $\{\sigma \in \mathscr{M}(n+1; n+1) | n \notin \mathrm{Im}(\sigma)\}$ indexhalmaz *üres*, tehát

$$\sum_{\substack{\sigma\in\mathscr{M}(n+1;n+1)\\ n\notin\mathrm{Im}(\sigma)}} \mathrm{Card}\Big(\bigcap_{i\in n+1} E_{\sigma(i)}\Big) = 0.$$

Ezért írható, hogy

$$\operatorname{Card}\Big(\bigcup_{i\in n+1} E_i\Big) =$$

$$= \sum_{k=1}^{n+1}(-1)^{k-1}\Big(\sum_{\substack{\sigma\in\mathscr{M}(k;n+1)\\ n\notin\operatorname{Im}(\sigma)}} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big) + \sum_{j=1}^{n+1}(-1)^{j-1}\Big(\sum_{\substack{\sigma'\in\mathscr{M}(j;n+1)\\ n\in\operatorname{Im}(\sigma')}} \operatorname{Card}\Big(\bigcap_{i\in j} E_{\sigma'(i)}\Big)\Big) =$$

$$= \sum_{k=1}^{n+1}(-1)^{k-1}\left(\sum_{\substack{\sigma\in\mathscr{M}(k;n+1)\\ n\notin\operatorname{Im}(\sigma)}} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big) + \sum_{\substack{\sigma'\in\mathscr{M}(k;n+1)\\ n\in\operatorname{Im}(\sigma')}} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma'(i)}\Big)\right) =$$

$$= \sum_{k=1}^{n+1}(-1)^{k-1}\Big(\sum_{\sigma\in\mathscr{M}(k;n+1)} \operatorname{Card}\Big(\bigcap_{i\in k} E_{\sigma(i)}\Big)\Big),$$

vagyis a $(*)$ formula teljesül n helyett $n+1$-re is. ∎

9.1.6. Állítás. *Ha $n\in\mathbb{N}$, és $(a_k)_{k\in[\![0,n]\!]}$, $(b_k)_{k\in[\![0,n]\!]}$ olyan $\mathbb{N}$-ben haladó rendszerek, hogy minden $k\in[\![0,n]\!]$ esetén $a_k\le b_k$, akkor*

$$\sum_{k=0}^{n} a_k \le \sum_{k=0}^{n} b_k,$$
$$\prod_{k=0}^{n} a_k \le \prod_{k=0}^{n} b_k.$$

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk.

Ha $n=0$, akkor az a hipotézis, hogy $a_0\le b_0$, ezért 8.3.5. a) alapján

$$\sum_{k=0}^{n} a_k = a_0 \le b_0 = \sum_{k=0}^{n} b_k,$$
$$\prod_{k=0}^{n} a_k = a_0 \le b_0 = \prod_{k=0}^{n} b_k.$$

Tegyük fel, hogy az egyenlőtlenségek teljesülnek az $n\in\mathbb{N}$ számra, és legyenek $(a_k)_{k\in[\![0,n+1]\!]}$, $(b_k)_{k\in[\![0,n+1]\!]}$ olyan $\mathbb{N}$-ben haladó rendszerek, hogy minden $k\in[\![0,n+1]\!]$ esetén $a_k\le b_k$. Ekkor

$$\sum_{k=0}^{n+1} a_k \overset{(1)}{=} \Big(\sum_{k=0}^{n} a_k\Big) + a_{n+1} \overset{(2)}{\le} \Big(\sum_{k=0}^{n} b_k\Big) + a_{n+1} \overset{(3)}{\le} \Big(\sum_{k=0}^{n} b_k\Big) + b_{n+1} \overset{(4)}{=} \sum_{k=0}^{n+1} b_k,$$

ahol

– az $\overset{(1)}{=}$ és $\overset{(4)}{=}$ egyenlőségeknél a 8.3.5. b) állítást alkalmazzuk az $\mathbb{N}$ feletti összeadás műveletre,

– a $\overset{(2)}{\le}$ egyenlőtlenségnél az indukciós hipotézist alkalmazzuk az $(a_k)_{k\in[\![0,n]\!]}$ és $(b_k)_{k\in[\![0,n]\!]}$ rendszerekre, valmint felhasználjuk a 7.9.2. állítást,

– a $\overset{(3)}{\le}$ egyenlőtlenségnél ismét a 7.9.2. állításra hivatkozunk.

Hasonlóan írható, hogy

$$\prod_{k=0}^{n+1} a_k \overset{(1)}{=} \left(\prod_{k=0}^{n} a_k\right) \cdot a_{n+1} \overset{(2)}{\leq} \left(\prod_{k=0}^{n} b_k\right) \cdot a_{n+1} \overset{(3)}{\leq} \left(\prod_{k=0}^{n} b_k\right) \cdot b_{n+1} \overset{(4)}{=} \prod_{k=0}^{n+1} b_k,$$

ahol

– az $\overset{(1)}{=}$ és $\overset{(4)}{=}$ egyenlőségeknél a 8.3.5. b) állítást alkalmazzuk az $\mathbb{N}$ feletti szorzás műveletre,

– a $\overset{(2)}{\leq}$ egyenlőtlenségnél az indukciós hipotézist alkalmazzuk az $(a_k)_{k\in[\![0,n]\!]}$ és $(b_k)_{k\in[\![0,n]\!]}$ rendszerekre, valmint felhasználjuk a 7.9.5. állítást,

– a $\overset{(3)}{\leq}$ egyenlőtlenségnél ismét a 7.9.5. állításra hivatkozunk. ■

9.2. Természetes szám felbontása bázisrendszer szerint

9.2.1. Definíció. *Egy $\mathbb{N}$-ben haladó $(d_k)_{k\in\mathbb{N}}$ szigorúan monoton növő sorozatot* **bázisrendszernek** *nevezünk, ha $d_0 = 1$, és minden $k \in \mathbb{N}$ esetén d_k osztója d_{k+1}-nek.*

Például minden $a \in \mathbb{N}$ számra, ha $a > 1$, akkor $(a^k)_{k\in\mathbb{N}}$ bázisrendszer, és a $((k+1)!)_{k\in\mathbb{N}}$ sorozat szintén bázisrendszer.

Megjegyezzük, hogy ha $(d_k)_{k\in\mathbb{N}}$ bázisrendszer, akkor teljes indukcióval könnyen belátható, hogy minden $k \in \mathbb{N}$ esetén $d_k \geq 2^k$. Valóban, ez az egyenlőtlenség igaz $k = 0$ esetén, és ha $k \in \mathbb{N}$ olyan, hogy $d_k \geq 2^k$, akkor a bázisrendszer szigorú monoton növése miatt $\dfrac{d_{k+1}}{d_k} \geq 2$, tehát $d_{k+1} = \left(\dfrac{d_{k+1}}{d_k}\right) d_k \geq 2d_k \geq 2 \cdot 2^k = 2^{k+1}$, vagyis az egyenlőtlenség teljesül a $k+1$ számra is.

9.2.2. Tétel. (**Természetes szám felbontása bázisrendszer szerint**) *Ha $(d_k)_{k\in\mathbb{N}}$ bázisrendszer, akkor minden $n \in \mathbb{N}^*$ számhoz egyértelműen létezik olyan $m \in \mathbb{N}$ és olyan $(c_k)_{k\in[\![0,m]\!]}$ rendszer, hogy minden $k \in [\![0,m]\!]$ esetén $c_k \in \left[\!\!\left[0, \dfrac{d_{k+1}}{d_k} - 1\right]\!\!\right]$, és $c_m \neq 0$, és*

$$n = \sum_{k=0}^{m} c_k d_k.$$

Bizonyítás. (*Egzisztencia.*) n szerinti teljes indukcióval bizonyítunk.

Az $n := 1$ esetben $m := 0$ és $c_0 := 1$ olyan természetes számok, hogy $c_0 \leq \dfrac{d_1}{d_0} - 1$, és $n = c_0 d_0$.

Legyen $n \in \mathbb{N}$ olyan, hogy $n \geq 2$, és az állítás teljesül minden n-nél kisebb, nem nulla természetes számra. Minden $k \in \mathbb{N}$ esetén $d_k \geq 2^k > k$, ezért $\{k \in \mathbb{N} | n < d_{k+1}\} \neq \emptyset$, így vehetjük az

$$m := \min\left(\{k \in \mathbb{N} | n < d_{k+1}\}\right)$$

természetes számot. Az m szám minimalitási tulajdonsága miatt $d_m \leq n$. Nyilvánvaló, hogy $\left\{j \in \left[\!\!\left[1, \dfrac{d_{m+1}}{d_m} - 1\right]\!\!\right] \;\middle|\; n < (j+1)d_m\right\} \neq \emptyset$, így vehetjük a

$$c_m := \min\left(\left\{j \in \left[\!\!\left[1, \frac{d_{m+1}}{d_m} - 1\right]\!\!\right] \;\middle|\; n < (j+1)d_m\right\}\right)$$

természetes számot. A c_m szám minimalitási tulajdonsága miatt $c_m d_m \leq n$, tehát $1 \leq c_m$ miatt $d_m \leq c_m d_m \leq n < (c_m+1)d_m$.

Ha $c_m d_m = n$, akkor minden $k < m$ természetes számra legyen $c_k := 0$, tehát ekkor $(c_k)_{k\in[\![0,m]\!]}$ olyan rendszer, hogy minden $k \in [\![0,m]\!]$ esetén $c_k \in \left[\!\!\left[0, \frac{d_{k+1}}{d_k} - 1\right]\!\!\right]$, és $c_m \neq 0$, és

$$n = 0 + c_m d_m = \sum_{k=0}^{m-1} c_k d_k + c_m d_m = \sum_{k=0}^{m} c_k d_k,$$

vagyis az egzisztencia teljesül.

Ha $c_m d_m < n$, akkor $n - c_m d_m < n$, így az indukciós hipotézis miatt van olyan $m' \in \mathbb{N}$ és olyan $(c'_k)_{k\in[\![0,m']\!]}$ rendszer, hogy minden $k \in [\![0,m']\!]$ esetén $c'_k \in \left[\!\!\left[0, \frac{d_{k+1}}{d_k} - 1\right]\!\!\right]$, és $c'_{m'} \neq 0$, és

$$n - c_m d_m = \sum_{k=0}^{m'} c'_k d_k.$$

Ekkor $m' < m$. Valóban, fennáll a következő egyenlőtlenség-lánc

$$d_{m'} \leq c'_{m'} d_{m'} \leq \sum_{k=0}^{m'} c'_k d_k = n - c_m d_m < (c_m+1)d_m - c_m d_m = d_m,$$

vagyis $d_{m'} < d_m$, ezért $m' < m$, hiszen a $(d_k)_{k\in\mathbb{N}}$ bázisrendszer szigorúan monoton növő. Most látható, hogy

$$n = (n - c_m d_m) + c_m d_m = \sum_{k=0}^{m'} c'_k d_k + c_m d_m,$$

tehát, ha $(c_k)_{k\in[\![0,m-1]\!]}$ az a rendszer, amelyre

$$c_k := \begin{cases} c'_k & \text{, ha } k \leq m', \\ 0 & \text{, ha } m'+1 \leq k \leq m-1, \end{cases}$$

akkor a $(c_k)_{k\in[\![0,m]\!]}$ rendszerre minden $k \in [\![0,m]\!]$ esetén $c_k \in \left[\!\!\left[0, \frac{d_{k+1}}{d_k} - 1\right]\!\!\right]$ teljesül, és $c_m \neq 0$, és

$$n = \sum_{k=0}^{m'} c'_k d_k + c_m d_m = \sum_{k=0}^{m} c_k d_k$$

vagyis az egzisztencia teljesül.

(*Unicitás.*) Először azt mutatjuk meg, hogy ha $n \in \mathbb{N}^*$, és $m \in \mathbb{N}$ olyan szám, valamint $(c_k)_{k\in[\![0,m]\!]}$ olyan rendszer, hogy minden $k \in [\![0,m]\!]$ esetén $c_k \in \left[\!\!\left[0, \frac{d_{k+1}}{d_k} - 1\right]\!\!\right]$, és $c_m \neq 0$, és $n = \sum_{k=0}^{m} c_k d_k$, akkor szükségképpen $m = \min(\{j \in \mathbb{N} | n < d_{j+1}\})$, tehát m egyértelműen van meghatározva.

Valóban, 9.1.6. alapján

$$n = \sum_{k=0}^{m} c_k d_k \leq \sum_{k=0}^{m} \left(\frac{d_{k+1}}{d_k} - 1\right) d_k = \sum_{k=0}^{m} (d_{k+1} - d_k) = d_{m+1} - 1 < d_{m+1},$$

tehát $m \in \{j \in \mathbb{N} | n < d_{j+1}\}$. Másfelől, ha $j \in \mathbb{N}$ és $n < d_{j+1}$, akkor $1 \leq c_m$ miatt

$$d_m \leq d_m c_m \leq \sum_{k=0}^{m} c_k d_k = n < d_{j+1},$$

ezért $m < j+1$, különben a bázisrendszer monoton növése miatt $d_{j+1} \leq d_m$ teljesülne. Ez azt jelenti, hogy m a $\{j \in \mathbb{N} | n < d_{j+1}\}$ halmaz legkisebb eleme. Ezzel m egyértelműségét igazoltuk.

Legyen most $m \in \mathbb{N}$, valamint legyenek $(c_k)_{k \in [\![0,m]\!]}$ és $(c'_k)_{k \in [\![0,m]\!]}$ olyan rendszerek, hogy minden $k \in [\![0, m]\!]$ esetén $c_k, c'_k \in \left[\!\!\left[0, \dfrac{d_{k+1}}{d_k} - 1\right]\!\!\right]$, és $c_m \neq 0 \neq c'_m$, és $\sum_{k=0}^{m} c_k d_k = \sum_{k=0}^{m} c'_k d_k$. Meg fogjuk mutatni, hogy minden $k \in [\![0, m]\!]$ esetén $c_k = c'_k$. Ha $m = 0$, akkor a $d_0 = 1$ feltétel alapján a $c_0 d_0 = c'_0 d_0$ egyenlőség éppen azt jelenti, hogy $c_0 = c'_0$. Ezért a továbbiakban feltesszük, hogy $m > 0$.

Először azt igazoljuk, hogy $c_m = c'_m$. Indirekt bizonyítunk, tehát feltesszük, hogy $c_m \neq c'_m$: legyen például $c_m < c'_m$. Vegyünk olyan $a \in \mathbb{N}^*$ számot, hogy $c'_m = c_m + a$. Ekkor 8.3.5. b) kétszeri alkalmazásával nyerjük, hogy

$$\left(\sum_{k=0}^{m-1} c_k d_k\right) + c_m d_m = \sum_{k=0}^{m} c_k d_k = \sum_{k=0}^{m} c'_k d_k = \left(\sum_{k=0}^{m-1} c'_k d_k\right) + c'_m d_m = \left(\sum_{k=0}^{m-1} c'_k d_k\right) + c_m d_m + a d_m,$$

amiből az összeadás kancellativitása miatt

$$\sum_{k=0}^{m-1} c_k d_k = \left(\sum_{k=0}^{m-1} c'_k d_k\right) + a d_m$$

következik. Ugyanakkor 9.1.6. alapján

$$\sum_{k=0}^{m-1} c_k d_k \leq \sum_{k=0}^{m-1} \left(\frac{d_{k+1}}{d_k} - 1\right) d_k = \sum_{k=0}^{m-1} (d_{k+1} - d_k) = d_m - 1,$$

tehát $a \geq 1$ folytán azt kapjuk, hogy

$$d_m - 1 \geq \sum_{k=0}^{m-1} c_k d_k = \left(\sum_{k=0}^{m-1} c'_k d_k\right) + a d_m \geq a d_m \geq d_m,$$

ami lehetetlen. Hasonló érveléssel ellentmondásra jutunk akkor is, ha $c'_m < c_m$. Ezzel beláttuk, hogy $c_m = c'_m$.

Tekintsük most az $E := \{j \in [\![0, m]\!] \mid (\forall\ k \in [\![j, m]\!])\ c_k = c'_k\}$ halmazt. Az előzőek alapján $m \in E$, így $E \neq \emptyset$: legyen $m_* := \min(E)$. Az $m_* = 0$ kijelentés ekvivalens azzal, hogy $E = [\![0, m]\!]$, ami éppen azt jelenti, hogy minden $k \in [\![0, m]\!]$ esetén $c_k = c'_k$.

Az $m_* = 0$ egyenlőséget indirekt bizonyítjuk, tehát feltesszük, hogy $m_* \geq 1$. Világos, hogy $m_* \in E$ miatt minden $k \in [\![m_*, m]\!]$ számra $c_k = c'_k$, ugyanakkor az m_* szám minimalitási tulajdonságából következik, hogy $c_{m_*-1} \neq c'_{m_*-1}$. Tegyük fel például, hogy $c_{m_*-1} < c'_{m_*-1}$, és vegyünk olyan $a \in \mathbb{N}^*$ számot, amelyre $c'_{m_*-1} = c_{m_*-1} + a$. Ekkor

$$\left(\sum_{k=0}^{m_*-1} c_k d_k\right) + \left(\sum_{k=m_*}^{m} c_k d_k\right) = \sum_{k=0}^{m} c_k d_k = \sum_{k=0}^{m} c'_k d_k = \left(\sum_{k=0}^{m_*-1} c'_k d_k\right) + \left(\sum_{k=m_*}^{m} c'_k d_k\right),$$

és $\sum_{k=m_*}^{m} c_k d_k = \sum_{k=m_*}^{m} c'_k d_k$, így az összeadás kancellativitását alkalmazva

$$\sum_{k=0}^{m_*-1} c_k d_k = \sum_{k=0}^{m_*-1} c'_k d_k$$

adódik. Ha $m_* = 1$ volna, akkor ebből 8.3.5. a) és $d_0 = 1$ alapján $c_0 = c'_0$ következne, holott a hipotézis szerint $c_0 = c_{m_*-1} < c'_{m_*-1} = c'_0$. Ezért $m_* - 1 > 1$, tehát a 8.3.5. b) állítást kétszer alkalmazva kapjuk, hogy

$$\left(\sum_{k=0}^{(m_*-1)-1} c_k d_k\right) + c_{m_*-1} d_{m_*-1} = \sum_{k=0}^{m_*-1} c_k d_k = \sum_{k=0}^{m_*-1} c'_k d_k =$$
$$= \left(\sum_{k=0}^{(m_*-1)-1} c'_k d_k\right) + c'_{m_*-1} d_{m_*-1} = \left(\sum_{k=0}^{(m_*-1)-1} c'_k d_k\right) + c_{m_*-1} d_{m_*-1} + a d_{m_*-1}.$$

Ebből ismét az összeadás kancellativitása alapján

$$\sum_{k=0}^{(m_*-1)-1} c_k d_k = \left(\sum_{k=0}^{(m_*-1)-1} c'_k d_k\right) + a d_{m_*-1}$$

adódik. Ugyanakkor 9.1.6. alapján

$$\sum_{k=0}^{(m_*-1)-1} c_k d_k \leq \sum_{k=0}^{(m_*-1)-1} \left(\frac{d_{k+1}}{d_k} - 1\right) d_k = \sum_{k=0}^{(m_*-1)-1} (d_{k+1} - d_k) = d_{m_*-1} - 1,$$

tehát $a \geq 1$ folytán azt kapjuk, hogy

$$d_{m_*-1} - 1 \geq \sum_{k=0}^{(m_*-1)-1} c_k d_k = \left(\sum_{k=0}^{(m_*-1)-1} c'_k d_k\right) + a d_{m_*-1} \geq a d_{m_*-1} \geq d_{m_*-1},$$

ami lehetetlen. Hasonló érveléssel ellentmondásra jutunk akkor is, ha $c'_{m_*-1} < c_{m_*-1}$. Ezzel beláttuk, hogy $c_{m_*-1} = c'_{m_*-1}$. Ez viszont azt jelenti, hogy $m_* - 1 \in E$, ami ellentmond az m_* szám minimalitási tulajdonságának. ■

9.2.3. Következmény. (**Természetes szám felbontása** a**-alapú számrendszerben**) *Legyen $a \in \mathbb{N}$ olyan, hogy $a > 1$. Minden $n \in \mathbb{N}^*$ számhoz egyértelműen létezik olyan $m \in \mathbb{N}$ és olyan $(c_k)_{k\in[\![0,m]\!]}$ rendszer, hogy minden $k \in [\![0, m]\!]$ esetén $c_k \in [\![0, a-1]\!]$ és $c_m \neq 0$ és*

$$n = \sum_{k=0}^{m} c_k a^k.$$

Bizonyítás. Triviálisan következik az előző tételből, a $d_k := a^k$ $(k \in \mathbb{N})$ választással. ■

9.3. Prímszámok és a számelmélet alaptétele

A következő tétel előtt emlékeztetünk arra, hogy $\mathbb{P}$ jelöli a prímszámok halmazát (7.11.6.).

9.3.1. Tétel. *A prímszámok halmaza végtelen.*

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy $\mathbb{P}$ véges halmaz. Természetesen $\mathbb{P} \neq \emptyset$, így képezhető az $n := \prod_{p\in\mathbb{P}} p$ természetes szám. Világos, hogy $n \geq 2$, mert 8.5.4. b) és az egyenlőtlenségek szorzásának szabálya (7.9.6.) alapján

$$n = \Big(\prod_{p\in\mathbb{P}\setminus\{2\}} p\Big) \cdot 2 \geq 1 \cdot 2 = 2.$$

Ezért $n + 1 \geq 2$ is teljesül, így 7.11.7. szerint van olyan $q \in \mathbb{P}$, hogy $q|(n + 1)$, tehát van olyan $a \in \mathbb{N}$, amelyre $n + 1 = q \cdot a$. Ugyanakkor $q|n$, mert 8.5.4. b) alapján

$$n = \Big(\prod_{p\in\mathbb{P}\setminus\{q\}} p\Big) \cdot q,$$

vagyis $b := \prod_{p\in\mathbb{P}\setminus\{q\}} p \in \mathbb{N}$ olyan, hogy $n = q \cdot b$. Ekkor $q \cdot a = n + 1 > n = q \cdot b$, így a 7.9.5. állítás alkalmazásával kapjuk, hogy $a > b$, vagyis létezik olyan $c \in \mathbb{N}^*$, hogy $a = b + c$ (7.9.4.). Nyilvánvaló, hogy $q \cdot b + 1 = n + 1 = q \cdot a = q \cdot b + q \cdot c$, így az összeadás kancellativitása (7.7.3.) folytán $1 = q \cdot c$. Ebből viszont 7.7.6. c) alapján $q = 1$ következik, ami lehetetlen, mert q prímszám. ■

9.3.2. Lemma. *Legyen $p \in \mathbb{P}$ és $h : \mathbb{P} \rightarrowtail \mathbb{N}^*$ olyan függvény, amelyre* $\mathrm{Dom}(h)$ *nem üres, véges halmaz. Ha $p \notin \mathrm{Dom}(h)$, akkor $p \nmid \prod_{q\in\mathrm{Dom}(h)} q^{h(q)}$.*

Bizonyítás. A $\mathrm{Dom}(h)$ halmaz számossága szerinti teljes indukcióval bizonyítunk.

Ha $\mathrm{Card}(\mathrm{Dom}(h)) = 1$, akkor létezik olyan $q_* \in \mathrm{Dom}(h)$, hogy $\mathrm{Dom}(h) = \{q_*\}$. Ekkor 8.5.4. a) szerint $\prod_{q\in\mathrm{Dom}(h)} q^{h(q)} = q_*^{h(q_*)}$, és $p \notin \mathrm{Dom}(h)$ miatt $p \neq q_*$, így a 7.11.12. állításból $p \nmid \prod_{q\in\mathrm{Dom}(h)} q^{h(q)}$ hövetkezik.

Tegyük fel, hogy $n \in \mathbb{N}^*$ olyan szám, hogy az állítás igaz minden olyan $h : \mathbb{P} \rightarrowtail \mathbb{N}^*$ függvényre, amelynek definíciós tartománya véges és $\mathrm{Card}(\mathrm{Dom}(h)) = n$. Legyen $h : \mathbb{P} \rightarrowtail \mathbb{N}^*$ olyan függvény, amelyre $\mathrm{Dom}(h)$ véges és $\mathrm{Card}(\mathrm{Dom}(h)) = n+1$. Rögzítsünk egy $q_* \in \mathrm{Dom}(h)$ elemet, és legyen $h_* : \mathrm{Dom}(h) \setminus \{q_*\} \to \mathbb{N}^*$ a h függvény leszűkítése a $\mathrm{Dom}(h) \setminus \{q_*\}$ halmazra. Mivel $\mathrm{Card}(\mathrm{Dom}(h) \setminus \{q_*\}) = n$, így az indukciós hipotézis szerint $p \nmid \prod_{q\in\mathrm{Dom}(h)\setminus\{q_*\}} q^{h_*(q)}$, továbbá $p \notin \mathrm{Dom}(h)$ és $q_* \in \mathrm{Dom}(h)$ miatt $p \neq q_*$, így 7.11.12. alapján $p \nmid q_*^{h(q_*)}$. Ezért az Euklidész-lemma (7.11.11.) alapján

$$p \nmid \Big(\prod_{q\in\mathrm{Dom}(h)\setminus\{q_*\}} q^{h_*(q)}\Big) \cdot q_*^{h(q_*)}.$$

Ugyanakkor 8.5.4. b) szerint

$$\prod_{q\in\mathrm{Dom}(h)} q^{h(q)} = \Big(\prod_{q\in\mathrm{Dom}(h)\setminus\{q_*\}} q^{h(q)}\Big) \cdot q_*^{h(q_*)} = \Big(\prod_{q\in\mathrm{Dom}(h)\setminus\{q_*\}} q^{h_*(q)}\Big) \cdot q_*^{h(q_*)},$$

ami azt jelenti, hogy $p \nmid \prod_{q\in\mathrm{Dom}(h)} q^{h(q)}$. ■

9.3.3. Tétel. (**A számelmélet alaptétele**) *Minden* $n \in \mathbb{N}$ *természetes számhoz,* $n \geq 2$ *esetén egyértelműen létezik olyan* $f : \mathbb{P} \rightarrowtail \mathbb{N}^*$ *függvény, hogy* $\mathrm{Dom}(f) \subseteq \mathbb{P}$ *nem üres véges halmaz és*

$$n = \prod_{p \in \mathrm{Dom}(f)} p^{f(p)}.$$

Bizonyítás. (*Egzisztencia.*) Teljes indukcióval igazoljuk azt, hogy minden $n \in \mathbb{N}$ természetes számhoz, $n \geq 2$ esetén létezik olyan $m \in \mathbb{N}$ és létezik olyan $g : [\![0, m]\!] \to \mathbb{P}$ függvény, hogy

$$n = \prod_{i=0}^{m} g(i).$$

Ez $n = 2$ esetén az $m := 0$ és $g(0) := 2$ választással 8.3.5. a) alapján igaz. Legyen $n \geq 2$ olyan természetes szám, hogy az állítás minden n-nél kisebb, 2-nél nagyobb-egyenlő természetes számra igaz.

Ha $n \in \mathbb{P}$, akkor az $m := 0$ és $g(0) := n$ választással az állítás 8.3.5. a) alapján igaz. Tegyük fel, hogy $n \notin \mathbb{P}$, és legyenek $a, b \in \mathbb{N}$ olyanok, hogy $1 < a, b < n$ és $n = a \cdot b$. Az indukciós hipotézis szerint az állítás a-ra és b-re igaz, tehát léteznek olyan $m_a, m_b \in \mathbb{N}$ számok és olyan $g_a : [\![0, m_a]\!] \to \mathbb{P}$, valamint $g_a : [\![0, m_a]\!] \to \mathbb{P}$ függvények, hogy

$$a = \prod_{j=0}^{m_a} g_a(j), \quad b = \prod_{k=0}^{m_b} g_b(j).$$

Értelmezve a

$$g : [\![0, m_a + m_b + 1]\!] \to \mathbb{P}; \quad i \mapsto \begin{cases} g_a(i) & \text{, ha } 0 \leq i \leq m_a; \\ g_b(i - (m_a + 1)) & \text{, ha } m_a + 1 \leq i \leq m_a + m_b + 1 \end{cases}$$

függvényt, 8.3.5. d) alapján

$$n = a \cdot b = \left(\prod_{j=0}^{m_a} g_a(j) \right) \cdot \left(\prod_{k=0}^{m_b} g_b(j) \right) = \prod_{i=0}^{m_a+m_b+1} g(i),$$

tehát az állítás n-re is igaz. Ezért az állítás minden $n \geq 2$ természetes számra igaz.

Legyen $n \in \mathbb{N}$ olyan, hogy $n \geq 2$, és az előzőek alapján vegyünk olyan $m \in \mathbb{N}$ számot és $g : [\![0, m]\!] \to \mathbb{P}$ függvényt, amelyre $n = \prod_{i=0}^{m} g(i)$. Ekkor 9.1.2. alkalmazásával kapjuk, hogy

$$n = \prod_{i=0}^{m} g(i) = \prod_{i \in [\![0,m]\!]} g(i) = \prod_{p \in \mathrm{Im}(g)} p^{\mathrm{Card}(\overset{-1}{g}\langle\{p\}\rangle)},$$

tehát, ha $\mathrm{Dom}(f) := \mathrm{Im}(g)$ és értelmezzük az

$$f : \mathrm{Im}(g) \to \mathbb{N}^*; \quad p \mapsto \mathrm{Card}(\overset{-1}{g}\langle\{p\}\rangle)$$

függvényt, akkor $\mathrm{Dom}(f) \subseteq \mathbb{P}$ nem üres véges halmaz (és $\mathrm{Card}(\mathrm{Dom}(f)) \leq m + 1$), továbbá

$$n = \prod_{p \in \mathrm{Dom}(f)} p^{f(p)},$$

amivel az egzisztencia bizonyítását befejeztük.

(*Unicitás.*) Legyenek $f, g : \mathbb{P} \rightarrowtail \mathbb{N}^*$ olyan függvények, hogy $\mathrm{Dom}(f)$ és $\mathrm{Dom}(g)$ nem üres, véges halmazok, valamint

$$\prod_{p\in\mathrm{Dom}(f)} p^{f(p)} = \prod_{p\in\mathrm{Dom}(g)} p^{g(p)}.$$

Jelölje ezt a számot n, továbbá minden $p \in \mathrm{Dom}(f)$ esetén legyen

$$a(p) := \begin{cases} \prod\limits_{q\in\mathrm{Dom}(f)\setminus\{p\}} q^{f(q)} & \text{, ha } \mathrm{Dom}(f) \neq \{p\}; \\ 1 & \text{, ha } \mathrm{Dom}(f) = \{p\}, \end{cases}$$

valamint minden $p \in \mathrm{Dom}(g)$ esetén legyen

$$b(p) := \begin{cases} \prod\limits_{q\in\mathrm{Dom}(g)\setminus\{p\}} q^{g(q)} & \text{, ha } \mathrm{Dom}(g) \neq \{p\}; \\ 1 & \text{, ha } \mathrm{Dom}(g) = \{p\}. \end{cases}$$

A 8.5.4. a) és b) állításokból következik, hogy minden $p \in \mathrm{Dom}(f)$ esetén $n = a(p)\cdot p^{f(p)}$, és minden $p \in \mathrm{Dom}(g)$ esetén $n = b(p) \cdot p^{g(p)}$.

Most megmutatjuk, hogy $\mathrm{Dom}(f) = \mathrm{Dom}(g)$. Legyen $p \in \mathrm{Dom}(f)$ rögzített. Mivel $f(p) > 1$, így van olyan $k \in \mathbb{N}$, amelyre $f(p) = k + 1$, tehát $p^{f(p)} = p^k \cdot p$, amiből következik, hogy $p \mid p^{f(p)}$. Ugyanakkor $n = a(p) \cdot p^{f(p)}$, így $p^{f(p)} \mid n$. Ezért $p \mid n = \prod_{p\in\mathrm{Dom}(g)} p^{g(p)}$, amiből 9.3.2. alapján $p \in \mathrm{Dom}(g)$ következik. Ez azt jelenti, hogy $\mathrm{Dom}(f) \subseteq \mathrm{Dom}(g)$. Az f és g függvények felcserélésével, teljesen hasonló érveléssel kapjuk, hogy $\mathrm{Dom}(g) \subseteq \mathrm{Dom}(f)$. Tehát $\mathrm{Dom}(f) = \mathrm{Dom}(g)$; legyen E ez a halmaz.

Végül megmutatjuk, hogy minden $p \in E$ esetén $f(p) = g(p)$. Legyen $p \in E$ rögzített. Ekkor $a(p) \cdot p^{f(p)} = n = b(p) \cdot p^{g(p)}$, és két eset lehetséges: $E = \{p\}$ vagy $E \neq \{p\}$.

– Tegyük fel, hogy $E = \{p\}$. Ekkor a definíció szerint $a(p) = 1 = b(p)$, tehát $p^{f(p)} = n = p^{g(p)}$. Ha $f(p) \leq g(p)$, akkor létezik olyan $k \in \mathbb{N}$, hogy $f(p) + k = g(p)$, így a hatványozás azonosságai szerint $p^{f(p)} = p^{f(p)} \cdot p^k$. De $p \neq 0$ miatt 7.7.9. a) alapján $p^{f(p)} \neq 0$, így a szorzás kancellativitását alkalmazva kapjuk, hogy $1 = p^k$. Mivel $p \neq 1$, így 7.7.9. b) alapján ebből $k = 0$ következik, tehát $f(p) = g(p)$. Hasonlóan kapjuk, hogy $g(p) \leq f(p)$ esetén $g(p) = f(p)$.

– Tegyük fel, hogy $E \neq \{p\}$. Ekkor $a(p) \cdot p^{f(p)} = n = b(p) \cdot p^{g(p)}$. Ha $f(p) \leq g(p)$, akkor létezik olyan $k \in \mathbb{N}$, hogy $f(p) + k = g(p)$, így a hatványozás azonosságai szerint $a(p) \cdot p^{f(p)} = b(p) \cdot p^{f(p)} \cdot p^k$. De $p \neq 0$ miatt 7.7.9. a) alapján $p^{f(p)} \neq 0$, így a szorzás kancellativitását alkalmazva kapjuk, hogy $a(p) = b(p) \cdot p^k$. Ha $k \neq 0$, akkor $p \mid p^k$, így $p \mid a(p) = \prod_{q\in\mathrm{Dom}(f)\setminus\{p\}} q^{f(q)}$, ami 9.3.2. miatt lehetetlen. Ezért $k = 0$, következésképpen $f(p) = g(p)$. Hasonló érveléssel kapjuk, hogy $g(p) \leq f(p)$ esetén is $f(p) = g(p)$.

Ezzel igazoltuk, hogy $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ és minden $p \in \mathrm{Dom}(f)$ esetén $f(p) = g(p)$, tehát $f = g$. ■

A számelmélet alaptételét – kevésbé pontosan – úgy szokták megfogalmazni, hogy minden 1-nél nagyobb természetes szám előáll prímszámhatványok szorzataként, és az ebben a szorzatban szerelő prímszámok a sorrendjüktől eltekintve egyértelműen vannak meghatározva.

9.4. Faktoriálisok és binomiális együtthatók

A kombinatorika elemeiben különféleképpen értelmezett véges halmazok számosságát határozzuk meg. Rendszerint úgy jelölünk ki egy véges halmazt, amelynek a számosságára vagyunk kíváncsiak, hogy rögzítünk egy véges halmazt, és előírunk e halmaz elemeire vonatkozóan valamilyen kiválasztási feltételt, majd az adott feltételnek eleget tevő elemek halmazát tekintjük.

Az elemi kombinatorika szempontjából különösen fontos a következő definíció.

9.4.1. Definíció. *Az $1 \in \mathbb{N}$ kezdőpont és a*

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}; \quad (n, m) \mapsto m \cdot (n+1)$$

*függvény által elemi rekurzióval meghatározott $\mathbb{N}$-ben haladó sorozat n-edik tagját $n!$ jelöli és ezt a természetes számot $n-$***faktoriálisnak** *nevezzük.*

Tehát $0! := 1$ és minden $n \in \mathbb{N}$ esetén $(n+1)! = n! \cdot (n+1)$, következésképpen

$$\begin{aligned} 1! &= 0! \cdot 1 = 1, \\ 2! &= 1! \cdot 2 = 1 \cdot 2, \\ 3! &= 2! \cdot 3 = 1 \cdot 2 \cdot 3, \\ 4! &= 3! \cdot 4 = 1 \cdot 2 \cdot 3 \cdot 4, \end{aligned}$$

s.í.t. Könnyen látható, hogy ha $\mathbf{s}$ az az $\mathbb{N}$-ben haladó sorozat, amelyre minden $n \in \mathbb{N}$ esetén

$$\mathbf{s}(n) := \begin{cases} 1 & \text{, ha } n = 0, \\ \prod\limits_{k=1}^{n} k & \text{, ha } n > 0, \end{cases}$$

akkor minden $n \in \mathbb{N}$ számra, ha $n > 0$, akkor

$$\mathbf{s}(n+1) = \prod_{k=1}^{n+1} k = \left(\prod_{k=1}^{n} k \right) \cdot (n+1) = \mathbf{s}(n) \cdot (n+1),$$

ugyanakkor $\mathbf{s}(0) = 1$ miatt $\mathbf{s}(0+1) = \mathbf{s}(1) = \prod\limits_{k=1}^{1} k = 1 = 1 \cdot 1 = \mathbf{s}(0) \cdot 1 = \mathbf{s}(0) \cdot (0+1)$, amiből az elemi rekurzióval előállított sorozatok egyértelműsége alapján következik, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{s}(n) = n!$, tehát ha $n > 0$, akkor

$$n! = \prod_{k=1}^{n} k.$$

9.4.2. Definíció. *Minden E halmazra $\mathfrak{S}(E)$ jelöli az $E \to E$ bijekciók halmazát, és $\mathfrak{S}(E)$ elemeit az E halmaz* **permutációinak** *nevezzük.*

Ha $n \in \mathbb{N}$, akkor $\mathfrak{S}(n)$ helyett általában a $\mathfrak{S}_n$ jelölést alkalmazzuk az $n \to n$ bijekciók halmazának jelölésére.

9.4.3. Állítás. *Ha E véges halmaz, akkor $\mathfrak{S}(E)$ véges halmaz, és*

$$\mathrm{Card}(\mathfrak{S}(E)) = (\mathrm{Card}(E))!$$

teljesül.

Bizonyítás. Nyilvánvaló, hogy $\mathfrak{S}(E) \subseteq \mathscr{F}(E;E)$, ezért $\mathfrak{S}(E)$ végessége azonnal következik az 8.1.21. és 8.1.8. állításokból.

Az $\mathfrak{S}(E)$ halmaz számosságára vonatkozó egyenlőséget az E véges halmaz számossága szerinti teljes indukcióval bizonyítjuk, tehát azt igazoljuk, hogy minden $n \in \mathbb{N}$ számra és minden E véges halmazra, ha $\mathrm{Card}(E) = n$, akkor $\mathrm{Card}(\mathfrak{S}(E)) = n!$.

Ha $n = 0$, akkor $E = \emptyset$, következésképpen $\mathfrak{S}(E) = \{\emptyset\} =: 1$, tehát $\mathrm{Card}(\mathfrak{S}(E)) = 1 =: 0! = (\mathrm{Card}(E))!$.

Legyen $n \in \mathbb{N}$ olyan szám, amelyre teljesül az állítás, és legyen E olyan véges halmaz, amelyre $\mathrm{Card}(E) = n+1$. Rögzítsünk egy $\mathfrak{a} \in E$ elemet, és legyen $E' := E \setminus \{\mathfrak{a}\}$. Ekkor $\mathrm{Card}(E') = n$, tehát az indukciós hipotézis szerint $\mathrm{Card}(\mathfrak{S}(E')) = n!$. Nyilvánvaló, hogy

$$\mathfrak{S}(E) = \{f \in \mathfrak{S}(E) | f(\mathfrak{a}) \neq \mathfrak{a}\} \cup \{f \in \mathfrak{S}(E) | f(\mathfrak{a}) = \mathfrak{a}\},$$

és itt a jobb oldalon két diszjunkt halmaz áll, ezért 8.1.14. alapján

$$\mathrm{Card}(\mathfrak{S}(E)) = \mathrm{Card}(\{f \in \mathfrak{S}(E) | f(\mathfrak{a}) \neq \mathfrak{a}\}) + \mathrm{Card}(\{f \in \mathfrak{S}(E) | f(\mathfrak{a}) = \mathfrak{a}\}).$$

Ha $f \in \mathfrak{S}(E)$ és $f(\mathfrak{a}) = \mathfrak{a}$, akkor nyilvánvalóan $f|_{E'} \in \mathfrak{S}(E')$, és az

$$\{f \in \mathfrak{S}(E) | f(\mathfrak{a}) = \mathfrak{a}\} \to \mathfrak{S}(E'); \quad f \mapsto f|_{E'}$$

leképezés bijekció, ezért az indukciós hipotézis alapján

$$\mathrm{Card}(\{f \in \mathfrak{S}(E) | f(\mathfrak{a}) = \mathfrak{a}\}) = \mathrm{Card}(\mathfrak{S}(E')) = n!.$$

Vezessük be az $\mathscr{E} := \{f \in \mathfrak{S}(E) | f(\mathfrak{a}) \neq \mathfrak{a}\}$ jelölést. Ekkor az előzőek alapján írhatjuk, hogy

$$\mathrm{Card}(\mathfrak{S}(E)) = \mathrm{Card}(\mathscr{E}) + n!.$$

Értelmezzük a következő leképezést:

$$\Phi : \mathscr{E} \to E'; \quad f \mapsto f(\mathfrak{a}).$$

Világos, hogy $\mathfrak{a}' \in E'$ esetén $\overset{-1}{\Phi}\langle\{\mathfrak{a}'\}\rangle = \{f \in \mathfrak{S}(E) | f(\mathfrak{a}) = \mathfrak{a}'\}$, és nyilvánvaló, hogy a

$$\overset{-1}{\Phi}\langle\{\mathfrak{a}'\}\rangle \mapsto \mathscr{F}(E'; E \setminus \{\mathfrak{a}'\}); \quad f \mapsto f|_{E'}$$

leképezés bijekció $\overset{-1}{\Phi}\langle\{\mathfrak{a}'\}\rangle$ és az $E' \to E \setminus \{\mathfrak{a}'\}$ bijekciók halmaza között. Ugyanakkor, $\mathfrak{a}' \in E'$ esetén az $E \setminus \{\mathfrak{a}'\}$ halmaz ekvipotens E'-vel, ezért az $E' \to E \setminus \{\mathfrak{a}'\}$ bijekciók halmaza ekvipotens az $E' \to E'$ bijekciók halmazával, vagyis $\mathfrak{S}(E')$-vel. Ezért a 6.8.2. állítás szerint $\mathscr{E}$ és $E' \times \mathfrak{S}(E')$ ekvipotensek, tehát 8.1.17. és az indukciós hipotézis alapján

$$\mathrm{Card}(\mathscr{E}) = \mathrm{Card}(E') \cdot \mathrm{Card}(\mathfrak{S}(E')) = n \cdot n!,$$

amiből következik a bizonyítandó

$$\mathrm{Card}(\mathfrak{S}(E)) = n \cdot n! + n! = n! \cdot n + n! = n! \cdot (n+1) =: (n+1)! = (\mathrm{Card}(E))!$$

egyenlőség. ■

Ha E véges halmaz, akkor a $\mathscr{P}(E)$ hatványhalmaz is véges (8.1.22.), továbbá véges halmaz minden részhalmaza véges (8.1.8.), ezért értelmes a következő definíció.

9.4.4. Definíció. *Minden $k, n \in \mathbb{N}$ számra*

$$\binom{n}{k} := \mathrm{Card}(\{H \in \mathscr{P}(n) \mid \mathrm{Card}(H) = k\}),$$

vagyis $\binom{n}{k}$ *az n természetes szám k-számosságú részhalmazai halmazának számossága. Ezeket a természetes számokat* **binomiális együtthatóknak** *nevezzük.*

9.4.5. Állítás. *Minden $k, n \in \mathbb{N}$ számra,*
– ha $k \leq n$, akkor

$$k! \cdot (n-k)! \cdot \binom{n}{k} = n!,$$

– ha $k > n$, akkor

$$\binom{n}{k} = 0.$$

Bizonyítás. Megállapodunk abban, hogy a bizonyításban $\mathscr{B}(X;Y)$ jelöli az $X \to Y$ bijekciók halmazát és $\mathscr{I}(X;Y)$ jelöli az $X \to Y$ injekciók halmazát.

Legyenek $k, n \in \mathbb{N}$ olyan természetes számok, hogy $k \leq n$. Ha $f \in \mathscr{B}(n;n)$, akkor az $f|_k : k \to n$ és $f|_{n\setminus k} : n \setminus k \to n$ leszűkített függvények olyan injekciók, hogy $\mathrm{Im}(f|_k) \cap \mathrm{Im}(f|_{n\setminus k}) = \emptyset$. Világos, hogy $f \in \mathscr{B}(n;n)$ esetén $f = (f|_k) \cup (f|_{n\setminus k})$. Továbbá, ha (g,h) olyan pár, hogy $g : k \to n$ injekció és $h : n\setminus k \to n$ injekció, és $\mathrm{Im}(g) \cap \mathrm{Im}(h) = \emptyset$, akkor az $f := g \cup h$ halmaz olyan $n \to n$ bijekció, amelyre $f|_k = g$ és $f|_{n\setminus k} = h$. Ez azt jelenti, hogy az

$$\mathscr{B}(n;n) \to \{(g,h) \in \mathscr{I}(k;n) \times \mathscr{I}(n \setminus k;n) \mid \mathrm{Im}(g) \cap \mathrm{Im}(h) = \emptyset\}; \quad f \mapsto (f|_k, f|_{n\setminus k})$$

leképezés bijekció, amiből 9.4.3. alapján kapjuk, hogy

$$n! = \mathrm{Card}(\mathscr{B}(n;n)) = \mathrm{Card}(\{(g,h) \in \mathscr{I}(k;n) \times \mathscr{I}(n \setminus k;n) \mid \mathrm{Im}(g) \cap \mathrm{Im}(h) = \emptyset\}).$$

Könnyen látható, hogy

$$\begin{aligned}\{(g,h) \in \mathscr{I}(k;n) \times \mathscr{I}(n \setminus k;n) \mid \mathrm{Im}(g) \cap \mathrm{Im}(h) = \emptyset\} = \\ = \bigcup_{\substack{H \subseteq n \\ \mathrm{Card}(H)=k}} \left(\mathscr{B}(k;H) \times \mathscr{B}(n \setminus k; n \setminus H)\right),\end{aligned}$$

és nyilvánvaló, hogy itt a jobb oldalon diszjunkt halmazrendszer uniója áll. Ebből a 8.7.1. és 8.1.17. állítások, valamint a binomiális együtthatók értelmezése alapján kapjuk, hogy

$$\begin{aligned}n! &= \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=k}} \left(\mathrm{Card}(\mathscr{B}(k;H)) \cdot \mathrm{Card}(\mathscr{B}(n \setminus k; n \setminus H))\right) = \\ &= \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=k}} (k! \cdot (n-k)!) = k! \cdot (n-k)! \cdot \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=k}} 1 = k! \cdot (n-k)! \cdot \binom{n}{k},\end{aligned}$$

amit bizonyítani kellett. ■

9.4.6. Következmény. *Minden $k, n \in \mathbb{N}$ számra, ha $k \leq n$, akkor $k! \cdot (n-k)!$ nem nulla osztója $n!$-nak, és*

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

(ld. 7.11.3.).

9.4.7. Állítás. *Legyenek $k, n \in \mathbb{N}$, és jelölje $\mathscr{M}(k;n)$ a $k \to n$ szigorúan monoton növő függvények halmazát, valamint $\mathscr{I}(k;n)$ a $k \to n$ injektív függvények halmazát.*

a) *Az $\mathscr{M}(k;n) \to \mathscr{P}(n)$; $\varrho \mapsto \operatorname{Im}(\varrho)$ leképezés bijekció az $\mathscr{M}(k;n)$ halmaz és az n halmaz k-elemű részhalmazainak halmaza között, és fennáll a*

$$\operatorname{Card}(\mathscr{M}(k;n)) = \binom{n}{k}$$

egyenlőség.

b) *A $(\{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\})_{\varrho \in \mathscr{M}(k;n)}$ halmazrendszer diszjunkt, és*

$$\mathscr{I}(k;n) = \bigcup_{\varrho \in \mathscr{M}(k;n)} \{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\},$$

továbbá fennáll a

$$\operatorname{Card}(\mathscr{I}(k;n)) = k! \binom{n}{k}$$

egyenlőség.

Bizonyítás. a) Ha $\varrho \in \mathscr{M}(k;n)$, akkor ϱ injektív, tehát ϱ bijekció k és $\operatorname{Im}(\varrho)$ között, így $\operatorname{Card}(\operatorname{Im}(\varrho)) = k$, tehát a vizsgált függvény az n halmaz k-elemű részhalmazainak halmazába érkezik. Továbbá, az $\mathscr{M}(k;n) \to \mathscr{P}(n)$; $\varrho \mapsto \operatorname{Im}(\varrho)$ leképezés injektív, mert ha $\varrho, \varrho' \in \mathscr{M}(k;n)$ és $\operatorname{Im}(\varrho) = \operatorname{Im}(\varrho')$, akkor $\varrho^{-1} \circ \varrho' : k \to k$ szigorúan monoton növő bijekció, így 6.13.11. alapján $\varrho^{-1} \circ \varrho' = \mathrm{id}_k$, tehát $\varrho = \varrho'$. Ebből és a binomiális együtthatók definíciójából következik, hogy a) bizonyításához elég azt igazolni, hogy a $\mathscr{M}(k;n) \to \mathscr{P}(n)$; $\varrho \mapsto \operatorname{Im}(\varrho)$ leképezés *ráképez* az n halmaz k-elemű részhalmazainak halmazára.

Legyen $H \subseteq n$ olyan halmaz, amelyre $\operatorname{Card}(H) = k$, és vegyünk olyan $f : k \to H$ függvényt, amely bijekció. A 8.2.4. állítás szerint van olyan $\sigma \in \mathfrak{S}_k$, hogy a $\varrho := f \circ \sigma : k \to H$ függvény szigorúan monoton növő, tehát $\varrho \in \mathscr{M}(k;n)$ és $\operatorname{Im}(\varrho) = \operatorname{Im}(f) = H$. Ez azt jelenti, hogy az $\mathscr{M}(k;n) \to \mathscr{P}(n)$; $\varrho \mapsto \operatorname{Im}(\varrho)$ függvény ráképez az n halmaz k-elemű részhalmazainak halmazára.

b) Az előző bekezdésből következik, hogy minden $f \in \mathscr{I}(k;n)$ esetén van olyan $\sigma \in \mathfrak{S}_k$, hogy $\varrho := f \circ \sigma \in \mathscr{M}(k;n)$, így $f = (f \circ \sigma) \circ \sigma^{-1} \in \{\varrho \circ \sigma' | \sigma' \in \mathfrak{S}_k\}$, tehát fennáll az $\mathscr{I}(k;n) \subseteq \bigcup_{\varrho \in \mathscr{M}(k;n)} \{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\}$ összefüggés. A fordított tartalmazás nyilvánvaló, így itt egyenlőség áll. Tegyük fel, hogy $\varrho, \varrho' \in \mathscr{M}(k;n)$ és $\{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\} \cap \{\varrho' \circ \sigma | \sigma \in \mathfrak{S}_k\} \neq \emptyset$. Ekkor vehetünk olyan $\sigma, \sigma' \in \mathfrak{S}_k$ permutációkat, amelyekre $\varrho \circ \sigma = \varrho' \circ \sigma'$, tehát $(\varrho')^{-1} \circ \varrho = \sigma' \circ \sigma^{-1} : k \to k$ szigorúan monoton növő bijekció, így 6.13.11. alapján $\varrho^{-1} \circ \varrho' = \mathrm{id}_k$, tehát $\varrho = \varrho'$. Ez azt jelenti, hogy a $(\{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\})_{\varrho \in \mathscr{M}(k;n)}$ halmazrendszer diszjunkt, ezért 8.7.1. alkalmazásával kapjuk, hogy

$$\operatorname{Card}(\mathscr{I}(k;n)) = \sum_{\varrho \in \mathscr{M}(k;n)} \operatorname{Card}(\{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\}).$$

Nyilvánvaló, hogy minden $\varrho \in \mathscr{M}(k;n)$ esetén az $\mathfrak{S}_k \to \{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\}$; $\sigma \mapsto \varrho \circ \sigma$ leképezés bijekció, így 9.4.3. szerint $\mathrm{Card}(\{\varrho \circ \sigma | \sigma \in \mathfrak{S}_k\}) = \mathrm{Card}(\mathfrak{S}_k) = k!$. Ebből 9.1.1. és az a) állítás alkalmazásával adódik, hogy

$$\mathrm{Card}(\mathscr{I}(k;n)) = k!\mathrm{Card}(\mathscr{M}(k;n)) = k!\binom{n}{k}. \blacksquare$$

9.4.8. Állítás. *Minden $k, n \in \mathbb{N}$ számra, ha $k < n$, akkor*

$$\binom{n}{k+1} + \binom{n}{k} = \binom{n+1}{k+1}.$$

Bizonyítás. Ha $(k,n) \in \mathbb{N} \times \mathbb{N}$ és $k \leq n$, akkor 7.11.4. b) alkalmazásával kapjuk, hogy

$$\binom{n}{k+1} = \frac{n!}{(k+1)!(n-(k+1))!} = \frac{n!(n-k)}{(k+1)!(n-(k+1))!(n-k)} = \frac{n!(n-k)}{(k+1)!(n-k)!},$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!(k+1)}{k!(n-k)!(k+1)} = \frac{n!(k+1)}{(k+1)!(n-k)!}.$$

Ezekből az egyenlőségekből 7.11.4. a) alapján kapjuk, hogy

$$\binom{n}{k+1} + \binom{n}{k} = \frac{n!(n-k)}{(k+1)!(n-k)!} + \frac{n!(k+1)}{(k+1)!(n-k)!} = \frac{n!(n-k)+n!(k+1)}{(k+1)!(n-k)!} =$$

$$= \frac{n!(n+1)}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} = \binom{n+1}{k+1},$$

hiszen $(n-k)+(k+1) = n+1$ és $n-k = (n+1)-(k+1)$. $\blacksquare$

Az egész számok halmaza felett a $+$ (összeadás) és $\cdot$ (szorzás) műveletek kommutatívak és asszociatívak. Megállapodunk abban, hogy ha $m, n \in \mathbb{N}$, $m \leq n$ és f olyan függvény, hogy $[\![m,n]\!] \subseteq \mathrm{Dom}(f)$ és $f\langle[\![m,n]\!]\rangle \subseteq \mathbb{Z}$, akkor a

$$\sum_{k=m}^{n} f(k) := \mathop{+}_{k=m}^{n} f(k)$$

$$\mathop{\mathrm{P}}_{k=m}^{n} f(k) := \mathop{\cdot}_{k=m}^{n} f(k)$$

definíciókat, illetve jelöléseket alkalmazzuk. Továbbá, ha I nem üres véges halmaz és f olyan függvény, hogy $I \subseteq \mathrm{Dom}(f)$ és $f\langle I\rangle \subseteq \mathbb{Z}$, akkor a

$$\sum_{i \in I} f(i) := \mathop{+}_{i \in I} f(i)$$

$$\mathop{\mathrm{P}}_{i \in I} f(i) := \mathop{\cdot}_{i \in I} f(i)$$

definíciókat, illetve jelöléseket alkalmazzuk.

9.4.9. Állítás. *Ha $a, b \in \mathbb{Z}$, akkor minden $n \in \mathbb{N}$ esetén*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

teljesül. (**Binomiális formula $\mathbb{Z}$-re**)

Bizonyítás. Rögzített $a, b \in \mathbb{Z}$ esetén n szerinti teljes indukcióval bizonyítunk. Ha $n = 0$, akkor $(a+b)^0 := 1$ és $\sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = 1$. Legyen $n \in \mathbb{N}$ olyan, amelyre igaz a formula. Ekkor a $\mathbb{Z}$ feletti hatványozás értelmezése és a $\mathbb{Z}$ feletti műveletek tulajdonságai, valamint az indukciós hipotézis miatt

$$(a+b)^{n+1} = (a+b)^n(a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right)(a+b) =$$

$$= \left(\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}\right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}\right) =$$

$$= \left(\sum_{k=0}^{n-1} \binom{n}{k} a^{k+1} b^{n-k}\right) + a^{n+1} + \left(\sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k}\right) + b^{n+1} =$$

$$= \left(\sum_{j=1}^{n} \binom{n}{j-1} a^j b^{n+1-j}\right) + a^{n+1} + \left(\sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k}\right) + b^{n+1} =$$

$$= a^{n+1} + \left(\sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{n+1-k}\right) + b^{n+1} =$$

$$= a^{n+1} + \left(\sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k}\right) + b^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{(n+1)-k},$$

vagyis az egyenlőség teljesül az $n+1$ számra is. ■

9.4.10. Következmény. *Minden $n \in \mathbb{N}$ esetén*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Bizonyítás. A binomiális formula szerint

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n. \ ■$$

9.4.11. Következmény. *Minden $n \in \mathbb{N}$ esetén*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \begin{cases} 1 & , \textit{ha } n = 0; \\ 0 & , \textit{ha } n \neq 0. \end{cases}$$

Bizonyítás. A binomiális formula szerint

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = ((-1)+1)^n = 0^n,$$

és $n \neq 0$ esetén $0^n = 0$, valamint (a hatványozás definíciója szerint) $0^0 := 1$. ■

9.4.12. Állítás. *Tekintsük a következő függvényeket:*

$$C : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}^{\mathbb{N}} \quad ; \quad \mathbf{s} \mapsto \left(n \mapsto \sum_{k=0}^{n} \binom{n}{k} \mathbf{s}(k)\right)$$

$$T : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}^{\mathbb{N}} \quad ; \quad \mathbf{s} \mapsto \left(n \mapsto (-1)^n \mathbf{s}(n)\right).$$

Ekkor teljesülnek a következők.

a) *T bijekció és $T^{-1} = T$.*

b) *$C \circ T : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}^{\mathbb{N}}$ bijekció és $(C \circ T)^{-1} = C \circ T$.*

c) *C bijekció és $C^{-1} = T \circ C \circ T$.*

Bizonyítás. a) Ha $\mathbf{s} \in \mathbb{Z}^{\mathbb{N}}$, akkor minden $n \in \mathbb{N}$ esetén

$$((T \circ T)(\mathbf{s}))(n) = (T(T(\mathbf{s})))(n) := (-1)^n (T(\mathbf{s}))(n) := (-1)^n (-1)^n \mathbf{s}(n) = \mathbf{s}(n),$$

ami azt jelenti, hogy $T \circ T = \mathrm{id}_{\mathbb{Z}^{\mathbb{N}}}$, ezért T bijekció és $T^{-1} = T$.

b) Ha $\mathbf{s} \in \mathbb{Z}^{\mathbb{N}}$, akkor minden $n \in \mathbb{N}$ esetén

$$((C \circ T)(\mathbf{s}))(n) = (C(T(\mathbf{s})))(n) := \sum_{k=0}^{n} \binom{n}{k} (T(\mathbf{s}))(k) := \sum_{k=0}^{n} \binom{n}{k} (-1)^k \mathbf{s}(k).$$

Ebből következik, hogy $\mathbf{s} \in \mathbb{Z}^{\mathbb{N}}$ és $n \in \mathbb{N}$ esetén

$$((C \circ T \circ C \circ T)(\mathbf{s}))(n) = ((C \circ T)((C \circ T)(\mathbf{s})))(n) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k ((C \circ T)(\mathbf{s}))(k) =$$

$$= \sum_{k=0}^{n} \binom{n}{k} (-1)^k \left(\sum_{j=0}^{k} \binom{k}{j} (-1)^j \mathbf{s}(j) \right) = \sum_{k=0}^{n} \sum_{j=0}^{k} (-1)^{k+j} \binom{n}{k} \binom{k}{j} \mathbf{s}(j) \overset{(1)}{=}$$

$$\overset{(1)}{=} \sum_{j=0}^{n} \left(\sum_{k=j}^{n} (-1)^{k+j} \binom{n}{k} \binom{k}{j} \mathbf{s}(j) \right) = \sum_{j=0}^{n} (-1)^j \left(\sum_{k=j}^{n} (-1)^k \binom{n}{k} \binom{k}{j} \right) \mathbf{s}(j) \overset{(2)}{=}$$

$$\overset{(2)}{=} \sum_{j=0}^{n} (-1)^j \left(\sum_{l=0}^{n-j} (-1)^{j+l} \binom{n}{j+l} \binom{j+l}{j} \right) \mathbf{s}(j) \overset{(3)}{=}$$

$$\overset{(3)}{=} \sum_{j=0}^{n} \left(\sum_{l=0}^{n-j} (-1)^l \frac{n!}{(n-j-l)!} \frac{1}{j!l!} \right) \mathbf{s}(j) = \sum_{j=0}^{n} \frac{n!}{j!(n-j)!} \left(\sum_{l=0}^{n-j} (-1)^l \frac{(n-j)!}{(n-j-l)!l!} \right) \mathbf{s}(j) =$$

$$= \sum_{j=0}^{n} \binom{n}{j} \left(\sum_{l=0}^{n-j} (-1)^l \binom{n-j}{l} \right) \mathbf{s}(j) \overset{(4)}{=} \binom{n}{n} \mathbf{s}(n) = \mathbf{s}(n),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.4.2. állításban felírt felcserélési formulát alkalmazzuk;

– a $\overset{(2)}{=}$ egyenlőségnél adott $0 \le j \le n$ esetén a k összegzőindexről áttérünk az $l := k - j$ összegzőindexre;

– a $\overset{(3)}{=}$ egyenlőségnél a binomiális együtthatókat felírjuk faktoriálisokkal és egyszerűsítünk a $(j+l)!$ számmal;

– a $\overset{(4)}{=}$ egyenlőségnél felhasználjuk azt, hogy az előző állítás szerint minden $0 \le j \le n$ esetén

$$\sum_{l=0}^{n-j} (-1)^l \binom{n-j}{l} = \begin{cases} 1 & \text{, ha } j = n; \\ 0 & \text{, ha } j < n \end{cases}.$$

Ezzel beláttuk, hogy $(C \circ T) \circ (C \circ T) = \mathrm{id}_{\mathbb{Z}^{\mathbb{N}}}$, így $C \circ T$ bijekció és $(C \circ T)^{-1} = C \circ T$.

c) A b) állításban igazolt $(C \circ T)^{-1} = C \circ T$ egyenlőséget jobbról komponálva T-vel, és figyelembe véve a)-t kapjuk, hogy $C \circ T)^{-1} \circ T = C \circ (T \circ T) = C$, ezért a $C : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}^{\mathbb{N}}$ függvény is bijekció. Ebből a $C \circ (T \circ C \circ T) = \mathrm{id}_{\mathbb{Z}^{\mathbb{N}}}$ egyenlőség alapján következik, hogy $C^{-1} = T \circ C \circ T$. Ez azt jelenti, hogy minden $\mathbf{s} \in \mathbb{Z}^{\mathbb{N}}$ és $n \in \mathbb{N}$ esetén

$$(C^{-1}(\mathbf{s}))(n) = (-1)^n \sum_{k=0}^{n} (-1)^k \binom{n}{k} \mathbf{s}(k). \blacksquare$$

9.4.13. Következmény. *Ha $m, n \in \mathbb{N}$, $m \geq n$, és $S_{m,n}$ az $m \to n$ szürjekciók halmazának számossága, akkor*

$$S_{m,n} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.$$

Bizonyítás. Először az 9.4.12. állításban bevezetett C függvényt alkalmazva igazoljuk, hogy minden $m, p \in \mathbb{N}$ számra, ha $p \leq m$, akkor $p^m = C((S_{m,n})_{n \in \mathbb{N}})(p)$ teljesül.

Legyenek $m, p \in \mathbb{N}$ olyanok, hogy $p \leq m$. Ekkor fennáll az

$$\mathscr{F}(m;p) = \bigcup_{k=0}^{p} \bigcup_{\substack{H \subseteq p \\ \mathrm{Card}(H) = k}} \{f \in \mathscr{F}(m;H) | \mathrm{Im}(f) = H\}$$

egyenlőség, és természetesen $\{f \in \mathscr{F}(m;H) | \mathrm{Im}(f) = H\}$ ekvipotens az $m \to \mathrm{Card}(H)$ szürjekciók halmazával, ezért $\mathrm{Card}(\{f \in \mathscr{F}(m;H) | \mathrm{Im}(f) = H\}) = S_{m,\mathrm{Card}(H)}$. Ebből következik, hogy

$$p^m = \mathrm{Card}(\mathscr{F}(m;p)) = \sum_{k=0}^{p} \sum_{\substack{H \subseteq p \\ \mathrm{Card}(H) = k}} S_{m,k} = \sum_{k=0}^{p} \binom{p}{k} S_{m,k}.$$

Most minden $m \in \mathbb{N}$ esetén értelmezzük az $\mathbf{s}_m := C\left((S_{m,k})_{k \in \mathbb{N}}\right)$ sorozatot, ahol C a 9.4.12. állításban bevezetett függvény. Az előzőek szerint minden $m, p \in \mathbb{N}$ esetén, ha $p \leq m$, akkor $\mathbf{s}_m(p) = p^m$. Ha $m \in \mathbb{N}$, akkor $\mathbf{s}_m$ definíciója és 9.4.12. c) szerint

$$(S_{m,k})_{k \in \mathbb{N}} = C^{-1}(\mathbf{s}_m) = (T \circ C \circ T)(\mathbf{s}_m).$$

Ezért $m, n \in \mathbb{N}$ és $n \leq m$ esetén

$$S_{m,n} = \left((T \circ C \circ T)(\mathbf{s}_m)\right)(n) = (-1)^n \sum_{j=0}^{n} \binom{n}{j} (T(\mathbf{s}_m))(j) =$$

$$= \sum_{j=0}^{n} (-1)^{n+j} \binom{n}{j} j^m = \sum_{k=0}^{n} (-1)^{2n-k} \binom{n}{n-k} (n-k)^m = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m,$$

amit bizonyítani kellett. ■

9.4.14. Következmény. *Ha $n \in \mathbb{N}$, és p_n azon $f : n \to n$ bijekciók halmazának számossága, amelyekre minden $k \in n$ esetén $f(k) \neq k$, akkor*

$$p_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!.$$

Bizonyítás. Emlékeztetünk arra, hogy minden E halmazra $\mathfrak{S}_E$ jelöli az $E \to E$ bijekciók halmazát. Nyilvánvaló, hogy minden $n \in \mathbb{N}$ számra

$$\mathfrak{S}_n = \bigcup_{k=0}^{n} \bigcup_{\substack{H \subseteq n \\ \mathrm{Card}(H)=k}} \{\, f \in \mathfrak{S}_n \mid H = \{j \in n | f(j) = j\}\,\}.$$

Ugyanakkor $n \in \mathbb{N}$ esetén minden $H \subseteq n$ halmazra az

$$\{\, f \in \mathfrak{S}_n \mid H = \{j \in n | f(j) = j\}\,\} \to \{\, f \in \mathfrak{S}_{n \setminus H} \mid (\forall j \in n \setminus H) : f(j) \neq j\,\}; \quad f \mapsto f|_{n \setminus H}$$

leképezés *bijekció*, ezért

$$\begin{gathered}\mathrm{Card}\left(\{\, f \in \mathfrak{S}_n \mid H = \{j \in n | f(j) = j\}\,\}\right) = \\ = \mathrm{Card}\left(\{\, f \in \mathfrak{S}_{n \setminus H} \mid (\forall j \in n \setminus H) : f(j) \neq j\,\}\right) = p_{n-\mathrm{Card}(H)}.\end{gathered}$$

Ebből következik, hogy minden $n \in \mathbb{N}$ esetén

$$n! = \mathrm{Card}(\mathfrak{S}_n) = \sum_{k=0}^{n} \binom{n}{k} p_{n-k} = \sum_{k=0}^{n} \binom{n}{n-k} p_k = \sum_{k=0}^{n} \binom{n}{k} p_k.$$

Ez azt jelenti, hogy ha $\mathbf{s} := C((p_k)_{k \in \mathbb{N}})$, ahol C a 9.4.12. állításban bevezetett függvény, akkor minden $n \in \mathbb{N}$ esetén $\mathbf{s}(n) = n!$. Ugyanakkor $(p_k)_{k \in \mathbb{N}} = C^{-1}(\mathbf{s})$, tehát 9.4.12. c) alapján minden $n \in \mathbb{N}$ esetén

$$\begin{gathered} p_n = \left(C^{-1}(\mathbf{s})\right)(n) = ((T \circ C \circ T)(\mathbf{s}))(n) = (-1)^n \sum_{j=0}^{n} \binom{n}{j} (T(\mathbf{s}))(j) = \\ = \sum_{j=0}^{n} (-1)^{n+j} \binom{n}{j} j! = \sum_{k=0}^{n} (-1)^{2n-k} \binom{n}{n-k} (n-k)! = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!, \end{gathered}$$

amit bizonyítani kellett. ■

9.5. Polinomiális együtthatók és a polinomiális tétel

A binomiális együtthatók természetes általánosításai a *polinomiális együtthatók*. Ezek bevezetését készíti elő a következő lemma.

9.5.1. Lemma. *Ha $m, n \in \mathbb{N}^*$, és $\alpha = (\alpha_i)_{i \in m} \in \mathbb{N}^m$, és $\sum_{i \in m} \alpha_i = n$, akkor a $\prod_{i \in m} (\alpha_i!)$ szám osztója $n!$-nak.*

Bizonyítás. Rögzített $n \in \mathbb{N}^*$ mellett, m szerinti teljes indukcióval bizonyítunk. Az állítás nyilvánvalóan igaz, ha $m = 1 = \{0\}$, mert minden $\alpha \in \mathbb{N}^1$ elemre az $\alpha_0 = \sum_{i \in \{0\}} \alpha_i = n$ egyenlőség maga után vonja, hogy $\prod_{i \in \{0\}} (\alpha_i!) = \alpha_0! = n!$.

Az állítás $m = 2 = \{0, 1\}$ esetén is igaz, hiszen ekkor minden $\alpha \in \mathbb{N}^2$ esetén, ha $\alpha_0 + \alpha_1 = n$, akkor

$$\prod_{i \in \{0,1\}} (\alpha_i!) = \alpha_0! \alpha_1! = \alpha_0!(n - \alpha_0)!,$$

és tudjuk, hogy ez a szám osztója $n!$-nak.

Legyen $m \in \mathbb{N}$ olyan, hogy $m \geq 2$ és m-re teljesül az állítás. Rögzítsünk egy $\alpha = (\alpha_i)_{i\in m} \in \mathbb{N}^{m+1}$ rendszert, amelyre $\sum\limits_{i\in m+1} \alpha_i = n$, és vezessük be azt az $\beta := (\beta_i)_{i\in m} \in \mathbb{N}^m$ rendszert, amelyre minden $i \in m$ esetén

$$\beta_i := \begin{cases} \beta_i & \text{, ha } i < m-1; \\ \alpha_{m-1} + \alpha_m & \text{, ha } i = m-1. \end{cases}$$

Nyilvánvaló, hogy

$$\sum_{i\in m} \beta_i = \Big(\sum_{i\in m-1} \beta_i\Big) + \beta_{m-1} = \Big(\sum_{i\in m-1} \alpha_i\Big) + \alpha_{m-1} + \alpha_m = \sum_{i\in m+1} \alpha_i = n,$$

így az indukciós hipotézis szerint a $\mathop{\mathrm{P}}\limits_{i\in m} (\beta_i!)$ szám osztója $n!$-nak, tehát (egyértelműen) létezik olyan $a \in \mathbb{N}$, hogy

$$\begin{aligned} n! = a \mathop{\mathrm{P}}_{i\in m} (\beta_i!) &= a\Big(\mathop{\mathrm{P}}_{i\in m-1} (\beta_i!)\Big)\beta_{m-1}! = a\Big(\mathop{\mathrm{P}}_{i\in m-1} (\alpha_i!)\Big)(\alpha_{m-1}+\alpha_m)! = qnotag \quad (9.1) \\ &= a\Big(\mathop{\mathrm{P}}_{i\in m-1} (\alpha_i!)\Big)\alpha_{m-1}!\alpha_m!\binom{\alpha_{m-1}+\alpha_m}{\alpha_m} = a\Big(\mathop{\mathrm{P}}_{i\in m+1} (\alpha_i!)\Big)\binom{\alpha_{m-1}+\alpha_m}{\alpha_m}, \end{aligned}$$

ahol felhasználtuk az

$$(\alpha_{m-1}+\alpha_m)! = \alpha_{m-1}!\alpha_m!\binom{\alpha_{m-1}+\alpha_m}{\alpha_m}$$

egyenlőséget. Tehát a $\mathop{\mathrm{P}}\limits_{i\in m+1} (\alpha_i!)$ szám osztója $n!$-nak. ■

9.5.2. Definíció. *Ha $m, n \in \mathbb{N}^*$ és $\alpha = (\alpha_i)_{i\in m} \in \mathbb{N}^m$ olyan, hogy $\sum\limits_{i\in m} \alpha_i = n$, akkor*

$$\binom{n}{\alpha} := \frac{n!}{\mathop{\mathrm{P}}\limits_{i\in m} (\alpha_i!)},$$

és az így értelmezett természetes számokat **polinomiális együtthatóknak** *nevezzük.*

A binomiális együtthatók alkalmazásával tudtuk megfogalmazni a binomiális tételt $\mathbb{Z}$-re. Most a polinomiális együtthatók segítségével megfogalmazhatjuk a *polinomiális tételt.*

9.5.3. Tétel. *Legyenek $m, n \in \mathbb{N}^*$, és legyen $\mathrm{I}_{m,n} := \Big\{ \alpha \in \mathbb{N}^m \;\Big|\; \sum\limits_{i\in m} \alpha_i = n \Big\}$. Ekkor minden $(x_i)_{i\in m} \in \mathbb{Z}^m$ esetén fennáll a*

$$\Big(\sum_{i\in m} x_i\Big)^n = \sum_{\alpha\in \mathrm{I}_{m,n}} \binom{n}{\alpha} \mathop{\mathrm{P}}_{i\in m} x_i^{\alpha_i}$$

egyenlőség. (**Polinomiális formula $\mathbb{Z}$-re**)

Bizonyítás. Rögzített $n \in \mathbb{N}^*$ mellett, m szerinti teljes indukcióval bizonyítunk. Az állítás nyilvánvalóan igaz, ha $m = 1 = \{0\}$, mert minden $(x_i)_{i\in\{0\}} \in \mathbb{Z}^1$ esetén $\Big(\sum\limits_{i\in\{0\}} x_i\Big)^n = x_0^n$, ugyanakkor minden $\alpha \in \mathbb{N}^1$ elemre a $\sum\limits_{i\in\{0\}} \alpha_i = n$ egyenlőség maga után vonja, hogy $\alpha_0 = n$, tehát

$$\sum_{\alpha\in\mathrm{I}_{1,n}} \binom{n}{\alpha} \prod_{i\in\{0\}} x_i^{\alpha_i} = x_0^n.$$

Az állítás $m = 2 = \{0,1\}$ esetén is igaz a binomiális tétel szerint, hiszen ekkor minden $(x_i)_{i\in\{0,1\}} \in \mathbb{Z}^2$ esetén $\Big(\sum\limits_{i\in\{0,1\}} x_i\Big)^n = (x_0 + x_1)^n$, ugyanakkor az

$$\mathrm{I}_{2,n} \to [\![0, n]\!]; \quad \alpha \mapsto \alpha_0$$

leképezés nyilvánvalóan bijekció, és ha $\alpha \in \mathrm{I}_{2,n}$, akkor

$$\binom{n}{\alpha} = \frac{n!}{\prod\limits_{i\in\{0,1\}} (\alpha_i!)} = \frac{n!}{\alpha_0!\alpha_1!} = \frac{n!}{\alpha_0!(n-\alpha_0)!} = \binom{n}{\alpha_0},$$

következésképpen

$$\sum_{\alpha\in\mathrm{I}_{2,n}} \binom{n}{\alpha} \prod_{i\in\{0,1\}} x_i^{\alpha_i} = \sum_{k\in[\![0,n]\!]} \binom{n}{k} x_0^k x_1^{n-k},$$

tehát a binomiális tétel szerint a bizonyítandó egyenlőség két oldala egyenlő.

Legyen $m \in \mathbb{N}$ olyan, hogy $m \geq 2$ és m-re teljesül az állítás. Rögzítsünk egy $(x_i)_{i\in m+1} \in \mathbb{Z}^{m+1}$ rendszert, és vezessük be azt az $(y_i)_{i\in m} \in \mathbb{Z}^m$ rendszert, amelyre minden $i \in m$ esetén

$$y_i := \begin{cases} x_i & \text{, ha } i < m-1; \\ x_{m-1} + x_m & \text{, ha } i = m-1. \end{cases}$$

Nyilvánvaló, hogy

$$\Big(\sum_{i\in m+1} x_i\Big)^n = \Big(\Big(\sum_{i\in m-1} x_i\Big) + x_{m-1} + x_m\Big)^n = \Big(\Big(\sum_{i\in m-1} y_i\Big) + y_{m-1}\Big)^n = \Big(\sum_{i\in m} y_i\Big)^n,$$

ezért az indukciós hipotézis és a binomiális tétel alapján:

$$\begin{aligned}
\Big(\sum_{i\in m+1} x_i\Big)^n &= \Big(\sum_{i\in m} y_i\Big)^n = \sum_{\beta\in\mathrm{I}_{m,n}} \binom{n}{\beta} \prod_{i\in m} y_i^{\beta_i} = \\
&= \sum_{\beta\in\mathrm{I}_{m,n}} \binom{n}{\beta} \Big(\prod_{i\in m-1} y_i^{\beta_i}\Big) y_{m-1}^{\beta_{m-1}} = \sum_{\beta\in\mathrm{I}_{m,n}} \binom{n}{\beta} \Big(\prod_{i\in m-1} x_i^{\beta_i}\Big) (x_{m-1} + x_m)^{\beta_{m-1}} = \\
&= \sum_{\beta\in\mathrm{I}_{m,n}} \binom{n}{\beta} \Big(\prod_{i\in m-1} x_i^{\beta_i}\Big) \Bigg(\sum_{\gamma\in\mathrm{I}_{2,\beta_{m-1}}} \binom{\beta_{m-1}}{\gamma_0} x_{m-1}^{\gamma_0} x_m^{\gamma_1}\Bigg) = \\
&= \sum_{\beta\in\mathrm{I}_{m,n}} \Bigg(\sum_{\gamma\in\mathrm{I}_{2,\beta_{m-1}}} \binom{n}{\beta} \binom{\beta_{m-1}}{\gamma_0} \Big(\prod_{i\in m-1} x_i^{\beta_i}\Big) x_{m-1}^{\gamma_0} x_m^{\gamma_1}\Bigg).
\end{aligned}$$

Vezessük be az

$$\tilde{\mathrm{I}} := \left\{ \ (\beta,\gamma) \ \middle| \ (\beta \in \mathrm{I}_{m,n}) \wedge (\gamma \in \mathrm{I}_{2,\beta_{m-1}}) \ \right\}$$

halmazt, és minden $\beta \in \mathrm{I}_{m,n}$ esetén legyen

$$\tilde{\mathrm{I}}_\beta := \left\{ \ (\beta,\gamma) \,\middle|\, \gamma \in \mathrm{I}_{2,\beta_{m-1}} \ \right\}.$$

Világos, hogy $\left(\tilde{\mathrm{I}}_\beta\right)_{\beta\in\mathrm{I}_{m,n}}$ olyan diszjunkt halmazrendszer, hogy $\tilde{\mathrm{I}} = \bigcup\limits_{\beta\in\mathrm{I}_{m,n}} \tilde{\mathrm{I}}_\beta$. Továbbá nyilvánvaló, hogy minden $\beta \in \mathrm{I}_{m,n}$ esetén az

$$\tilde{\mathrm{I}}_\beta \to \mathrm{I}_{2,\beta_{m-1}}; \quad (\beta,\gamma) \mapsto \gamma$$

leképezés bijekció. Ebből következik, hogy

$$\sum_{\beta\in\mathrm{I}_{m,n}} \left(\sum_{\gamma\in\mathrm{I}_{2,\beta_{m-1}}} \binom{n}{\beta}\binom{\beta_{m-1}}{\gamma_0}\Big(\prod_{i\in m-1} x_i^{\beta_i}\Big) x_{m-1}^{\gamma_0} x_m^{\gamma_1} \right) =$$
$$= \sum_{(\beta,\gamma)\in\tilde{\mathrm{I}}} \binom{n}{\beta}\binom{\beta_{m-1}}{\gamma_0}\Big(\prod_{i\in m-1} x_i^{\beta_i}\Big) x_{m-1}^{\gamma_0} x_m^{\gamma_1}.$$

A bizonyítást azzal fejezzük be, hogy egy alkalmasan választott bijekciót értelmezünk $\tilde{\mathrm{I}}$ és $\mathrm{I}_{m+1,n}$ között.

Legyen $\Phi : \tilde{\mathrm{I}} \to \mathbb{N}^{m+1}$ az a leképezés, amelyre minden $(\beta,\gamma) \in \tilde{\mathrm{I}}$ esetén $\Phi(\beta,\gamma) \in \mathbb{N}^{m+1}$ az a rendszer, amelyre minden $i \in m+1$ indexre

$$\Phi(\beta,\gamma)_i := \begin{cases} \beta_i & \text{, ha } i < m-1; \\ \gamma_0 & \text{, ha } i = m-1; \\ \gamma_1 & \text{, ha } i = m. \end{cases}$$

Világos, hogy minden $(\beta,\gamma) \in \tilde{\mathrm{I}}$ párra $\beta \in I_{m,n}$ és $\gamma_0 + \gamma_1 = \beta_{m-1}$ miatt

$$\sum_{i\in m+1} \Phi(\beta,\gamma)_i = \sum_{i\in m-1} \beta_i + \gamma_0 + \gamma_1 = \sum_{i\in m-1} \beta_i + \beta_{m-1} = \sum_{i\in m} \beta_i = n,$$

ezért $\Phi(\beta,\gamma) \in \mathrm{I}_{m+1,n}$. Tehát $\Phi : \tilde{\mathrm{I}} \to \mathrm{I}_{m+1,n}$ függvény.

Legyen $\Psi : \mathrm{I}_{m+1,n} \to \mathbb{N}^m \times \mathbb{N}^2$ az a függvény, amelyre minden $\alpha \in \mathrm{I}_{m+1,n}$ esetén $\Psi(\alpha) = (\beta,\gamma)$, ahol minden $i \in m$ indexre

$$\beta_i := \begin{cases} \alpha_i & \text{, ha } i < m-1; \\ \alpha_{m-1} + \alpha_m & \text{, ha } i = m-1, \end{cases}$$

valamint $\gamma_0 := \alpha_{m-1}$ és $\gamma_1 := \alpha_m$. Ha $\alpha \in \mathrm{I}_{m+1,n}$ és $\Psi(\alpha) = (\beta,\gamma)$, akkor Ψ definíciója szerint

$$\sum_{i\in m} \beta_i = \sum_{i\in m-1} \beta_i + \beta_{m-1} = \sum_{i\in m-1} \alpha_i + \alpha_{m-1} + \alpha_m = \sum_{i\in m+1} \alpha_i = n,$$

vagyis $\beta \in \mathrm{I}_{m,n}$, és $\gamma_0 + \gamma_1 = \alpha_{m-1} + \alpha_m = \beta_{m-1}$, ezért $\Psi(\alpha) = (\beta,\gamma) \in \tilde{\mathrm{I}}$. Tehát $\Psi : \mathrm{I}_{m+1,n} \to \tilde{\mathrm{I}}$ függvény.

Könnyen ellenőrizhető, hogy $\Psi \circ \Phi = \mathrm{id}_{\tilde{\mathrm{I}}}$ és $\Phi \circ \Psi = \mathrm{id}_{\mathrm{I}_{m+1,n}}$, tehát $\Phi : \tilde{\mathrm{I}} \to \mathrm{I}_{m+1,n}$ bijekció (és természetesen $\Phi^{-1} = \Psi$). Továbbá, ha $(\beta, \gamma) \in \tilde{\mathrm{I}}$, akkor a polinomiális együtthatók és a Φ függvény definíciója szerint

$$\binom{n}{\beta}\binom{\beta_{m-1}}{\gamma_0} = \left(\frac{n!}{\prod\limits_{i\in m}(\beta_i!)}\right)\left(\frac{\beta_{m-1}!}{\gamma_0!\gamma_1!}\right) = \left(\frac{n!}{\Big(\prod\limits_{i\in m-1}(\beta_i!)\Big)\beta_{m-1}!}\right)\left(\frac{\beta_{m-1}!}{\gamma_0!\gamma_1!}\right) =$$

$$= \frac{n!}{\Big(\prod\limits_{i\in m-1}(\beta_i!)\Big)\gamma_0!\gamma_1!} = \binom{n}{\Phi(\beta,\gamma)},$$

valamint

$$\Big(\prod_{i\in m-1} x_i^{\beta_i}\Big)x_{m-1}^{\gamma_0}x_m^{\gamma_1} = \prod_{i\in m+1} x_i^{\Phi(\beta,\gamma)_i}.$$

Tehát a $\mathbb{Z}$-beli összeadás általánosított kommutativitását alkalmazva kapjuk, hogy

$$\Big(\sum_{i\in m+1} x_i\Big)^n = \sum_{(\beta,\gamma)\in\tilde{\mathrm{I}}}\binom{n}{\beta}\binom{\beta_{m-1}}{\gamma_0}\Big(\prod_{i\in m-1} x_i^{\beta_i}\Big)x_{m-1}^{\gamma_0}x_m^{\gamma_1} =$$

$$= \sum_{(\beta,\gamma)\in\tilde{\mathrm{I}}}\binom{n}{\Phi(\beta,\gamma)}\prod_{i\in m+1} x_i^{\Phi(\beta,\gamma)_i} = \sum_{\alpha\in\mathrm{I}_{m+1,n}}\binom{n}{\alpha}\prod_{i\in m+1} x_i^{\alpha_i},$$

amivel az indukciós bizonyítást befejeztük. ■

9.6. Elemi aritmetikai függvények

9.6.1. Definíció. *Az $\mathbb{N}^* \to \mathbb{N}$ függvényeket* **elemi aritmetikai függvényeknek** *nevezzük, és ezek halmazát $\mathfrak{A}$ jelöli, tehát*

$$\mathfrak{A} := \mathscr{F}(\mathbb{N}^*; \mathbb{N}).$$

9.6.2. Definíció. *Minden $f, g \in \mathfrak{A}$ esetén $f \circledast g$ jelöli azt az elemi aritmetikai függvényt, amelyre minden $n \in \mathbb{N}^*$ esetén*

$$(f \circledast g)(n) = \sum_{\substack{d\in\mathbb{N}^*\\ d|n}} f(d)g\left(\frac{n}{d}\right),$$

és az $f \circledast g \in \mathfrak{A}$ függvényt az f és g elemi aritmetikai függvények **Dirichlet-szorzatának** *nevezzük. Továbbá, az*

$$\mathfrak{A} \times \mathfrak{A} \to \mathfrak{A}; \quad (f, g) \mapsto f \circledast g$$

leképezést az $\mathfrak{A}$ feletti **Dirichlet-szorzásnak** *nevezzük.*

9.6.3. Állítás. *A Dirichlet-szorzás asszociatív, kommutatív, neutráliselemes, és disztributív az összeadásra nézve. Továbbá, a*

$$\delta : \mathbb{N}^* \to \mathbb{N}; \quad n \mapsto \begin{cases} 1 & , \text{ha } n = 1, \\ 0 & , \text{ha } n \neq 1 \end{cases}$$

elemi aritmetikai függvény a neutrális elem a Dirichlet-szorzásra nézve.

Bizonyítás. (I) A $\circledast$ művelet asszociativitásának bizonyításához legyenek $f, g, h \in \mathfrak{A}$ és $n \in \mathbb{N}^*$. Ekkor

$$((f \circledast g) \circledast h)(n) = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} (f \circledast g)(d) h\left(\frac{n}{d}\right) = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \left(\sum_{\substack{d' \in \mathbb{N}^* \\ d'|d}} f(d') g\left(\frac{d}{d'}\right) \right) h\left(\frac{n}{d}\right) =$$

$$= \sum_{(d,d') \in I_n} f(d') g\left(\frac{d}{d'}\right) h\left(\frac{n}{d}\right) = \sum_{(d,d') \in I_n} F_n(d, d'), \tag{1}$$

ahol bevezettük az

$$I_n := \{(d, d') \in \mathbb{N}^* \times \mathbb{N}^* | (d|n) \wedge (d'|d)\}$$

halmazt, és az

$$F_n : I_n \to \mathbb{N}; \quad (d, d') \mapsto f(d') g\left(\frac{d}{d'}\right) h\left(\frac{n}{d}\right)$$

függvényt. Továbbá

$$(f \circledast (g \circledast h))(n) = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} f(d)(g \circledast h)\left(\frac{n}{d}\right) = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} f(d) \left(\sum_{\substack{d' \in \mathbb{N}^* \\ d'|(n/d)}} g(d') h\left(\frac{(n/d)}{d'}\right) \right) =$$

$$= \sum_{(d,d') \in J_n} f(d) g(d') h\left(\frac{n}{dd'}\right) = \sum_{(d,d') \in J_n} G_n(d, d'), \tag{2}$$

ahol bevezettük a

$$J_n := \{(d, d') \in \mathbb{N}^* \times \mathbb{N}^* | (d|n) \wedge (d'|(n/d))\}$$

halmazt, és a

$$G_n : J_n \to \mathbb{N}; \quad (d, d') \mapsto f(d) g(d') h\left(\frac{n}{dd'}\right)$$

függvényt.

Ha $(d, d') \in I_n$, vagyis $d|n$ és $d'|d$, akkor az oszthatóság-reláció tranzitivitása miatt $d'|n$ és $(d/d')|(n/d')$, tehát $(d', d/d') \in J_n$, így jól értelmezett a

$$\sigma : I_n \to J_n; \quad (d, d') \mapsto (d', d/d')$$

függvény. Ha $(d, d') \in J_n$, vagyis $d|n$ és $d'|(n/d)$, akkor $dd'|n$ és $d|dd'$, tehát $(dd', d) \in I_n$, így jól értelmezett a

$$\tau : J_n \to I_n; \quad (d, d') \mapsto (dd', d)$$

függvény. Világos, hogy $(d, d') \in I_n$ esetén

$$(\tau \circ \sigma)(d, d') = \tau(d', d/d') = (d'(d/d'), d') = (d, d'),$$

valamint $(d, d') \in J_n$ esetén

$$(\sigma \circ \tau)(d, d') = \sigma(dd', d) = (d, (dd')/d) = (d, d').$$

Ez azt jelenti, hogy $\sigma : I_n \to J_n$ bijekció (és $\sigma^{-1} = \tau$). Továbbá, minden $(d, d') \in I_n$ esetén

$$(G_n \circ \sigma)(d, d') = G_n(d', d/d') = f(d') g\left(\frac{d}{d'}\right) h\left(\frac{n}{d'(d/d')}\right) =$$

$$= f(d') g\left(\frac{d}{d'}\right) h\left(\frac{n}{d}\right) = F_n(d, d'),$$

vagyis $G_n \circ \sigma = F_n$. Ezért $\mathbb{N}$ összeadásának általános kommutatvitása miatt

$$\sum_{(d,d')\in J_n} G_n(d,d') = \sum_{(d,d')\in I_n} (G_n \circ \sigma)(d,d') = \sum_{(d,d')\in I_n} F_n(d,d'),$$

így (1) és (2) alapján kapjuk, hogy $((f \circledast g) \circledast h)(n) = (f \circledast (g \circledast h))(n)$.

(II) A $\circledast$ művelet kommutativitásának bizonyításához legyenek $f, g \in \mathfrak{A}$ és $n \in \mathbb{N}^*$. Nyilvánvaló, hogy ha $D_n := \{d \in \mathbb{N}^* |\ d|n\}$, akkor minden $d \in D_n$ esetén $\dfrac{n}{d} \in D_n$, és a

$$D_n \to D_n; \quad d \mapsto \frac{n}{d}$$

leképezés bijekció (amelynek az inverze önmaga), így az $\mathbb{N}$ feletti véges összeadás általános kommutativitása és az $\mathbb{N}$ feletti szorzás kommutativitása miatt

$$(g \circledast f)(n) = \sum_{d\in D_n} g(d) f\left(\frac{n}{d}\right) = \sum_{d\in D_n} g\left(\frac{n}{d}\right) f(d) = \sum_{d\in D_n} f(d) g\left(\frac{n}{d}\right) = (f \circledast g)(n).$$

Ezért $g \circledast f = f \circledast g$, tehát az $\mathfrak{A}$ feletti Dirichlet-szorzás kommutatív.

(III) Ha $f \in \mathfrak{A}$ és $n \in \mathbb{N}^*$, akkor minden $d \in \mathbb{N}^*$ számra, ha $d|n$ és $d \neq n$, akkor $\delta\left(\dfrac{n}{d}\right) = 0$, ezért

$$(f \circledast \delta)(n) = \sum_{\substack{d\in\mathbb{N}^*\\ d|n}} f(d)\delta\left(\frac{n}{d}\right) = f(n)\delta\left(\frac{n}{n}\right) = f(n),$$

vagyis $f \circledast \delta = f$. Ezért a $\circledast$ művelet kommutatvitása folytán δ a neutrális elem $\circledast$ műveletre nézve.

(IV) Legyenek $f, g, h \in \mathfrak{A}$ és $n \in \mathbb{N}^*$. Ekkor az $\mathbb{N}$ feletti szorzás összeadásra vonatkozó disztributivitása miatt

$$((f+g) \circledast h)(n) = \sum_{\substack{d\in\mathbb{N}^*\\ d|n}} (f+g)(d) h\left(\frac{n}{d}\right) = \sum_{\substack{d\in\mathbb{N}^*\\ d|n}} (f(d)+g(d)) h\left(\frac{n}{d}\right) =$$

$$= \sum_{\substack{d\in\mathbb{N}^*\\ d|n}} \left(f(d)h\left(\frac{n}{d}\right) + g(d)h\left(\frac{n}{d}\right)\right) = \sum_{\substack{d\in\mathbb{N}^*\\ d|n}} f(d)h\left(\frac{n}{d}\right) + \sum_{\substack{d\in\mathbb{N}^*\\ d|n}} g(d)h\left(\frac{n}{d}\right) =$$

$$= (f \circledast h)(n) + (g \circledast h)(n) = (f \circledast h + g \circledast h)(n).$$

Ezért $(f+g) \circledast h = f \circledast h + g \circledast h$, igy a $\circledast$ művelet kommutativitása folytán a $\circledast$ művelet disztributív az $\mathfrak{A}$ feletti összeadásra nézve. ∎

9.6.4. Definíció. *A* $\mu \in \mathfrak{A}$ **Möbius-függvényt** *a következőképpen értelmezzük:* $\mu(1) :=$ 1 *és minden* $n \in \mathbb{N}$, $n \geq 2$ *számra*

$$\mu(n) := \begin{cases} (-1)^{\mathrm{Card}(A)} & \text{, ha } A \subseteq \mathbb{P} \text{ olyan véges halmaz, hogy } A \neq \emptyset \text{ és } n = \prod_{p\in A} p; \\ 0 & \text{, egyébként.} \end{cases}$$

9.6.5. Állítás. *A Möbius-függvény invertálható a Dirichlet-szorzás szerint és* μ^{-1} *egyenlő az* 1 *értékű* $\mathbb{N}^* \to \mathbb{N}$ *konstansfüggvénnyel.*

Bizonyítás. Azt kell igazolni, hogy $\mu \circledast \mathbf{1} = \delta$, ahol $\mathbf{1}$ jelöli az 1 értékű $\mathbb{N}^* \to \mathbb{N}$ konstansfüggvényt, és δ a neutrális elem $\mathfrak{A}$-ban a $\circledast$ műveletre nézve, vagyis $\delta(1) = 1$ és minden $n > 1$ természetes számra $\delta(n) = 0$. Mivel $\mu(1) = 1$, így

$$(\mu \circledast \mathbf{1})(1) = \sum_{\substack{d \in \mathbb{N}^* \\ d|1}} \mu(d) = \mu(1) = 1 = \delta(1),$$

tehát csak azt kell belátni, hogy minden $n > 1$ természetes számra $(\mu \circledast \mathbf{1})(n) = 0 = \delta(n)$, vagyis

$$\sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \mu(d) = 0.$$

Ehhez legyen $n \in \mathbb{N}$, $n \geq 2$ rögzített szám, és a számelmélet alaptétele szerint vegyük azt az $f : \mathbb{P} \rightarrowtail \mathbb{N}^*$ függvényt, amelyre $\mathrm{Dom}(f) \subseteq \mathbb{P}$ nem üres véges halmaz és $n = \prod_{p \in \mathrm{Dom}(f)} p^{f(p)}$. Világos, hogy ha $D := \{d \in \mathbb{N}^* | (d|n) \wedge (\mu(d) \neq 0)\}$, akkor az

$$\mathscr{P}(\mathrm{Dom}(f)) \to D; \quad A \mapsto \prod_{p \in A} p$$

leképezés *bijekció*, azzal a konvencióval, hogy $\prod_{p \in \emptyset} p := 1$. Ezért, bevezetve az $N := \mathrm{Card}(\mathrm{Dom}(f)) \in \mathbb{N}^*$ számot, az $\mathbb{N}$ feletti véges összeadás általános kommutativitását alkalmazva kapjuk, hogy

$$\sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \mu(d) = \sum_{d \in D} \mu(d) = \sum_{A \in \mathscr{P}(\mathrm{Dom}(f))} \mu\Big(\prod_{p \in A} p\Big) =$$

$$= \sum_{A \in \mathscr{P}(\mathrm{Dom}(f))} (-1)^{\mathrm{Card}(A)} = \sum_{k=0}^{N} \Bigg(\sum_{\substack{A \in \mathscr{P}(\mathrm{Dom}(f)), \\ \mathrm{Card}(A) = k}} (-1)^k \Bigg) = \sum_{k=0}^{N} (-1)^k \binom{N}{k} = 0,$$

ahol az utolsó egyenlőségnél a 9.4.11. állítást alkalmaztuk. ■

9.6.6. Állítás. *Minden $f \in \mathfrak{A}$ függvényre és $n \in \mathbb{N}^*$ számra legyen*

$$\widehat{f} : \mathbb{N}^* \to \mathbb{N}; \quad n \mapsto \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} f(d).$$

Ekkor minden $f \in \mathfrak{A}$ és $n \in \mathbb{N}$ esetén

$$f(n) = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \mu(d) \widehat{f}\left(\frac{n}{d}\right).$$

(**Möbius-féle inverziós formula**)

Bizonyítás. Ha $\mathbf{1}$ jelöli az 1 értékű $\mathbb{N}^* \to \mathbb{N}$ konstansfüggvényt, akkor világos, hogy minden $f \in \mathfrak{A}$ esetén $\widehat{f} = f \circledast \mathbf{1}$. Továbbá, az előző állítás szerint $\mathbf{1}$ invertálható a Dirichlet-szorzás szerint és $\mathbf{1}^{-1} = \mu$, ezért minden $f \in \mathfrak{A}$ függvényre a Dirichlet-szorzás asszocativitása és kommutativitása miatt

$$\mu \circledast \widehat{f} = \mu \circledast (f \circledast \mathbf{1}) = \mu \circledast (\mathbf{1} \circledast f) = (\mu \circledast \mathbf{1}) \circledast f = \delta \circledast f = f,$$

ahol δ a neutrális elem $\mathfrak{A}$-ban a $\circledast$ műveletre nézve. Tehát minden $f \in \mathfrak{A}$ és $n \in \mathbb{N}^*$ esetén

$$f(n) = (\mu \circledast \widehat{f})(n) = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \mu(d) \widehat{f}\left(\frac{n}{d}\right),$$

amit bizonyítani kellett. ■

9.6.7. Definíció. *A* $\phi \in \mathfrak{A}$ **Euler-féle** ϕ **függvényt** *a következőképpen értelmezzük:* $\phi(1) := 1$, *és minden* $n \geq 2$ *természetes számra*

$$\phi(n) := \operatorname{Card}(\{k \in [\![1, n-1]\!] | \text{"}k \textit{ és } n-1 \textit{ relatív prímek"}\}).$$

9.7. Gyakorlatok

1. Ha E halmaz és $A, B \subseteq E$, akkor minden $x \in E$ elemre

$$\begin{gathered}\chi_{E \setminus A}(x) = 1 - \chi_A(x); \\ \chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x); \\ \chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x).\end{gathered}$$

2. Ha E és F véges halmazok, akkor az az $E \to F$ *injekciók* halmazának számossága 0, ha $\operatorname{Card}(E) > \operatorname{Card}(F)$, és egyenlő a

$$\frac{\operatorname{Card}(F)!}{(\operatorname{Card}(F) - \operatorname{Card}(E))!}$$

számmal, ha $\operatorname{Card}(E) \leq \operatorname{Card}(F)$.

3. Ha $n \in \mathbb{N}^*$, akkor

$$\begin{aligned}\operatorname{Card}(\{(i,j) \in \mathbb{N} \times \mathbb{N} | \ 1 \leq i \leq j \leq n\}) &= \frac{n(n+1)}{2} \\ \operatorname{Card}(\{(i,j) \in \mathbb{N} \times \mathbb{N} | \ 1 \leq i < j \leq n\}) &= \frac{n(n-1)}{2}.\end{aligned}$$

4. Bizonyítsuk be a következő egyenlőségeket.

a) Ha $n, p \in \mathbb{N}^*$ és $p \leq n$, akkor

$$\begin{gathered}\sum_{k=0}^{p} \binom{n}{k} \binom{n-k}{p-k} = 2^p \binom{n}{p} \\ \sum_{k=0}^{p} (-1)^k \binom{n}{k} \binom{n-k}{p-k} = 0.\end{gathered}$$

b) Ha $n, p \in \mathbb{N}^*$, akkor

$$\sum_{k=0}^{p} (-1)^k \binom{p}{k} \binom{n+p-k}{p} = 0.$$

(*Útmutatás.* Az a) pontban szereplő formulák a binomiális együtthatók definíciójából közvetlenül kaphatóak, míg a b) pontban található formula az a) második kifejezéséből nyerhető, ha az ottani n helyére az $n+p$ értéket helyettesítjük, és némi egyszerűsítést végzünk.)

5. Legyen minden $m, n \in \mathbb{N}$ számra $S_{m,n}$ az $m \to n$ *szürjekciók* halmazának a számossága. Igazoljuk a következő állításokat.

a) Minden $m, n \in \mathbb{N}^*$ számra:

$$S_{m,n} = n \cdot (S_{m-1,n} + S_{m-1,n-1}).$$

b) Minden $n \in \mathbb{N}^*$ számra:

$$S_{n+1,n} = \frac{(n+1)!n}{2}$$
$$S_{n+2,n} = \frac{(n+2)!(3n+1)n}{24}.$$

(*Útmutatás.* Fennáll az

$$\frac{(n+1)!n}{2} = \binom{n+1}{2} \cdot n \cdot (n-1)!$$

egyenlőség. Próbáljuk megindokolni, hogy az egyenlőség jobb oldalán $S_{n+1,n}$ áll!)

6. Legyenek $m, n \in \mathbb{N}^*$ és jelölje $p_{m,n}$ azon $f : [\![1, m]\!] \to [\![1, n]\!]$ szigorúan monoton növő függvények halmazának számosságát, amelyekre teljesül az, hogy minden $k \in [\![1, m]\!]$ páros (ill. páratlan) számra az $f(k) \in [\![1, n]\!]$ szám páros (ill. páratlan).

a) Ha $m > 0$ és $n > 1$, akkor

$$p_{m,n} = p_{m-1,n-1} + p_{m,n-2}.$$

b) Ha $m \leq n$, akkor

$$p_{m,n} = \binom{\left[\frac{m+n}{2}\right]}{m},$$

ahol $\left[\frac{m+n}{2}\right]$ az $\frac{m+n}{2}$ racionális szám egész részét jelöli.

10. fejezet

Végtelen halmazok

10.1. Dedekind-véges és Dedekind-végtelen halmazok

10.1.1. Definíció. *Azt mondjuk, hogy egy halmaz* **Dedekind-véges**, *ha nem ekvipotens egyetlen valódi részhalmazával sem. Azt mondjuk, hogy egy halmaz* **Dedekind-végtelen**, *ha nem Dedekind-véges, vagyis létezik olyan valódi részhalmaza, amellyel ekvipotens.*

10.1.2. Állítás. *Minden végtelen halmaznak létezik* $\mathbb{N}$*-nel ekvipotens részhalmaza.*

Bizonyítás. Ennek a fontos tételnek két lényegesen különböző bizonyítását adjuk.

(*I. bizonyítás*) Az állítás azzal ekvivalens, hogy ha E végtelen halmaz, akkor létezik E-ben haladó *injektív* sorozat. Ilyen sorozat előállításához a kiválasztási axiómával kombinált rekurzió tételét (7.6.1.) fogjuk alkalmazni.

Minden $n \in \mathbb{N}$ esetén legyen F_n az $n \to E$ injekciók halmaza, tehát $F_n \subseteq \mathscr{F}(n; E)$. Ekkor képezhető az $(F_n)_{n \in \mathbb{N}}$ halmazsorozat, mert minden $n \in \mathbb{N}$ esetén F_n részhalmaza az $\mathbb{N} \rightarrowtail E$ függvények $\mathscr{F}_0(\mathbb{N}; E)$ halmazának, így a $(\exists n)((n \in \mathbb{N}) \wedge (x = (n, F_n))$ kijelentés kollektivizáló az x változóban, hiszen ebből következik, hogy $x \in \mathbb{N} \times \mathscr{P}(\mathscr{F}_0(\mathbb{N}; E))$. Világos, hogy $F_0 = \{\emptyset\}$.

Legyen $n \in \mathbb{N}$ és $\mathbf{a} \in F_n$. Ekkor $\mathbf{a} : n \to E$ injekció, tehát ha $\mathrm{Im}(\mathbf{a}) = E$ teljesülne, akkor E ekvipotens volna n-nel, ami lehetetlen, mert E végtelen. Ezért $E \setminus \mathrm{Im}(\mathbf{a}) \neq \emptyset$; legyen $x \in E \setminus \mathrm{Im}(\mathbf{a})$ rögzített elem. Értelmezzük az

$$\mathbf{a}' : n+1 \to \mathbb{N}; \quad k \mapsto \begin{cases} \mathbf{a}(k) & \text{, ha } k < n; \\ x & \text{, ha } k = n \end{cases}$$

függvényt. Nyilvánvaló, hogy $\mathbf{a}' : n+1 \to E$ injekció, vagyis $\mathbf{a}' \in F_{n+1}$, továbbá triviális, hogy $\mathbf{a}'|_n = \mathbf{a}$. Ezért a kiválasztási axiómával kombinált rekurzió tétele (7.6.1.) alapján létezik olyan E-ben haladó $\mathbf{s}$ sorozat, hogy minden $n \in \mathbb{N}$ számra $\mathbf{s}|_n \in F_n$, vagyis $\mathbf{s}|_n : n \to E$ injekció. Ha $j, k \in \mathbb{N}$ és $j \neq k$, akkor véve $n \in \mathbb{N}$ elemet, amelyre $j, k < n$ kapjuk, hogy $\mathbf{s}(j) = (\mathbf{s}|_n)(j) \neq (\mathbf{s}|_n)(k) = \mathbf{s}(k)$, tehát $\mathbf{s}$ egy E-ben haladó injektív sorozat.

(*II. bizonyítás*) Legyen E végtelen halmaz és R jólrendezés az E halmaz felett (6.15.2.). Az $(\mathbb{N}, \leq)$ pár jólrendezett halmaz, ezért 6.15.4. szerint két eset lehetséges:

a) Létezik olyan $S \subseteq \mathbb{N}$ halmaz, amely szegmense az $(\mathbb{N}, \leq)$ jólrendezett halmaznak, és az (E, R) és $(S, \leq_S)$ jólrendezett halmazok izomorfak.

b) Létezik olyan $S' \subseteq E$ halmaz, amely szegmense az (E, R) jólrendezett halmaznak, és az $(\mathbb{N}, \leq)$ és $(S', R_{S'})$ jólrendezett halmazok izomorfak.

A b) esetben S' az E-nek $\mathbb{N}$-nel ekvipotens részhalmaza. Az a) esetben S nem lehet $\mathbb{N}$-től különböző (valódi) szegmense az $(\mathbb{N}, \leq)$ jólrendezett halmaznak, hiszen ennek minden valódi szegmense $]\leftarrow, n[$ alakú, ahol $n \in \mathbb{N}$; vagyis az $(\mathbb{N}, \leq)$ minden valódi szegmense *természetes szám*, ugyanakkor S ekvipotens E-vel, így S végtelen, tehát nem létezik bijekció S és egy természetes szám között. Ezért az a) esetben $S = \mathbb{N}$, így E ekvipotens $\mathbb{N}$-nel. ■

10.1.3. Állítás. a) *A kiválasztási axióma nélkül teljesül az, hogy minden véges halmaz Dedekind-véges, és minden Dedekind-végtelen halmaz végtelen.*

b) *A kiválasztási axióma és a végtelenségi axióma nélkül teljesül az, hogy minden E halmazra a következő állítások ekvivalensek:*

(i) *Minden $\mathfrak{a}$ halmazra E és $E \cup \{\mathfrak{a}\}$ ekvipotensek.*

(ii) *Létezik olyan $\mathfrak{a}$ halmaz, hogy $\mathfrak{a} \notin E$, valamint E és $E \cup \{\mathfrak{a}\}$ ekvipotensek.*

(iii) *Az E halmaz Dedekind-végtelen.*

c) *A kiválasztási axióma és a végtelenségi axióma nélkül teljesül az, hogy minden Dedekind-végtelen halmaz ekvipotens a saját szukcesszorával.*

d) *A kiválasztási axióma és a végtelenségi axióma felhasználásával kapjuk, hogy minden Dedekind-véges halmaz véges. Tehát a kiválasztási axiómát és a végtelenségi axiómát elfogadva, a halmazok végessége ekvivalens a Dedekind-végességgel, és a halmazok végtelensége ekvivalens a Dedekind-végtelenséggel.*

Bizonyítás. a) Legyen E véges halmaz. Vegyünk olyan $n \in \mathbb{N}$ számot és $f : n \to E$ függvényt, amely bijekció. Legyen $H \subseteq E$ olyan részhalmaz, hogy $H \neq E$. Ha H ekvipotens volna E-vel (tehát E nem volna Dedekind-véges), akkor létezne $g : E \to H$ bijekció, és akkor $f^{-1}\langle H\rangle \subseteq n$ olyan halmaz volna, hogy $f^{-1}\langle H\rangle \neq n$ és $(f^{-1}|_H) \circ g \circ f : n \to f^{-1}\langle H\rangle$ bijekció. Ez viszont 8.1.2. miatt lehetetlen, ezért E Dedekind-véges. Ebből következik, hogy minden Dedekind-végtelen halmaz végtelen.

b) (i)⇒(ii) Nyilvánvaló, mert létezik olyan $\mathfrak{a}$ halmaz, hogy $\mathfrak{a} \notin E$, különben E az összes halmazok halmaza volna.

(ii)⇒(iii) Legyen $\mathfrak{a}$ olyan halmaz, hogy $\mathfrak{a} \notin E$, valamint E és $E \cup \{\mathfrak{a}\}$ ekvipotensek. Rögzítsünk egy $g : E \cup \{\mathfrak{a}\} \to E$ bijekciót. Ekkor $g\langle E\rangle = E \setminus \{g(\mathfrak{a})\}$ valódi részhalmaza E-nek, és $g|_E : E \to g\langle E\rangle$ bijekció, vagyis E ekvipotens $g\langle E\rangle$-vel, így E Dedekind-végtelen halmaz.

(iii)⇒(i) Tegyük fel, hogy az E halmaz Dedekind-végtelen, és legyen $\mathfrak{a}$ tetszőleges olyan halmaz, hogy $\mathfrak{a} \notin E$. Megmutatjuk, hogy E és $E \cup \{\mathfrak{a}\}$ ekvipotensek. Ehhez vegyünk olyan $F \subseteq E$ halmazt, hogy $F \neq E$ és F ekvipotens E-vel. Legyen $g : F \to E$ bijekció, $z \in E \setminus F$ rögzített elem, és értelmezzük a következő függvényt:

$$f : F \cup \{z\} \to E \cup \{\mathfrak{a}\}; \quad x \mapsto f(x) := \begin{cases} g(x) & \text{, ha } x \in F; \\ \mathfrak{a} & \text{, ha } x = z. \end{cases}$$

Könnyen látható, hogy f bijekció (ehhez kell az $\mathfrak{a} \notin E$ feltétel). Ugyanakkor $F \cup \{z\} \subseteq E$, ezért $F \cup \{z\}$ kisebb-egyenlő számosságú E-nél, így $E \cup \{\mathfrak{a}\}$ is kisebb-egyenlő számosságú E-nél. Másfelől, $E \subseteq E \cup \{\mathfrak{a}\}$, tehát E kisebb-egyenlő számosságú $E \cup \{\mathfrak{a}\}$-nál. A Schröder–Bernstein-tételt (6.5.5.) alkalmazva kapjuk, hogy az E és $E \cup \{\mathfrak{a}\}$ halmazok ekvipotensek.

c) Tegyük fel, hogy az E halmaz Dedekind-végtelen. Ha $E \in E$, akkor $E^+ = E$, így E és E^+ még akkor is ekvipotensek, ha nem tesszük fel az E halmaz Dedekind-végtelenségét. Ha $E \notin E$, akkor a b) állításban szereplő (iii)⇒(i) következtetésből kapjuk, hogy E és $E \cup \{E\}$ ekvipotensek.

d) Tegyük fel a kiválasztási és a végtelenségi axiómát, és legyen E végtelen halmaz. Megmutatjuk, hogy ekkor E Dedekind-végtelen. Az 10.1.2. állítás szerint létezik olyan $D \subseteq E$ halmaz, amely ekvipotens $\mathbb{N}$-nel. (Ehhez használjuk fel a kiválasztási és a végtelenségi axiómát.) Az $\mathbb{N}$ halmaznak létezik olyan valódi részhalmaza, amellyel $\mathbb{N}$ ekvipotens. Például az $\mathbb{N} \to \mathbb{N} \setminus \{0\};\ n \mapsto n^+$ függvény bijekció. Ezért létezik olyan $D' \subseteq D$ halmaz, hogy $D' \neq D$ és D' ekvipotens D-vel. Legyen $g : D' \to D$ bijekció, és értelmezzük a következő függvényt:

$$f : D' \cup (E \setminus D) \to E; \quad x \mapsto f(x) := \begin{cases} g(x) & \text{, ha } x \in D'; \\ x & \text{, ha } x \in E \setminus D. \end{cases}$$

Könnyen látható, hogy f bijekció, ugyanakkor $D' \cup (E \setminus D)$ valódi részhalmaza E-nek, ezért E Dedekind-végtelen. Ebből következik, hogy minden Dedekind-véges halmaz véges. ■

10.1.4. Állítás. *Az E halmaz pontosan akkor végtelen, ha minden $f : E \to E$ függvényhez létezik olyan $S \subseteq E$ halmaz, hogy $S \neq \emptyset$, $S \neq E$ és $f\langle S \rangle \subseteq S$ (amit úgy is kifejezhetünk, hogy létezik f-hez nem triviális invariáns részhalmaza E-nek).*

Bizonyítás. (I) Minden $f : E \to E$ függvényre és $\mathfrak{a} \in E$ elemre jelölje $\mathbf{s}_{f,\mathfrak{a}}$ azt az iterációval meghatározott, E-ben haladó sorozatot, amelyre $\mathbf{s}_{f,\mathfrak{a}}(0) = \mathfrak{a}$, és minden $n \in \mathbb{N}$ esetén $\mathbf{s}_{f,\mathfrak{a}}(n^+) = f(\mathbf{s}_{f,\mathfrak{a}}(n))$ teljesül. Most néhány megállapítást teszünk az $\mathbf{s}_{f,\mathfrak{a}}$ alakú sorozatokra vonatkozóan, ahol $f : E \to E$ függvény és $\mathfrak{a} \in E$.

Először is nyilvánvaló, hogy $\mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}}) \subseteq E$ olyan halmaz, hogy $f\langle \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}}) \rangle \subseteq \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}})$, vagyis az $\mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}})$ halmaz f-invariáns, hiszen $n \in \mathbb{N}$ esetén $f(\mathbf{s}_{f,\mathfrak{a}}(n)) = \mathbf{s}_{f,\mathfrak{a}}(n^+) \in \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}})$.

Továbbá, minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}_{f,\mathbf{s}_{f,\mathfrak{a}}(n)}(m) = \mathbf{s}_{f,\mathfrak{a}}(n+m)$. Valóban, legyen $n \in \mathbb{N}$ rögzítve. Ekkor $\mathbf{s}_{f,\mathbf{s}_{f,\mathfrak{a}}(n)}(0) = \mathbf{s}_{f,\mathfrak{a}}(n) = \mathbf{s}_{f,\mathfrak{a}}(n+0)$. Ha $m \in \mathbb{N}$ olyan, hogy $\mathbf{s}_{f,\mathbf{s}_{f,\mathfrak{a}}(n)}(m) = \mathbf{s}_{f,\mathfrak{a}}(n+m)$, akkor az $\mathbf{s}_{f,\mathbf{s}_{f,\mathfrak{a}}(n)}$ és $\mathbf{s}_{f,\mathfrak{a}}$ sorozatok iterációs definíciója szerint:

$$\mathbf{s}_{f,\mathbf{s}_{f,\mathfrak{a}}(n)}(m^+) = f(\mathbf{s}_{f,\mathbf{s}_{f,\mathfrak{a}}(n)}(m)) = f(\mathbf{s}_{f,\mathfrak{a}}(n+m)) = \mathbf{s}_{f,\mathfrak{a}}((n+m)^+) = \mathbf{s}_{f,\mathfrak{a}}(n+m^+),$$

ezért a teljes indukció elve alapján minden $m \in \mathbb{N}$ számra $\mathbf{s}_{f,\mathbf{s}_{f,\mathfrak{a}}(n)}(m) = \mathbf{s}_{f,\mathfrak{a}}(n+m)$.
Az előző bekezdés alapján nyilvánvaló, hogy ha $n \in \mathbb{N}$ olyan, hogy $\mathbf{s}_{f,\mathfrak{a}}(n) = \mathfrak{a}$, akkor minden $m \in \mathbb{N}$ esetén $\mathbf{s}_{f,\mathfrak{a}}(m) = \mathbf{s}_{f,\mathfrak{a}}(n+m)$, vagyis az $\mathbf{s}_{f,\mathfrak{a}}$ sorozat *n-periódusú.* Ebből viszont teljes indukcióval azonnal következik, hogy ha az $n \in \mathbb{N}$ számra $\mathbf{s}_{f,\mathfrak{a}}(n) = \mathfrak{a}$, akkor minden $p \in \mathbb{N}$ esetén $\mathbf{s}_{f,\mathfrak{a}}(p \cdot n) = \mathfrak{a}$, hiszen $\mathbf{s}_{f,\mathfrak{a}}$ definíciója alapján igaz a $p = 0$ számra, és ha $p \in \mathbb{N}$ olyan, hogy $\mathbf{s}_{f,\mathfrak{a}}(p \cdot n) = \mathfrak{a}$, akkor

$$\mathbf{s}_{f,\mathfrak{a}}(p^+ \cdot n) = \mathbf{s}_{f,\mathfrak{a}}(p \cdot n + n) = \mathbf{s}_{f,\mathfrak{a}}(p \cdot n) = \mathfrak{a}.$$

Ebből következik, hogy ha az $n \in \mathbb{N}$ számra $\mathbf{s}_{f,\mathfrak{a}}(n) = \mathfrak{a}$, akkor minden $p, q \in \mathbb{N}$ esetén $\mathbf{s}_{f,\mathfrak{a}}(p \cdot n + q) = \mathbf{s}_{f,\mathfrak{a}}(q)$, hiszen adott n és q esetén ez nyilván igaz a $p = 0$ számra, és ha a $p \in \mathbb{N}$ számra igaz, akkor

$$\mathbf{s}_{f,\mathfrak{a}}(p^+ \cdot n + q) = \mathbf{s}_{f,\mathfrak{a}}((p \cdot n + q) + n) = \mathbf{s}_{f,\mathfrak{a}}(p \cdot n + q) = \mathbf{s}_{f,\mathfrak{a}}(q).$$

(II) Most megmutatjuk, hogy ha E olyan halmaz, hogy létezik olyan $f : E \to E$ *szürjekció*, és olyan $\mathfrak{a} \in E$, hogy $E = \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}})$, akkor E *véges*. Ekkor ugyanis

$$\mathfrak{a} \in E = \mathrm{Im}(f) = f\langle E\rangle = f\langle \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}})\rangle,$$

tehát van olyan $m \in \mathbb{N}$, amelyre $\mathfrak{a} = f(\mathbf{s}_{f,\mathfrak{a}}(m)) = \mathbf{s}_{f,\mathfrak{a}}(m^+)$, vagyis az $\{m|(m \in \mathbb{N}^*) \wedge (\mathfrak{a} = \mathbf{s}_{f,\mathfrak{a}}(m))\}$ halmaz nem üres. Legyen n a legkisebb eleme ennek a halmaznak. Minden $m \in \mathbb{N}$ számhoz egyértelműen léteznek olyan $q, p \in \mathbb{N}$ számok, hogy $m = p \cdot n + q$ és $q < n$ (7.11.8.); így az (I) állítás alapján $\mathbf{s}_{f,\mathfrak{a}}(m) = \mathbf{s}_{f,\mathfrak{a}}(q)$. Ez azt jelenti, hogy $E = \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}}) = \mathbf{s}_{f,\mathfrak{a}}\langle] \leftarrow, n[\rangle$, tehát E véges halmaz.

(III) Ha E végtelen halmaz és $f : E \to E$ tetszőleges függvény, akkor:

– $\mathrm{Im}(f) = E$ esetén az előző bekezdés alapján minden $\mathfrak{a} \in E$ pontra $E \neq \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}})$; és ekkor $S := \mathrm{Im}(\mathbf{s}_{f,\mathfrak{a}})$ olyan, hogy $S \neq E$, $S \neq \emptyset$ és $f\langle S\rangle \subseteq S$;

– $\mathrm{Im}(f) \neq E$ esetén $S := \mathrm{Im}(f)$ olyan, hogy $S \neq E$, $S \neq \emptyset$ és $f\langle S\rangle \subseteq S$.

(IV) Legyen $n \in \mathbb{N}$ és $f : n \to n$ az a függvény, amelyre minden $m < n$ természetes szám esetén, ha $m + 1 < n$, akkor $f(m) := m + 1$, és ha $m + 1 = n$, akkor $f(m) := 0$. Ekkor f olyan függvény, hogy minden $S \subseteq n$ halmazra, ha $S \neq \emptyset$ és $S \neq n$, akkor $f\langle S\rangle \nsubseteq S$. Valóban, legyen $S \subseteq n$ nem üres halmaz, amelyre $f\langle S\rangle \subseteq S$, és jelölje n_* az S halmaz *legnagyobb* elemét. Ekkor $n_* + 1 < n$ esetén $n_* + 1 = f(n_*) \in S$, ami lehetetlen, mert n_* az S legnagyobb eleme. Ezért $n_* + 1 = n$, amiből következik, hogy $f(n_*) = 0 \in S$. Ha $n \setminus S \neq \emptyset$ teljesülne, és m_* volna ennek a *legkisebb* eleme, akkor $m_* \neq 0$ (hiszen $0 \in S$), így létezne olyan $j \in \mathbb{N}$, hogy $j + 1 = m_* < n$, és ekkor $j \in S$ (hiszen $j < m_*$ és m_* az $n \setminus S$ halmaz legkisebb eleme), így $m_* = j + 1 = f(j) \in S$, ami lehetetlen. Ebből következik, hogy $S = n$. Tehát, ha $S \neq \emptyset$ és $S \neq n$, akkor $f\langle S\rangle \nsubseteq S$.

(V) Végül, legyen E tetszőleges véges halmaz, és $n := \mathrm{Card}(E)$. Legyen $g : E \to n$ rögzített bijekció. A (IV) állítás alapján vehetünk olyan $f' : n \to n$ függvényt, hogy minden $S' \subseteq n$ halmazra, ha $S' \neq \emptyset$ és $S' \neq n$, akkor $f'\langle S'\rangle \nsubseteq S'$. Ekkor $f := g^{-1} \circ f' \circ g : E \to E$ olyan függvény, hogy ha $S \subseteq E$, és $S \neq E$ és $S \neq \emptyset$, akkor a $g\langle S\rangle \subseteq n$ halmaz nem üres és nem egyenlő n-nel, tehát $f'\langle g\langle S\rangle\rangle \nsubseteq g\langle S\rangle$, amiből következik, hogy $f\langle S\rangle = g^{-1}\langle f'\langle g\langle S\rangle\rangle\rangle \nsubseteq S$. ■

10.2. Megszámlálható halmazok

10.2.1. Definíció. *Az $\mathbb{N}$ halmaznál kisebb-egyenlő számosságú halmazokat* **megszámlálhatóaknak** *nevezzük.*

A definíció alapján nyilvánvaló, hogy megszámlálható halmaznál kisebb-egyenlő számosságú halmaz szintén megszámlálható. Speciálisan, minden véges halmaz megszámlálható. A természetes számok halmaza megszámlálható és végtelen (8.1.7.), amit úgy is mondunk, hogy *megszámlálhatóan végtelen.*

10.2.2. Állítás. *Megszámlálható halmaz minden részhalmaza megszámlálható.*

Bizonyítás. Ha E megszámlálható halmaz, akkor létezik $f : E \to \mathbb{N}$ injekció, és ekkor minden $F \subseteq E$ halmazra az $f|_F : F \to \mathbb{N}$ leszűkített függvény szintén injekció, tehát F megszámlálható halmaz. ■

A következő állítás bizonyítása előtt megjegyezzük, hogy minden $n \in \mathbb{N}$ esetén 2 osztója $n(n+1)$-nek. Valóban, ez igaz $n=0$ esetén, és ha igaz az $n \in \mathbb{N}$ számra, akkor $(n+1)((n+1)+1) = n(n+1)+2(n+1)$ miatt 2 osztója $(n+1)((n+1)+1)$-nek, hiszen az indukciós hipotézis szerint osztója $n(n+1)$-nek, és 2 nyilvánvalóan osztója $2(n+1)$-nek is. Tehát a teljes indukció elve szerint minden $n \in \mathbb{N}$ esetén 2 osztója $n(n+1)$-nek.

10.2.3. Állítás. *Az $\mathbb{N}$ és $\mathbb{N} \times \mathbb{N}$ halmazok ekvipotensek.*

Bizonyítás. Értelmezzük a következő függvényt:

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}; \quad (p, q) \mapsto p + \frac{(p+q)(p+q+1)}{2}.$$

Megmutatjuk, hogy az f függvény bijekció. Ehhez szükséges és elegendő azt belátni, hogy minden $n \in \mathbb{N}$ számhoz egyértelműen létezik olyan $(j, k) \in \mathbb{N} \times \mathbb{N}$ pár, hogy $n = j + \dfrac{k(k+1)}{2}$ és $j \leq k$.

Először n-szerinti teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ számhoz létezik olyan $(j, k) \in \mathbb{N} \times \mathbb{N}$ pár, amelyre $n = j + \dfrac{k(k+1)}{2}$ és $j \leq k$. Ez $n := 0$ esetén triviálisan igaz. Legyen $n \in \mathbb{N}$ olyan, hogy a $(j, k) \in \mathbb{N} \times \mathbb{N}$ párra fennáll az, hogy $n = j + \dfrac{k(k+1)}{2}$ és $j \leq k$. Ha $j < k$, akkor a $(j+1, k) \in \mathbb{N} \times \mathbb{N}$ pár olyan, hogy $n+1 = (j+1) + \dfrac{k(k+1)}{2}$ és $j+1 \leq k$, tehát az állítás igaz $n+1$-re. Ha $j = k$, akkor a $(0, k+1) \in \mathbb{N} \times \mathbb{N}$ pár olyan, hogy $n+1 = k+1+\dfrac{k(k+1)}{2} = 0 + \dfrac{(k+1)(k+2)}{2}$ és $0 \leq k+1$, tehát az állítás igaz $n+1$-re.

Megmutatjuk, hogy ha $j, k, j', k' \in \mathbb{N}$ olyan számok, hogy $j \leq k$ és $j' \leq k'$ és $j + \dfrac{k(k+1)}{2} = j' + \dfrac{k'(k'+1)}{2}$, akkor $j = j'$ és $k = k'$.

– Tegyük fel, hogy $j' \geq j$. Ekkor $k \geq k'$ és $2(j'-j) = (k-k')(k+k'+1)$. Ha $k > k'$ igaz volna, akkor $2j' \geq 2(j'-j) = (k-k')(k+k'+1) \geq k+k'+1 > 2k'+1 \geq 2j'+1 > 2j'$, ami lehetetlen. Ezért $k = k'$, tehát $j = j'$.

– Tegyük fel, hogy $j \geq j'$. Ekkor $k' \geq k$ és $2(j-j') = (k'-k)(k'+k+1)$. Ha $k' > k$ igaz volna, akkor $2j \geq 2(j-j') = (k'-k)(k'+k+1) \geq k'+k+1 > 2k+1 \geq 2j+1 > 2j$, ami lehetetlen. Ezért $k = k'$, tehát $j = j'$. ■

Az előző állítást könnyen igazolhatjuk a Schröder–Bernstein-tétel (6.5.5.) alkalmazásával, ha ismerjük a prímszámok fogalmát (7.11.6.) és a számelmélet alaptételét (9.3.3.). Ugyanis nyilvánvaló, hogy az

$$\mathbb{N} \to \mathbb{N} \times \mathbb{N}; \quad n \mapsto (n, 0)$$

leképezés injektív, tehát $\mathbb{N}$ kisebb-egyenlő számosságú, mint az $\mathbb{N} \times \mathbb{N}$ szorzathalmaz. Továbbá, kevésbé nyilvánvaló, de a számelmélet alaptételének unicitás-része alapján igaz, hogy az

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}; \quad (m, n) \mapsto 2^m 3^n$$

leképezés is injektív, így a $\mathbb{N} \times \mathbb{N}$ szorzathalmaz is kisebb-egyenlő számosságú, mint $\mathbb{N}$. Világos, hogy itt 2 és 3 helyére bármely két különböző prímszámot írhatunk.

10.2.4. Állítás. *Ha $(E_i)_{i \in I}$ olyan halmazrendszer, hogy I megszámlálható halmaz és minden $i \in I$ esetén E_i megszámlálható halmaz, akkor $\bigcup_{i \in I} E_i$ megszámlálható halmaz.*

Bizonyítás. Legyen $g : I \to \mathbb{N}$ injekció és a kiválasztási axióma alkalmazásával vegyünk olyan $(f_i)_{i\in I}$ rendszert, hogy minden $i \in I$ esetén $f_i : E_i \to \mathbb{N}$ injekció. Legyen $E := \bigcup_{i\in I}(\{i\} \times E_i)$, vagyis E az $(E_i)_{i\in I}$ halmazrendszer diszjunkt uniója. Ekkor az

$$E \to \mathbb{N} \times \mathbb{N} \quad ; \qquad (i, x) \mapsto (g(i), f_i(x))$$

függvény injekció, mert $(i, x), (i', x') \in E$ és $(g(i), f_i(x)) = (g(i'), f_{i'}(x'))$ esetén $g(i) = g(i')$ és $f_i(x) = f_{i'}(x')$, tehát a g injektivitása miatt $i = i'$, így $x, x' \in E_i$ és $f_i(x) = f_i(x')$, tehát az $f_i : E_i \to \mathbb{N}$ függvény injektivitása folytán $x = x'$, vagyis $(i, x) = (i', x')$. Tehát E kisebb-egyenlő számosságú $\mathbb{N}\times\mathbb{N}$-nél, és az $\mathbb{N}\times\mathbb{N}$ és $\mathbb{N}$ halmazok ekvipotensek (10.2.3.), következésképpen E kisebb-egyenlő számosságú $\mathbb{N}$-nél. Ugyanakkor az

$$E \to \bigcup_{i\in I} E_i; \quad (i, x) \mapsto x$$

leképezés nyilvánvalóan szürjekció, ezért $\bigcup_{i\in I} E_i$ kisebb-egyenlő számosságú E-nél. Ebből következik, hogy $\bigcup_{i\in I} E_i$ megszámlálható halmaz. ■

10.2.5. Állítás. *Ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy I véges halmaz, és minden $i \in I$ esetén E_i megszámlálható halmaz, akkor a $\prod_{i\in I} E_i$ szorzathalmaz megszámlálható. (Vagyis véges sok megszámlálható halmaz szorzata megszámlálható.)*

Bizonyítás. Az állítást az I halmaz számossága szerinti teljes indukcióval igazoljuk.
Ha $\mathrm{Card}(I) = 0$, vagyis $I = \emptyset$, akkor $\prod_{i\in I} E_i = \{\emptyset\}$, tehát a szorzathalmaz véges.
Legyen $n \in \mathbb{N}$ olyan, hogy minden $(E_i)_{i\in I}$ halmazrendszerre, ha I véges és $\mathrm{Card}(I) = n$, és minden $i \in I$ esetén E_i megszámlálható, akkor $\prod_{i\in I} E_i$ megszámlálható. Legyen $(E_i)_{i\in I}$ olyan halmazrendszer, hogy I véges és $\mathrm{Card}(I) = n + 1$, és minden $i \in I$ esetén E_i megszámlálható halmaz. Legyen $i_* \in I$ rögzített elem és $I_* := I\setminus\{i_*\}$. Ekkor $\mathrm{Card}(I_*) = n$ és az $(E_i)_{i\in I_*}$ halmazrendszer olyan, hogy minden $i \in I_*$ esetén E_i megszámlálható. Ezért az indukciós hipotézis szerint a $\prod_{i\in I_*} E_i$ szorzathalmaz megszámlálható. Rögzítsünk egy $g : \prod_{i\in I_*} E_i \to \mathbb{N}$ injekciót, továbbá legyen $g_* : E_{i_*} \to \mathbb{N}$ injekció. Ekkor a

$$\left(\prod_{i\in I_*} E_i\right) \times E_{i_*} \to \mathbb{N} \times \mathbb{N}; \quad (h, x) \mapsto (g(h), g_*(x))$$

leképezés injekció, és 10.2.3. miatt $\mathbb{N}\times\mathbb{N}$ megszámlálható, tehát a $\left(\prod_{i\in I_*} E_i\right) \times E_{i_*}$ halmaz megszámlálható. Ugyanakkor a

$$\prod_{i\in I} E_i \to \left(\prod_{i\in I_*} E_i\right) \times E_{i_*}; \quad f \mapsto (f|_{I_*}, f(i_*))$$

függvény bijekció, tehát $\prod_{i\in I} E_i$ is megszámlálható. ■

Z

Vigyázzunk arra, hogy ha $(E_i)_{i\in I}$ olyan halmazrendszer, hogy I (akár megszámlálhatóan) végtelen és minden $i \in I$ esetén az E_i halmaz legalább két elemű, akkor a $\prod\limits_{i\in I} E_i$ szorzathalmaz nem megszámlálhatóan végtelen.

10.2.6. Állítás. *Ha E végtelen halmaz és F megszámlálható halmaz, akkor az $E \cup F$ halmaz ekvipotens E-vel.*

Bizonyítás. Elég arra az esetre bizonyítani, amikor $E \cap F = \emptyset$. Ha $N \subseteq E$ megszámlálhatóan végtelen halmaz (10.1.2.), akkor 10.2.4. szerint $N \cup F$ megszámlálhatóan végtelen halmaz, és ha $f : N \cup F \to N$ bijekció, akkor az

$$E \cup F \to E \quad ; \quad x \mapsto \begin{cases} f(x) & , \text{ha } x \in N \cup F \\ x & , \text{ha } x \in E \setminus N \end{cases}$$

függvény bijekció. ■

10.3. A számosságaritmetika alaptétele

10.3.1. Tétel. (A számosságaritmetika alaptétele) *Ha E végtelen halmaz, akkor E és $E \times E$ ekvipotens halmazok.*

Bizonyítás. Legyen $D \subseteq E$ rögzített megszámlálhatóan végtelen halmaz (10.1.2.), és jelölje $\mathfrak{S}$ azon $f : E \rightarrowtail E \times E$ függvények halmazát, amelyek injektívek, $D \subseteq \mathrm{Dom}(f)$ és $\mathrm{Im}(f) = \mathrm{Dom}(f) \times \mathrm{Dom}(f)$, tehát f bijekció a $\mathrm{Dom}(f)$ és $\mathrm{Dom}(f) \times \mathrm{Dom}(f)$ halmazok között. Láttuk, hogy D és $D \times D$ ekvipotensek (10.2.3.), ezért $\mathfrak{S} \neq \emptyset$. Jelölje $\leq$ a tartalmazás-relációt a $\mathfrak{S}$ halmaz felett; ekkor $(\mathfrak{S}, \leq)$ rendezett halmaz.

Megmutatjuk, hogy $(\mathfrak{S}, \leq)$ *induktívan* rendezett halmaz. Valóban, legyen $\mathfrak{H} \subseteq \mathfrak{S}$ olyan halmaz, amelynek bármely két eleme összehasonlítható a $\leq$ rendezés szerint. Ekkor 6.2.10. szerint $f := \bigcup \mathfrak{H}$ olyan injektív függvény, amely minden $h \in \mathfrak{H}$ függvénynek kiterjesztése, és $\mathrm{Dom}(f) = \bigcup\limits_{h\in\mathfrak{H}} \mathrm{Dom}(h)$, valamint $\mathrm{Im}(f) = \bigcup\limits_{h\in\mathfrak{H}} \mathrm{Im}(h)$. Ekkor $\mathfrak{H} \neq \emptyset$ esetén $D \subseteq \mathrm{Dom}(f)$ nyilvánvalóan teljesül. (Ha $\mathfrak{H} = \emptyset$, akkor az $\mathfrak{S}$ bármely eleme felső korlátja $\mathfrak{H}$-nak, ezért létezik felső korlátja $\mathfrak{H}$-nak, hiszen $\mathfrak{S} \neq \emptyset$; ilymódon feltehető, hogy $\mathfrak{H} \neq \emptyset$.) Minden $h \in \mathfrak{H}$ esetén $\mathrm{Im}(h) = \mathrm{Dom}(h) \times \mathrm{Dom}(h) \subseteq \mathrm{Dom}(f) \times \mathrm{Dom}(f)$, ezért $\mathrm{Im}(f) \subseteq \mathrm{Dom}(f) \times \mathrm{Dom}(f)$. Ha $(x, x') \in \mathrm{Dom}(f) \times \mathrm{Dom}(f)$, akkor léteznek olyan $h, h' \in \mathfrak{H}$ függvények, amelyekre $x \in \mathrm{Dom}(h)$ és $x' \in \mathrm{Dom}(h')$; ekkor $h \leq h'$ esetén $x, x' \in \mathrm{Dom}(h)$, tehát $(x, x') \in \mathrm{Dom}(h) \times \mathrm{Dom}(h) = \mathrm{Im}(h) \subseteq \mathrm{Im}(f)$; és hasonlóan kapjuk, hogy ha $h' \leq h$, akkor szintén $(x, x') \in \mathrm{Im}(f)$. Ez azt jelenti, hogy $\mathrm{Dom}(f) \times \mathrm{Dom}(f) \subseteq \mathrm{Im}(f)$, így $\mathrm{Im}(f) = \mathrm{Dom}(f) \times \mathrm{Dom}(f)$ teljesül. Tehát $f \in \mathfrak{S}$, és f a $\mathfrak{H}$ halmaznak *felső korlátja* (sőt valójában szuprémuma) a $\mathfrak{H}$ halmaznak a $\leq$ rendezés szerint.

Tehát az $(\mathfrak{S}, \leq)$ pár induktívan rendezett halmaz, így a Zorn lemma alapján létezik maximális eleme; legyen $f \in \mathfrak{S}$ ilyen elem, és legyen $F := \mathrm{Dom}(f)$. Ekkor $D \subseteq F$, tehát F végtelen, és $F \times F$ ekvipotens F-fel.

Megmutatjuk, hogy az F halmaz *ekvipotens* E-vel, amiből azonnal következik, hogy E ekvipotens az $E \times E$ halmazzal. Indirekt bizonyítunk, tehát feltesszük, hogy F kisebb számosságú E-nél, és megmutatjuk, hogy ez a hipotézis ellentmondásra vezet.

Ehhez először azt igazoljuk, hogy F kisebb-egyenlő számosságú az $E \setminus F$ halmaznál. Ennek bizonyításához megjegyezzük, hogy az $E \setminus F$ halmaz biztosan legalább két elemű, különben volna olyan P egy elemű halmaz, amelyre $E \setminus F \subseteq P$ teljesül; ekkor $E = F \cup (E \setminus F) \subseteq F \cup P$ is igaz volna, és az F végtelensége miatt $F \cup P$ ekvipotens F-fel (10.1.3.), így E kisebb-egyenlő számosságú volna F-nél, amiből a Schröder-Bernstein-tétel (6.5.5.) alapján következne, hogy F ekvipotens E-vel, ellentétben az indirekt feltevéssel. Ugyanakkor F is legalább két elemű (sőt $D \subseteq F$ miatt *végtelen*). Ha F nem volna kisebb-egyenlő számosságú $E \setminus F$-nél, akkor a 6.14.5. állítás szerint $E \setminus F$ kisebb számosságú volna F-nél, tehát a fentiek, és 6.5.9. c) szerint az $E = F \cup (E \setminus F)$ halmaz kisebb-egyenlő számosságú volna $F \times F$-nél, ami ekvipotens F-fel, így ismét a Schröder-Bernstein-tétel (6.5.5.) alkalmazásával adódna, hogy F ekvipotens E-vel, holott az indirekt feltevés alapján F kisebb számosságú E-nél.

Tehát az indirekt hipotézis (vagyis, hogy F kisebb számosságú E-nél) maga után vonja azt, hogy F kisebb-egyenlő számosságú az $E \setminus F$ halmaznál. Legyen $H \subseteq E \setminus F$ olyan halmaz, hogy F ekvipotens H-val. Az $F \times H$ és $H \times F$ halmazok ekvipotensek $F \times F$-fel, tehát F-fel, ezért ismét 6.5.9. c) alapján $(F \times H) \cup (H \times F)$ kisebb-egyenlő számosságú $F \times F$-nél, így F-nél is kisebb-egyenlő számosságú. A $H \times H$ halmaz ekvipotens $F \times F$-fel, így F-fel is, ezért ismét 6.5.9. c) szerint az $(F \times H) \cup (H \times F) \cup (H \times H)$ kisebb-egyenlő számosságú $F \times F$-nél, tehát F-nél is kisebb-egyenlő számosságú. Az nyilvánvaló, hogy F kisebb-egyenlő számosságú a $(F \times H) \cup (H \times F) \cup (H \times H)$ halmaznál, tehát a Schröder-Bernstein tétel (6.5.5.) alapján $(F \times H) \cup (H \times F) \cup (H \times H)$ és F ekvipotens halmazok. Ezért az $(F \times H) \cup (H \times F) \cup (H \times H)$ és H halmazok is ekvipotensek. Legyen

$$g : H \to (F \times H) \cup (H \times F) \cup (H \times H)$$

rögzített bijekció. Ekkor az

$$(F \cup H) \times (F \cup H) = (F \times F) \cup (F \times H) \cup (H \times F) \cup (H \times H)$$

egyenlőség miatt a

$$h : F \cup H \to (F \cup H) \times (F \cup H) \quad ; \quad x \mapsto \begin{cases} f(x) & \text{, ha } x \in F \\ g(x) & \text{, ha } x \in H \end{cases},$$

függvény *bijekció*, tehát $h \in \mathfrak{S}$ és $f \subseteq h$, és természetesen $f \neq h$, vagyis $f < h$ az $\mathfrak{S}$ feletti $\leq$ rendezés szerint; ez viszont ellentmond az f maximalitásának az $(\mathfrak{S}, \leq)$ rendezett halmazban. ■

10.3.2. Állítás. *Legyenek E és F olyan halmazok, hogy legalább az egyik végtelen.*
a) *Az $E \cup F$ halmaz ekvipotens az E és F közül nagyobb-egyenlő számosságú halmazzal.*
b) *Ha E és F egyike sem üres, akkor az $E \times F$ halmaz ekvipotens az E és F közül nagyobb-egyenlő számosságú halmazzal.*

Bizonyítás. Tegyük fel, hogy E kisebb-egyenlő számosságú F-nél (6.14.5.). Ekkor a hipotézis szerint F szükségképpen végtelen halmaz.

a) Ha $E = \emptyset$, akkor $E \cup F = F$, tehát az $E \cup F$ halmaz ekvipotens az F halmazzal. Ha E egy elemű halmaz, akkor F végtelensége miatt $E \cup F$ ekvipotens F-fel (10.1.3.).

Ha E legalább két elemű, akkor 6.5.9. c) szerint $E \cup F$ kisebb-egyenlő számosságú az $F \times F$ halmaznál, amely a számosságaritmetika alaptétele szerint ekvipotens F-fel. Másfelől nyilvánvaló, hogy F kisebb-egyenlő számosságú $E \cup F$-nél, hiszen $F \subseteq E \cup F$.

Ezért a Schröder–Bernstein-tételből (6.5.5.) következik, hogy ekkor $E \cup F$ ekvipotens F-fel.

b) Tegyük fel, hogy $E \neq \emptyset$. Ekkor F kisebb-egyenlő számosságú az $E \times F$ halmaznál, mert $x \in E$ esetén az

$$F \to E \times F; \quad y \mapsto (x, y)$$

függvény injekció. Továbbá, 6.5.9. b) szerint az $E \times F$ halmaz kisebb-egyenlő számosságú az $F \times F$ halmaznál, amely a számosságaritmetika alaptétele szerint ekvipotens F-fel. Ezért ismét a Schröder–Bernstein-tételből (6.5.5.) következik, hogy $E \times F$ ekvipotens F-fel. ■

10.3.3. Állítás. *Ha E végtelen halmaz és F nem üres megszámlálható halmaz, akkor $E \times F$ ekvipotens E-vel.*

Bizonyítás. A hipotézis szerint létezik $F \to \mathbb{N}$ injekció, és 10.1.2. szerint E-nek létezik megszámlálhatóan végtelen részhalmaza, ezért létezik $\mathbb{N} \to E$ injekció. Ebből következik, hogy létezik $F \to E$ injekció, vagyis F kisebb-egyenlő számosságú E-nél. Ugyanakkor $F \neq \emptyset$ és E végtelen, így 10.3.2. b) alapján $F \times E$ ekvipotens E-vel. Mivel $E \times F$ és $F \times E$ ekvipotens halmazok, ebből következik, hogy $E \times F$ ekvipotens E-vel. ■

10.3.4. Állítás. (**Kettőzési tétel**) *Az $E \neq \emptyset$ halmaz pontosan akkor végtelen, ha létezik olyan $X \subseteq E$ halmaz, hogy az X és $E \setminus X$ halmazok mindketten ekvipotensek E-vel.*

Bizonyítás. Tegyük fel, hogy E végtelen, és a számosságaritmetika alaptételének alkalmazásával vegyünk egy $f : E \times E \to E$ bijekciót. Legyen $x \in E$ rögzített elem és $X := f\langle\{x\} \times E\rangle$. Ekkor az f függvény leszűkítése az $\{x\} \times E$ halmazra bijekció $\{x\} \times E$ és X között, és $\{x\} \times E$ nyilvánvalóan ekvipotens E-vel, ezért X és E ekvipotensek. Világos, hogy $E \setminus X = f\langle(E \setminus \{x\}) \times E\rangle$ és az f függvény leszűkítése az $(E \setminus \{x\}) \times E$ halmazra bijekció $(E \setminus \{x\}) \times E$ és $E \setminus X$ között, tehát $E \setminus X$ és $(E \setminus \{x\}) \times E$ ekvipotens halmazok. Továbbá, az $E \setminus \{x\}$ halmaz is végtelen különben $E = (E \setminus \{x\}) \cup \{x\}$ véges volna (8.1.10.). Ezért E ekvipotens az $E \setminus \{x\}$ halmazzal (10.1.3.), így $(E \setminus \{x\}) \times E$ ekvipotens az $E \times E$ halmazzal, ami a számosságaritmetika alaptétele szerint ekvipotens E-vel. Tehát $E \setminus X$ is ekvipotens E-vel, vagyis X olyan halmaz, amelynek a létezését állítottuk.

Tegyük fel, hogy $E \neq \emptyset$ véges halmaz. Ha $X \subseteq E$ olyan, hogy X ekvipotens E-vel, akkor $\operatorname{Card}(X) = \operatorname{Card}(E)$, és 8.1.14. szerint $\operatorname{Card}(X) + \operatorname{Card}(E \setminus X) = \operatorname{Card}(E)$, vagyis $\operatorname{Card}(E \setminus X) = 0$. Ez azt jelenti, hogy ekkor $E \setminus X = \emptyset$, ezért $E \setminus X$ nem lehet ekvipotens E-vel, hiszen E nem üres. Tehát nem létezik olyan $X \subseteq E$ halmaz, hogy az X és $E \setminus X$ halmazok mindketten ekvipotensek E-vel. ■

10.3.5. Állítás. *Ha E végtelen halmaz és az F halmaz ekvipotens $\mathscr{P}(E)$-vel, akkor az $\mathscr{F}(E; F)$ függvényhalmaz ekvipotens az F halmazzal.*

Bizonyítás. A $\mathscr{P}(E)$ halmaz ekvipotens az $\mathscr{F}(E; \{0, 1\})$ függvényhalmazzal, és a hipotézis szerint F ekvipotens $\mathscr{P}(E)$-vel, ezért F is ekvipotens az $\mathscr{F}(E; \{0, 1\})$ függvényhalmazzal. Ebből következik, hogy $\mathscr{F}(E; F)$ ekvipotens az $\mathscr{F}(E; \mathscr{F}(E; \{0, 1\}))$ függvényhalmazzal. Ugyanakkor $\mathscr{F}(E \times E; \{0, 1\})$ és $\mathscr{F}(E; \mathscr{F}(E; \{0, 1\}))$ kanonikusan ekvipotensek (6.5.7.), és a számosságaritmetika alaptétele szerint $E \times E$ ekvipotens E-vel, így $\mathscr{F}(E \times E; \{0, 1\})$ és $\mathscr{F}(E; \{0, 1\})$ ekvipotensek. Tehát az $\mathscr{F}(E; F)$ függvényhalmaz ekvipotens $\mathscr{F}(E; \{0, 1\})$-vel, és ez utóbbi ekvipotens $\mathscr{P}(E)$-vel, így az $\mathscr{F}(E; F)$ függvényhalmaz ekvipotens F-fel. ■

10.3.6. Definíció. *A $\mathscr{P}(\mathbb{N})$ hatványhalmazzal ekvipotens halmazokat* **kontinuum-számosságúaknak** *nevezzük.*

A Cantor-tétel (6.5.4.) alapján kontinuum számosságú halmaz nagyobb számosságú minden megszámlálható halmaznál.

10.3.7. Következmény. *Kontinuum-számosságú halmazban haladó sorozatok halmaza kontinuum-számosságú.*

Bizonyítás. Elég a 10.3.5. állítást alkalmazni az $E := \mathbb{N}$ választással. ■

10.3.8. Állítás. *Ha E nem üres véges halmaz és F végtelen halmaz, akkor az $\mathscr{F}(E;F)$ függvényhalmaz ekvipotens az F halmazzal.*

Bizonyítás. Az E halmaz számossága szerinti teljes indukcióval bizonyítunk, tehát azt mutatjuk meg, hogy minden $n \in \mathbb{N}^*$ esetén, ha E olyan halmaz, amely ekvipotens n-nel és F végtelen halmaz, akkor $\mathscr{F}(E;F)$ és F ekvipotensek.
Ez $n = 1$ esetén nyilvánvalóan igaz, mert ekkor van olyan $\mathfrak{a}$, hogy $E = \{\mathfrak{a}\}$, és az

$$\mathscr{F}(\{\mathfrak{a}\};F) \to F; \quad f \mapsto f(\mathfrak{a})$$

leképezés nyilvánvalóan bijekció.
Tegyük fel, hogy $n \in \mathbb{N}^*$ olyan, hogy minden n-nel ekvipotens E halmazra és minden F végtelen halmazra $\mathscr{F}(E;F)$ és F ekvipotensek. Legyen E olyan véges halmaz, amelyre $\mathrm{Card}(E) = n+1$, és legyen F végtelen halmaz. Rögzítsünk egy $\mathfrak{a} \in E$ elemet és legyen $E' := E \setminus \{\mathfrak{a}\}$. Ekkor E' olyan véges halmaz, hogy $\mathrm{Card}(E') = n$, tehát az indukciós hipotézis szerint $\mathscr{F}(E';F)$ és F ekvipotensek. Nyilvánvaló, hogy az

$$\mathscr{F}(E;F) \to \mathscr{F}(E';F) \times F \quad ; \quad f \mapsto (f|_{E'}, f(\mathfrak{a}))$$

leképezés bijekció. Ugyanakkor $\mathscr{F}(E';F) \times F$ ekvipotens az $F \times F$ halmazzal, amely a számosságaritmetika alaptétele szerint ekvipotens F-fel. Ezért $\mathscr{F}(E;F)$ és F ekvipotensek. ■

10.3.9. Állítás. *Ha E halmaz és $(E_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén E_i kisebb-egyenlő számosságú E-nél, akkor a $\bigcup_{i\in I} E_i$ halmaz kisebb-egyenlő számosságú az $I \times E$ halmaznál.*

Bizonyítás. (I) Először tegyük fel, hogy az $(E_i)_{i\in I}$ halmazrendszer *diszjunkt.* Ekkor jól értelmezett az a

$$\iota : \bigcup_{i\in I} E_i \to I$$

függvény, amely minden $x \in \bigcup_{i\in I} E_i$ elemhez *azt* a $\iota(x) \in I$ indexet rendeli, amelyre $x \in E_{\iota(x)}$. Továbbá, minden $i \in I$ esetén E_i kisebb-egyenlő számosságú E-nél, ezért a kiválasztási axióma alkalmazásával kapunk olyan $(f_i)_{i\in I}$ függvényrendszert, hogy minden $i \in I$ indexre $f_i : E_i \to E$ *injekció.* Ekkor az

$$\bigcup_{i\in I} E_i \to I \times E; \quad x \mapsto (\iota(x), f_{\iota(x)}(x))$$

függvény nyilvánvalóan injektív, tehát $\bigcup\limits_{i\in I} E_i$ kisebb-egyenlő számosságú az $I \times E$ halmaznál.

(II) Ha $(E_i)_{i\in I}$ tetszőleges halmazrendszer, akkor az $(\{i\} \times E_i)_{i\in I}$ halmazrendszer diszjunkt, és minden $i \in E$ esetén $\{i\} \times E_i$ ekvipotens E_i-vel, így a hipotézis alapján kisebb-egyenlő számosságú E-nél. Ezért (I) miatt $\bigcup\limits_{i\in I}(\{i\} \times E_i)$ kisebb-egyenlő számosságú az $I \times E$ halmaznál. Ugyanakkor az

$$\bigcup_{i\in I}(\{i\} \times E_i) \to \bigcup_{i\in I} E_i; \quad (i, x) \mapsto x$$

leképezés nyilvánvalóan szürjektív, ezért $\bigcup\limits_{i\in I} E_i$ kisebb-egyenlő számosságú az $\bigcup\limits_{i\in I}(\{i\} \times E_i)$ halmaznál. Ezért $\bigcup\limits_{i\in I} E_i$ kisebb-egyenlő számosságú az $I \times E$ halmaznál. ■

10.3.10. Következmény. *Ha I végtelen halmaz és $(E_i)_{i\in I}$ olyan diszjunkt halmazrendszer, hogy minden $i \in I$ esetén E_i nem üres megszámlálható halmaz, akkor az $\bigcup\limits_{i\in I} E_i$ halmaz ekvipotens I-vel.*

Bizonyítás. Az $(E_i)_{i\in I}$ rendszer diszjunktsága miatt jól értelmezett az a

$$\iota : \bigcup_{i\in I} E_i \to I$$

függvény, amely minden $x \in \bigcup\limits_{i\in I} E_i$ elemhez *azt* a $\iota(x) \in I$ indexet rendeli, amelyre $x \in E_{\iota(x)}$. Minden $i \in I$ esetén $E_i \neq \emptyset$, ezért a ι függvény *szürjektív*, így I kisebb-egyenlő számosságú $\bigcup\limits_{i\in I} E_i$-nél.

Ugyanakkor az előző állítás szerint az $\bigcup\limits_{i\in I} E_i$ halmaz kisebb-egyenlő számosságú $I \times \mathbb{N}$-nél, és 10.3.3. szerint $I \times \mathbb{N}$ ekvipotens I-vel.

Ezért a Schröder–Bernstein tétel (6.5.5.) alapján $\bigcup\limits_{i\in I} E_i$ ekvipotens I-vel. ■

10.3.11. Következmény. *Ha E és F halmazok, F végtelen és $f : E \to F$ olyan szürjekció, hogy minden $y \in F$ esetén az $\overset{-1}{f}\langle\{y\}\rangle$ halmaz megszámlálható, akkor E és F ekvipotensek.*

Bizonyítás. Az $(\overset{-1}{f}\langle\{y\}\rangle)_{y\in F}$ halmazrendszer nyilvánvalóan diszjunkt, és f szürjektivitása miatt minden tagja nem üres halmaz, és a hipotézis szerint megszámlálható is, ezért az $\bigcup\limits_{y\in F} \overset{-1}{f}\langle\{y\}\rangle$ halmaz az előző állítás alapján ekvipotens F-fel. Ugyanakkor nyilvánvaló, hogy $\bigcup\limits_{y\in F} \overset{-1}{f}\langle\{y\}\rangle = E$. ■

10.3.12. Állítás. *Ha E végtelen halmaz, akkor az E véges részhalmazainak halmaza ekvipotens E-vel.*

Bizonyítás. Minden $n \in \mathbb{N}$ számra legyen $\mathscr{P}_n(E)$ az E halmaz n-elemű részhalmazainak halmaza; ekkor $\mathscr{P}_n(E)$ kisebb-egyenlő számosságú az $\mathscr{F}(n;E)$ függvényhalmaznál. Valóban, minden $X \in \mathscr{P}_n(E)$ halmazhoz létezik $n \to X$ bijekció, ezért a kiválasztási axióma alkalmazásával vehetünk olyan $(f_X)_{X\in\mathscr{P}_n(E)}$ rendszert, hogy minden $X \in \mathscr{P}_n(E)$ esetén $f_X : n \to X$ bijekció. Ekkor az $(f_X)_{X\in\mathscr{P}_n(E)}$ rendszer olyan $\mathscr{P}_n(E) \to \mathscr{F}(n;E)$ függvény, amely *injektív*, hiszen minden $X \in \mathscr{P}_n(E)$ esetén $X = \operatorname{Im}(f_X)$.

Ezért az 10.3.8. állítás szerint minden $n \in \mathbb{N}^*$ esetén $\mathscr{P}_n(E)$ kisebb-egyenlő számosságú E-nél, és természetesen $\mathscr{P}_0(E) = \{\emptyset\}$ is kisebb-egyenlő számosságú E-nél. Ezért 10.3.9. alapján az E véges részhalmazainak halmaza, vagyis az $\bigcup_{n\in\mathbb{N}} \mathscr{P}_n(E)$ halmaz kisebb-egyenlő számosságú $\mathbb{N} \times E$-nél, ami ekvipotens E-vel (10.3.3.). Másfelől, az

$$E \to \mathscr{P}_1(E); \quad x \mapsto \{x\}$$

leképezés bijekció, ezért E kisebb-egyenlő számosságú az E véges részhalmazai halmazánál. Ezért a Schröder–Bernstein-tétel (6.5.5.) alapján E ekvipotens az E véges részhalmazainak halmazával. ∎

10.3.13. Lemma. *Legyenek E és E' olyan halmazok, amelyek közül legalább az egyik végtelen. Legyenek továbbá F és F' olyan halmazok, hogy E kisebb számosságú F-nél, és E' kisebb számosságú F'-nél.*

a) *Az $E \cup E'$ halmaz kisebb számosságú az $F \cup F'$ halmaznál.*

b) *Ha F és F' egyike sem üres, akkor $E \times E'$ kisebb számosságú az $F \times F'$ halmaznál.*

Bizonyítás. A hipotézis szerint az F és F' halmazok közül valamelyik végtelen. Szintén a hipotézis szerint az E és E' halmazok közül nagyobb-egyenlő számosságú halmaz kisebb számosságú az F és F' halmazok közül nagyobb-egyenlő számosságú halmaznál.

a) A 10.3.2. a) állítás szerint $E \cup E'$ ekvipotens az E és E' halmazok közül a nagyobb-egyenlő számosságú halmazzal, és $F \cup F'$ ekvipotens az F és F' halmazok közül nagyobb-egyenlő számosságú halmaznál. Ezért az $E \cup E'$ halmaz kisebb számosságú az $F \cup F'$ halmaznál.

b) Ha E és E' nem üres, akkor 10.3.2. b) szerint $E \times E'$ ekvipotens az E és E' halmazok közül a nagyobb-egyenlő számosságú halmazzal, és mivel ekkor F és F' egyike sem üres, így ismét 10.3.2. b) szerint $F \times F'$ ekvipotens az F és F' halmazok közül nagyobb-egyenlő számosságú halmazzal. Tehát ekkor $E \times E'$ kisebb számosságú az $F \times F'$ halmaznál.

Ha E és E' közül az egyik üres, akkor $E \times E' = \emptyset$, ugyanakkor a hiptézis szerint $F \times F'$ nem üres (sőt végtelen), így $E \times E'$ kisebb számosságú az $F \times F'$ halmaznál. ∎

10.3.14. Állítás. *Ha E végtelen halmaz, akkor az E halmaz E-vel ekvipotens részhalmazainak halmaza ekvipotens $\mathscr{P}(E)$-vel.*

Bizonyítás. Legyen $\mathbf{A}$ az E halmaz E-vel ekvipotens részhalmazainak halmaza, és legyen $\mathbf{B}$ az E halmaz E-nél kisebb számosságú részhalmazainak halmaza. Ekkor nyilvánvalóan $\mathscr{P}(E) = \mathbf{A} \cup \mathbf{B}$ és $\mathbf{A} \cap \mathbf{B} = \emptyset$. Ha $H \subseteq E$ olyan halmaz, amely E-nél kisebb számosságú, akkor H vagy $E \setminus H$ végtelen (8.1.14.), így $E \setminus H$ ekvipotens E-vel, különben 10.3.13. a) szerint az $E = H \cup (E \setminus H)$ kisebb számosságú volna E-nél. Ez azt jelenti, hogy minden $H \in \mathbf{B}$ halmazra $E \setminus H \in \mathbf{A}$. Nyilvánvaló, hogy a

$$\mathbf{B} \to \mathbf{A} \quad ; \quad H \mapsto E \setminus H$$

leképezés injektív, így $\mathbf{B}$ kisebb-egyenlő számosságú $\mathbf{A}$-nál. Az $\mathbf{A}$ és $\mathbf{B}$ halmazok valamelyike végtelen, különben $\mathscr{P}(E) = \mathbf{A} \cup \mathbf{B}$ is véges volna (8.1.14.), ezért a Cantor-tétel alapján E is véges lenne. Ha $\mathbf{A}$ kisebb számosságú volna $\mathscr{P}(E)$-nél, akkor $\mathbf{B}$ is kisebb számosságú volna $\mathscr{P}(E)$-nél, így ismét alkalmazva az 10.3.13. állítás a) pontját kapnánk, hogy $\mathbf{A} \cup \mathbf{B}$ kisebb számosságú volna $\mathscr{P}(E)$-nél, ami lehetetlen, mert $\mathbf{A} \cup \mathbf{B} = \mathscr{P}(E)$. ■

10.3.15. Állítás. *Ha E végtelen halmaz, akkor az $E \to E$ bijekciók halmaza, az $E \to E$ függvények halmaza és az $E \rightarrowtail E$ függvények halmaza ekvipotens a $\mathscr{P}(E)$ hatványhalmazzal.*

Bizonyítás. Jelölje $\mathfrak{S}(E)$ az $E \to E$ bijekciók halmazát és $\mathscr{F}_0(E;E)$ az $E \rightarrowtail E$ függvények halmazát. Világos, hogy $\mathfrak{S}(E) \subseteq \mathscr{F}(E;E) \subseteq \mathscr{F}_0(E;E) \subseteq \mathscr{P}(E \times E)$, és a számosságaritmetika alaptétele szerint $\mathscr{P}(E \times E)$ és $\mathscr{P}(E)$ ekvipotensek. Ezért a Schröder–Bernstein-tétel (6.5.5.) alapján elég azt igazolni, hogy $\mathscr{P}(E)$ kisebb-egyenlő számosságú $\mathfrak{S}(E)$-nél.

Legyen minden $H \subseteq E$ halmazra $\mathfrak{S}_H(E)$ azon $f : E \to E$ bijekciók halmaza, amelyekre $H = \{x|(x \in E) \wedge (f(x) = x)\}$ (vagyis H egyenlő az f *fixpontjainak* halmazával). Ekkor $\bigcup_{H\in\mathscr{P}(E)} \mathfrak{S}_H(E) = \mathfrak{S}(E)$, és az $(\mathfrak{S}_H(E))_{H\in\mathscr{P}(E)}$ halmazrendszer diszjunkt, hiszen ha $H, H' \in \mathscr{P}(E)$ és $f \in (\mathfrak{S}_H(E)) \cap (\mathfrak{S}_{H'}(E))$, akkor $H = \{x|x \in E) \wedge (f(x) = x)\}H'$.

Bebizonyítjuk, hogy minden nem egy elemű X halmazhoz létezik olyan $f : X \to X$ bijekció, amelyre minden $x \in X$ esetén $f(x) \neq x$ teljesül. Ez nyilvánvalóan igaz $X = \emptyset$ esetén, ezért legyen $X \neq \emptyset$. Két eset lehetséges.

– Az X halmaz véges és $\mathrm{Card}(X) > 1$. Legyen $n := \mathrm{Card}(X)$ és értelmezzük a

$$\varphi : n \to n; \quad k \mapsto \begin{cases} k+1 & \text{, ha } k < n-1 \\ 0 & \text{, ha } k = n-1 \end{cases}$$

függvényt. Világos, hogy $\varphi : n \to n$ olyan bijekció, amelyre minden $k \in n$ esetén $\varphi(k) \neq k$, ezért ha $g : n \to X$ tetszőleges bijekció, akkor $f := g \circ \varphi \circ g^{-1} : X \to X$ olyan bijekció, hogy minden $x \in X$ esetén $f(x) \neq x$.

– Az X halmaz végtelen. Ekkor a kettőzési tétel (10.3.4.) alapján van olyan $X' \subseteq X$, hogy X' és $X \setminus X'$ ekvipotensek X-szel. Ekkor X' és $X \setminus X'$ is ekvipotensek, és ha $\varphi : X' \to X \setminus X'$ tetszőleges bijekció, akkor az $f := \varphi \cup \varphi^{-1}$ összeragasztott függvény, vagyis az

$$X \to X \quad ; \quad x \mapsto \begin{cases} \varphi(x) & \text{, ha } x \in X' \\ \varphi^{-1}(x) & \text{, ha } x \in X \setminus X' \end{cases}$$

leképezés olyan bijekció, hogy minden $x \in X$ esetén $f(x) \neq x$.

Megmutatjuk, hogy ha $H \subseteq E$ és $E \setminus H$ nem egy elemű halmaz, akkor $\mathfrak{S}_H(E) \neq \emptyset$. Ha $E \setminus H = \emptyset$, azaz $E = H$, akkor $\mathrm{id}_E \in \mathfrak{S}_E(E)$, ezért feltehető, hogy $E \setminus H \neq \emptyset$ (és persze nem is egy elemű). Az előzőek szerint van olyan $g : E \setminus H \to E \setminus H$ bijekció, amelyre minden $x \in E \setminus H$ esetén $g(x) \neq x$. Ekkor az $\mathrm{id}_H \cup g$ összeragasztott függvény, vagyis az

$$E \to E \quad ; \quad x \mapsto \begin{cases} x & \text{, ha } x \in H \\ g(x) & \text{, ha } x \in E \setminus H \end{cases}$$

leképezés olyan bijekció, amely eleme $\mathfrak{S}_H(E)$-nek. Megjegyezzük, hogy ha $E \setminus H$ éppen egy elemű, akkor nyilvánvalóan $\mathfrak{S}_H(E) = \emptyset$.

A bizonyítás utolsó lépéseként jelölje $\mathbf{A}$ azon $H \subseteq E$ halmazok halmazát, amelyekre $E \setminus H$ nem egy elemű. Legyen továbbá $\mathbf{B} := \mathscr{P}(E) \setminus \mathbf{A}$. Az előzőek alapján, ha $H \in \mathbf{A}$, akkor $\mathfrak{S}_H(E) \neq \emptyset$, ugyanakkor $H \in \mathbf{B}$ esetén $\mathfrak{S}_H(E) = \emptyset$. Ezért

$$\bigcup_{H \in \mathscr{P}(E)} \mathfrak{S}_H(E) = \Big(\bigcup_{H \in \mathbf{A}} \mathfrak{S}_H(E) \Big) \cup \Big(\bigcup_{H \in \mathbf{B}} \mathfrak{S}_H(E) \Big) = \bigcup_{H \in \mathbf{A}} \mathfrak{S}_H(E).$$

Ha $f \in \prod_{H \in \mathbf{A}} \mathfrak{S}_H(E)$, akkor az $f : \mathbf{A} \to \mathfrak{S}(E)$ függvény injekció, mert az $(\mathfrak{S}_H(E))_{H \in \mathbf{A}}$ halmazrendszer diszjunkt. Tehát $\mathbf{A}$ kisebb-egyenlő számosságú az $E \to E$ bijekciók halmazánál. Világos, hogy az

$$E \to \mathbf{B}; \quad x \mapsto E \setminus \{x\}$$

leképezés bijekció, tehát $\mathbf{B}$ ekvipotens E-vel, így a Cantor-tétel szerint kisebb számosságú $\mathscr{P}(E)$-nél. De $\mathscr{P}(E) = \mathbf{A} \cup \mathbf{B}$, ezért 10.3.13. a) alapján $\mathbf{A}$ nem lehet kisebb számosságú $\mathscr{P}(E)$-nél. Tehát $\mathbf{A}$ és $\mathscr{P}(E)$ ekvipotensek, így $\mathscr{P}(E)$ kisebb-egyenlő számosságú az $E \to E$ bijekciók halmazánál. ■

10.3.16. Lemma. *Legyenek E, F és H olyan halmazok, hogy E végtelen, és F kisebb-egyenlő számosságú E-nél, és $H \subseteq F$. Jelölje $\mathscr{S}(E; H)$ (illetve $\mathscr{S}(E; F)$) az $E \to H$ (illetve $E \to F$) szürjekciók halmazát. Ekkor $\mathscr{S}(E; H)$ kisebb-egyenlő számosságú az $\mathscr{S}(E; F)$ halmaznál.*

Bizonyítás. Természetesen a $H \neq F$ esetet az érdekes. Ekkor $F \setminus H$ az F halmaznak nem üres részhalmaza, és F kisebb-egyenlő számosságú E-nél, ezért $F \setminus H$ is kisebb-egyenlő számosságú E-nél. Legyen $g : E \to F \setminus H$ rögzített szürjekció. Továbbá, az E halmaz végtelensége és a kettőzési tétel (10.3.4.) alapján vegyünk olyan $X \subseteq E$ halmazt, hogy X és $E \setminus X$ mindketten ekvipotensek E-vel. Legyen $h : X \to E$ és $h' : E \setminus X \to E$ bijekció. Ekkor $g \circ h' : E \setminus X \to F \setminus H$ szürjekció, továbbá minden $f \in \mathscr{S}(E; H)$ esetén $f \circ h : X \to H$ szintén szürjekció, ezért az $(f \circ h) \cup (g \circ h')$ összeragasztott függvény az $X \cup (E \setminus X)$ halmazon van értelmezve és értékkészlete egyenlő a $H \cup (F \setminus H)$ halmazzal, vagyis ez a függvény eleme az $\mathscr{S}(E; F)$ függvényhalmaznak. Tehát jól értelmezett a

$$\Phi : \mathscr{S}(E; H) \to \mathscr{S}(E; F); \quad f \mapsto (f \circ h) \cup (g \circ h')$$

leképezés. Ez injekció, mert ha $f, f' \in \mathscr{S}(E; H)$ olyan függvények, hogy $\Phi(f) = \Phi(f')$, akkor $f \circ h = \Phi(f)|_X = \Phi(f')|_X = f' \circ h$, így a $h : X \to E$ függvény szürjektivitása miatt $f = f'$. Tehát $\mathscr{S}(E; H)$ kisebb-egyenlő számosságú az $\mathscr{S}(E; F)$ halmaznál. ■

10.3.17. Állítás. *Minden E és F halmazra jelölje $\mathscr{I}(E; F)$ (illetve $\mathscr{S}(E; F)$) az $E \to F$ injekciók (illetve szürjekciók) halmazát, továbbá legyen $\mathscr{F}_0(E; F)$ az $E \rightarrowtail F$ függvények halmaza.*

a) *Ha F végtelen halmaz, és F kisebb-egyenlő számosságú E-nél, akkor az $\mathscr{S}(E; F)$, $\mathscr{F}(E; F)$, $\mathscr{F}_0(E; F)$ és $\mathscr{P}(E)$ halmazok ekvipotensek.*

b) *Ha E végtelen halmaz, és E kisebb-egyenlő számosságú F-nél, akkor az $\mathscr{I}(E; F)$, $\mathscr{F}(E; F)$ és $\mathscr{F}_0(E; F)$ függvényhalmazok ekvipotensek az F halmaz E-vel ekvipotens részhalmazainak halmazával.*

Bizonyítás. a) Világos, hogy $\mathscr{F}_0(E;F) \subseteq \mathscr{P}(E\times F)$ és a hipotézis alapján $E\times F$ kisebb-egyenlő számosságú $E\times E$-nél (6.5.9. b)), ezért a számosságaritmetika alaptétele szerint $\mathscr{F}_0(E;F)$ kisebb-egyenlő számosságú $\mathscr{P}(E)$-nél. Ugyanakkor $\mathscr{S}(E;F) \subseteq \mathscr{F}(E;F) \subseteq \mathscr{F}_0(E;F)$, így a Schröder–Bernstein-tételt (6.5.5.) alkalmazva kapjuk, hogy az a) bizonyításához elég azt megmutatni, hogy $\mathscr{P}(E)$ kisebb-egyenlő számosságú $\mathscr{S}(E;F)$-nél (feltéve, hogy F végtelen halmaz, és F kisebb-egyenlő számosságú E-nél).

Az F halmaz legalább két elemű (sőt végtelen), ezért létezik $g:\{0,1\}\to F$ injekció, és ekkor az

$$\mathscr{F}(E;\{0,1\}) \to \mathscr{F}(E;F); \quad f\mapsto g\circ f$$

függvény nyilvánvalóan injektív, vagyis $\mathscr{F}(E;\{0,1\})$ kisebb-egyenlő számosságú az $\mathscr{F}(E;F)$ halmaznál. Ugyanakkor a $\mathscr{P}(E)$ és $\mathscr{F}(E;\{0,1\})$ halmazok ekvipotensek, tehát a $\mathscr{P}(E)$ hatványhalmaz kisebb-egyenlő számosságú az $\mathscr{F}(E;F)$ függvényhalmaznál. Ezért az a) állítás bizonyításának befejezéséhez elég azt megmutatni, hogy $\mathscr{F}(E;F)$ kisebb-egyenlő számosságú $\mathscr{S}(E;F)$-nél (feltéve, hogy F végtelen halmaz, és F kisebb-egyenlő számosságú E-nél).

Ehhez először megjegyezzük, hogy nyilvánvalóan

$$\mathscr{F}(E;F) = \bigcup_{H\in\mathscr{P}(F)} \mathscr{S}(E;H),$$

hiszen minden $f\in\mathscr{F}(E;F)$ esetén $f\in\mathscr{S}(E;\mathrm{Im}(f))$ és $\mathrm{Im}(f)\in\mathscr{P}(F)$. Továbbá, az E halmaz végtelen és F kisebb-egyenlő számosságú E-nél, ezért az előző lemma szerint minden $H\in\mathscr{P}(F)$ elemre $\mathscr{S}(E;H)$ kisebb-egyenlő számosságú $\mathscr{S}(E;F)$-nél, ezért $\mathscr{F}(E;F)$ kisebb-egyenlő számosságú a $\mathscr{P}(F)\times\mathscr{S}(E;F)$ halmaznál (10.3.9.). Ha most $\mathfrak{S}(F)$ jelöli az $F\to F$ bijekciók halmazát, és $g:E\to F$ rögzített szürjekció, akkor az

$$\mathfrak{S}(F)\to\mathscr{S}(E;F) \quad ; \quad f\mapsto f\circ g$$

leképezés injekció, tehát $\mathfrak{S}(F)$ kisebb-egyenlő számosságú a $\mathscr{S}(E;F)$ halmaznál. Az 10.3.15. állítás szerint $\mathfrak{S}(F)$ ekvipotens $\mathscr{P}(F)$-fel, mert F végtelen. Ebből következik, hogy $\mathscr{F}(E;F)$ kisebb-egyenlő számosságú az $\mathscr{S}(E;F)\times\mathscr{S}(E;F)$ halmaznál (6.5.9. b)), ami viszont a számosságaritmetika alaptétele szerint ekvipotens $\mathscr{S}(E;F)$-vel, hiszen $\mathscr{S}(E;F)$ is végtelen halmaz.

b) Legyen $\mathbf{A}$ az F halmaz E-vel ekvipotens részhalmazainak halmaza. Az

$$\mathscr{I}(E;F)\to\mathbf{A} \quad ; \quad f\mapsto \mathrm{Im}(f)$$

függvény szürjektív, hiszen $H\in\mathbf{A}$ esetén létezik $f:E\to H$ bijekció, és ekkor $f\in\mathscr{I}(E;F)$ és $\mathrm{Im}(f)=H$. Ezért $\mathbf{A}$ kisebb-egyenlő számosságú az $\mathscr{I}(E;F)$ függvényhalmaznál. Ugyanakkor világos, hogy $\mathscr{I}(E;F)\subseteq\mathscr{F}(E;F)\subseteq\mathscr{F}_0(E;F)$, így a Schröder–Bernstein-tétel (6.5.5.) alapján a b) állítás bizonyításához elegendő azt megmutatni, hogy $\mathscr{F}_0(E;F)$ kisebb-egyenlő számosságú $\mathbf{A}$-nál.

Ehhez először megmutatjuk, hogy $\mathscr{F}_0(E;F) \subseteq \bigcup_{H\in\mathbf{A}} \mathscr{P}(E\times H)$, vagyis $f\in\mathscr{F}_0(E;F)$ esetén létezik olyan $H\in\mathbf{A}$, hogy $f\subseteq E\times H$. Valóban, nyilvánvaló, hogy $f\subseteq E\times\mathrm{Im}(f)$ és $f:\mathrm{Dom}(f)\to\mathrm{Im}(f)$ szürjekció, így $\mathrm{Im}(f)$ kisebb-egyenlő számosságú a $\mathrm{Dom}(f)$ halmaznál, így E-nél is kisebb-egyenlő számosságú, hiszen $\mathrm{Dom}(f)\subseteq E$. Két eset lehetséges.

– Az $\mathrm{Im}(f)$ halmaz ekvipotens E-vel. Ekkor $\mathrm{Im}(f)\in\mathbf{A}$ és $f\subseteq E\times\mathrm{Im}(f)$.

– Az $\mathrm{Im}(f)$ halmaz kisebb számosságú E-nél. Legyen $j : \mathrm{Im}(f) \to E$ injekció és $g : E \to F$ szintén injekció. Világos, hogy $\mathrm{Im}(j)$ ekvipotens az $\mathrm{Im}(f)$ halmazzal, tehát az E-nek E-nél kisebb számossgú részhalmaza. Ugyanakkor $E = \mathrm{Im}(j) \cup (E \setminus \mathrm{Im}(j))$, így az E halmaz végtelensége miatt $\mathrm{Im}(j)$ vagy $E \setminus \mathrm{Im}(j)$ végtelen (8.1.14.). Ezért 10.3.13. a) alapján $E \setminus \mathrm{Im}(j)$ ekvipotens E-vel. A g függvény injektivitásából következik, hogy $g\langle E \setminus \mathrm{Im}(j)\rangle$ ekvipotens az $E \setminus \mathrm{Im}(j)$ halmazzal, tehát ekvipotens E-vel. Az 10.3.2. a) állításból következik, hogy a $H := \mathrm{Im}(f) \cup g\langle E \setminus \mathrm{Im}(j)\rangle$ halmaz ekvipotens, tehát $H \in \mathbf{A}$ és $\mathrm{Im}(f) \subseteq H$, így $f \subseteq E \times H$.

Minden $H \in \mathbf{A}$ esetén $E \times H$ ekvipotens $E \times E$-vel, így a számosságaritmetika alaptétele szerint ekvipotens E-vel. Tehát $H \in \mathbf{A}$ esetén $\mathscr{P}(E \times H)$ ekvipotens $\mathscr{P}(E)$-vel, így az 10.3.9. állítás alkalmazásával kapjuk, hogy $\bigcup\limits_{H \in \mathbf{A}} \mathscr{P}(E \times H)$ kisebb-egyenlő számosságú a $\mathbf{A} \times \mathscr{P}(E)$ halmaznál. Tehát az $\mathscr{F}_0(E;F) \subseteq \bigcup\limits_{H \in \mathbf{A}} \mathscr{P}(E \times H)$ összefüggés miatt $\mathscr{F}_0(E;F)$ kisebb-egyenlő számosságú a $\mathbf{A} \times \mathscr{P}(E)$ halmaznál.

Végül, ha $g : E \to F$ injekció, és $\mathbf{B}$ jelöli az E halmaz E-vel ekvipotens részhalmazainak halmazát, akkor a

$$\mathbf{B} \to \mathbf{A} \quad ; \quad H \mapsto g\langle H\rangle$$

leképezés injekció, és 10.3.14. szerint $\mathbf{B}$ ekvipotens a $\mathscr{P}(E)$ hatványhalmazzal. Tehát $\mathscr{P}(E)$ kisebb-egyenlő számosságú $\mathbf{A}$-nál, így $\mathbf{A} \times \mathscr{P}(E)$ kisebb-egyenlő számosságú a $\mathbf{A} \times \mathbf{A}$ halmaznál, ami a számosságaritmetika alaptétele szerint ekvipotens $\mathbf{A}$-val. Ebből következik, hogy $\mathscr{F}_0(E;F)$ kisebb-egyenlő számosságú $\mathbf{A}$-nál. ■

A Zermelo-féle jólrendezés tétel (6.15.2.) szerint minden halmaz felett létezik jólrendezés. A következő állítás megmutatja, hogy végtelen halmaz felett milyen sok jólrendezés létezik.

10.3.18. Állítás. *Ha E végtelen halmaz, akkor az E feletti jólrendezések halmaza ekvipotens $\mathscr{P}(E)$-vel.*

Bizonyítás. Nyilvánvaló, hogy az *összes* E feletti relációk halmaza kisebb-egyenlő számosságú $\mathscr{P}(E \times E)$-nél, tehát a számosságaritmetika alaptétele szerint kisebb-egyenlő számosságú $\mathscr{P}(E)$-nél.

Megfordítva, legyen R rögzített jólrendezés E felett, ami a Zermelo-féle jólrendezési tétel (6.15.2.) szerint létezik. Ha $f : E \to E$ bijekció, akkor az

$$f_*(R) := \{(x_1, x_2) \in E \times E \mid (f(x_1), f(x_2)) \in R\}$$

reláció szintén jólrendezés E felett, méghozzá olyan, hogy f izomorfizmus az $(E, f_*(R))$ és (E, R) jólrendezett halmazok között. Ebből következik, hogy ha f és g mindketten $E \to E$ bijekciók, akkor a $g^{-1} \circ f$ függvény izomorfizmus az $(E, f_*(R))$ és $(E, g_*(R))$ jólrendezett halmazok között. Tehát, ha $f, g : E \to E$ bijekciók, akkor $f_*(R) = g_*(R)$ esetén $g^{-1} \circ f = \mathrm{id}_E$ (6.13.11.), vagyis $f = g$. Ez azt jelenti, hogy ha $\mathfrak{S}(E)$ jelöli az $E \to E$ bijekciók halmazát, és $\mathbf{W}(E)$ jelöli az E feletti jólrendezések halmazát, akkor az

$$\mathfrak{S}(E) \to \mathbf{W}(E) \quad ; \quad f \mapsto f_*(R)$$

leképezés *injekció*, vagyis $\mathfrak{S}(E)$ kisebb-egyenlő számosságú az E feletti jólrendezések halmazánál. Ugyanakkor 10.3.15. szerint $\mathfrak{S}(E)$ ekvipotens a $\mathscr{P}(E)$ hatványhalmazzal, ezért $\mathscr{P}(E)$ kisebb-egyenlő számosságú az E feletti jólrendezések halmazánál.

A bizonyítást a Schröder–Bernstein-tételre (6.5.5.) hivatkozással fejezzük be. ■

10.4. Rendszámok és transzfinit indukció

10.4.1. Definíció. *Azt mondjuk, hogy az α halmaz* **rendszám**, *ha teljesülnek rá a következők:*

$(\mathrm{ON_I})$ *Az α halmaz tranzitív, vagyis minden $x \in \alpha$ elemre $x \subseteq \alpha$.*

$(\mathrm{ON_{II}})$ *Minden $x \in \alpha$ elemre $x \notin x$.*

$(\mathrm{ON_{III}})$ *A $\leq_\alpha := \{(x,y) \in \alpha \times \alpha | (x \in y) \vee (x = y)\}$ reláció jólrendezés az α halmaz felett.*

Az "α **rendszám**" *kijelentést az* $\mathrm{Ord}(\alpha)$ *szimbólummal jelöljük.*

10.4.2. Állítás. *Teljesülnek a következő állítások.*

a) *Minden természetes szám rendszám, és az $\mathbb{N}$ halmaz is rendszám.*

b) *Minden α rendszámra $\alpha \notin \alpha$.*

c) *Ha α rendszám és $\beta \subseteq \alpha$ olyan tranzitív halmaz, hogy $\beta \neq \alpha$, akkor $\beta \in \alpha$.*

d) *Ha α és β rendszámok, akkor*

$$(\beta \in \alpha) \Leftrightarrow ((\beta \subseteq \alpha) \wedge (\beta \neq \alpha)),$$
$$(\beta \subseteq \alpha) \Leftrightarrow ((\beta \in \alpha) \vee (\beta = \alpha)).$$

Bizonyítás. a) Tudjuk, hogy minden $n \in \mathbb{N}$ esetén n tranzitív halmaz és $n \notin n$ (7.3.2. b) és c) pont). Ugyanakkor 7.8.1. szerint minden $n \in \mathbb{N}$ esetén a $\leq_n$ reláció jólrendezés az n halmaz felett. Ezért minden természetes szám rendszám.

Láttuk, hogy $\mathbb{N}$ tranzitív halmaz (7.3.2.), és $\mathbb{N} \notin \mathbb{N}$ (8.1.7.), valamint az $\leq_\mathbb{N}$ reláció jólrendezés $\mathbb{N}$ felett (7.8.3.), ezért $\mathbb{N}$ is rendszám.

b) Ha α rendszám, akkor $\alpha \in \alpha$ esetén $(\mathrm{ON_{II}})$ miatt $\alpha \notin \alpha$ teljesülne, ami ellentmondás. Ezért minden α rendszámra $\alpha \notin \alpha$.

c) Legyen α rendszám és $\beta \subseteq \alpha$ olyan tranzitív halmaz, hogy $\beta \neq \alpha$. Ekkor $\alpha \setminus \beta \neq \emptyset$ és $\leq_\alpha$ jólrendezés α felett, ezért létezik $\alpha \setminus \beta$-nak legkisebb eleme $\leq_\alpha$ szerint: legyen ez β'. Megmutatjuk, hogy $\beta = \beta'$.

Legyen $\gamma \in \beta'$. Az $(\mathrm{ON_I})$ feltétel alapján $\beta' \subseteq \alpha$, tehát $\gamma \in \alpha$. Ekkor $\gamma <_\alpha \beta'$, következésképpen $\gamma \notin \alpha \setminus \beta$, hiszen β' az $\alpha \setminus \beta$ halmaz legkisebb eleme az $\leq_\alpha$ rendezés szerint. Ugyanakkor $\alpha = \beta \cup (\alpha \setminus \beta)$, tehát $\gamma \in \beta$. Ez azt jelenti, hogy $\beta' \subseteq \beta$.

Megfordítva, legyen $\gamma \in \beta$. A hipotézis szerint $\beta \subseteq \alpha$, így $\gamma \in \alpha$. $(\mathrm{ON_{III}})$ alapján a $\leq_\alpha$ rendezés lineáris, tehát γ és β' összehasonlíthatóak $\leq_\alpha$ szerint, így $\gamma \in \beta'$, vagy $\beta' \in \gamma$, vagy $\beta' = \gamma$. De $\beta' = \gamma$ esetén $\beta' \in \beta$ teljesülne, holott $\beta' \in \alpha \setminus \beta$. Továbbá, $\beta' \in \gamma$ esetén a β halmaz tranzitivitása folytán ismét azt kapnánk, hogy $\beta' \in \beta$, holott $\beta' \in \alpha \setminus \beta$. Ezért $\gamma \in \beta'$ teljesül, vagyis $\beta \subseteq \beta'$.

d) Ha $\beta \in \alpha$, akkor α tranzitivitása miatt $\beta \subseteq \alpha$ és b) alapján $\beta \neq \alpha$. Megfordítva, ha $\beta \subseteq \alpha$ és $\beta \neq \alpha$, akkor a β halmaz tranzitivitása és c) miatt $\beta \in \alpha$.

Ha $\beta \subseteq \alpha$, akkor β tranzitív részhalmaza α-nak, így $\beta \neq \alpha$ esetén c) alapján $\beta \in \alpha$. Megfordítva, ha $\beta \in \alpha$, akkor α tranzitivitása folytán $\beta \subseteq \alpha$, ha pedig $\beta = \alpha$, akkor $\beta \subseteq \alpha$ triviálisan teljesül. ■

Jelölés. Az $\mathbb{N}$ halmazt, mint rendszámot, az ω betűvel jelöljük.

10.4.3. Állítás. *Ha α és β rendszámok, akkor a "$\beta \in \alpha$", "$\alpha \in \beta$" és "$\beta = \alpha$" kijelentések közül pontosan az egyik teljesül. Ha α és β rendszámok, akkor $\beta \subseteq \alpha$ vagy $\alpha \subseteq \beta$ teljesül.*

Bizonyítás. Legyenek α és β rendszámok.

Tranzitív halmazok tetszőleges nem üres rendszerének a metszete nyilvánvalóan tranzitív halmaz, ezért $\alpha \cap \beta$ tranzitív halmaz, vagyis $\alpha \cap \beta$-ra ($\mathrm{ON_I}$) teljesül. Ha egy halmaz minden eleme nem eleme önmagának, akkor a halmaz bármely részhalmaza még inkább rendelkezik ezzel a tulajdonsággal, ezért $\alpha \cap \beta$-ra ($\mathrm{ON_{II}}$) teljesül. A definíció alapján nyilvánvaló, hogy a $\leq_{\alpha\cap\beta}$ reláció egyenlő a $\leq_\alpha$ jólrendezés $\alpha \cap \beta$-ra vett megszorításával, ezért $\leq_{\alpha\cap\beta}$ jólrendezés $\alpha \cap \beta$ felett (6.13.2.), vagyis $\alpha \cap \beta$-ra ($\mathrm{ON_{II}}$) is teljesül. Ezzel megmutattuk, hogy $\alpha \cap \beta$ rendszám.

Ha $\alpha \cap \beta \neq \alpha$ és $\alpha \cap \beta \neq \beta$, akkor az előző állítás c) pontja szerint $\alpha \cap \beta \in \alpha \cap \beta$ hiszen $\alpha \cap \beta$ tranzitív halmaz. Ez viszont az előző állítás b) pontja miatt lehetetlen, hiszen $\alpha \cap \beta$ rendszám. Tehát $\alpha \cap \beta = \alpha$ *vagy* $\alpha \cap \beta = \beta$ teljesül, vagyis $\alpha \subseteq \beta$ vagy $\beta \subseteq \alpha$.

Ha $\alpha \neq \beta$, akkor $\alpha \nsubseteq \beta$ vagy $\beta \nsubseteq \alpha$. Az előző bekezdés szerint az első esetben $\beta \subseteq \alpha$, és a második esetben $\alpha \subseteq \beta$, ezért az előző állítás c) pontja alapján: az első esetben $\beta \in \alpha$, és a második esetben $\alpha \in \beta$. Ez azt jelenti, hogy a "$\beta \in \alpha$", "$\alpha \in \beta$" és "$\beta = \alpha$" kijelentések közül valamelyik teljesül. A rendszámok tranzitivitása és az előző állítás b) pontja alapján e három kijelentés közül bármely kettőnek a konjunkciója hamis. ■

10.4.4. Állítás. *Rendszám minden eleme rendszám.*

Bizonyítás. Legyen α rendszám és $x \in \alpha$.

Az α halmaz tranzitivitása miatt $x \subseteq \alpha$, ezért minden $y \in x$ esetén $y \in \alpha$, következésképpen $y \notin y$.

Az α halmaz tranzitivitása miatt $x \subseteq \alpha$, és a definíció alapján nyilvánvaló, hogy a $\leq_x$ reláció egyenlő a $\leq_\alpha$ reláció x-re vett megszorításával, ezért $\leq_x$ jólrendezés x felett (6.13.2.).

Azt kell még igazolni, hogy x tranzitív halmaz. Ehhez legyenek y és z olyan halmazok, hogy $z \in y \in x$. Ekkor az α halmaz tranzitivitása és $y \in x \in \alpha$ miatt $y \in \alpha$, tehát ismét α tranzitivitása és $z \in y$ következtében $z \in \alpha$. Tehát $x, y, z \in \alpha$ és $z \in y$, valamint $y \in x$. Ebből következik, hogy $z \leq_\alpha y$ és $y \leq_\alpha x$. Ezért a $\leq_\alpha$ reláció tranzitivitása folytán $z \leq_\alpha x$, vagyis $z \in x$ vagy $z = x$. Ha $z = x$ teljesülne, akkor igazak volnának az $x \leq_\alpha y$ és $y \leq_\alpha x$ összefüggések, tehát a $\leq_\alpha$ reláció antiszimmetrikusságából $x = y$ következne, így azt kapnánk, hogy $x = y \in x$, ami lehetetlen, mert $x \in \alpha$ és α-ra ($\mathrm{ON_{II}}$) teljesül. Ezért szükségképpen $z \in x$, vagyis x tranzitív halmaz. ■

Jelölés. Ha α és β rendszámok, akkor az $\alpha \subseteq \beta$ kijelentés helyett azt írjuk, hogy $\alpha \leq \beta$. Továbbá, ha α és β rendszámok, akkor az $(\alpha \subseteq \beta) \wedge (\alpha \neq \beta)$ (vagy az ezzel ekvivalens $\alpha \in \beta$) kijelentés helyett azt írjuk, hogy $\alpha < \beta$.

Minden halmaz egyenlő az elemeinek halmazával, így az előző állítás szerint minden rendszám egyenlő a nála kisebb rendszámok halmazával.

10.4.5. Állítás. *Ha H olyan halmaz, amelynek minden eleme rendszám, akkor a*

$$\leq_H := \{(\alpha, \beta) \in H \times H \mid (\alpha \in \beta) \vee (\alpha = \beta)\}$$

reláció jólrendezés a H halmaz felett.

Bizonyítás. A 10.4.2. állítás d) pontja szerint $\leq_H = \{(\alpha, \beta) \in H \times H | \alpha \subseteq \beta\}$. Nyilvánvaló, hogy ez a H feletti reláció rendezés. Annak bizonyításához, hogy $\leq_H$ jólrendezés, legyen

$X \subseteq H$ nem üres halmaz. Legyen $\alpha \in X$ rögzített elem. Ekkor két eset lehetséges.

– Ha $\alpha \cap H = \emptyset$, akkor $\gamma \in H$ esetén $\gamma \notin \alpha$, tehát 10.4.3. miatt $(\alpha \in \gamma) \vee (\alpha = \gamma)$ teljesül, ami 10.4.2. d) szerint azzal ekvivalens, hogy $\alpha \subseteq \gamma$, vagyis $\alpha \leq_H \gamma$. Tehát α a H halmaz legkisebb eleme $\leq_H$ szerint.

– Ha $\alpha \cap H \neq \emptyset$, akkor ennek a halmaznak létezik legkisebb eleme $\leq_\alpha$ szerint, hiszen $\leq_\alpha$ jólrendezés α felett. Legyen ez az elem α_*. Ha $\gamma \in H$ és $\gamma \in \alpha$, akkor $\gamma \in \alpha \cap H$, tehát az α_* rendszám értelmezése alapján $\alpha_* \leq_\alpha \gamma$, vagyis $(\alpha_* \in \gamma) \vee (\alpha_* = \gamma)$ teljesül, ami azt jelenti, hogy $\alpha_* \leq_H \gamma$. Ha $\gamma \in H$ és $\gamma \notin \alpha$, akkor 10.4.3. miatt $(\alpha \in \gamma) \vee (\alpha = \gamma)$ teljesül, tehát $\alpha \leq_H \gamma$. Ugyanakkor $\alpha_* \in \alpha$ is igaz, tehát $\alpha_* \leq_H \alpha$, így a $\leq_H$ reláció tranzitivitása folytán $\alpha_* \leq_H \gamma$. Tehát α_* a H halmaz legkisebb eleme $\leq_H$ szerint. ■

10.4.6. Tétel. *Az "x rendszám" kijelentés nem kollektivizáló az x változóban, tehát nem létezik az összes rendszámok halmaza.*

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy az "x rendszám" (vagyis $\mathrm{Ord}(x)$) kijelentés kollektivizáló az x változóban. Ekkor elkészíthetjük az $\mathbf{On} := \{x|\mathrm{Ord}(x)\}$ halmazt, amelyre teljesül a

$$(\forall x)\ ((x \in \mathbf{On}) \Leftrightarrow \mathrm{Ord}(x))$$

kijelentés. Megmutatjuk, hogy $\mathbf{On}$ rendszám, így 10.4.2. b) alapján $\mathbf{On} \notin \mathbf{On}$, ugyanakkor $\mathrm{Ord}(\mathbf{On})$ teljesül, tehát $\mathbf{On} \in \mathbf{On}$, ami ellentmondás.

A 10.4.4. állítás alapján $(\mathrm{ON_I})$ teljesül a $\mathbf{On}$ halmazra, és 10.4.2. b) szerint $(\mathrm{ON_{II}})$ is teljesül $\mathbf{On}$-ra. Végül, a 10.4.5. állításból következik, hogy $(\mathrm{ON_{III}})$ is igaz a $\mathbf{On}$ halmazra, tehát $\mathbf{On}$ rendszám. ■

10.4.7. Állítás. *Teljesülnek a következő állítások.*

a) *Ha α rendszám, akkor az α^+ szukcesszor is rendszám.*

b) *Ha α rendszám, akkor nem létezik olyan β rendszám, amelyre $\alpha < \beta < \alpha^+$.*

c) *Ha α és β rendszámok, akkor $\alpha = \beta \Leftrightarrow \alpha^+ = \beta^+$.*

Bizonyítás. a) Legyenek x és y olyan halmazok, hogy $x \in y \in \alpha^+$. Ekkor $y \in \alpha$ vagy $y = \alpha$. Ha $y \in \alpha$, akkor α tranzitivitása miatt $x \in \alpha$, ezért $x \in \alpha^+$. Ha $y = \alpha$, akkor $x \in \alpha$, ezért $x \in \alpha^+$. Ez azt jelenti, hogy α^+ tranzitív halmaz.

Legyen $x \in \alpha^+$. Ekkor $x \in \alpha$ vagy $x = \alpha$. Ha $x \in \alpha$, akkor $x \notin x$, mert $(\mathrm{ON_{II}})$ teljesül α-ra. Ha $x = \alpha$, akkor a 10.4.2. állítás b) pontja szerint $x \notin x$. Ez azt jelenti, hogy $(\mathrm{ON_{II}})$ teljesül α^+-ra.

Az α^+ halmaz minden eleme rendszám, ezért 10.4.5. szerint az $\{(x, y) \in \alpha^+ \times \alpha^+|(x \in y) \vee (x = y)\}$ reláció jólrendezés α^+ felett, vagyis α^+-ra $(\mathrm{ON_{III}})$ is teljesül.

b) Indirekt tegyük fel, hogy α és β olyan rendszámok, hogy $\alpha < \beta < \alpha^+$, vagyis $\alpha \in \beta \in \alpha^+$. Ekkor $\beta \in \alpha$ vagy $\beta = \alpha$. Ha $\beta \in \alpha$, akkor α tranzitivitása miatt $\alpha \in \alpha$, ami 10.4.2. b) miatt lehetetlen. Tehát $\beta = \alpha$, és ekkor $\alpha \in \alpha$ teljesül, ami ellentmondás.

c) Tegyük fel, hogy $\alpha^+ = \beta^+$, és legyen $\gamma \in \alpha$. Ekkor $\alpha \subseteq \alpha^+$ miatt $\gamma \in \alpha^+$, tehát $\gamma \in \beta^+$, vagyis $\gamma \in \beta$ vagy $\gamma = \beta$. Megmutatjuk, hogy $\gamma = \beta$ lehetetlen. Ha $\gamma = \beta$ teljesülne, akkor $\beta \in \alpha$, így $\beta \subseteq \alpha$ is igaz volna, mert α tranzitív halmaz. Ekkor viszont $\beta^+ = \beta \cup \{\beta\} \subseteq \alpha$, így 10.4.2. d) alapján $\beta^+ \in \alpha$ vagy $\beta^+ = \alpha$. Ugyanakkor $\alpha \in \beta^+$, ezért β^+ tranzitivitása miatt mindkét esetben $\beta^+ \in \beta^+$, ami 10.4.2. b) miatt lehetetlen, hiszen a) alapján β^+ rendszám. Ezzel bebizonyítottuk, hogy $\alpha \subseteq \beta$. Ebből α és β felcserélésével következik, hogy $\beta^+ = \alpha^+$ esetén $\beta \subseteq \alpha$. ■

10.4.8. Következmény. *Ha α rendszám, akkor az α^+ jólrendezett halmaznak α a legnagyobb eleme.*

Bizonyítás. Ha volna olyan $\beta \in \alpha^+$, hogy $\alpha < \beta$, akkor $\alpha \in \beta \in \alpha^+$, ami az előző állítás b) pontja szerint lehetetlen. ■

10.4.9. Definíció. *Azt mondjuk, hogy az α rendszám* **szukcesszor***, ha van olyan β rendszám, hogy $\alpha = \beta^+$. Azt mondjuk, hogy az α rendszám* **elsőfajú rendszám***, ha $\alpha = 0$ vagy α szukcesszor. A nem elsőfajú rendszámokat* **limeszrendszámoknak** *nevezzük, és az "α limeszrendszám" kijelentést a $\mathrm{Lim}(\alpha)$ szimbólummal rövidítjük.*

10.4.10. Tétel. *Az "x elsőfajú rendszám és minden x-nél kisebb rendszám elsőfajú" kijelentés kollektivizáló az x változóban, és ha $\mathscr{N}(x)$ jelöli ezt a kijelentést, akkor*

$$\mathbb{N} \;=\; \{x \mid \mathscr{N}(x)\}.$$

Az ω rendszám a legkisebb limeszrendszám.

Bizonyítás. Megmutatjuk, hogy $(\forall\alpha)(\mathscr{N}(\alpha) \Rightarrow \alpha \in \omega)$ igaz. Az állítással ellentétben tegyük fel, hogy α olyan halmaz, amelyre $\mathscr{N}(\alpha)$ teljesül, de $\alpha \notin \omega$ (azaz $\alpha \notin \mathbb{N}$). Legyen

$$H := \{\beta | \mathscr{N}(\beta) \wedge (\beta \leq \alpha) \wedge (\beta \notin \omega)\}.$$

Ekkor H minden eleme olyan rendszám, amely részhalmaza az α rendszámnak, tehát $H \subseteq \alpha^+$. Az $(\alpha^+, \leq_{\alpha^+})$ pár jólrendezett halmaz, ezért létezik H-nak legkisebb eleme a $\leq_{\alpha^+}$ rendezés szerint; legyen ez β. Világos, hogy $0 \in \omega$, ezért $\mathscr{N}(\beta)$ miatt $\beta \neq 0$, így van olyan γ rendszám, amelyre $\beta = \gamma^+$, hiszen β elsőfajú rendszám. Ekkor $\gamma < \beta$, tehát $\mathscr{N}(\beta)$ miatt γ is elsőfajú rendszám. Ha egy rendszám kisebb γ-nál, akkor β-nál is kisebb, tehát $\mathscr{N}(\beta)$ alapján elsőfajú. Ez azt jelenti, hogy $\mathscr{N}(\gamma)$ teljesül. Ugyanakkor a β minimalitási tulajdonsága és $\gamma < \beta$ miatt $\gamma \notin H$, tehát $\gamma \in \omega = \mathbb{N}$. Ekkor azonban $\beta = \gamma^+ \in \mathbb{N} = \omega$, ami ellentmond annak, hogy $\beta \notin \omega$.

Ez azt jelenti, hogy $(\forall\alpha)(\mathscr{N}(\alpha) \Rightarrow \alpha \in \omega)$ tétel, tehát a részhalmaz-axióma szerint az $\mathscr{N}(\alpha)$ kijelentés kollektivizáló az α változóban, sőt az is igaz, hogy $\{\alpha|\mathscr{N}(\alpha)\} \subseteq \omega = \mathbb{N}$. Másfelől, a teljes indukció tételének alkalmazásával könnyen belátható, hogy $(\forall n)((n \in \mathbb{N}) \Rightarrow \mathscr{N}(n))$ igaz, így $\mathbb{N} \subseteq \{\alpha|\mathscr{N}(\alpha)\}$ is teljesül. ■

10.4.11. Állítás. *Ha H rendszámok tetszőleges halmaza, akkor $\bigcup H$ is rendszám, és erre teljesülnek az alábbiak:*

- *minden $\alpha \in H$ rendszámra $\alpha \leq \bigcup H$;*
- *minden β rendszámra, ha minden $\alpha \in H$ esetén $\alpha \leq \beta$, akkor $\bigcup H \leq \beta$.*

(*Ezért az $\bigcup H$ halmazt a H rendszám-halmaz* **rendszám-szuprémumának***, vagy* **legkisebb felső rendszám-korlátjának** *nevezzük.*)

Bizonyítás. Ha $x \in \bigcup H$, akkor van olyan $\alpha \in H$, hogy $x \in \alpha$, így 10.4.4. miatt x rendszám. Tehát $\bigcup H$ minden eleme rendszám, így 10.4.2. b) miatt $(\mathrm{ON_{II}})$ és 10.4.5. alapján $(\mathrm{ON_{III}})$ teljesül $\bigcup H$-ra. Ha $\alpha \in \bigcup H$ és $\beta \in \alpha$, akkor van olyan $\gamma \in H$, hogy $\alpha \in \gamma$, így γ tranzitivitása miatt $\alpha \subseteq \gamma$, következésképpen $\beta \in \gamma$ és $\gamma \in H$, tehát $\beta \in \bigcup H$. Ez azt jelenti, hogy $\bigcup H$ tranzitív halmaz, tehát $(\mathrm{ON_I})$ is teljesül rá.

Ezzel megmutattuk, hogy $\bigcup H$ rendszám. Ha $\alpha \in H$ és $\beta \in \alpha$, akkor az unió-halmaz definíciója szerint $\beta \in \bigcup H$, tehát $\alpha \subseteq \bigcup H$, ami azt jelenti, hogy $\alpha \leq \bigcup H$. Ha β olyan rendszám, hogy minden $\alpha \in H$ esetén $\alpha \leq \beta$, akkor $\beta \in \bigcup H$ lehetetlen, különben létezne olyan $\alpha \in H$, hogy $\beta \in \alpha$, ezért 10.4.3. alapján $\bigcup H \leq \beta$. ■

Az előző állításból következik, hogy rendszámok bármely halmazához létezik olyan rendszám, amely a halmaz minden eleménél nagyobb, hiszen ha H rendszámok halmaza, akkor 10.4.11. miatt a $(\bigcup H)^+$ rendszám H minden eleménél nagyobb.

10.4.12. Állítás. *Ha H rendszámok olyan nem üres halmaza, amelynek nincs legnagyobb eleme (tehát minden $\alpha \in H$ esetén van olyan $\beta \in H$, hogy $\alpha < \beta$), akkor $\bigcup H$ limeszrendszám.*

Bizonyítás. Az unió-halmaz definíciójából könnyen látható, hogy a H-ra vonatkozó hipotézis ekvivalens azzal, hogy $H \subseteq \bigcup H$. Ebből azonnal következik, hogy $\bigcup H \neq 0$, különben H üres volna. Ugyanakkor $\bigcup H$ szukcesszor sem lehet. Tegyük fel ugyanis, hogy α olyan rendszám, amelyre $\alpha^+ = \bigcup H$. Ekkor $\alpha \in \bigcup H$ miatt vehetünk olyan $\beta \in H$ elemet, hogy $\alpha \in \beta$. A H halmaznak nincs legnagyobb eleme, ezért van olyan $\gamma \in H$, amelyre $\beta \in \gamma$. Ha $\gamma \leq \alpha^+$ teljesülne, akkor $\alpha \in \beta \in \alpha^+$ teljesülne, ami 10.4.7. b) miatt lehetetlen. Ezért $\alpha^+ \in \gamma \in H$, tehát $\alpha^+ \in \bigcup H = \alpha^+$, ami ellentmond $(\mathrm{ON_{II}})$-nek. Ezért $\bigcup H$ limeszrendszám. ■

10.4.13. Állítás. *Ha az α rendszám szukcesszor, akkor $\alpha = (\bigcup \alpha)^+$. Ha α olyan rendszám, amely nem szukcesszor, akkor $\alpha = \bigcup \alpha$.*

Bizonyítás. Legyen β olyan rendszám, hogy $\alpha = \beta^+$. Ekkor a 10.4.7. c) állítás szerint az $\alpha = (\bigcup \alpha)^+$ egyenlőség ekvivalens azzal, hogy $\beta = \bigcup \alpha$. Ha $\gamma \in \beta$, akkor $\beta \in \beta^+ = \alpha$ miatt $\gamma \in \bigcup \alpha$, tehát $\beta \subseteq \bigcup \alpha$. Megfordítva, ha $\gamma \in \bigcup \beta$, akkor van olyan $\delta \in \alpha$, hogy $\gamma \in \delta$. Ekkor α tranzitiviása miatt $\gamma \in \alpha = \beta^+$, ezért $\gamma = \beta$ vagy $\gamma \in \beta$. Az első eset lehetetlen, különben $\beta = \gamma \in \delta \in \alpha = \beta^+$ teljesülne, ami ellentmond a 10.4.7. b) állításnak, ezért $\gamma \in \beta$. Ez azt jelenti, hogy $\bigcup \alpha \subseteq \beta$.

A második állítás bizonyításához tegyük fel, hogy $\alpha \neq \bigcup \alpha$. Megmutatjuk, hogy ekkor α szukcesszor. Valóban, 10.4.4. és 10.4.11. alapján $\bigcup \alpha$ rendszám, így a hipotézisből következik, hogy $\alpha \in \bigcup \alpha$ vagy $\bigcup \alpha \in \alpha$. Ha $\alpha \in \bigcup \alpha$, akkor van olyan $\beta \in \alpha$, hogy $\alpha \in \beta$, ami α tranzitivitása és $\alpha \notin \alpha$ miatt lehetetlen, ezért $\bigcup \alpha \in \alpha$. Ha $\beta \in \alpha$, akkor minden $\gamma \in \beta$ esetén $\gamma \in \bigcup \alpha$, tehát $\beta \subseteq \bigcup \alpha$, így $\bigcup \alpha \subseteq \left(\bigcup \alpha\right)^+$ miatt $\beta \in \left(\bigcup \alpha\right)^+$. Tehát ekkor $\alpha \subseteq \left(\bigcup \alpha\right)^+$, ugyanakkor $\bigcup \alpha \in \alpha$. Ha $\alpha \neq \left(\bigcup \alpha\right)^+$ teljesülne, akkor $\alpha \in \left(\bigcup \alpha\right)^+$, ami ellentmond az 10.4.7. b) állításnak. Ezért $\alpha = \left(\bigcup \alpha\right)^+$, vagyis α szukcesszor. ■

A következő állítás előtt megjegyezzük, hogy ha α rendszám, akkor $\beta \in \alpha$ esetén a β halmaz *szegmense* az $(\alpha, \leq_\alpha)$ jólrendezett halmaznak, mert α tranzitivitása folytán

$\beta \subseteq \alpha$ és ha $\gamma \in \beta$, akkor a $\leq_\alpha$ rendezés szerinti $]\leftarrow, \gamma]$ intervallum minden eleme olyan rendszám, amely eleme β-nak.

10.4.14. Állítás. *Ha α és β olyan rendszámok, hogy $\alpha \in \beta$, akkor minden $H \subseteq \alpha$ halmazra a $(H, \leq_H)$ és $(\beta, \leq_\beta)$ jólrendezett halmazok nem izomorfak.*

Bizonyítás. Az állítással ellentétben tegyük fel, hogy α és β olyan rendszámok, és $H \subseteq \alpha$ olyan halmaz, amelyekre teljesül az, hogy $\alpha \in \beta$ és a $(H, \leq_H)$ és $(\beta, \leq_\beta)$ jólrendezett halmazok *izomorfak*. Legyen $h : \beta \to H$ izomorfizmus. Mivel β tranzitív halmaz, így $\alpha \subseteq \beta$, ezért $H \subseteq \beta$. Tehát $h : \beta \to \beta$ olyan függvény, amely szigorúan monoton növő a $\leq_\beta$ rendezés szerint, továbbá $h(\alpha) \in \mathrm{Im}(h) = H \subseteq \alpha$, vagyis $h(\alpha) \in \alpha$, azaz $h(\alpha) < \alpha$ a $\leq_\beta$ rendezés szerint. Ugyanakkor az $\mathrm{id}_\beta : \beta \to \beta$ leképezés monoton növő az $\leq_\beta$ rendezés szerint, és $\mathrm{Im}(\mathrm{id}_\beta) = \beta$ szegmense a $(\beta, \leq_\beta)$ jólrendezett halmaznak. Ezért a 6.13.9. szerint minden $\gamma \in \beta$ elemre $\gamma = \mathrm{id}_\beta(\gamma) \leq h(\gamma)$, tehát $\alpha \leq h(\alpha)$, ami ellent mond a $h(\alpha) < \alpha$ egyenlőtlenségnek. ■

10.4.15. Tétel. *Ha α és β rendszámok, akkor az $(\alpha, \leq_\alpha)$ és $(\beta, \leq_\beta)$ jólrendezett halmazok pontosan akkor izomorfak, ha $\alpha = \beta$. Ha α rendszám, akkor egyetlen izomorfizmus létezik az $(\alpha, \leq_\alpha)$ és $(\alpha, \leq_\alpha)$ jólrendezett halmazok között (és persze az egyenlő az id_α függvénnyel).*

Bizonyítás. Ha α és β olyan rendszámok, hogy $\alpha \neq \beta$, akkor $\alpha \in \beta$ vagy $\beta \in \alpha$, és mindkét esetben, megfelelő szereposztással, az előző állításból kapjuk, hogy az $(\alpha, \leq_\alpha)$ és $(\beta, \leq_\beta)$ jólrendezett halmazok *nem izomorfak*. A második állítás tiriválisan következik a 6.13.10. állításból. ■

10.4.16. Tétel. (**A transzfinit indukció halmazelméleti formája.**) *Legyen $(E, \leq)$ jólrendezett halmaz és $\mathfrak{S}$ az $(E, \leq)$ szegmenseinek olyan halmaza, amelyre teljesülnek a következők:*

a) *Minden $\mathfrak{S}$-ben haladó $(S_i)_{i\in I}$ rendszerre $\bigcup_{i\in I} S_i \in \mathfrak{S}$.*

b) *Minden $x \in E$ elemre, ha $]\leftarrow, x[\in \mathfrak{S}$, akkor $]\leftarrow, x] \in \mathfrak{S}$.*

Ekkor $\mathfrak{S}$ egyenlő az $(E, \leq)$ összes szegmenseinek halmazával, tehát az is igaz, hogy $E \in \mathfrak{S}$.

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy $\mathfrak{S}$ nem egyenlő az $(E, \leq)$ összes szegmenseinek halmazával. Tudjuk, hogy az $(E, \leq)$ jólrendezett halmaz összes szegmenseinek halmaza felett a tartalmazás-reláció jólrendezés (6.13.6.), így az indirekt feltevés alapján van olyan S szegmense $(E, \leq)$-nek, amelyre $S \notin \mathfrak{S}$, és amely tartalmazás tekintetében legkisebb ilyen tulajdonságú szegmense $(E, \leq)$-nek. Ha S-nek nincs legnagyobb eleme a $\leq$ rendezés szerint, akkor $S = \bigcup_{x\in S}]\leftarrow, x[$, ugyanakkor minden $x \in S$ elemre $]\leftarrow, x[$ olyan szegmense $(E, \leq)$-nek, amely S-nek valódi részhalmaza, tehát az S minimalitása miatt $]\leftarrow, x[\in \mathfrak{S}$. Ekkor azonban az a) alapján $S \in \mathfrak{S}$ is teljesülne, ami nem igaz; ezért S-nek létezik legnagyobb eleme; legyen ez x. Tehát $S =]\leftarrow, x]$ teljesül, ugyanakkor $]\leftarrow, x[$ olyan szegmense $(E, \leq)$-nek, amely S-nek valódi részhalmaza, így $]\leftarrow, x[\in \mathfrak{S}$. Ebből viszont a b) alapján következik, hogy $S =]\leftarrow, x] \in \mathfrak{S}$, ami ellentmondás. ■

10.4.17. Definíció. *Ha $\mathscr{A}$ kijelentés, x változó és T halmaz, akkor $(T|x)\mathscr{A}$ jelöli azt a kijelentést, amit úgy nyerünk, hogy $\mathscr{A}$-ban az x minden előfordulásának helyére T-t helyettesítünk. Azt mondjuk, hogy az $\mathscr{A}$ kijelentés* **egyértelmű az x változóban**, *ha a*

$$(\forall z)(\forall z')(((z|x)\mathscr{A}) \wedge ((z'|x)\mathscr{A})) \Rightarrow (z = z'))$$

kijelentés tétel, ahol a z és z' változók nem szerepelnek $\mathscr{A}$-ban.

Helyettesítés axiómája – *Ha $\mathscr{A}$ kijelentés, x, y változók, és $\mathscr{A}$ az y változóban egyértelmű, akkor minden olyan E halmazra, amelyben x és y nem szerepel, a*

$$(\exists x)((x \in E) \wedge \mathscr{A})$$

kijelentés kollektivizáló az y változóban, tehát létezik olyan F halmaz, hogy minden y-ra az $y \in F$ kijelentés ekvivalens azzal, hogy $(\exists x)((x \in E) \wedge \mathscr{A})$.

10.4.18. Tétel. *A kiválasztási axióma helyett a helyettesítés axiómáját felvéve igaz az, hogy ha $(E, \leq)$ jólrendezett halmaz, akkor egyértelműen létezik olyan α rendszám, amelyre az $(E, \leq)$ és $(\alpha, \leq_\alpha)$ jólrendezett halmazok izomorfak.*

Bizonyítás. A 10.4.15. tétel szerint α unicitása nyilvánvaló, és persze ahhoz nem szükséges a helyettesítés axiómája. Az α létezésének bizonyításához jelölje $\mathfrak{S}$ az $(E, \leq)$ jólrendezett halmaz azon S szegmenseinek halmazát, amelyekhez létezik olyan α rendszám, hogy az $(S, \leq_S)$ és $(\alpha, \leq_\alpha)$ jólrendezett halmazok izomorfak. (Megjegyezzük, hogy itt $\leq_S$ a $\leq$ jólrendezés S halmazra vett megszorítását jelöli.) Megmutatjuk, hogy $\mathfrak{S}$-re teljesülnek a 10.4.16. tétel a) és b) feltételei, ezért $E \in \mathfrak{S}$, ami az állítást bizonyítja.

Legyen $(S_i)_{i \in I}$ tetszőleges $\mathfrak{S}$-ben haladó rendszer, és legyen $S := \bigcup_{i \in I} S_i$. Minden $i \in I$ esetén jelölje $\leq_i$ a $\leq$ rendezés S_i-re vett megszorítását. Legyen $\mathscr{A}(\mathbf{x}, \mathbf{y})$ a következő kijelentés rövidítése:

$$\begin{gathered}(\exists H)(\exists R)(\ \mathbf{x} = (H, R) \wedge \text{"}(H, R)\text{ jólrendezett halmaz"}) \wedge \mathrm{Ord}(\mathbf{y}) \wedge \\ \text{"a }(H, R)\text{ és }(\mathbf{y}, \leq_{\mathbf{y}})\text{ jólrendezett halmazok izomorfak"}\ ).\end{gathered}$$

A 10.4.15. tétel szerint az $\mathscr{A}(\mathbf{x}, \mathbf{y})$ kijelentés az $\mathbf{y}$ változóban egyértelmű, így a helyettesítés axiómája alapján a $\mathscr{H} := \{(S_i, \leq_i) | i \in I\}$ halmaz olyan, hogy a $(\exists \mathbf{x})((\mathbf{x} \in \mathscr{H}) \wedge \mathscr{A}(\mathbf{x}, \mathbf{y}))$ kijelentés az $\mathbf{y}$ változóban kollektivizáló, tehát az

$$\{\mathbf{y} | (\exists \mathbf{x})((\mathbf{x} \in \mathscr{H}) \wedge \mathscr{A}(\mathbf{x}, \mathbf{y}))\}$$

halmaz rendelkezik azzal a tulajdonsággal, hogy minden $\mathbf{y}$-ra: $\mathbf{y}$ pontosan akkor eleme neki, ha $(\exists \mathbf{x})((\mathbf{x} \in \mathscr{H}) \wedge \mathscr{A}(\mathbf{x}, \mathbf{y}))$ teljesül. A $\mathscr{H}$ halmaz értelmezése alapján nyilvánvaló, hogy

$$(\exists \mathbf{x})((\mathbf{x} \in \mathscr{H}) \wedge \mathscr{A}(\mathbf{x}, \mathbf{y}))\} \Leftrightarrow (\exists i)((i \in I) \wedge \mathscr{A}((S_i, \leq_i), \mathbf{y})),$$

ahol a $((S_i, \leq_i)|\mathbf{x})\mathscr{A}(\mathbf{x}, \mathbf{y})$ kifejezést a szokásosabb $\mathscr{A}((S_i, \leq_i), \mathbf{y})$ kifejezéssel rövidítettük. Tehát jól értelmezett az

$$A := \{\mathbf{y} | (\exists i)((i \in I) \wedge \mathscr{A}((S_i, \leq_i), \mathbf{y}))\}$$

rendszám-halmaz. (A helyettesítés axiómájára kizárólag azért volt szükség, hogy ezt a halmazt értelmezhessük!) A 10.4.11. állítás szerint képezhető az $\alpha := \bigcup A$ rendszám;

megmutatjuk, hogy az $(S, \leq_S)$ és $(\alpha, \leq_\alpha)$ rendezett halmazok izomorfak. Ehhez minden $i \in I$ esetén legyen E_i azon $f : S_i \to \alpha$ függvények halmaza, amelyekre $\mathrm{Im}(f)$ rendszám és f izomorfizmus az $(S_i, \leq_i)$ és $(\mathrm{Im}(f), \leq_{\mathrm{Im}(f)})$ rendezett halmazok között. A részhalmaz-axióma alapján az $(E_i)_{i\in I}$ halmazrendszer jól értelmezett, és 6.13.10. szerint E_i egy elemű halmaz. Ezért a $\prod\limits_{i\in I} E_i$ szorzathalmaz is egy elemű; legyen $(f_i)_{i\in I}$ az egyetlen eleme ennek a szorzathalmaznak. Ekkor $(f_i)_{i\in I}$ olyan függvényrendszer, hogy minden $i \in I$ indexre $f_i : S_i \to \alpha$ szigorúan monoton növő a $\leq_i$ és $\leq_\alpha$ rendezések szerint, továbbá $\mathrm{Im}(f)$ egy α-nál kisebb-egyenlő rendszám. Könnyen látható, hogy minden $i, j \in I$ esetén $f_i \subseteq f_j$ vagy $f_j \subseteq f_i$ teljesül, ezért jól értelmezett az $f := \bigcup\limits_{i\in I} f_i : S \to \alpha$ függvény, ami izomorfizmus az $(S, \leq_S)$ és $(\alpha, \leq_\alpha)$ rendezett halmazok között. Ezért $S \in \mathfrak{S}$, vagyis $\mathfrak{S}$-re teljesül a 10.4.16. tétel a) feltétele.

Legyen most $x \in E$ olyan, hogy $S :=] \leftarrow, x[\in \mathfrak{S}$. Ekkor létezik egyetlen olyan α rendszám, hogy az $(S, \leq_S)$ és $(\alpha, \leq_\alpha)$ rendezett halmazok izomorfak; legyen $f : S \to \alpha$ izomorfizmus. Értelmezzük azt az $] \leftarrow, x] \to \alpha^+$ függvényt, amely f-nek kiterjesztése, és az x-hez α-t rendeli. Ez a függvény izomorfizmus az $(] \leftarrow, x], \leq_{] \leftarrow, x]})$ és $(\alpha^+, \leq_{\alpha^+})$ rendezett halmazok között, így $] \leftarrow, x] \in \mathfrak{S}$, ami azt jelenti, hogy $\mathfrak{S}$-re teljesül a 10.4.16. tétel b) feltétele is. ■

10.5. Számosságok és számosságaritmetika

10.5.1. Definíció. *Azt mondjuk, hogy az* $\mathfrak{a}$ *halmaz* **számosság** (*vagy* **kardinális szám**), *ha* $\mathfrak{a}$ *olyan rendszám, amely semmilyen nála kisebb rendszámmal nem ekvipotens.*

10.5.2. Állítás. *Minden természetes szám számosság, és ω is számosság. A természetes számok éppen a véges számosságok.*

Bizonyítás. Minden természetes szám rendszám, és ω is rendszám (10.4.2. a)). Természetes számnál kisebb rendszám valódi részhalmaza az adott természetes számnak, így ezek nem ekvipotensek (8.1.2.). Ezért minden természetes szám számosság. Minden ω-nál kisebb rendszám eleme ω-nak, tehát természetes szám, így nem lehet ω-val ekvipotens, mert természetes szám véges halmaz és ω végtelen (8.1.7.). Ezért ω is számosság. ■

Megállapodunk abban, hogy a természetes számok halmazát, mint számosságot az $\aleph_0$ szimbólummal jelöljük.

10.5.3. Állítás. *Minden α rendszámhoz létezik egyetlen olyan $\mathfrak{a}$ számosság, hogy α és $\mathfrak{a}$ ekvipotensek.*

Bizonyítás. (*Egzisztencia.*) Legyen α rendszám és

$$H_\alpha := \{\beta | (\beta \in \alpha^+) \wedge \text{"}\beta \text{ ekvipotens } \alpha\text{-val"}\}.$$

Ekkor H_α nem üres részhalmaza α^+-nak, mert $\alpha \in H_\alpha$, és $(\alpha^+, \leq_{\alpha^+})$ jólrendezett halmaz, tehát H_α-nak létezik legkisebb eleme α^+-ban a $\leq_{\alpha^+}$ rendezés szerint: legyen ez $\mathfrak{a}$. Ez az elem olyan számosság, amelynek a létezését állítjuk.

Valóban, a definíció szerint, $\mathfrak{a}$ olyan rendszám, amely α-val ekvipotens. Ha β olyan rendszám, hogy $\beta < \mathfrak{a}$, akkor $\beta \in \alpha^+$ mert $\alpha \in H_\alpha$ miatt $\mathfrak{a} \leq \alpha$, így β nem lehet ekvipotens α-val, különben $\beta \in H_\alpha$ teljesülne, tehát $\beta <_{\alpha^+} \mathfrak{a}$ miatt ez ellentmond $\mathfrak{a}$ minimalitási tulajdonságának. Mivel $\mathfrak{a}$ ekvipotens α-val, így minden $\mathfrak{a}$-nál kisebb rendszám nem ekvipotens $\mathfrak{a}$-val, vagyis $\mathfrak{a}$ számosság.

(*Unicitás.*) Legyen $\mathfrak{b}$ olyan számosság, amely ekvipotens α rendszámmal, és jelölje $\mathfrak{a}$ az imént értelmezett H_α halmaz legkisebb elemét. Ekkor $\mathfrak{b} \leq \alpha$, különben $\alpha < \mathfrak{b}$ és α és $\mathfrak{b}$ ekvipotensek, ami ellentmond annak, hogy $\mathfrak{b}$ számosság. Ezért $\mathfrak{b} \in \alpha^+$, vagyis $\mathfrak{b} \in H_\alpha$, amiből $\mathfrak{a}$ minimalitási tulajdonsága miatt következik, hogy $\mathfrak{a} \leq_{\alpha^+} \mathfrak{b}$, vagyis $\mathfrak{a} \leq \mathfrak{b}$. Mivel $\mathfrak{a}$ és $\mathfrak{b}$ ekvipotensek egymással, hiszen mindketten α-val ekvipotensek, így a $\mathfrak{a} < \mathfrak{b}$ hipotézis ellentmond annak, hogy $\mathfrak{b}$ számosság, ezért $\mathfrak{a} = \mathfrak{b}$. Tehát $\mathfrak{a}$ az egyetlen olyan számosság, amely α-val ekvipotens. ■

10.5.4. Állítás. *Két számosság pontosan akkor ekvipotens, ha egyenlőek.*

Bizonyítás. Ha két számosság nem egyenlő, akkor közülük az egyik kisebb rendszám a másiknál, ezért a számosságok definíciója alapján nem lehetnek ekvipotensek. Tehát ekvipotens számosságok egyenlőek. ■

Ezzel szemben különböző rendszámok lehetnek ekvipotensek. Például ω és ω^+ mindketten megszámlálhatóan végtelen, tehát ekvipotens rendszámok, de különbözőek. Itt ω számosság, de ω^+ nem számosság.

10.5.5. Tétel. *A kiválasztási axiómát a helyettesítés axiómájával kicserélve belátható, hogy ha E olyan halmaz, amely felett létezik jólrendezés (ilyenkor azt mondjuk, hogy E jólrendezhető), akkor egyértelműen létezik olyan $\mathfrak{a}$ számosság, hogy E és $\mathfrak{a}$ ekvipotensek.*

Bizonyítás. A helyettesítés axiómáját alkalmazva, a **39**. gyakorlat szerint minden E feletti R jólrendezéshez létezik egyetlen olyan α rendszám, hogy az (E, R) és $(\alpha, \mathbf{E}_\alpha)$ rendezett halmazok izomorfak. Ekkor E és α ekvipotensek, ezért a b) alapján létezik olyan számosság, amely E-vel ekvipotens. A c) szerint ez a számosság egyértelműen van meghatározva. ■

10.5.6. Definíció. *Ha E jólrendezhető halmaz, akkor ebben a halmazelméletben az E halmaz számosságának nevezzük és a* $\mathrm{Card}(E)$ *szimbólummal jelöljük azt a számosságot, amely E-vel ekvipotens.*

10.5.7. Tétel. *A helyettesítés axiómájával bővített halmazelméletben minden halmaznak létezik számossága, és teljesül az, hogy bármely két E és F halmazra* $\mathrm{Card}(E) = \mathrm{Card}(F)$ *ekvivalens azzal, hogy az E és F halmazok ekvipotensek.*

Bizonyítás. A kiválasztási axióma alkalmazásával bizonyítottuk a Zermelo-féle jólrendezési tételt (2. **54**. gyakorlat), tehát azt, hogy minden halmaz jólrendezhető. Ezért elég a d)-re hivatkozni. ■

41. (*Számosságaritmetika.*) A következő definíciók és állítások a helyettesítés axiómájával bővített halmazelméletben értelmesek, illetve igazak.

a) Ha $\mathfrak{a}$ és $\mathfrak{b}$ számosságok, akkor a következő definíciókat adjuk:

$$\mathfrak{a} + \mathfrak{b} := \mathrm{Card}((\{0\} \times \mathfrak{a}) \cup (\{1\} \times \mathfrak{b})); \mathfrak{a} \cdot \mathfrak{b} := \mathrm{Card}(\mathfrak{a} \times \mathfrak{b});$$

$$\mathfrak{b}^{\mathfrak{a}} := \mathrm{Card}(\mathscr{F}(\mathfrak{a}; \mathfrak{b})).$$

Ha $\mathfrak{a}$ és $\mathfrak{b}$ véges számosságok (vagyis természetes számok), akkor $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}\cdot\mathfrak{b}$ és $\mathfrak{b}^{\mathfrak{a}}$ megegyeznek az $\mathbb{N}$ halmaz feletti korábban értelmezett összeadás, szorzás és hatványozás műveletek eredményeivel.

b) Legyen $(\mathfrak{a}_i)_{i\in I}$ számosságok tetszőleges rendszere. Ekkor definíció szerint:

$$\sum_{i\in I}\mathfrak{a}_i := \operatorname{Card}\Big(\bigcup_{i\in I}(\{i\}\times\mathfrak{a}_i)\Big),$$

és ezt a számosságot az $(\mathfrak{a}_i)_{i\in I}$ számosság-rendszer *összegének* nevezzük; továbbá:

$$\mathop{\mathrm{P}}_{i\in I}\mathfrak{a}_i := \operatorname{Card}\Big(\prod_{i\in I}\mathfrak{a}_i\Big),$$

és ezt a számosságot az $(\mathfrak{a}_i)_{i\in I}$ számosság-rendszer *szorzatának* nevezzük. Ha I véges halmaz és minden $i\in I$ indexre $\mathfrak{a}_i$ véges számosság, akkor $\sum_{i\in I}\mathfrak{a}_i$ és $\mathop{\mathrm{P}}_{i\in I}\mathfrak{a}_i$ megegyezik a **4**. gyakorlatban rekurzívan értelmezett véges összeggel és véges szorzattal.

c) Számosságok között a $\le$ kapcsolatot ugyanúgy értelmezzük, mint a rendszámok között, ami értelmes, hiszen a számosságok speciális rendszámok. Tehát ha $\mathfrak{a}$ és $\mathfrak{b}$ számosságok, akkor $\mathfrak{a}\le\mathfrak{b}$ azt jelenti, hogy $\mathfrak{a}\subseteq\mathfrak{b}$, és $\mathfrak{a}<\mathfrak{b}$ azt jelenti, hogy $\mathfrak{a}\in\mathfrak{b}$. Ha $(\mathfrak{a}_i)_{i\in I}$ számosságok tetszőleges rendszere, akkor definíció szerint:

$$\sup_{i\in I}\mathfrak{a}_i := \operatorname{Card}\Big(\bigcup_{i\in I}\mathfrak{a}_i\Big).$$

Ekkor az $\mathfrak{a} := \sup_{i\in I}\mathfrak{a}_i$ számosság olyan, hogy minden $i\in I$ esetén $\mathfrak{a}_i\le\mathfrak{a}$, továbbá minden $\mathfrak{b}$ számosságra, ha minden $i\in I$ esetén $\mathfrak{a}_i\le\mathfrak{b}$, akkor $\mathfrak{a}\le\mathfrak{b}$ teljesül.

d) Ha E és F olyan halmazok, hogy létezik $E\to F$ *szürjekció*, akkor $\operatorname{Card}(F)\le\operatorname{Card}(E)$.

e) Ha $(E_i)_{i\in I}$ halmazrendszer, akkor $\operatorname{Card}\Big(\bigcup_{i\in I}E_i\Big)\le\sum_{i\in I}\operatorname{Card}(E_i)$, és ha az $(E_i)_{i\in I}$ halmazrendszer diszjunkt, akkor $\operatorname{Card}\Big(\bigcup_{i\in I}E_i\Big)=\sum_{i\in I}\operatorname{Card}(E_i)$.

f) (*A számosságok összeadásának és szorzásának kommutativitása.*) Ha $(\mathfrak{a}_i)_{i\in I}$ számosságok tetszőleges rendszere, J halmaz és $\sigma : J\to I$ bijekció, akkor

$$\sum_{i\in I}\mathfrak{a}_i=\sum_{j\in J}\mathfrak{a}_{\sigma(j)},$$

$$\mathop{\mathrm{P}}_{i\in I}\mathfrak{a}_i=\mathop{\mathrm{P}}_{j\in J}\mathfrak{a}_{\sigma(j)}$$

teljesül. Ha $\mathfrak{a}$ és $\mathfrak{b}$ számosságok, akkor

$$\mathfrak{a}+\mathfrak{b}=\mathfrak{b}+\mathfrak{a},\quad \mathfrak{a}\cdot\mathfrak{b}=\mathfrak{b}\cdot\mathfrak{a}$$

teljesül.

g) (*A számosságok összeadásának és szorzásának asszociativitása.*) Ha $(\mathfrak{a}_i)_{i\in I}$ számosságok tetszőleges rendszere és $(I_j)_{j\in J}$ az I halmaz partíciója, akkor

$$\sum_{i\in I}\mathfrak{a}_i=\sum_{j\in J}\sum_{i\in I_j}\mathfrak{a}_i,$$

$$\mathop{\mathrm{P}}\limits_{i\in I} \mathfrak{a}_i = \mathop{\mathrm{P}}\limits_{j\in J} \mathop{\mathrm{P}}\limits_{i\in I_j} \mathfrak{a}_j$$

teljesül. Ha $\mathfrak{a}$, $\mathfrak{b}$ és $\mathfrak{c}$ számosságok, akkor

$$(\mathfrak{a}+\mathfrak{b})+\mathfrak{c} = \mathfrak{a}+(\mathfrak{b}+\mathfrak{c}),$$

$$(\mathfrak{a}\cdot\mathfrak{b})\cdot\mathfrak{c} = \mathfrak{a}\cdot(\mathfrak{b}\cdot\mathfrak{c})$$

teljesül.

10.5.8. Állítás. (**A számosságok szorzásának disztributivitása a számosságok összegzésére nézve.**) *Legyen* $(I_j)_{j\in J}$ *halmazrendszer és minden* $j \in J$ *esetén* $(\mathfrak{a}_{j,i})_{i\in I_j}$ *tetszőleges számosság-rendszer. Ha* $I := \prod\limits_{j\in J} I_j$*, akkor*

$$\mathop{\mathrm{P}}\limits_{j\in J} \sum_{i\in I_j} \mathfrak{a}_{j,i} = \sum_{f\in I} \mathop{\mathrm{P}}\limits_{j\in J} \mathfrak{a}_{j,f(j)}$$

teljesül. Ha $\mathfrak{a}$, $\mathfrak{b}$ *és* $\mathfrak{c}$ *számosságok, akkor*

$$\mathfrak{a}\cdot(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}\cdot\mathfrak{b})+(\mathfrak{a}\cdot\mathfrak{c})$$

teljesül.

Bizonyítás. Minden $j \in J$ és $i \in I_j$ esetén legyen $E_{j,i} := \{i\} \times \mathfrak{a}_{j,i}$, tehát rögzített $j \in J$ esetén az $(E_{j,i})_{i\in I_j}$ halmazrendszer *diszjunkt*, és $i \in I_j$ esetén $\mathrm{Card}(E_{j,i}) = \mathfrak{a}_{j,i}$, hiszen az $E_{j,i}$ és $\mathfrak{a}_{j,i}$ halmazok nyilvánvalóan ekvipotensek. A 6.9.8. állítás szerint fennáll a

$$\prod_{j\in J} \bigcup_{i\in I_j} E_{j,i} = \bigcup_{f\in I} \prod_{j\in J} E_{j,f(j)}$$

egyenlőség, ahol $I := \prod\limits_{j\in J} I_j$. Ebből a definíciók alapján következik, hogy

$$\mathop{\mathrm{P}}\limits_{j\in J} \sum_{i\in I_j} \mathfrak{a}_{j,i} = \mathop{\mathrm{P}}\limits_{j\in J} \mathrm{Card}\Big(\bigcup_{i\in I_j} E_{j,i}\Big) =$$

■

h) (*A számosságok szorzásának disztributivitása a számosságok összegzésére nézve.*) Legyen $(I_j)_{j\in J}$ halmazrendszer és minden $j \in J$ esetén $(\mathfrak{a}_{j,i})_{i\in I_j}$ tetszőleges számosság-rendszer. Ha $I := \prod\limits_{j\in J} I_j$, akkor

$$\mathop{\mathrm{P}}\limits_{j\in J} \sum_{i\in I_j} \mathfrak{a}_{j,i} = \sum_{f\in I} \mathop{\mathrm{P}}\limits_{j\in J} \mathfrak{a}_{j,f(j)}$$

teljesül. Ha $\mathfrak{a}$, $\mathfrak{b}$ és $\mathfrak{c}$ számosságok, akkor

$$\mathfrak{a}\cdot(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}\cdot\mathfrak{b})+(\mathfrak{a}\cdot\mathfrak{c})$$

teljesül.

i) Ha $(\mathfrak{a}_i)_{i\in I}$ számosságok tetszőleges rendszere, és J (illetve K) olyan részhalmaza I-nek, hogy minden $i \in I \setminus J$ (illetve $i \in I \setminus K$) esetén $\mathfrak{a}_i = 0$ (illetve $\mathfrak{a}_i = 1$), akkor

$$\sum_{i\in I} \mathfrak{a}_i = \sum_{i\in J} \mathfrak{a}_i, \quad \prod_{i\in I} \mathfrak{a}_i = \prod_{i\in K} \mathfrak{a}_i$$

teljesül. Minden $\mathfrak{a}$ számosságra $\mathfrak{a} + 0 = \mathfrak{a}$ és $\mathfrak{a} \cdot 1 = \mathfrak{a}$.

j) Legyenek $\mathfrak{a}$ és $\mathfrak{b}$ számosságok, I olyan halmaz, hogy $\mathrm{Card}(I) = \mathfrak{b}$ és minden $i \in I$ esetén legyen $\mathfrak{a}_i := \mathfrak{a}$ és $\mathfrak{c}_i := 1$. Ekkor

$$\mathfrak{a} \cdot \mathfrak{b} = \sum_{i\in I} \mathfrak{a}_i, \quad \mathfrak{b} = \sum_{i\in I} \mathfrak{c}_i, \quad \mathfrak{a}^{\mathfrak{b}} = \prod_{i\in I} \mathfrak{a}_i.$$

k) Ha $(\mathfrak{a}_i)_{i\in I}$ számosságok tetszőleges rendszere, akkor $\prod_{i\in I} \mathfrak{a}_i \neq 0$ pontosan akkor teljesül, ha minden $i \in I$ esetén $\mathfrak{a}_i \neq 0$.

l) Ha $\mathfrak{a}$ és $\mathfrak{b}$ számosságok, akkor az $\mathfrak{a}+1 = \mathfrak{b}+1$ és $\mathfrak{a} = \mathfrak{b}$ kijelentések ekvivalensek. Az $\mathfrak{a}$ számosság pontosan akkor véges, ha $\mathfrak{a} = \mathfrak{a} + 1$ teljesül. Az $\mathfrak{a}$ számosság pontosan akkor véges, ha $\mathfrak{a} + 1$ véges.

m) Ha $\mathfrak{a}$ és $\mathfrak{b}$ számosságok, valamint $(\mathfrak{a}_i)_{i\in I}$ és $(\mathfrak{b}_i)_{i\in I}$ számosság-rendszerek, akkor:

$$\mathfrak{a}^{\sum_{i\in I} \mathfrak{b}_i} = \prod_{i\in I} \mathfrak{a}^{\mathfrak{b}_i}, \quad \left(\prod_{i\in I} \mathfrak{a}_i\right)^{\mathfrak{b}} = \prod_{i\in I} \mathfrak{a}_i^{\mathfrak{b}}$$

teljesül. Ha $\mathfrak{a}$, $\mathfrak{b}$ és $\mathfrak{c}$ számosságok, akkor:

$$\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \left(\mathfrak{a}^{\mathfrak{b}}\right) \cdot \left(\mathfrak{a}^{\mathfrak{c}}\right), \quad \mathfrak{a}^{\mathfrak{b}\cdot\mathfrak{c}} = \left(\mathfrak{a}^{\mathfrak{b}}\right)^{\mathfrak{c}}.$$

n) Ha $\mathfrak{a}$ számosság, akkor $\mathfrak{a}^0 = 1$, $\mathfrak{a}^1 = \mathfrak{a}$, és $\mathfrak{a} \neq 0$ esetén $0^{\mathfrak{a}} = 0$. Ha E halmaz, akkor:

$$\mathrm{Card}(\mathscr{P}(E)) = 2^{\mathrm{Card}(E)}.$$

o) Ha $\mathfrak{a}$ és $\mathfrak{b}$ számosságok, és $\mathfrak{a} \leq \mathfrak{b}$, akkor *létezik* olyan $\mathfrak{c}$ számosság, hogy $\mathfrak{b} = \mathfrak{a} + \mathfrak{c}$, azonban $\mathfrak{c}$ nem szükségképpen egyértelmű, tehát az $\mathfrak{b} - \mathfrak{a}$ *számosság-különbség* általában nem értelmezhető.

p) Ha $(\mathfrak{a}_i)_{i\in I}$ és $(\mathfrak{b}_i)_{i\in I}$ olyan számosság-rendszerek, hogy minden $i \in I$ indexre teljesül az $\mathfrak{a}_i \leq \mathfrak{b}_i$ egyenlőtlenség, akkor fennállnak a

$$\sum_{i\in I} \mathfrak{a}_i \leq \sum_{i\in I} \mathfrak{b}_i, \quad \prod_{i\in I} \mathfrak{a}_i \leq \prod_{i\in I} \mathfrak{b}_i$$

egyenlőtlenségek.

q) Ha $(\mathfrak{a}_i)_{i\in I}$ számosságok tetszőleges rendszere, akkor minden $J \subseteq I$ halmazra

$$\sum_{i\in J} \mathfrak{a}_i \leq \sum_{i\in I} \mathfrak{a}_i,$$

és ha minden $i \in I \setminus J$ esetén $\mathfrak{a}_i \neq 0$, akkor

$$\prod_{i\in J} \mathfrak{a}_i \leq \prod_{i\in I} \mathfrak{a}_i.$$

r) Ha $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{b}_1$ és $\mathfrak{b}_2$ számosságok, továbbá $\mathfrak{a}_1 \leq \mathfrak{a}_2$ és $\mathfrak{b}_1 \leq \mathfrak{b}_2$, akkor $\mathfrak{a}_1^{\mathfrak{b}_1} \leq \mathfrak{a}_2^{\mathfrak{b}_2}$.

s) Minden $\mathfrak{a}$ számosságra $\mathfrak{a} < 2^{\mathfrak{a}}$ teljesül.

t) Az "$\mathfrak{a}$ számosság" kijelentés *nem kollektivizáló* az $\mathfrak{a}$ változóban.

(*Útmutatás.* e) Legyen $(E_i)_{i\in I}$ halmazrendszer, és tekintsük az $(\{i\} \times E_i)_{i\in I}$ diszjunkt halmazrendszert. Legyen $E := \bigcup_{i\in I} E_i$ és $E' := \bigcup_{i\in I}(\{i\} \times E_i)$. Ekkor $E' \subseteq I \times E$, és a $\mathrm{pr}_E : I \times E \to E$ projekció E'-re vett leszűkítése szürjektív, és ha az $(E_i)_{i\in I}$ halmazrendszer diszjunkt, akkor ez a leszűkítés bijekció E' és E között.

f)-g)-h) Ha $(E_i)_{i\in I}$ diszjunkt halmazrendszer és F halmaz, akkor az

$$\mathscr{F}\Big(\bigcup_{i\in I} E_i; F\Big) \to \prod_{i\in I} \mathscr{F}(E_i; F), \qquad f \mapsto (f|_{E_i})_{i\in I}$$

leképezés bijekció. Ha E halmaz és $(F_i)_{i\in I}$ halmazrendszer, akkor az

$$\mathscr{F}\Big(E; \prod_{i\in I} F_i\Big) \to \prod_{i\in I} \mathscr{F}(E; F_i), \qquad f \mapsto (\mathrm{pr}_i \circ f)_{i\in I}$$

leképezés bijekció.

t) Ha az "$\mathfrak{a}$ számosság" kijelentés kollektivizáló volna, akkor az

$$E := \{\mathfrak{a} | \text{"}\mathfrak{a} \text{ számosság"}\}$$

halmaz olyan lenne, hogy a $\mathfrak{b} := \sup_{\mathfrak{a}\in E} \mathfrak{a}$ számosság minden számosságnál nagyobb-egyenlő volna, holott a Cantor-tétel alapján $2^{\mathfrak{b}}$ a $\mathfrak{b}$-nél nagyobb számosság.)

42. Legyenek $(\mathfrak{a}_i)_{i\in I}$ és $(\mathfrak{b}_i)_{i\in I}$ számosság-rendszerek, és tegyük fel, hogy minden $i \in I$ esetén $\mathfrak{b}_i \geq 2$.

a) Ha minden $i \in I$ indexre $\mathfrak{a}_i \leq \mathfrak{b}_i$, akkor:

$$\sum_{i\in I} \mathfrak{a}_i \leq \mathop{\mathrm{P}}_{i\in I} \mathfrak{b}_i.$$

b) (*König-tétel.*) Ha minden $i \in I$ indexre teljesül a $\mathfrak{a}_i < \mathfrak{b}_i$ szigorú egyenlőtlenség, akkor:

$$\sum_{i\in I} \mathfrak{a}_i < \mathop{\mathrm{P}}_{i\in I} \mathfrak{b}_i.$$

(*Útmutatás.* a) Ha $I = \emptyset$, akkor $\sum_{i\in I} \mathfrak{a}_i = 0$ és $\mathop{\mathrm{P}}_{i\in I} \mathfrak{b}_i = 1$. Ha I egy elemű, akkor $\sum_{i\in I} \mathfrak{a}_i = \mathop{\mathrm{P}}_{i\in I} \mathfrak{b}_i$. Ha I két elemű, akkor az állítás a 2. **40**. gyakorlatból következik. Ezért elég azt megmutatni, hogy ha $(E_i)_{i\in I}$ olyan diszjunkt halmazrendszer, hogy I legalább három elemű és minden $i \in I$ esetén E_i legalább két elemű, akkor létezik $\bigcup_{i\in I} E_i \to \prod_{i\in I} E_i$ injekció.

Ennek bizonyításához először kétszer alkalmazva a kiválasztási axiómát rögzítünk olyan

$e, e' \in \prod_{i \in I} E_i$ elemeket, amelyekre minden $i \in I$ esetén $e(i) \neq e'(i)$ teljesül. Jelölje ι azt az $\bigcup_{i \in I} E_i \to I$ leképezést, amelyre minden $x \in \bigcup_{i \in I} E_i$ esetén $x \in E_{\iota(x)}$ teljesül (ez a függvény az $(E_i)_{i \in I}$ halmazrendszer diszjunktsága miatt értelmezhető). Ezután minden $x \in \bigcup_{i \in I} E_i$ elemre legyen $f(x) \in \prod_{i \in I} E_i$ az a rendszer, amelyre $\mathrm{pr}_{\iota(x)}(f(x)) := x$ és ha $j \in I \setminus \{\iota(x)\}$, akkor

– ha $x \neq e(\iota(x))$, akkor $\mathrm{pr}_j(f(x)) := e(j)$,

– ha $x = e(\iota(x))$, akkor $\mathrm{pr}_j(f(x)) := e'(j)$.

Ez az $f : \bigcup_{i \in I} E_i \to \prod_{i \in I} E_i$ függvény injekció. Legyenek ugyanis $x, x' \in \bigcup_{i \in I} E_i$ és $x \neq x'$. Ha $\iota(x) = \iota(x')$, akkor $\mathrm{pr}_{\iota(x)}(f(x)) := x \neq x' =: \mathrm{pr}_{\iota(x')}(f(x'))$, következésképpen $f(x) \neq f(x')$. Ha viszont $\iota(x) \neq \iota(x')$, akkor a következő esetek lehetségesek:

- $x \neq e(\iota(x))$ és $x' \neq e(\iota(x'))$; ekkor $\mathrm{pr}_{\iota(x)}(f(x)) = x \neq e(\iota(x)) = \mathrm{pr}_{\iota(x)}(f(x'))$,

– $x \neq e(\iota(x))$ és $x' = e(\iota(x'))$; ekkor van olyan $k \in I$, hogy $\iota(x) \neq k \neq \iota(x')$, és akkor $\mathrm{pr}_k(f(x)) = e(k) \neq e'(k) = \mathrm{pr}_k(f(x'))$,

– $x = e(\iota(x))$ és $x' \neq e(\iota(x'))$; ekkor van olyan $k \in I$, hogy $\iota(x) \neq k \neq \iota(x')$, és akkor $\mathrm{pr}_k(f(x)) = e'(k) \neq e(k) = \mathrm{pr}_k(f(x'))$,

– $x = e(\iota(x))$ és $x' = e(\iota(x'))$; ekkor $\mathrm{pr}_{\iota(x)}(f(x)) = x = e(\iota(x)) \neq e'(\iota(x)) = \mathrm{pr}_{\iota(x)}(f(x'))$,

tehát minden esetben $f(x) \neq f(x')$.

b) Elég azt megmutatni, hogy ha $(E_i)_{i \in I}$ diszjunkt halmazrendszer, és $(F_i)_{i \in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén E_i kisebb számosságú F_i-nél, akkor *nem létezik* $\bigcup_{i \in I} E_i \to \prod_{i \in I} F_i$ szürjekció. Indirekt bizonyíthatunk, tehát feltesszük, hogy $f : \bigcup_{i \in I} E_i \to \prod_{i \in I} F_i$ szürjekció. Minden $i \in I$ indexre az $E_i \to F_i$, $x \mapsto \mathrm{pr}_i(f(x))$ leképezés nem szürjekció, így $F_i \setminus \{\mathrm{pr}_i(f(x)) | x \in E_i\} \neq \emptyset$. Ezért a kiválasztási axióma alkalmazásával vehetünk egy $e \in \prod_{i \in I} (F_i \setminus \{\mathrm{pr}_i(f(x)) | x \in E_i\})$ elemet. Ekkor $e \in \prod_{i \in I} F_i$, tehát az f szürjektivitása folytán van olyan $x \in \bigcup_{i \in I} E_i$ elem, amelyre $f(x) = e$ teljesül. Legyen $i \in I$ az az index, amelyre $x \in E_i$; ekkor $\mathrm{pr}_i(f(x)) = e(i) \notin \{\mathrm{pr}_i(f(x)) | x \in E_i\}$, ugyanakkor világos, hogy $\mathrm{pr}_i(f(x)) \in \{\mathrm{pr}_i(f(x')) | x' \in E_i\}$, ami ellentmondás.)

43. Legyen E halmaz és $f : \mathscr{P}(E) \setminus \{\emptyset\} \to E$ olyan függvény, hogy minden $X \subseteq E$ nem üres halmazra $f(X) \in X$.

a) Legyen $\mathfrak{b}$ olyan számosság, hogy $\mathfrak{b} \leq \mathrm{Card}(E)$, és legyen

$$A := \{x \in E | \mathrm{Card}(\overset{-1}{f} \langle \{x\} \rangle) \leq \mathfrak{b}\}.$$

Ekkor az $\mathfrak{a} := \mathrm{Card}(A)$ számosságra $2^{\mathfrak{a}} \leq \mathfrak{a} \cdot \mathfrak{b} + 1$ teljesül.

b) Értelmezzük a következő halmazt:

$$B := \{x \in E | (\forall X \in \overset{-1}{f} \langle \{x\} \rangle)(\mathrm{Card}(X) \leq \mathfrak{b})\}.$$

Ekkor $\mathrm{Card}(B) \leq \mathfrak{b}$ teljesül.

44. a) Ha $\mathfrak{a}$ végtelen számosság, akkor minden $n \in \mathbb{N}^*$ természetes számra $\mathfrak{a}^n = \mathfrak{a}$ teljesül.

b) Ha $(\mathfrak{a}_i)_{i\in I}$ nem nulla számosságoknak olyan rendszere, hogy I véges és az $\mathfrak{a} := \max\limits_{i\in I} \mathfrak{a}_i$ számosság végtelen, akkor $\sum\limits_{i\in I} \mathfrak{a}_i = \mathfrak{a}$.

c) Legyen $\mathfrak{a}$ végtelen számosság, és $(\mathfrak{a}_i)_{i\in I}$ számosságoknak olyan rendszere, hogy $\mathrm{Card}(I) \leq \mathfrak{a}$ és minden $i \in I$ indexre $\mathfrak{a}_i \leq \mathfrak{a}$. Ekkor $\sum\limits_{i\in I} \mathfrak{a}_i \leq \mathfrak{a}$, és ha létezik olyan $i \in I$, amelyre $\mathfrak{a}_i = \mathfrak{a}$, akkor $\sum\limits_{i\in I} \mathfrak{a}_i = \mathfrak{a}$.

d) Ha $\mathfrak{a}$ és $\mathfrak{b}$ olyan nem nulla számosságok, amelyek közül az egyik végtelen, akkor

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b} = \max(\mathfrak{a}, \mathfrak{b}).$$

10.6. Gyakorlatok

45. *Korlátozottsági axiómának* nevezzük a következő kijelentést:

$$(\forall x)(\ (x \neq \emptyset) \Rightarrow (\exists y)((y \in x) \wedge (x \cap y = \emptyset))\ ).$$

Tehát a korlátozottsági axióma azt jelenti, hogy minden nem üres halmaznak van olyan eleme, amelynek nincs közös eleme az adott halmazzal.

Fundáltsági axiómának nevezzük a következő kijelentést:

$$\neg(\exists f)(\ Fnc(f) \wedge (\mathrm{Dom}(f) = \mathbb{N}) \wedge (\forall n)(\ (n \in \mathrm{Dom}(f)) \Rightarrow (f(n^+) \in f(n))\ )\ ),$$

ahol $Fnc(f)$ annak a kijelentésnek a rövidítése, hogy "f függvény". Tehát a fundáltsági axióma azt jelenti, hogy nem létezik olyan halmazsorozat, amelynek mindegyik tagjának eleme a rákövetkező tagja; vagyis nem létezik (megszámlálhatóan) végtelen "leszálló" elem-lánc.

a) A korlátozottsági axiómából (a kiválasztási axióma alkalmazása nélkül) következik a fundáltsági axióma.

b) A kiválasztási axiómából következik, hogy a fundáltsági axióma és a korlátozottsági axióma *ekvivalensek*.

c) A korlátozottsági axiómából következik, hogy semmilyen *véges* "leszálló" elem-lánc nem létezik, vagyis

$$\neg(\exists f)(\ Fnc(f) \wedge (\mathrm{Dom}(f) \in \mathbb{N}) \wedge (\forall n)(\ (n^+ \in \mathrm{Dom}(f)) \Rightarrow (f(n^+) \in f(n))\ )$$

$$\wedge (f((\mathrm{Dom}(f))^-) \in f(0))\ )$$

teljesül. Speciálisan, a korlátozottsági axiómából kapjuk, hogy $(\forall x)(x \notin x)$ teljesül.

46. Mutassuk meg, hogy az indexsorozatok (tehát az $\mathbb{N} \to \mathbb{N}$ szigorúan monoton növő függvények) halmaza kontinuumszámosságú. Bármely *injektív* sorozat részsorozatainak halmaza kontinuumszámosságú.

(*Útmutatás.* Ha $X \subseteq \mathbb{N}$ végtelen halmaz, akkor létezik olyan σ indexsorozat, amelyre $\mathrm{Im}(\sigma) = X$. Ehhez elegendő venni a $\min(X)$ kezdőpont és az

$$f : \mathbb{N} \to \mathbb{N}; \quad n \mapsto \min\{k \in X | k > n\}$$

függvény által meghatározott iterációs sorozatot. Tehát az indexsorozatok halmaza ráképezhető az $\mathbb{N}$ végtelen részhalmazainak halmazára, ami a **30**. gyakorlat szerint ekvipotens $\mathscr{P}(\mathbb{N})$-nel. Tehát az indexsorozatok halmaza legalább kontinuumszámosságú. Másfelől, az indexsorozatok halmaza része az $\mathbb{N} \to \mathbb{N}$ injekciók halmazának, amely a **32**. b) gyakorlat szerint ekvipotens az $\mathbb{N}$ végtelen részhalmazainak halmazával. A bizonyítás befejezéséhez elegendő a Schröder -Bernstein tételt (6.5.5.) alkalmazni.

Ha $\mathbf{s}$ injektív sorozat, akkor az indexsorozatok halmazán értelmezett és az $\mathbf{s}$ részsorozatainak halmazába vezető $\sigma \mapsto \mathbf{s} \circ \sigma$ leképezés nyilvánvalóan bijekció.)

47. Mutassuk meg, hogy ha $(\sigma_i)_{i \in I}$ indexsorozatok olyan nem üres rendszere, hogy a $\bigcap_{i \in I} \mathrm{Im}\,(\sigma_i)$ halmaz végtelen, akkor létezik indexsorozatoknak olyan $(\sigma'_i)_{i \in I}$ rendszere, hogy minden $i, j \in I$ esetén $\sigma_i \circ \sigma'_i = \sigma_j \circ \sigma'_j$ teljesül.

(*Útmutatás.* Ha $n \in \mathbb{N}$, akkor a $\bigcap_{i \in I} \mathrm{Im}\,(\sigma_i)$ halmaz nem részhalmaza n-nek, tehát van olyan $k \in \bigcap_{i \in I} \mathrm{Im}\,(\sigma_i)$, amelyre $n < k$. Ezért jól értelmezett az

$$f : \mathbb{N} \to \mathbb{N}; \quad n \mapsto \min \left\{ k \in \bigcap_{i \in I} \mathrm{Im}\,(\sigma_i) \;\middle|\; n < k \right\}$$

függvény. Jelölje σ a $\min \left\{ k \in \bigcap_{i \in I} \mathrm{Im}\,(\sigma_i) \middle| 0 < k \right\}$ kezdőpont és f függvény által meghatározott iterációs sorozatot. Ekkor minden $n \in \mathbb{N}$ esetén $\sigma(n+1) = f(\sigma(n)) \in \left\{ k \in \bigcap_{i \in I} \mathrm{Im}\,(\sigma_i) \middle| \sigma(n) < k \right\}$, tehát $\sigma(n) < \sigma(n+1)$, vagyis σ indexsorozat. Ugyanakkor, minden $n \in \mathbb{N}$ esetén $\sigma(n) \in \bigcap_{i \in I} \mathrm{Im}\,(\sigma_i)$, vagyis minden $I \ni i$-re $\mathrm{Im}(\sigma) \subseteq \mathrm{Im}(\sigma_i)$. Minden $I \ni i$-re legyen

$$\sigma'_i := \sigma_i^{-1} \circ \sigma.$$

Ekkor minden $i \in I$ esetén $\sigma'_i : \mathbb{N} \to \mathbb{N}$ szigorúan monoton növő függvény, és a definíció szerint, $\sigma_i \circ \sigma'_i = \sigma$.)

1. Mutassuk meg, hogy minden X nem üres halmaz felett létezik olyan R jólrendezés, hogy létezik X-nek legnagyobb eleme R szerint.

(*Útmutatás* Ha X véges, akkor minden X feletti jólrendezés ilyen. Tegyük fel, hogy X végtelen, és legyen S tetszőleges jólrendezés X felett. Ha $\mathfrak{a}$ olyan halmaz, hogy $\mathfrak{a} \notin X$, akkor az $X' := X \cup \{\mathfrak{a}\}$ halmaz felett az $S' := S \cup (X \times \{\mathfrak{a}\}) \cup \{(\mathfrak{a}, \mathfrak{a})\}$ reláció olyan jólrendezés, amely szerint $\mathfrak{a}$ az X' legnagyobb eleme (6.13.3.). Az X végtelensége miatt X és X' ekvipotensek (10.1.3.); legyen $f : X \to X'$ tetszőleges bijekció. Ekkor az

$$R := \{(x, y) \in X \times X \mid (f(x), f(y)) \in S'\}$$

reláció olyan jólrendezés X felett, amely szerint $f^{-1}(\mathfrak{a})$ az X legnagyobb eleme.)

III. rész

A matematikai analízis algebrai alapjai

BEVEZETÉS

Irodalomjegyzék

[1] N. Bourbaki, **Éleménts de mathématique. Algébre**, Hermann, Paris

[2] G. Birkhoff, **Lattice Theory**, Providence, Rhode Island, 1967

[3] L. Rédei, **Algebra**, Akadémiai Kiadó, Budapest, 1967.

[4] S. Lang, **Algebra**, Addison-Wesley Publishing Company, Reading, Mass., 1965.

[5] C. Faith, **Algebra: Rings, Modules and Categories I**, Springer-Verlag, Berlin-Heidelberd-New York, 1973.

[6] C. Faith, **Algebra II, Ring Theory**, Springer-Verlag, Berlin-Heidelberd-New York, 1973.

[7] Paul. R. Halmos, **Finite-dimensional vector spaces**, Springer-Verlag, 1974.

11. fejezet

Műveletek és algebrai objektumok

11.1. Műveletek elemi tulajdonságai

11.1.1. Definíció. *Az E halmaz feletti* (*belső, kétváltozós*) **műveletnek** *nevezünk minden $E \times E \to E$ típusú függvényt.*

A műveletek adott helyen felvett értékének jelölésére háromféle konvenciót alkalmaznak. Ha E halmaz és $\top : E \times E \to E$ művelet, akkor $(x, y) \in E \times E$ esetén a $\top((x, y)) \in E$ értéket a következőképpen jelölhetjük:

– *prefix* jelöléssel $\top\, x\, y$,

– *infix* jelöléssel $x \top y$,

– *postfix* jelöléssel $x\, y\, \top$.

Mi az infix jelölési konvenciót alkalmazzuk.

11.1.2. Definíció. *Legyen E halmaz és $\top : E \times E \to E$ művelet.*

– *A $\top$ műveletet* **asszociatívnak** *nevezzük, ha minden $x, y, z \in E$ elemre*

$$x \top (y \top z) = (x \top y) \top z.$$

– *A $\top$ műveletet* **kommutatívnak** *nevezzük, ha minden $x, y \in E$ elemre*

$$x \top y = y \top x.$$

– *A $\top$ műveletetet* **neutrális-elemesnek** *nevezzük, ha létezik olyan $e \in E$, hogy minden $x \in E$ elemre*

$$x \top e = e \top x = x.$$

Minden ilyen tulajdonságú $e \in E$ elemet a $\top$ művelet **neutrális elemének** *nevezünk.* (*Megjegyezzük, hogy legfeljebb egy neutrális elem létezhet, mert ha $e, e' \in E$ neutrális elemek, akkor $e = e \top e' = e'$.*)

– *Ha $\top$ neutrális-elemes és $e \in E$ a $\top$ neutrális eleme, akkor az $x \in E$ elem* **inverzének** *nevezünk minden olyan $x' \in E$ elemet, amelyre*

$$x \top x' = x' \top x = e.$$

(*Megjegyezzük, hogy ha $\top$ asszociatív és neutrális-elemes művelet, akkor minden $x \in E$ elemnek legfeljebb egy inverze létezik, mert ha $x', x'' \in E$ inverzei x-nek, akkor $x' = e \top x' = (x'' \top x) \top x' = x'' \top (x \top x') = x'' \top e = x''$.*)

– *A neutrális-elemes $\top$ műveletet* **inverzelemesnek** *nevezzük, ha E minden elemének létezik inverze.*

11.1.3. Definíció. *Ha $\top$ művelet az E halmaz felett, akkor azt mondjuk, hogy az $X \subseteq E$* **halmaz asszociatív** (*illetve* **kommutatív**) *a $\top$ művelet szerint, ha minden $x, y, z \in X$ esetén $(x \top y) \top z = x \top (y \top z)$ (illetve minden $x, y \in X$ esetén $x \top y = y \top x$).*

11.1.4. Definíció. *Legyenek $\top$ és $\perp$ műveletek az E halmaz felett.*

a) *Azt mondjuk, hogy a $\top$ művelet* **disztributív** *a $\perp$ műveletre nézve, ha minden $x, y, z \in E$ elemre*

$$\begin{aligned} x \top (y \perp z) &= (x \top y) \perp (x \top z) \\ (y \perp z) \top x &= (y \top x) \perp (z \top x). \end{aligned}$$

b) *Azt mondjuk, hogy a $\top$ művelet* **elnyelő** *a $\perp$ műveletre nézve, ha minden $x, y \in E$ elemre*

$$\begin{aligned} x \top (y \perp z) &= (x \top y) \perp (x \top z) \\ (y \perp z) \top x &= (y \top x) \perp (z \top x). \end{aligned}$$

11.2. Morfizmusok és izomorfizmusok

11.2.1. Definíció. *Legyenek $(S, \top)$ és $(T, \perp)$ magmák (8.3.1.). Azt mondjuk, hogy az $f : S \to T$ függvény* **morfizmus** *az $(S, \top)$ és $(T, \perp)$ magmák között, ha minden $s, s' \in S$ esetén $f(s \top s') = f(s) \perp f(s')$. Azt mondjuk, hogy az $f : S \to T$ függvény* **izomorfizmus** *az $(S, \top)$ és $(T, \perp)$ magmák között, ha f morfizmus az $(S, \top)$ és $(T, \perp)$ magmák között, és f bijekció, és az $f^{-1} : T \to S$ függvény morfizmus a $(T, \perp)$ és $(S, \top)$ magmák között. Azt mondjuk, hogy az $(S, \top)$ és $(T, \perp)$ magmák* **izomorfak**, *ha létezik izomorfizmus az $(S, \top)$ és $(T, \perp)$ magmák között.*

11.2.2. Állítás. *Legyenek $(S, \top)$ és $(T, \perp)$ magmák és $f : S \to T$ bijekció. Az f függvény pontosan akkor izomorfizmus az $(S, \top)$ és $(T, \perp)$ magmák között, ha morfizmus az $(S, \top)$ és $(T, \perp)$ magmák között, vagyis minden $s, s' \in S$ esetén $f(s \top s') = f(s) \perp f(s')$.*

Bizonyítás. Csak az elégségesség szorul bizonyításra. Ha f bijektív morfizmus az $(S, \top)$ és $(T, \perp)$ magmák között, és $t, t' \in T$, akkor az $f^{-1}(t), f^{-1}(t') \in S$ elemekre

$$f\left(f^{-1}(t) \top f^{-1}(t')\right) = f\left(f^{-1}(t)\right) \perp f\left(f^{-1}(t')\right) = t \perp t',$$

következésképpen

$$f^{-1}(t) \top f^{-1}(t') = f^{-1}\left(f\left(f^{-1}(t) \top f^{-1}(t')\right)\right) = f^{-1}(t \perp t'),$$

tehát az $f^{-1} : T \to S$ függvény morfizmus a $(T, \perp)$ és $(S, \top)$ magmák között, így f izomorfizmus az $(S, \top)$ és $(T, \perp)$ magmák között. ■

11.2.3. Állítás. *Legyenek $(S, \top)$ és $(T, \perp)$ magmák, és $f : S \to T$ morfizmus $(S, \top)$ és $(T, \perp)$ között. Ha az $X \subseteq S$ halmaz asszociatív (illetve kommutatív) a $\top$ művelet szerint, akkor az $f\langle X \rangle \subseteq T$ halmaz asszociatív (illetve kommutatív) a $\perp$ művelet szerint.*

Bizonyítás. Legyenek $s, s', s'' \in S$ olyanok, hogy $s \top (s' \top s'') = (s \top s') \top s''$. Ekkor

$$\begin{aligned} &f(s) \perp (f(s') \perp f(s'')) = f(s) \perp f(s' \top s'') = f(s \top (s' \top s'')) = \\ &= f((s \top s') \top s'') = f(s \top s') \perp f(s'') = (f(s) \top f(s')) \top f(s''), \end{aligned}$$

tehát ha az $X \subseteq S$ halmaz asszociatív a $\top$ művelet szerint, akkor az $f\langle X\rangle \subseteq T$ halmaz asszociatív a $\perp$ művelet szerint.

Legyenek $s, s' \in S$ olyanok, hogy $s\top s' = s'\top s$. Ekkor

$$f(s)\perp f(s') = f(s\top s') = f(s'\top s) = f(s')\perp f(s),$$

tehát ha az $X \subseteq S$ halmaz kommutatív a $\top$ művelet szerint, akkor az $f\langle X\rangle \subseteq T$ halmaz kommutatív a $\perp$ művelet szerint. ■

11.2.4. Következmény. *Legyenek $(S,\top)$ és $(T,\perp)$ magmák, és $f : S \to T$ morfizmus $(S,\top)$ és $(T,\perp)$ között. Ha f szürjekció és az $(S,\top)$ magma asszociatív (illetve kommutatív), akkor a $(T,\perp)$ magma is asszociatív (illetve kommutatív).*

Bizonyítás. A hipotézisek és az előző állítás alapján a $T = f\langle S\rangle$ halmaz asszociatív (illetve kommutatív) a $\perp$ művelet szerint. ■

11.2.5. Állítás. *Legyenek $(S,\top)$ és $(T,\perp)$ asszociatív magmák, és $f : S \to T$ morfizmus $(S,\top)$ és $(T,\perp)$ között. Ha $(s_i)_{i\in I}$ olyan nem üres véges rendszer S-ben, hogy minden $i, j \in I$ esetén $s_i\top s_j = s_j\top s_i$, akkor minden $i, j \in I$ indexre $f(s_i)\perp f(s_j) = f(s_j)\perp f(s_i)$ és*

$$f\Big(\mathop{\top}_{i\in I} s_i\Big) = \mathop{\perp}_{i\in I} f(s_i).$$

Ha az $(S,\top)$ és $(T,\perp)$ magmák neutrális-elemesek is, és f neutráliselem-tartó, akkor az előzőek $I = \emptyset$ esetén is teljesülnek.

Bizonyítás. Ha $(s_i)_{i\in I}$ tetszőleges S-ben haladó rendszer (tehát $I = \emptyset$ vagy végtelen I indexhalmaz is meg van engedve), akkor abból, hogy $i, j \in I$ és $s_i\top s_j = s_j\top s_i$ következik, hogy

$$f(s_i)\perp f(s_j) = f(s_i\top s_j) = f(s_j\top s_i) = f(s_j)\perp f(s_i),$$

hiszen f morfizmus az $(S,\top)$ és $(T,\perp)$ magmák között. Ezért, ha I véges és nem üres, akkor a $\mathop{\top}_{i\in I} s_i \in S$ és $\mathop{\perp}_{i\in I} f(s_i) \in T$ elemek képezhetőek, így a felírt egyenlőség *értelmes*. Az egyenlőségre vonatkozó állítást a rendszer indexhalmazának számossága szerinti teljes indukcióval igazoljuk.

Ha $(s_i)_{i\in I}$ olyan S-ben haladó rendszer, amelyre $\mathrm{Card}(I) = 1$, akkor i_*-gal jelölve I egyetlen elemét, 8.5.4. a) alkalmazásával kapjuk, hogy

$$f\Big(\mathop{\top}_{i\in I} s_i\Big) = f\Big(\mathop{\top}_{i\in \{i_*\}} s_i\Big) = f(s_{i_*}) = \mathop{\perp}_{i\in\{i_*\}} f(s_i) = \mathop{\perp}_{i\in I} f(s_i),$$

tehát az egyenlőség teljesül.

Legyen $n \in \mathbb{N}^*$ olyan természetes szám, hogy az egyenlőség igaz minden olyan I indexhalmaz esetében, amelyre $\mathrm{Card}(I) = n$. Legyen I olyan véges halmaz, hogy $\mathrm{Card}(I) = n+1$, és legyen $(s_i)_{i\in I}$ olyan rendszer S-ben, hogy minden $i, j \in I$ esetén $s_i\top s_j = s_j\top s_i$, vagyis $\{s_i | i \in I\}$ a $\top$ művelet szerint kommutatív halmaz. Legyen $i_* \in I$ rögzített elem és $I_* := I \setminus \{i_*\}$. Ekkor

$$f\Big(\mathop{\top}_{i\in I} s_i\Big) \overset{(1)}{=} f\Big(\Big(\mathop{\top}_{i\in I_*} s_i\Big)\top s_{i_*}\Big) \overset{(2)}{=} f\Big(\mathop{\top}_{i\in I_*} s_i\Big)\perp f(s_{i_*}) \overset{(3)}{=} \Big(\mathop{\perp}_{i\in I_*} f(s_i)\Big)\perp f(s_{i_*}) \overset{(4)}{=} \mathop{\perp}_{i\in I} f(s_i),$$

ahol

– az $\stackrel{(1)}{=}$ és $\stackrel{(4)}{=}$ egyenlőségnél a 8.5.4. b) állítást alkalmaztuk;

– a $\stackrel{(2)}{=}$ egyenlőségnél felhasználtuk, hogy f morfizmus az $(S, \top)$ és $(T, \perp)$ magmák között;

– a $\stackrel{(3)}{=}$ egyenlőségnél alkalmaztuk az indukciós hipotézist az $(s_i)_{i \in I_{i_*}}$ rendszerre.

Ezzel a teljes indukciót végrehajtottuk. ■

11.3. Komplexusműveletek

11.3.1. Definíció. *Ha $\top$ művelet az E halmaz felett, akkor minden $X, Y \subseteq E$ halmazra*

$$X \top Y := \{\ x \top y \mid (x \in X) \wedge (y \in Y)\ \},$$

továbbá, a

$$\mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E); \quad (X, Y) \mapsto X \top Y$$

$\mathscr{P}(E)$ feletti műveletet a $\top$ művelet által meghatározott **komplexusműveletnek** *nevezzük.*

11.3.2. Állítás. *Ha $\top$ asszociatív (illetve kommutatív) művelet az E halmaz felett, akkor a*

$$\mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E); \quad (X, Y) \mapsto X \top Y$$

komplexusművelet is asszociatív (illetve kommutatív) művelet $\mathscr{P}(E)$ felett.

Bizonyítás. Tegyük fel, hogy a $\top$ művelet asszociatív, és legyenek $X, Y, Z \in \mathscr{P}(E)$. Ha $u \in X \top (Y \top Z)$, akkor léteznek olyan $x \in X$, $y \in Y$ és $z \in Z$ elemek, hogy $u = x \top (y \top z)$, tehát $\top$ asszociativitása miatt $u = (x \top y) \top z \in (X \top Y) \top Z$. Ez azt jelenti, hogy $X \top (Y \top Z) \subseteq (X \top Y) \top Z$. Ha $u \in (X \top Y) \top Z$, akkor léteznek olyan $x \in X$, $y \in Y$ és $z \in Z$ elemek, hogy $u = (x \top y) \top z$, tehát $\top$ asszociativitása miatt $u = x \top (y \top z) \in X \top (Y \top Z)$. Ez azt jelenti, hogy $(X \top Y) \top Z \subseteq X \top (Y \top Z)$. Ezért $X \top (Y \top Z) = (X \top Y) \top Z$, vagyis a

$$\mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E); \quad (X, Y) \mapsto X \top Y$$

komplexusművelet asszociatív.

Tegyük fel, hogy a $\top$ művelet kommutatív, és legyenek $X, Y \in \mathscr{P}(E)$. Ha $u \in X \top Y$, akkor léteznek olyan $x \in X$ és $y \in Y$ elemek, hogy $u = x \top y$, tehát $\top$ kommutativitása miatt $u = y \top x \in Y \top X$. Ez azt jelenti, hogy $X \top Y \subseteq Y \top X$. Ha $u \in Y \top X$, akkor léteznek olyan $y \in Y$ és $x \in X$ elemek, hogy $u = y \top x$, tehát $\top$ kommutativitása miatt $u = x \top y \in X \top Y$. Ez azt jelenti, hogy $Y \top X \subseteq X \top Y$. Ezért $X \top Y = Y \top X$, vagyis a

$$\mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E); \quad (X, Y) \mapsto X \top Y$$

komplexusművelet kommutatív. ■

Z Vigyázzunk arra, hogy ha $\top$ és $\perp$ olyan műveletek az E halmaz felett, hogy $\top$ disztributív (illetve elnyelő) a $\perp$ műveletre nézve, akkor a

$$\mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E); \quad (X, Y) \mapsto X \top Y$$

komplexusművelet *nem feltétlenül* disztributív (illetve elnyelő) a

$$\mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E); \quad (X, Y) \mapsto X \perp Y$$

komplexusműveletre nézve.

11.4. Műveletek szorzata

11.4.1. Definíció. *Ha $((S_i, \top_i))_{i\in I}$ magma-rendszer, akkor a*

$$\Big(\prod_{i\in I} S_i\Big) \times \Big(\prod_{i\in I} S_i\Big) \to \prod_{i\in I} S_i; \quad ((s_i)_{i\in I}, (s'_i)_{i\in I}) \mapsto (s_i \top_i s'_i)_{i\in I}$$

függvényt a $(\top_i)_{i\in I}$ művelet-rendszer **szorzatának** *nevezzük, és a $\bigtimes_{i\in I} \top_i$ szimbólummal jelöljük, továbbá a $\Big(\prod_{i\in I} S_i, \bigtimes_{i\in I} \top_i\Big)$ magmát a $((S_i, \top_i))_{i\in I}$* **magma-rendszer szorzatának** *nevezzük.*

11.4.2. Tétel. *Legyen $((S_i, \top_i))_{i\in I}$ magma-rendszer, $S := \prod_{i\in I} S_i$ és $\top := \bigtimes_{i\in I} \top_i$.*

a) *Minden $i \in I$ esetén a $\mathrm{pr}_i : S \to S_i$ projekció morfizmus az $(S, \top)$ és $(S_i, \top_i)$ magmák között.*

b) *Ha minden $i \in I$ esetén a $\top_i$ művelet asszociatív (illetve kommutatív), akkor a $\top$ művelet is asszociatív (illetve kommutatív).*

c) *Ha minden $i \in I$ esetén a $\top_i$ művelet neutrális-elemes és e_i a $\top_i$ művelet szerinti neutrális elem, akkor a $\top$ művelet is neutrális-elemes, és $(e_i)_{i\in I}$ a $\top$ művelet szerinti neutrális elem.*

d) *Ha minden $i \in I$ esetén a $\top_i$ művelet neutrális-elemes, és $(s_i)_{i\in I} \in S$ olyan rendszer, hogy minden $i \in I$ esetén s_i invertálható $\top_i$ szerint, akkor $(s_i)_{i\in I}$ invertálható a $\top$ művelet szerint, és ha $(s'_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ indexre s'_i az s_i elem inverze a $\top_i$ művelet szerint, akkor $(s'_i)_{i\in I}$ az $(s_i)_{i\in I}$ rendszer inverze a $\top$ művelet szerint.*

Bizonyítás. a) A szorzatművelet definíciója (11.4.1.), valamint a morfizmusok definíciója (11.2.1.) szerint triviális.

b) Tegyük fel, hogy minden $i \in I$ esetén a $\top_i$ művelet asszociatív, és legyenek $(s_i)_{i\in I}$, $(s'_i)_{i\in I}$, $(s''_i)_{i\in I} \in S$. Ekkor

$$\begin{aligned}&(s_i)_{i\in I} \top \left((s'_i)_{i\in I} \top (s''_i)_{i\in I}\right) = (s_i)_{i\in I} \top (s'_i \top_i s''_i)_{i\in I} = (s_i \top_i (s'_i \top s''_i))_{i\in I} \stackrel{(1)}{=} \\ &\stackrel{(1)}{=} ((s_i \top_i s'_i) \top_i s''_i)_{i\in I} = (s_i \top_i s'_i)_{i\in I} \top (s''_i)_{i\in I} = \left((s_i)_{i\in I} \top (s'_i)_{i\in I}\right) \top (s''_i)_{i\in I},\end{aligned}$$

ahol a $\stackrel{(1)}{=}$ egyenlőségnél használtuk ki, hogy minden $i \in I$ esetén a $\top_i$ művelet asszociatív. Ezért a $\top$ művelet asszociatív.

Tegyük fel, hogy minden $i \in I$ esetén a $\top_i$ művelet kommutatív, és legyenek $(s_i)_{i\in I}$, $(s'_i)_{i\in I} \in S$. Ekkor

$$(s_i)_{i\in I} \top (s'_i)_{i\in I} = (s_i \top_i s'_i)_{i\in I} \stackrel{(2)}{=} (s'_i \top_i s_i)_{i\in I} = (s'_i)_{i\in I} \top (s_i)_{i\in I},$$

ahol a $\stackrel{(2)}{=}$ egyenlőségnél használtuk ki, hogy minden $i \in I$ esetén a $\top_i$ művelet kommutatív. Ezért a $\top$ művelet kommutatív.

c) Tegyük fel, hogy minden $i \in I$ esetén a $\top_i$ művelet neutrális-elemes, és legyen $e_i \in S_i$ a $\top_i$ művelet szerinti neutrális elem. Ekkor $(s_i)_{i\in I} \in S$ esetén minden $i \in I$ elemre $s_i \top_i e_i = s_i = e_i \top_i s_i$, következésképpen

$$(s_i)_{i\in I} \top (e_i)_{i\in I} = (s_i \top_i e_i)_{i\in I} = (s_i)_{i\in I} = (e_i \top_i s_i)_{i\in I} = (e_i)_{i\in I} \top (s_i)_{i\in I},$$

tehát az $(e_i)_{i\in I} \in S$ rendszer neutrális elem a $\top$ művelet szerint.

d) Tegyük fel, hogy minden $i \in I$ esetén a $\top_i$ művelet neutrális-elemes, és legyen $e_i \in S_i$ a $\top_i$ művelet szerinti neutrális elem, továbbá legyen $(s_i)_{i\in I} \in S$ olyan rendszer, hogy minden $i \in I$ esetén s_i invertálható $\top_i$ szerint. Ekkor minden $i \in I$ elemre $\{s \in S_i \mid s\top_i s_i = e_i = s\top_i e_i\} \neq \emptyset$, ezért a kiválasztási axióma szerint

$$\prod_{i\in I}\{s \in S_i \mid s\top_i s_i = e_i = s\top_i e_i\} \neq \emptyset.$$

Legyen $(s'_i)_{i\in I}$ tetszőleges eleme ennek a szorzathalmaznak, vagyis $(s'_i)_{i\in I} \in S$ olyan rendszer, hogy minden $i \in I$ indexre s'_i az s_i elem inverze a $\top_i$ művelet szerint. Ekkor $(s'_i)_{i\in I} \in S$ és

$$(s_i)_{i\in I}\top(s'_i)_{i\in I} = (s_i\top_i s'_i)_{i\in I} = (e_i)_{i\in I} = (s'_i\top_i s_i)_{i\in I} = (s'_i)_{i\in I}\top(s_i)_{i\in I},$$

tehát $(s'_i)_{i\in I}$ inverze az $(s_i)_{i\in I}$ elemnek a $\top$ művelet szerint. ■

11.4.3. Következmény. *Legyen $(S,\top)$ magma és T halmaz. Minden $f,g \in \mathscr{F}(T;S)$ esetén értelmezzük az*

$$f\widehat{\top}g : T \to S; \quad t \mapsto f(t)\top g(t)$$

függvényt. Ekkor a

$$\widehat{\top} : \mathscr{F}(T;S) \times \mathscr{F}(T;S) \to \mathscr{F}(T;S); \quad (f,g) \mapsto f\widehat{\top}g$$

leképezés $\mathscr{F}(T;S)$ feletti művelet, és ha $\top$ asszociatív (illetve kommutatív, illetve neutrális-elemes), akkor a $\widehat{\top}$ művelet is asszociatív (illetve kommutatív, illetve neutrális-elemes). Ha a $\top$ művelet neutrális-elemes és $f \in \mathscr{F}(T;S)$ olyan függvény, hogy minden $t \in T$ esetén $f(t)$ invertálható $\top$ szerint, akkor f invertálható a $\widehat{\top}$ művelet szerint.

Bizonyítás. Legyen minden $t \in T$ esetén $S_t := S$ és $\top_t := \top$. Ekkor $\prod_{t\in T} S_t = \mathscr{F}(T;S)$ és $\widehat{\top} = \times_{t\in T} \top_t$, ezért elegendő alkalmazni az előző tételt. ■

11.4.4. Állítás. *Legyen $(S_i)_{i\in I}$ halmazrendszer és $(\top_i)_{i\in I}$ valamint $(\perp_i)_{i\in I}$ olyan rendszerek, hogy minden $i \in I$ esetén $\top_i$ és $\perp_i$ művelet az S_i halmaz felett. Ha minden $i \in I$ elemre a $\top_i$ művelet disztributív (illetve elnyelő) a $\perp_i$ műveletre nézve, akkor a $\prod_{i\in I} S_i$ halmaz feletti $\times_{i\in I} \top_i$ művelet disztributív (illetve elnyelő) a $\times_{i\in I} \perp_i$ műveletre nézve.*

Bizonyítás. Legyen $\top := \times_{i\in I} \top_i$ és $\perp := \times_{i\in I} \perp_i$, valamint $S := \prod_{i\in I} S_i$.

Tegyük fel, hogy minden $i \in I$ esetén a $\top_i$ művelet disztributív a $\perp_i$ műveletre nézve, és legyenek $(s_i)_{i\in I}$, $(s'_i)_{i\in I}$, $(s''_i)_{i\in I} \in S$. Ekkor

$$\begin{aligned}(s_i)_{i\in I}\top\left((s'_i)_{i\in I}\perp(s''_i)_{i\in I}\right) = (s_i)_{i\in I}\top(s'_i\perp_i s''_i)_{i\in I} =\\ = (s_i\top_i(s'_i\perp_i s''_i))_{i\in I} \overset{(1)}{=} ((s_i\top_i s'_i)\perp_i(s_i\top_i s''_i))_{i\in I} =\\ = (s_i\top_i s'_i)_{i\in I}\perp(s_i\top_i s''_i)_{i\in I} = \left((s_i)_{i\in I}\top(s'_i)_{i\in I}\right)\perp\left((s_i)_{i\in I}\top(s''_i)_{i\in I}\right),\end{aligned}$$

ahol az $\stackrel{(1)}{=}$ egyenlőségnél felhasználtuk, hogy minden $i \in I$ esetén a $\top_i$ művelet disztributív a $\perp_i$ műveletre nézve. Hasonlóan kapjuk, hogy

$$\begin{aligned}((s_i')_{i\in I}\perp(s_i'')_{i\in I})\top(s_i)_{i\in I} &= (s_i'\perp_i s_i'')_{i\in I}\top(s_i)_{i\in I} = \\ &= ((s_i'\perp_i s_i'')\top_i s_i)_{i\in I} \stackrel{(2)}{=} ((s_i'\top_i s_i)\perp_i(s_i''\top_i s_i))_{i\in I} = \\ = (s_i'\top_i s_i)_{i\in I}\perp(s_i''\top_i s_i)_{i\in I} &= ((s_i')_{i\in I}\top(s_i)_{i\in I})\perp((s_i'')_{i\in I}\top(s_i)_{i\in I}),\end{aligned}$$

ahol a $\stackrel{(2)}{=}$ egyenlőségnél felhasználtuk, hogy minden $i \in I$ esetén a $\top_i$ művelet disztributív a $\perp_i$ műveletre nézve. Ezért a $\top$ művelet disztributív a $\perp$ műveletre nézve.

Tegyük fel, hogy minden $i \in I$ esetén a $\top_i$ művelet elnyelő a $\perp_i$ műveletre nézve, és legyenek $(s_i)_{i\in I}$, $(s_i')_{i\in I} \in S$. Ekkor

$$(s_i)_{i\in I}\top((s_i)_{i\in I}\perp(s_i')_{i\in I}) = (s_i)_{i\in I}\top(s_i\perp_i s_i')_{i\in I} = (s_i\top_i(s_i\perp_i s_i'))_{i\in I} \stackrel{(3)}{=} (s_i)_{i\in I},$$

ahol az $\stackrel{(3)}{=}$ egyenlőségnél felhasználtuk, hogy minden $i \in I$ esetén a $\top_i$ művelet elnyelő a $\perp_i$ műveletre nézve. Hasonlóan kapjuk, hogy

$$((s_i')_{i\in I}\perp(s_i)_{i\in I})\top(s_i)_{i\in I} = (s_i'\perp_i s_i)_{i\in I}\top(s_i)_{i\in I} = ((s_i'\perp_i s_i)\top_i s_i)_{i\in I} \stackrel{(4)}{=} (s_i)_{i\in I},$$

ahol az $\stackrel{(4)}{=}$ egyenlőségnél felhasználtuk, hogy minden $i \in I$ esetén a $\top_i$ művelet elnyelő a $\perp_i$ műveletre nézve. Ezért a $\top$ művelet elnyelő a $\perp$ műveletre nézve. ■

11.4.5. Állítás. *Legyen $((S_i,\top_i))_{i\in I}$ asszociatív magmák rendszere, $S := \prod_{i\in I} S_i$ és $\top := \times_{i\in I} \top_i$. Legyen $\big((s_{\alpha,i})_{i\in I}\big)_{\alpha\in A}$ olyan rendszer, hogy A nem üres, véges halmaz és minden $\alpha \in A$ esetén $(s_{\alpha,i})_{i\in I} \in S$. Tegyük fel, hogy minden $i \in I$ esetén az $\{s_{\alpha,i}|\alpha \in A\}$ halmaz kommutatív S_i-ben a $\top_i$ művelet szerint. Ekkor az $\big\{(s_{\alpha,i})_{i\in I}|\alpha \in A\big\}$ halmaz kommutatív a S szorzathalmazban a $\top$ szorzatművelet szerint és*

$$\mathop{\top}_{\alpha\in A}(s_{\alpha,i})_{i\in I} = \left(\mathop{\top_i}_{\alpha\in A} s_{\alpha,i}\right)_{i\in I}.$$

Bizonyítás. Ha minden $i \in I$ esetén az $\{s_{\alpha,i}|\alpha \in A\}$ halmaz kommutatív S_i-ben a $\top_i$ művelet szerint, akkor minden $\alpha,\beta \in A$ indexre a szorzatművelet definíciója szerint

$$(s_{\alpha,i})_{i\in I}\top(s_{\beta,i})_{i\in I} = (s_{\alpha,i}\top_i s_{\beta,i})_{i\in I} = (s_{\beta,i}\top_i s_{\alpha,i})_{i\in I} = (s_{\beta,i})_{i\in I}\top(s_{\alpha,i})_{i\in I},$$

tehát az $\big\{(s_{\alpha,i})_{i\in I}|\alpha \in A\big\}$ halmaz kommutatív a S szorzathalmazban a $\top$ szorzatművelet szerint, ezért a bizonyítandó egyenlőség bal oldalán álló kifejezés *értelmes* (figyelembe véve azt, hogy a $\top$ szorzatművelet is asszociatív).

Az állításban szereplő egyenlőséget az A nem üres, véges halmaz számossága szerinti teljes indukcióval bizonyítjuk.

Ha $\mathrm{Card}(A) = 1$ és α_* az az elem, amelyre $A = \{\alpha_*\}$, akkor 8.5.4. a) szerint minden $i \in I$ esetén $\mathop{\top_i}_{\alpha\in A} s_{\alpha,i} = s_{\alpha_*,i}$, és

$$\mathop{\top}_{\alpha\in A}(s_{\alpha,i})_{i\in I} \stackrel{(1)}{=} (s_{\alpha_*,i})_{i\in I} \stackrel{(2)}{=} \left(\mathop{\top_i}_{\alpha\in A} s_{\alpha,i}\right)_{i\in I},$$

ahol az $\overset{(1)}{=}$ egyenlőségnél a 8.5.4. a) állítást alkalmaztuk a $\top$ szorzatműveletre és az $A = \{\alpha_*\}$ egy elemű halmaz, továbbá, a $\overset{(2)}{=}$ egyenlőségnél minden $i \in I$ esetén a 8.5.4. a) állítást alkalmaztuk a $\top_i$ műveletre és az $A = \{\alpha_*\}$ egy elemű halmazra. Tehát az állítás igaz, ha A egy elemű halmaz.

Legyen $n \in \mathbb{N}^*$ olyan, hogy az állítás igaz minden olyan A indexhalmaz esetén, amelyre $\mathrm{Card}(A) = n$. Legyen A olyan véges halmaz, hogy $\mathrm{Card}(A) = n+1$, és rögzítsünk egy $\alpha_* \in A$ elemet. Vezessük be az $A_* := A \setminus \{\alpha_*\}$ halmazt, amelyre $\mathrm{Card}(A_*) = n$, tehát az indukciós hipotézis alkalmazható az $\big((s_{\alpha,i})_{i\in I}\big)_{\alpha\in A_*}$ rendszerre. Ekkor

$$\mathop{\top}_{\alpha\in A}(s_{\alpha,i})_{i\in I} \overset{(3)}{=} \Big(\mathop{\top}_{\alpha\in A_*}(s_{\alpha,i})_{i\in I}\Big)\top\big((s_{\alpha_*,i})_{i\in I}\big) \overset{(4)}{=} \left(\mathop{\top_i}_{\alpha\in A_*} s_{\alpha,i}\right)_{i\in I}\top\big((s_{\alpha_*,i})_{i\in I}\big) \overset{(5)}{=}$$
$$\overset{(5)}{=} \left(\left(\mathop{\top_i}_{\alpha\in A_*} s_{\alpha,i}\right)\top_i s_{\alpha_*,i}\right)_{i\in I} \overset{(6)}{=} \left(\mathop{\top_i}_{\alpha\in A} s_{\alpha,i}\right)_{i\in I},$$

ahol

- a $\overset{(3)}{=}$ egyenlőségnél a 8.5.4. b) állítást alkalmaztuk a $\top$ szorzatműveletre;
- a $\overset{(4)}{=}$ egyenlőségnél felhasználtuk az indukciós hipotézist az $\big((s_{\alpha,i})_{i\in I}\big)_{\alpha\in A_*}$ rendszerre;
- az $\overset{(5)}{=}$ egyenlőségnél a $\top$ szorzatművelet definícióját alkalmaztuk;
- a $\overset{(6)}{=}$ egyenlőségnél minden $i \in I$ indexre a 8.5.4. b) állítást alkalmaztuk a $\top_i$ műveletre.

Tehát az állítás igaz az $n+1$ elemű A halmaz esetében is. ■

11.4.6. Következmény. *Legyen $(S, \top)$ asszociatív magma és T halmaz. Minden $f, g \in \mathscr{F}(T;S)$ esetén értelmezzük az*

$$f\widehat{\top}g : T \to S; \quad t \mapsto f(t)\top g(t)$$

függvényt, és a

$$\widehat{\top} : \mathscr{F}(T;S)\times\mathscr{F}(T;S) \to \mathscr{F}(T;S); \quad (f,g)\mapsto f\widehat{\top}g$$

asszociatív műveletet a $\mathscr{F}(T;S)$ függvényhalmaz felett. Ha $(f_\alpha)_{\alpha\in A}$ nem üres, véges rendszer $\mathscr{F}(T;S)$-ben és minden $t \in T$ esetén az $\{f_\alpha(t)|\alpha \in A\}$ halmaz kommutatív S-ben a $\top$ művelet szerint, akkor az $\{f_\alpha|\alpha \in A\}$ halmaz kommutatív $\mathscr{F}(T;S)$-ben a $\widehat{\top}$ művelet szerint, és minden $t \in T$ esetén

$$\Big(\mathop{\widehat{\top}}_{\alpha\in A} f_\alpha\Big)(t) = \mathop{\top}_{\alpha\in A} f_\alpha(t).$$

Bizonyítás. Legyen minden $t \in T$ esetén $S_t := S$ és $\top_t := \top$, továbbá, minden $t \in T$ és $\alpha \in A$ esetén $s_{\alpha,t} := f_\alpha(t)$. Ekkor $\prod_{t\in T} S_t = \mathscr{F}(T;S)$ és $\widehat{\top} = \mathop{\times}_{t\in T}\top_t$, ezért az $I := T$ választással elegendő alkalmazni az előző tételt, amely szerint

$$\mathop{\widehat{\top}}_{\alpha\in A} f_\alpha = \Big(\mathop{\top}_{\alpha\in A} f_\alpha(t)\Big)_{t\in T}. \blacksquare$$

11.5. Műveletek faktorizációja

11.5.1. Tétel. *Legyen* $(S, \top)$ *magma és* R *ekvivalencia* S *felett. Akkor és csak akkor létezik olyan* $\widetilde{\top}$ *művelet az* S/R *faktorhalmaz felett, amelyre minden* $s, t \in S$ *esetén* $\pi_{S/R}(s \top t) = \pi_{S/R}(s) \widetilde{\top} \pi_{S/R}(t)$*, ha igaz a következő állítás.*

(FAC) *Minden* $s, s', t, t' \in S$ *esetén, ha* $(s, s') \in R$ *és* $(t, t') \in R$*, akkor* $(s \top t, s' \top t') \in R$ *teljesül.*

Továbbá, ha a (FAC) *feltétel igaz, akkor egyetlen olyan* S/R *feletti* $\widetilde{\top}$ *művelet létezik, amelyre minden* $s, t \in S$ *esetén* $\pi_{S/R}(s \top t) = \pi_{S/R}(s) \widetilde{\top} \pi_{S/R}(t)$*.*

Bizonyítás. (I) Legyen $\widetilde{\top}$ olyan művelet az S/R faktorhalmaz felett, amelyre teljesül az, hogy minden $s, t \in S$ esetén $\pi_{S/R}(s \top t) = \pi_{S/R}(s) \widetilde{\top} \pi_{S/R}(t)$. Legyenek $s, s', t, t' \in S$ olyan elemek, amelyekre $(s, s') \in R$ és $(t, t') \in R$. Ekkor $\pi_{S/R}(s) = \pi_{S/R}(s')$ és $\pi_{S/R}(t) = \pi_{S/R}(t')$, ezért

$$\pi_{S/R}(s \top t) = \pi_{S/R}(s) \widetilde{\top} \pi_{S/R}(t) = \pi_{S/R}(s') \widetilde{\top} \pi_{S/R}(t') = \pi_{S/R}(s' \top t'),$$

tehát $(s \top t, s' \top t') \in R$.

(II) Tegyük fel, hogy minden $s, s', t, t' \in S$ esetén, ha $(s, s') \in R$ és $(t, t') \in R$, akkor $(s \top t, s' \top t') \in R$. Ha $(\zeta, \eta) \in (S/R) \times (S/R)$, akkor $\zeta \times \eta \neq \emptyset$, ezért a kiválasztási axióma alapján vehetünk egy

$$\varphi \in \prod_{(\zeta,\eta) \in (S/R) \times (S/R)} (\zeta \times \eta)$$

kiválasztó függvényt. Rögzítsünk egy ilyen függvényt és vezessük be a

$$\begin{aligned} \varphi_1 &: (S/R) \times (S/R) \to S; \quad (\zeta, \eta) \mapsto \mathrm{pr}_1(\varphi(\zeta, \eta)), \\ \varphi_2 &: (S/R) \times (S/R) \to S; \quad (\zeta, \eta) \mapsto \mathrm{pr}_2(\varphi(\zeta, \eta)) \end{aligned}$$

függvényeket. Ekkor minden $(\zeta, \eta) \in (S/R) \times (S/R)$ esetén

$$\varphi(\zeta, \eta) = (\mathrm{pr}_1(\varphi(\zeta, \eta)), \mathrm{pr}_2(\varphi(\zeta, \eta))) = (\varphi_1(\zeta, \eta), \varphi_2(\zeta, \eta)) \in \zeta \times \eta,$$

vagyis $\varphi_1(\zeta, \eta) \in \zeta$ és $\varphi_2(\zeta, \eta) \in \eta$. Értelmezzük a

$$\widetilde{\top} : (S/R) \times (S/R) \to S/R; \quad (\zeta, \eta) \mapsto \pi_{S/R}(\varphi_1(\zeta, \eta) \top \varphi_2(\zeta, \eta))$$

függvényt, amely természetesen művelet az S/R faktorhalmaz felett.

Legyenek $s, t \in S$. Ekkor $\varphi_1(\pi_{S/R}(s), \pi_{S/R}(t)) \in \pi_{S/R}(s)$, tehát $(\varphi_1(\pi_{S/R}(s), \pi_{S/R}(t)), s) \in R$. Hasonlóan, $\varphi_2(\pi_{S/R}(s), \pi_{S/R}(t)) \in \pi_{S/R}(t)$, tehát $(\varphi_2(\pi_{S/R}(s), \pi_{S/R}(t)), t) \in R$. Ezért a (FAC) feltétel alapján

$$(\varphi_1(\pi_{S/R}(s), \pi_{S/R}(t)) \top \varphi_2(\pi_{S/R}(s), \pi_{S/R}(t)),\ s \top t) \in R.$$

Ebből következik, hogy

$$\pi_{S/R}(s) \widetilde{\top} \pi_{S/R}(t) = \pi_{S/R}(\varphi_1(\pi_{S/R}(s), \pi_{S/R}(t)) \top \varphi_2(\pi_{S/R}(s), \pi_{S/R}(t))) = \pi_{S/R}(s \top t),$$

tehát $\widetilde{\top}$ olyan művelet S/R felett, amelynek a létezését állítottuk.

(III) A $\pi_{S/R} : S \to S/R$ függvény szürjektivitása miatt az előírt tulajdonságú $\widetilde{\top}$ művelet egyértelműsége nyilvánvaló. ■

11.5.2. Definíció. *Legyen $(S, \top)$ magma és R ekvivalencia S felett. Azt mondjuk, hogy a $\top$* **művelet faktorizálható** *az R ekvivalencia szerint, ha igaz a következő állítás.*

(FAC) *Minden $s, s', t, t' \in S$ esetén, ha $(s, s') \in R$ és $(t, t') \in R$, akkor $(s\top t, s'\top t') \in R$ teljesül.*

Ha (FAC) *teljesül, akkor az előző tételben értelmezett $\widetilde{\top}$ művelet a $\top/R$ szimbólummal jelöljük.*

Tehát a 11.5.1. tétel szerint, ha $(S, \top)$ magma és R ekvivalencia S felett, akkor a $\top$ művelet pontosan akkor faktorizálható R szerint, ha létezik olyan S/R feletti $\widetilde{\top}$ művelet, hogy minden $s, t \in S$ esetén $\pi_{S/R}(s\top t) = \pi_{S/R}(s)\widetilde{\top}\pi_{S/R}(t)$, vagyis a következő diagram kommutatív:

$$\begin{tikzcd}
S \times S \arrow[r, "\top"] \arrow[d, "\pi_{S/R}\times\pi_{S/R}"'] & S \arrow[d, "\pi_{S/R}"] \\
(S/R) \times (S/R) \arrow[r, "\top/R"'] & S/R
\end{tikzcd}$$

11.5.3. Állítás. *Legyen $(S, \top)$ magma és R ekvivalencia S felett. Tegyük fel, hogy a $\top$ művelet faktorizálható R szerint.*

a) *Ha $\top$ művelet asszociatív (illetve kommutatív), akkor az S/R faktorhalmaz feletti $\top/R$ művelet is asszociatív (illetve kommutatív).*

b) *Ha $e \in S$ neutrális elem a $\top$ művelet szerint, akkor $\pi_{S/R}(e) \in S/R$ neutrális elem a $\top/R$ művelet szerint.*

c) *Ha a $\top$ művelet neutrális elemes, és $s' \in S$ az $s \in S$ elem inverze a $\top$ művelet szerint, akkor $\pi_{S/R}(s') \in S/R$ a $\pi_{S/R}(s) \in S/R$ elem inverze a $\top/R$ művelet szerint.*

Bizonyítás. a) A 11.2.4. állításból következik, mert a definíció szerint $\pi_{S/R} : S \to S/R$ szürjektív morfizmus az $(S, \top)$ és $(S/R, \top/R)$ magmák között.

b) Ha $\xi \in S/R$, akkor van olyan $s \in S$, hogy $\xi = \pi_{S/R}(s)$, ezért

$$\begin{aligned}
\pi_{S/R}(e)(\top/R)\xi &= \pi_{S/R}(e)(\top/R)\pi_{S/R}(s) = \pi_{S/R}(e\top s) = \pi_{S/R}(s) = \\
&= \pi_{S/R}(s\top e) = \pi_{S/R}(s)(\top/R)\pi_{S/R}(e) = \xi(\top/R)\pi_{S/R},
\end{aligned}$$

$$= \pi_{S/R}(s\top e) = \pi_{S/R}(s)(\top/R)\pi_{S/R}(e) = \xi(\top/R)\pi_{S/R},$$

tehát $\pi_{S/R}(e) \in S/R$ neutrális elem a $\top/R$ művelet szerint.

c) Ha $e \in S$ neutrális elem a $\top$ művelet szerint, akkor b) alapján $\pi_{S/R}(e) \in S/R$ neutrális elem a $\top/R$ művelet szerint. Ha $s' \in S$ inverze az $s \in S$ elemnek a $\top$ művelet szerint, akkor

$$\pi_{S/R}(s')(\top/R)\pi_{S/R}(s) = \pi_{S/R}(s'\top s) = \pi_{S/R}(e) = \pi_{S/R}(s\top s') = \pi_{S/R}(s)(\top/R)\pi_{S/R}(s'),$$

tehát $\pi_{S/R}(s') \in S/R$ a $\pi_{S/R}(s) \in S/R$ elem inverze a $\top/R$ művelet szerint. ∎

11.6. Algebrai objektumok

12. fejezet

Félcsoportok

12.1. Félcsoportok és félcsoport-morfizmusok

12.1.1. Definíció. *Az $(S, \top)$ párt* **félcsoportnak** *nevezzük, ha $\top$ asszociatív művelet az S halmaz felett. Azt mondjuk, hogy az $(S, \top)$ pár* **monoid**, *ha $(S, \top)$ neutrális-elemes félcsoport.*

Tehát a 8.3.1. definíció alapján az "asszociatív magma" és a "félcsoport" kifejezések egymás szinonimái.

A továbbiakban félcsoportokra általában a multiplikatív jelölést alkalmazzuk, tehát a félcsoportot egyetlen szimbólummal, az alaphalmaz jelével jelöljük, és a műveletére a szorzás szimbólumot használjuk, ha ez nem vezet félreértésre.

12.1.2. Definíció. *Az S és T félcsoportok közötti* **morfizmusnak** *vagy* **félcsoport-morfizmusnak** *nevezünk minden olyan $f : S \to T$ függvényt, amely morfizmus az S és T magmák között, vagyis minden $s, s' \in S$ esetén $f(ss') = f(s)f(s')$. Azt mondjuk, hogy az $f : S \to T$ függvény* **izomorfizmus** *az S és T félcsoportok között vagy* **félcsoport-izomorfizmus**, *ha f morfizmus az S és T félcsoportok között, és f bijekció, és az $f^{-1} : T \to S$ függvény morfizmus a T és S félcsoportok között. Azt mondjuk, hogy az S és T félcsoportok* **izomorfak**, *ha létezik izomorfizmus az S és T félcsoportok között.*

12.2. Félcsoport idempotens elemei

12.2.1. Definíció. *Legyen S félcsoport. Azt mondjuk, hogy az $e \in S$ elem* **idempotens** *ha $e^2 = e$. Az S félcsoport idempotens elemeinek halmazát $\mathbf{I}(S)$ jelöli.*

Nyilvánvaló, hogy ha S félcsoport és 0 zéruseleme (illetve 1 neutrális eleme) S-nek, akkor $0 \in \mathbf{I}(S)$ (illetve $1 \in \mathbf{I}(S)$).

12.2.2. Állítás. *Legyen S félcsoport. Az $\mathbf{I}(S)$ halmaz feletti*

$$\leq := \{ (e, f) \in \mathbf{I}(S) \times \mathbf{I}(S) \mid e = ef = fe \}$$

reláció rendezés. Ha 0 zéruseleme S-nek, akkor 0 a legkisebb eleme $\mathbf{I}(S)$-nek, és ha 1 neutrális eleme S-nek, akkor 1 a legnagyobb eleme $\mathbf{I}(S)$-nek a $\leq$ rendezés szerint.

Bizonyítás. A $\leq$ reláció reflexív az $\mathbf{I}(S)$ halmazon, mert minden $e \in \mathbf{I}(S)$ esetén $e = e^2$. Ha $e, f \in \mathbf{I}(S)$ olyanok, hogy $e \leq f$ és $f \leq e$, akkor $e = ef = fe$ és $f = fe = ef$, amiből

$e = f$ következik, tehát a $\leq$ reláció antiszimmetrikus. Ha $e, f, g \in \mathbf{I}(S)$ olyanok, hogy $e \leq f$ és $f \leq g$, akkor $e = ef = fe$ és $f = fg = gf$, így S műveletének asszociativitása folytán $eg = (ef)g = e(fg) = ef = e$ és $ge = g(fe) = (gf)e = fe = e$, tehát $e(eg) = ge$, vagyis $e \leq g$, ami azt jelenti, hogy a $\leq$ reláció tranzitív.

Ha 0 zéruseleme S-nek, akkor minden $e \in \mathbf{I}(S)$ esetén $0 = 0e = e0$, tehát $0 \leq e$, vagyis 0 a legkisebb eleme $\mathbf{I}(S)$-nek a $\leq$ rendezés szerint. Ha 1 neutrális eleme S-nek, akkor minden $e \in \mathbf{I}(S)$ esetén $e = e1 = 1e$, tehát $e \leq 1$, vagyis 1 a legnagyobb eleme $\mathbf{I}(S)$-nek a $\leq$ rendezés szerint. ■

12.2.3. Definíció. *Ha S félcsoport, akkor az S idempotens elemeinek halmaza feletti* **természetes rendezésnek** *nevezzük az előző állításban értelmezett $\mathbf{I}(S)$ feletti $\leq$ rendezést, tehát minden $e, f \in \mathbf{I}(S)$ esetén*

$$e \leq f \quad \overset{\text{def}}{\Leftrightarrow} \quad e = ef = fe.$$

12.2.4. Állítás. *Ha S félcsoport és $e, f \in \mathbf{I}(S)$ olyanok, hogy $ef = fe$, akkor $ef \in \mathbf{I}(S)$ és*

$$\inf\{e, f\} = ef$$

teljesül az $\mathbf{I}(S)$ feletti természetes rendezés szerint.

Bizonyítás. Mivel az e és f idempotens elemek kommutálnak, így S műveletének asszociativitása miatt

$$\begin{aligned}(ef)^2 &= (ef)(ef) = e(f(ef)) = e((fe)f) = e((ef)f) = \\ &= (e(ef))f = ((ee)f)f = (ef)f = e(ff) = ef,\end{aligned}$$

vagyis $ef \in \mathbf{I}(S)$. Továbbá, S műveletének asszociativitása folytán $(ef)e = e(fe) = e(ef) = (ee)f = ef$ és $e(ef) = (ee)f = ef$, tehát $ef = (ef)e = e(ef)$, vagyis $ef \leq e$, valamint $(ef)f = e(ff) = ef$ és $f(ef) = (fe)f = (ef)f = e(ff) = ef$, tehát $ef = (ef)f = f(ef)$, vagyis $ef \leq f$. Ez azt jelenti, hogy ef alsó korlátja az $\{e, f\}$ halmaznak a $\leq$ rendezés szerint. Legyen $g \in \mathbf{I}(S)$ olyan, hogy g alsó korlátja az $\{e, f\}$ halmaznak a $\leq$ rendezés szerint, vagyis $g \leq e$ és $g \leq f$. Ekkor $g = ge = eg$ és $g = gf = fg$, amiből S műveletének asszociativitása folytán következik, hogy $g(ef) = (ge)f = gf = g$ és $(ef)g = e(fg) = eg = g$, vagyis $g \leq ef$. Ez azt jelenti, hogy ef a legnagyobb alsó korlátja az $\{e, f\}$ halmaznak, azaz $\inf\{e, f\} = ef$. ■

12.2.5. Állítás. *Legyen S félcsoport és $e, f \in \mathbf{I}(S)$. Tekintsük a következő állításokat.*

(i) $e \leq f$.

(ii) $eS \subseteq fS$.

(iii) $e = fe$.

Ekkor (i) $\Rightarrow$ (ii)$\Leftrightarrow$(iii) *teljesül.*

Bizonyítás. Ha $s \in S$, akkor $e \leq f$ esetén S asszociativitása folytán $es = (fe)s = f(es) \in fS$, tehát (i) $\Rightarrow$ (ii) teljesül. Az e elem idempotenciája miatt $e = ee \in eS$, tehát ha (ii) igaz, akkor $e \in fS$, vagyis létezik olyan $s \in S$, hogy $e = fs$, következésképpen $fe = f(fs) = (ff)s = fs = e$, tehát (iii) is igaz, ami azt jelenti, hogy (ii) $\Rightarrow$ (iii) teljesül. Végül, ha (iii) igaz, vagyis $e = fe$, akkor $x \in eS$ esetén van olyan $s \in S$, hogy $x = es = (fe)s = f(es) \in fS$, tehát $eS \subseteq fS$ is igaz, ami azt jelenti, hogy (iii) $\Rightarrow$ (ii) is teljesül. ■

12.3. Monoidok és egységelemesítés

12.3.1. Definíció. *A neutrális-elemes félcsoportokat* **monoidoknak** *nevezzük.*

12.3.2. Állítás. *Legyen* $(S, \top)$ *félcsoport és* $\mathfrak{e}$ *olyan halmaz, amelyre* $\mathfrak{e} \notin S$. *Legyen*

$$\widetilde{S} := S \cup \{\mathfrak{e}\},$$

és értelmezzük azt a

$$\widetilde{\top} : \widetilde{S} \times \widetilde{S} \to \widetilde{S}$$

műveletet, amelyre minden $s, s' \in \widetilde{S}$ *esetén*

$$s \widetilde{\top} s' := \begin{cases} s \top s' & \text{, ha } s \in S \text{ és } s' \in S, \\ s & \text{, ha } s \in S \text{ és } s' = \mathfrak{e}, \\ s' & \text{, ha } s = \mathfrak{e} \text{ és } s' \in S, \\ \mathfrak{e} & \text{, ha } s = \mathfrak{e} \text{ és } s' = \mathfrak{e}. \end{cases}$$

Ekkor $(\widetilde{S}, \widetilde{\top})$ *olyan monoid, amelynek* $\mathfrak{e}$ *a neutrális eleme, és amelyre* $\widetilde{\top}|_{S \times S} = \top$ *teljesül.*

Bizonyítás. Csak a $\widetilde{\top}$ művelet asszociativitása szorul bizonyításra, ami egyszerű esetszétválasztással elvégezhető. ■

12.3.3. Definíció. *Ha* $(S, \top)$ *félcsoport és* $\mathfrak{e}$ *olyan halmaz, amelyre* $\mathfrak{e} \notin S$, *akkor az előző állításban értelmezett* $(\widetilde{S}, \widetilde{\top})$ *monoidot az* $(S, \top)$ *félcsoport* $\mathfrak{e}$*-vel képzett* **egységelemesítésének** *nevezzük.*

12.4. Elem hatványai félcsoportban

12.4.1. Definíció. *Legyen* $(S, \top)$ *magma,* $s \in S$, *és minden* $i \in \mathbb{N}^*$ *esetén legyen* $s_i := s$. *Ekkor minden* $n \in \mathbb{N}^*$ *esetén*

$$\overset{n}{\top} s := \overset{n}{\underset{i=1}{\top}} s_i,$$

és S*-nek ezt az elemét az* s *elem* $\top$ *művelet szerinti* n**-edik hatványának** *nevezzük.*

Tehát ha $(S, \top)$ magma, $s \in S$, és minden $i \in \mathbb{N}^*$ esetén $s_i := s$, akkor $\left(\overset{n}{\top} s\right)_{n \in \mathbb{N}^*}$ olyan S-ben haladó rendszer, amelyre 8.3.5. a) alapján teljesül az, hogy

$$\overset{1}{\top} s = \overset{1}{\underset{i=1}{\top}} s_i = s_1 = s,$$

és 8.3.5. b) alapján minden $n \in \mathbb{N}^*$ esetén

$$\overset{n+1}{\top} s = \overset{n+1}{\underset{i=1}{\top}} s_i = \left(\overset{n}{\underset{i=1}{\top}} s_i \right) \top s_{n+1} = \left(\overset{n}{\top} s \right) \top s.$$

Könnyen látható, hogy ez a két tulajdonság egyértelműen meghatározza a $\left(\overset{n}{\top} s\right)_{n \in \mathbb{N}^*}$ rendszert, mert ha $\widetilde{s} : \mathbb{N}^* \to S$ olyan függvény, hogy $\widetilde{s}(1) = s$ és minden $n \in \mathbb{N}^*$ esetén

$\widetilde{s}(n+1) = \widetilde{s}(n)\top s$, akkor az $(\widetilde{s}(m+1))_{m\in\mathbb{N}}$ és $(\overset{m+1}{\top} s)_{m\in\mathbb{N}}$ sorozatok megegyeznek a $g : S \to S;\ s' \mapsto s'\top s$ függvény és $s \in S$ kezdőpont által elemi rekurzióval meghatározott sorozattal, így ennek egyértelműsége folytán minden $m \in \mathbb{N}$ esetén $\widetilde{s}(m+1) = \overset{m+1}{\top} s$, következésképpen $\widetilde{s}$ egyenlő a $\left(\overset{n}{\top} s\right)_{n\in\mathbb{N}^*}$ rendszerrel.

Figyeljük meg, hogy a $\overset{0}{\top} s$ elemet *nem értelmeztük*. Azonban neutrális-elemes magmában (speciálisan: monoidban) a következő definíciót alkalmazzuk.

12.4.2. Definíció. *Ha $(S,\top)$ neutrális-elemes magma, és $e \in S$ a $\top$ művelet szerinti neutrális elem, akkor minden $s \in S$ elemre*

$$\overset{0}{\top} s := e.$$

A definícióból következik, hogy ha $(S,\top)$ monoid és $e \in S$ a $\top$ művelet szerinti neutrális elem, akkor minden $n \in \mathbb{N}$ esetén

$$\overset{n}{\top} e = e.$$

Valóban, ez a definíció szerint igaz $n = 0$ esetén, és ha $n \in \mathbb{N}$ olyan, hogy $\overset{n}{\top} e = e$, akkor:
– ha $n = 0$, akkor $\overset{n+1}{\top} e = \overset{1}{\top} e = e$;
– ha $n > 0$, akkor $\overset{n+1}{\top} e = (\overset{n}{\top} e)\top e = e\top e = e$,
tehát $\overset{n+1}{\top} e = e$.

Természetesen a hatványozással kapcsolatban eddig megfogalmazott állítások tetszőleges magmában, illetve neutrális-elemes magmában érvényesek. Azonban a hatványozás "elvárható" tulajdonságai csak asszociatív magmában, vagyis félcsoportban igazak.

12.4.3. Állítás. *Legyen $(S,\top)$ félcsoport és $s \in S$. Ha I nem üres véges halmaz és minden $i \in I$ esetén $s_i := s$, akkor*

$$\overset{\mathrm{Card}(I)}{\top} s = \top_{i\in I} s_i.$$

(**Megjegyzés.** Az egyenlőség jobb oldalán álló kifejezés *értelmes*, mert az $\{s_i|i \in I\}$ halmaz egyenlő az $\{s\}$ egy elemű halmazzal, amely természetesen kommutatív a $\top$ művelet szerint.)

Bizonyítás. Legyen $\tau : \mathrm{Card}(I) \to I$ bijekció. Ekkor a véges műveletek definíciója (8.5.3.) szerint

$$\top_{i\in I} s_i = \top_{k=0}^{\mathrm{Card}(I)-1} s_{\tau(k)} \overset{(1)}{=} \top_{k=1}^{\mathrm{Card}(I)} s_{\tau(k-1)} = \top_{k=1}^{\mathrm{Card}(I)} s_{\tau(k-1)} \overset{(2)}{=} \overset{\mathrm{Card}(I)}{\top} s,$$

ahol az $\overset{(1)}{=}$ egyenlőségnél alkalmaztuk a 8.3.4. állítást, és a $\overset{(2)}{=}$ egyenlőségnél felhasználuk a hatványozás definícióját (12.4.1.) és azt, hogy minden $k \in [\![1, \mathrm{Card}(I)]\!]$ természetes számra $s_{\tau(k-1)} = s$. ■

12.4.4. Állítás. (**A hatványozás azonosságai.**) *Legyen* $(S, \top)$ *félcsoport.*
a) *Ha* $s \in S$*, akkor minden* $m, n \in \mathbb{N}^*$ *esetén*

$$\overset{m+n}{\top} s = (\overset{m}{\top} s)\top(\overset{n}{\top} s),$$
$$\overset{m\cdot n}{\top} s = \overset{n}{\top}(\overset{m}{\top} s).$$

Ha $(S, \top)$ *monoid, akkor ezek az egyenlőségek minden* $m, n \in \mathbb{N}$ *esetén érvényesek.*
b) *Ha* $s, t \in S$ *olyan elemek, hogy* $s\top t = t\top s$*, akkor minden* $n \in \mathbb{N}^*$ *esetén*

$$\overset{n}{\top}(s\top t) = (\overset{n}{\top} s)\top(\overset{n}{\top} t).$$

Ha $(S, \top)$ *monoid, akkor ez az egyenlőség minden* $n \in \mathbb{N}$ *esetén érvényes.*

Bizonyítás. a) Mindkét egyenlőséget rögzített $m \in \mathbb{N}^*$ esetén, 1-től indított, n szerinti teljes indukcióval bizonyítjuk.
Világos, hogy $\overset{m+1}{\top} s = (\overset{m}{\top} s)\top s = (\overset{m}{\top} s)\top(\overset{1}{\top} s)$, és ha $n \in \mathbb{N}^*$ olyan, hogy $\overset{m+n}{\top} s = (\overset{m}{\top} s)\top(\overset{n}{\top} s)$, akkor

$$\overset{m+(n+1)}{\top} s = \overset{(m+n)+1}{\top} s = (\overset{m+n}{\top} s)\top s \overset{(1)}{=} ((\overset{m}{\top} s)\top(\overset{n}{\top} s))\top s \overset{(2)}{=}$$
$$\overset{(2)}{=} (\overset{m}{\top} s)\top((\overset{n}{\top} s)\top s) = (\overset{m}{\top} s)\top(\overset{n+1}{\top} s),$$

ahol az $\overset{(1)}{=}$ egyenlőségnél az indukciós hipotézist alkalmaztuk, és a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk a $\top$ művelet asszociativitását. Ezért minden $m, n \in \mathbb{N}^*$ esetén fennáll a $\overset{m+n}{\top} s = (\overset{m}{\top} s)\top(\overset{n}{\top} s)$ egyenlőség.
Világos, hogy $\overset{m\cdot 1}{\top} s = \overset{m}{\top} s = \overset{1}{\top}(\overset{m}{\top} s)$, és ha $n \in \mathbb{N}^*$ olyan, hogy $\overset{m\cdot n}{\top} s = \overset{n}{\top}(\overset{m}{\top} s)$, akkor

$$\overset{m\cdot(n+1)}{\top} s = \overset{m\cdot n+m}{\top} s \overset{(3)}{=} (\overset{m\cdot n}{\top} s)\top(\overset{m}{\top} s) \overset{(4)}{=} (\overset{n}{\top}(\overset{m}{\top} s))\top(\overset{m}{\top} s) = \overset{n+1}{\top}(\overset{m}{\top} s),$$

ahol a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk az előző bekezdés eredményét, és a $\overset{(4)}{=}$ egyenlőségnél az indukciós hipotézist alkalmaztuk. Ezért minden $m, n \in \mathbb{N}^*$ esetén fennáll a $\overset{m\cdot n}{\top} s = \overset{n}{\top}(\overset{m}{\top} s)$ egyenlőség.
Tegyük fel, hogy $(S, \top)$ monoid és $e \in S$ a $\top$ művelet szerinti neutrális elem. Ha $m, n \in \mathbb{N}$, akkor:
– ha $m, n > 0$, akkor az előzőek szerint $\overset{m+n}{\top} s = (\overset{m}{\top} s)\top(\overset{n}{\top} s)$ és $\overset{m\cdot n}{\top} s = \overset{n}{\top}(\overset{m}{\top} s)$;
– ha $m = 0$, akkor a definíció szerint

$$\overset{m+n}{\top} s = \overset{0+n}{\top} s = \overset{n}{\top} s = e\top(\overset{n}{\top} s) = (\overset{0}{\top} s)\top(\overset{n}{\top} s) = (\overset{m}{\top} s)\top(\overset{n}{\top} s),$$
$$\overset{m\cdot n}{\top} s = \overset{0\cdot n}{\top} s = \overset{0}{\top} s = e = \overset{n}{\top} e = \overset{n}{\top}(\overset{0}{\top} s) = \overset{n}{\top}(\overset{m}{\top} s);$$

– ha $n=0$, akkor a definíció szerint

$$\overset{m+n}{\top} s = \overset{m+0}{\top} s = \overset{m}{\top} s = (\overset{m}{\top} s)\top e = (\overset{m}{\top} s)\top(\overset{0}{\top} s) = (\overset{m}{\top} s)\top(\overset{n}{\top} s),$$
$$\overset{m\cdot n}{\top} s = \overset{m\cdot 0}{\top} s = \overset{0}{\top} s = e = \overset{0}{\top}(\overset{m}{\top} s) = \overset{n}{\top}(\overset{m}{\top} s).$$

Ezért minden $m, n \in \mathbb{N}$ esetén $\overset{m+n}{\top} s = (\overset{m}{\top} s)\top(\overset{n}{\top} s)$ és $\overset{m\cdot n}{\top} s = \overset{n}{\top}(\overset{m}{\top} s)$.

b) Először 1-től indított, n szerinti teljes indukcióval megmutatjuk, hogy minden $n \in \mathbb{N}^*$ esetén $(\overset{n}{\top} t)\top s = s\top(\overset{n}{\top} t)$ teljesül. Valóban, a hipotézis szerint $(\overset{1}{\top} t)\top s = t\top s = s\top t = s\top(\overset{1}{\top} t)$, így állítás igaz, ha $n=1$. Ha $n \in \mathbb{N}^*$ olyan, hogy $(\overset{n}{\top} t)\top s = s\top(\overset{n}{\top} t)$, akkor

$$(\overset{n+1}{\top} t)\top s = ((\overset{n}{\top} t)\top t)\top s \overset{(5)}{=} (\overset{n}{\top} t)\top(t\top s) \overset{(6)}{=} (\overset{n}{\top} t)\top(s\top t) \overset{(7)}{=} ((\overset{n}{\top} t)\top s)\top t \overset{(8)}{=}$$
$$\overset{(8)}{=} (s\top(\overset{n}{\top} t))\top t \overset{(9)}{=} s\top((\overset{n}{\top} t)\top t) = s\top(\overset{n+1}{\top} t),$$

ahol az $\overset{(5)}{=}$, $\overset{(7)}{=}$ és $\overset{(9)}{=}$ egyenlőségeknél a $\top$ művelet asszociativitását alkalmaztuk, és a $\overset{(6)}{=}$ egyenlőségnél hivatkoztunk a $t\top s = s\top t$ hipotézisre, továbbá a $\overset{(8)}{=}$ egyenlőségnél felhasznátuk az $(\overset{n}{\top} t)\top s = s\top(\overset{n}{\top} t)$ indukciós hipotézist, így az egyenlőség az $n+1$ számra is igaz.

Ezután a bizonyítandó egyenlőséget 1-től indított, n szerinti teljes indukcióval fogjuk igazolni.

Világos, hogy $\overset{1}{\top}(s\top t) = s\top t = (\overset{1}{\top} s)\top(\overset{1}{\top} t)$, és ha $n \in \mathbb{N}^*$ olyan, hogy $\overset{n}{\top}(s\top t) = (\overset{n}{\top} s) \top (\overset{n}{\top} t)$, akkor

$$\overset{n+1}{\top}(s \top t) = (\overset{n}{\top}(s\top t))\top(s\top t) \overset{(10)}{=} ((\overset{n}{\top} s)\top(\overset{n}{\top} t))\top(s\top t) \overset{(11)}{=}$$
$$\overset{(11)}{=} (\overset{n}{\top} s)\top((\overset{n}{\top} t)\top(s\top t)) \overset{(12)}{=} (\overset{n}{\top} s)\top(((\overset{n}{\top} t)\top s)\top t) \overset{(13)}{=}$$
$$\overset{(13)}{=} (\overset{n}{\top} s)\top((s\top(\overset{n}{\top} t))\top t) \overset{(14)}{=} ((\overset{n}{\top} s)\top(s\top(\overset{n}{\top} t)))\top t \overset{(15)}{=}$$
$$\overset{(15)}{=} (((\overset{n}{\top} s)\top s)\top(\overset{n}{\top} t))\top t \overset{(16)}{=} ((\overset{n}{\top} s)\top s)\top((\overset{n}{\top} t)\top t) = (\overset{n+1}{\top} s)\top(\overset{n+1}{\top} t),$$

ahol a $\overset{(10)}{=}$ egyenlőségnél a $\overset{n}{\top}(s\top t) = (\overset{n}{\top} s)\top(\overset{n}{\top} t)$ indukciós hipotézist alkalmaztuk, és a $\overset{(13)}{=}$ egyenlőségnél felhasználtuk azt, hogy $(\overset{n}{\top} t)\top s = s\top(\overset{n}{\top} t)$, továbbá a $\overset{(11)}{=}$, $\overset{(12)}{=}$, $\overset{(14)}{=}$ $\overset{(15)}{=}$ és $\overset{(16)}{=}$ egyenlőségeknél kihasználtuk a $\top$ művelet asszociativitását, így az egyenlőség az $n+1$ számra is igaz.

Tegyük fel, hogy $(S, \top)$ monoid és $e \in S$ a $\top$ művelet szerinti neutrális elem. Ekkor

$$\overset{0}{\top}(s\top t) = e = e\top e = (\overset{0}{\top} s)\top(\overset{0}{\top} t),$$

így minden $n \in \mathbb{N}$ esetén $\overset{n}{\top}(s\top t) = (\overset{n}{\top} s)\top(\overset{n}{\top} t)$. ■

Egyszerű példát adhatunk olyan nem asszociatív magmára, amelyre a 12.4.4. állítás

a) pontjában szereplő egyenlőségek nem igazak. Legyen ugyanis S két elemű halmaz és $S = \{a, b\}$, továbbá a $\top$ műveletet úgy értelmezzük S felett, hogy

$$a \top a := b, \quad a \top b := a, \quad b \top a := b, \quad b \top b := a.$$

Ekkor

$$\overset{1+2}{\top} a = \overset{3}{\top} a = (\overset{2}{\top} a) \top a = (a \top a) \top a = b \top a = b,$$
$$(\overset{1}{\top} a) \top (\overset{2}{\top} a) = a \top (a \top a) = a \top b = a,$$

ezért $\overset{1+2}{\top} a \neq (\overset{1}{\top} a) \top (\overset{2}{\top} a)$, továbbá

$$\overset{2\cdot 2}{\top} a = \overset{4}{\top} a = (\overset{3}{\top} a) \top a = ((\overset{2}{\top} a) \top a) \top a = ((a \top a) \top a) \top a = (b \top a) \top a = b \top a = b,$$
$$\overset{2}{\top} (\overset{2}{\top} a) = \overset{2}{\top} (a \top a) = (a \top a) \top (a \top a) = b \top b = a,$$

ezért $\overset{2\cdot 2}{\top} a \neq \overset{2}{\top} (\overset{2}{\top} a)$.

Egyszerű példát adhatunk olyan kommutatív, nem asszociatív magmára, amelyre a 12.4.4. állítás b) pontjában szereplő egyenlőség nem igaz. Legyen ugyanis S két elemű halmaz és $S = \{a, b\}$, továbbá a $\top$ műveletet úgy értelmezzük S felett, hogy

$$a \top a := b, \quad a \top b := b \top a := a, \quad b \top b := a.$$

Ekkor $a \top b = b \top a$ és

$$\overset{2}{\top} (a \top b) = \overset{2}{\top} a = a \top a = b,$$
$$(\overset{2}{\top} a) \top (\overset{2}{\top} b) = (a \top a) \top (b \top b) = b \top a = a,$$

ezért $\overset{2}{\top} (a \top b) \neq (\overset{2}{\top} a) \top (\overset{2}{\top} b)$.

Megjegyezzük, hogy ha $(S, \top)$ félcsoport, és a $\top$ műveletet szorzással jelöljük (ilyenkor azt mondjuk, hogy S multiplikatívan jelölt félcsoport), akkor $s \in S$ és $n \in \mathbb{N}^*$ esetén a $\overset{n}{\top} s$ elemet az s^n szimbólummal jelöljük, így ekkor a 12.4.4. állításban szereplő egyenlőségek így írhatóak: minden $m, n \in \mathbb{N}^*$ esetén

$$s^{m+n} = s^m s^n,$$
$$s^{mn} = (s^m)^n,$$

és ha $s, t \in S$ olyan elemek, hogy $st = ts$, akkor

$$(st)^n = s^n t^n.$$

Ha S multiplikatívan jelölt monoid, akkor ezek az egyenlőségek $m = 0$ vagy $n = 0$ esetén is érvényesek.

12.4.5. Következmény. *Ha $(S, \top)$ félcsoport és $s \in S$, akkor az $\{\overset{n}{\top} s | n \in \mathbb{N}^*\}$ halmaz egyenlő a tartalmazás tekintetében legkisebb s-t tartalmazó részfélcsoporttal.*

Bizonyítás. Az előző állítás a) pontja szerint az $S' := \{\overset{n}{\top} s | n \in \mathbb{N}^*\}$ halmazra $S' \top S' \subseteq S'$ teljesül, mert ha $m, n \in \mathbb{N}^*$, akkor $(\overset{m}{\top} s) \top (\overset{n}{\top} s) = \overset{m+n}{\top} s \in S'$. Továbbá $s = \overset{1}{\top} s \in S'$, tehát S' olyan részfélcsoportja az $(S, \top)$ félcsoportnak, amelyre $s \in S'$. Ha S'' olyan részfélcsoportja az $(S, \top)$ félcsoportnak, amelyre $s \in S''$, akkor minden $n \in \mathbb{N}^*$ esetén $\overset{n}{\top} s \in S''$ (ezért $S' \subseteq S''$), mert ez igaz, ha $n = 1$, hiszen $\overset{1}{\top} s = s \in S''$, továbbá, ha $n \in \mathbb{N}^*$ olyan, hogy $\overset{n}{\top} s \in S''$, akkor $\overset{n+1}{\top} s = (\overset{n}{\top} s) \top s \in S'' \top S'' \subseteq S''$, így $\overset{n+1}{\top} s \in S''$. ■

12.5. Véges műveletek monoidban

12.5.1. Lemma. *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Ha $(s_i)_{i \in I}$ olyan S-ben haladó nem üres, véges rendszer, amelyre minden $i \in I$ esetén $s_i = e$, akkor*

$$\top_{i \in I} s_i = e.$$

Bizonyítás. Az állítást az I indexhalmaz számossága szerinti, 1-től indított teljes indukcióval igazoljuk. Ha $I = \{i_*\}$ egy elemű halmaz, akkor 8.5.4. a) szerint

$$\top_{i \in I} s_i = s_{i_*} = e.$$

Tegyük fel, hogy az állítás igaz minden olyan rendszerre, amelynek indexhalmazának számossága az $n \in \mathbb{N}^*$ természetes szám, és legyen $(s_i)_{i \in I}$ olyan S-ben haladó nem üres, véges rendszer, amelyre minden $i \in I$ esetén $s_i = e$, és $\mathrm{Card}(I) = n + 1$. Legyen $i_* \in I$ rögzített elem és $J := I \setminus \{i_*\}$. Ekkor $I = J \cup \{i_*\}$, és $i_* \notin J$, ezért J olyan nem üres véges halmaz, amelyre $\mathrm{Card}(J) = n$, így 8.5.4. b) szerint

$$\top_{i \in I} s_i = \top_{i \in J \cup \{i_*\}} s_i = \left(\top_{i \in J} s_i \right) \top s_{i_*} = e \top e = e,$$

hiszen az indukciós hipotézis alapján $\top_{i \in J} s_i = e$ és $s_{i_*} = e$. ■

12.5.2. Állítás. *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Ha $(s_i)_{i \in I}$ olyan S-ben haladó nem üres, véges rendszer, amelyre az $\{s_i | i \in I\}$ halmaz kommutatív a $\top$ művelet szerint, és $J \subseteq I$ olyan halmaz, hogy $\{i \in I | s_i \neq e\} \subseteq J$, akkor*

$$\top_{i \in I} s_i = \begin{cases} \top_{i \in J} s_i & , \text{ ha } J \neq \emptyset, \\ e & , \text{ ha } J = \emptyset. \end{cases}$$

Bizonyítás. Ha $J = \emptyset$, akkor minden $i \in I$ indexre $s_i = e$, így az előző lemma szerint $\top_{i \in I} s_i = e$. Tegyük fel, hogy $J \neq \emptyset$. Ha $J = I$, akkor triviális, hogy $\top_{i \in I} s_i = \top_{i \in J} s_i$. Ha $J \neq I$, akkor $I \setminus J \neq \emptyset$, és minden $i \in I \setminus J$ esetén $s_i = e$, ezért 8.5.5. és az előző lemma szerint

$$\top_{i \in I} s_i = \left(\top_{i \in J} s_i \right) \top \left(\top_{i \in I \setminus J} s_i \right) = \left(\top_{i \in J} s_i \right) \top e = \top_{i \in J} s_i. \ \blacksquare$$

Az előző állításból következik, hogy az alábbi definíció nem üres véges indexhalmazú rendszer esetén ugyanazt adja, mint a korábbi definíció (8.5.3.).

12.5.3. Definíció. *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Ha $(s_i)_{i \in I}$ olyan S-ben haladó rendszer, amelyre az $I_* := \{i \in I | s_i \neq e\}$ halmaz véges, és az $\{s_i | i \in I\}$ halmaz kommutatív a $\top$ művelet szerint (vagyis minden $i, j \in I$ esetén $s_i \top s_j = s_j \top s_i$), akkor*

$$\mathop{\top}_{i \in I} s_i := \begin{cases} \mathop{\top}\limits_{i \in I_*} s_i & , \textit{ha } I_* \neq \emptyset, \\ e & , \textit{ha } I_* = \emptyset. \end{cases}$$

Tehát a definíció szerint az üres rendszeren végrehajtott véges művelet eredménye monoidban a neutrális elem. Az is könnyen látható, hogy ha $(S, \top)$ monoid, és $e \in S$ jelöli $\top$ művelet szerinti neutrális elemet, és $(s_i)_{i \in I}$ az a tetszőleges indexhalmazú rendszer, amelyre minden $i \in I$ esetén $s_i = e$, akkor $\mathop{\top}\limits_{i \in I} s_i = e$, mert ekkor $I_* := \{i \in I | s_i \neq e\} = \emptyset$.

12.5.4. Állítás. *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Ha $H \subseteq S$ a $\top$ művelet szerint kommutatív halmaz, akkor a következő állítások ekvivalensek.*

(i) *Minden H-ban haladó $(s_i)_{i \in I}$ véges rendszerre $\mathop{\top}\limits_{i \in I} s_i \in H$.*

(ii) *$H \top H \subseteq H$ (vagyis minden $s, t \in H$ esetén $s \top t \in H$), és $e \in H$.*

Bizonyítás. (i)⇒(ii) Az (i) hipotézis szerint minden H-ban haladó $(s_i)_{i \in I}$ *nem üres* véges rendszerre $\mathop{\top}\limits_{i \in I} s_i \in H$, ezért 8.5.7. szerint $H \top H \subseteq H$. Ugyanakkor (i) szerint $e = \mathop{\top}\limits_{i \in \emptyset} s_i \in H$ is teljesül.

(ii)⇒(i) A (ii) hipotézis szerint $H \top H \subseteq H$, így 8.5.7. alapján minden H-ban haladó $(s_i)_{i \in I}$ *nem üres* véges rendszerre $\mathop{\top}\limits_{i \in I} s_i \in H$. Ugyanakkor (ii) szerint $\mathop{\top}\limits_{i \in \emptyset} s_i = e \in H$ is teljesül. ■

12.5.5. Állítás. *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Legyenek I és i_* olyan halmazok, hogy $i_* \notin I$, valamint legyen $(s_i)_{i \in I \cup \{i_*\}}$ olyan S-ben haladó rendszer, amelyre az $\{i \in I | s_i \neq e\}$ halmaz véges, és az $\{s_i | i \in I \cup \{i_*\}\}$ halmaz kommutatív a $\top$ művelet szerint. Ekkor*

$$\mathop{\top}_{i \in I \cup \{i_*\}} s_i = \left(\mathop{\top}_{i \in I} s_i \right) \top s_{i_*}.$$

Bizonyítás. Legyen $I_* := \{i \in I | s_i \neq e\}$, amely a hipotézis szerint véges halmaz. Két eset lehetséges.

1) Ha $s_{i_*} = e$, akkor $\{i \in I \cup \{s_{i_*}\} | s_i \neq e\} = I_*$, ezért a definíció alapján

$$\mathop{\top}_{i \in I \cup \{i_*\}} s_i = \begin{cases} \mathop{\top}\limits_{i \in I_*} s_i & , \text{ha } I_* \neq \emptyset, \\ e & , \text{ha } I_* = \emptyset. \end{cases}$$

és szintén a definíció alapján itt a jobb oldalon $\mathop{\top}\limits_{i \in I} s_i$ áll, amely $s_{i_*} = e$ miatt egyenlő a $\left(\mathop{\top}\limits_{i \in I} s_i \right) \top s_{i_*}$ elemmel, tehát a bizonyítandó egyenlőség teljesül.

2) Ha $s_{i_*} \neq e$, akkor $\{i \in I \cup \{s_{i_*}\} | s_i \neq e\} = I_* \cup \{i_*\}$ nem üres véges halmaz, ezért a definíció alapján

$$\top_{i \in I \cup \{i_*\}} s_i = \top_{i \in I_* \cup \{i_*\}} s_i .$$

Ha $I_* = \emptyset$, akkor 8.5.4. a) szerint

$$\top_{i \in I_* \cup \{i_*\}} s_i = \top_{i \in \{i_*\}} s_i = s_{i_*},$$

ugyanakkor a definíció szerint $\top_{i \in I} s_i = e$, következésképpen

$$\top_{i \in I_* \cup \{i_*\}} s_i = e \top s_{i_*} = \left(\top_{i \in I} s_i \right) \top s_{i_*},$$

tehát a bizonyítandó egyenlőség teljesül.

Ha $I_* \neq \emptyset$, akkor 8.5.4. b) és a definíció szerint

$$\top_{i \in I_* \cup \{i_*\}} s_i = \left(\top_{i \in I_*} s_i \right) \top s_{i_*} = \left(\top_{i \in I} s_i \right) \top s_{i_*},$$

tehát a bizonyítandó egyenlőség teljesül. ■

12.5.6. Állítás. *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Legyen $(s_i)_{i \in I}$ olyan S-ben haladó rendszer, amelyre az $\{i \in I | s_i \neq e\}$ halmaz véges, és az $\{s_i | i \in I\}$ halmaz kommutatív a $\top$ művelet szerint. Ha $A \subseteq I$ és $B \subseteq I$ diszjunkt részhalmazok, akkor*

$$\top_{i \in A \cup B} s_i = \left(\top_{i \in A} s_i \right) \top \left(\top_{i \in B} s_i \right).$$

Bizonyítás. Legyen $A_* := \{i \in A | s_i \neq e\}$ és $B_* := \{i \in B | s_i \neq e\}$. Mindkettő részhalmaza az $\{i \in I | s_i \neq e\}$ halmaznak, tehát ezek végesek, és $A_* \cap B_* \subseteq A \cap B = \emptyset$ miatt diszjunktak.

Ha $A_* = \emptyset = B_*$, akkor $\{i \in A \cup B | s_i \neq e\} = A_* \cup B_* = \emptyset$, ezért

$$\top_{i \in A \cup B} s_i = e = e \top e = \left(\top_{i \in A} s_i \right) \top \left(\top_{i \in B} s_i \right).$$

Ha $A_* \neq \emptyset$ és $B_* = \emptyset$, akkor $\{i \in A \cup B | s_i \neq e\} = A_* \neq \emptyset$, tehát a definíció szerint

$$\top_{i \in A \cup B} s_i = \top_{i \in A_*} s_i = \top_{i \in A} s_i = \left(\top_{i \in A} s_i \right) \top e = \left(\top_{i \in A} s_i \right) \top \left(\top_{i \in B} s_i \right).$$

Hasonlóan, ha $A_* = \emptyset$ és $B_* \neq \emptyset$, akkor $\{i \in A \cup B | s_i \neq e\} = B_* \neq \emptyset$, ezért

$$\top_{i \in A \cup B} s_i = \top_{i \in B_*} s_i = \top_{i \in B} s_i = e \top \left(\top_{i \in B} s_i \right) = \left(\top_{i \in A} s_i \right) \top \left(\top_{i \in B} s_i \right).$$

Végül, ha $A_* \neq \emptyset \neq B_*$, akkor $\{i \in A \cup B | s_i \neq e\} = A_* \cup B_* \neq \emptyset$, ezért 8.5.5. alapján

$$\top_{i \in A \cup B} s_i = \top_{i \in A_* \cup B_*} s_i = \left(\top_{i \in A_*} s_i \right) \top \left(\top_{i \in B_*} s_i \right) = \left(\top_{i \in A} s_i \right) \top \left(\top_{i \in B} s_i \right),$$

hiszen A_* és B_* nem üres véges halmazok és $A_* \cap B_* = \emptyset$. ■

12.5.7. Állítás. *Legyen* $(S, \top)$ *monoid, és jelölje* $e \in S$ *a* $\top$ *művelet szerinti neutrális elemet. Legyenek* $(s_i)_{i\in I}$ *és* $(t_j)_{j\in J}$ *olyan* S*-ben haladó rendszerek, amelyekre az* $\{i \in I | s_i \neq e\}$ *és* $\{j \in J | t_i \neq e\}$ *halmazok végesek, valamint az* $\{s_i | i \in I\}$ *és* $\{t_j | j \in J\}$ *halmazok kommutatívak a* $\top$ *művelet szerint. Ha minden* $(i, j) \in I \times J$ *esetén* $s_i \top t_j = t_j \top s_i$*, akkor*

$$\left(\top_{i\in I} s_i\right) \top \left(\top_{j\in J} t_j\right) = \left(\top_{j\in J} t_j\right) \top \left(\top_{i\in I} s_i\right).$$

Bizonyítás. (I) Először azt mutatjuk meg, hogy ha $s \in S$ olyan, hogy minden $j \in J$ esetén $s \top t_j = t_j \top s$, akkor $s \top \left(\top_{j\in J} t_j\right) = \left(\top_{j\in J} t_j\right) \top s$. Ez nyilvánvalóan igaz, ha $J_* := \{j \in J | t_i \neq e\} = \emptyset$, mert ekkor $\top_{j\in J} t_j = e$, és $s \top e = s = e \top s$. Ha pedig $J_* \neq \emptyset$, akkor $\top_{j\in J} t_j = \top_{j\in J_*} t_j$, és J_* nem üres véges halmaz, így 8.5.8. alapján

$$s \top \left(\top_{j\in J} t_j\right) = s \top \left(\top_{j\in J_*} t_j\right) = \left(\top_{j\in J_*} t_j\right) \top s = \left(\top_{j\in J} t_j\right) \top s.$$

(II) Az általános esetben (I)-t alkalmazva $i \in I$ esetén az $s := s_i$ választással kapjuk, hogy $s_i \top \left(\top_{j\in J} t_j\right) = \left(\top_{j\in J} t_j\right) \top s_i$. Ezután bevezetve az $s := \top_{j\in J} t_j$, és a $(t_j)_{j\in J}$ rendszer helyére az $(s_i)_{i\in I}$ rendszert helyettesítve (I)-ből kapjuk, hogy $s \top \left(\top_{i\in I} s_i\right) = \left(\top_{i\in I} s_i\right) \top s$, amit bizonyítani kellett. ■

12.5.8. Következmény. *Legyen* $(S, \top)$ *monoid, és jelölje* $e \in S$ *a* $\top$ *művelet szerinti neutrális elemet. Legyenek* $(s_i)_{i\in I}$ *és* $(t_i)_{i\in I}$ *olyan* S*-ben haladó (ugyanolyan indexhalmazú) rendszerek, amelyekre az* $\{i \in I | s_i \neq e\}$ *és* $\{i \in I | t_i \neq e\}$ *halmazok végesek, valamint az* $\{s_i | i \in I\} \cup \{t_i | i \in I\}$ *halmaz kommutatív a* $\top$ *művelet szerint. Ekkor az* $\{s_i \top t_i | i \in I\}$ *halmaz a* $\top$ *művelet szerint kommutatív és*

$$\top_{i\in I} (s_i \top t_i) = \left(\top_{i\in I} s_i\right) \top \left(\top_{i\in I} t_i\right).$$

Bizonyítás. Az $\{s_i | i \in I\} \cup \{t_i | i \in I\}$ halmaz $\top$ művelet szerint kommutativitását és a $\top$ művelet asszociativitását alkalmazva kapjuk, hogy minden $i, j \in I$ esetén

$$\begin{aligned}
(s_i \top t_i) \top (s_j \top t_j) &= (s_i \top (t_i \top s_j)) \top t_j \overset{(*)}{=} (s_i \top (s_j \top t_i)) \top t_j = \\
&= ((s_i \top s_j) \top t_i) \top t_j \overset{(*)}{=} ((s_j \top s_i) \top t_i) \top t_j = (s_j \top (s_i \top t_i)) \top t_j = \\
&= s_j \top ((s_i \top t_i) \top t_j) = s_j \top (s_i \top (t_i \top t_j)) \overset{(*)}{=} s_j \top (s_i \top (t_j \top t_i)) = \\
&= s_j \top ((s_i \top t_j) \top t_i) \overset{(*)}{=} s_j \top ((t_j \top s_i) \top t_i) = (s_j \top (t_j \top s_i)) \top t_i = \\
&= ((s_j \top t_j) \top s_i) \top t_i = (s_j \top t_j) \top (s_i \top t_i),
\end{aligned}$$

ahol a $\overset{(*)}{=}$ egyenlőségeknél az $\{s_i | i \in I\} \cup \{t_i | i \in I\}$ halmaz $\top$ művelet szerint kommutativitását, míg a többi egyenlőségnél a $\top$ művelet asszociativitását alkalmaztuk.

Vezessük be az

$$I_s := \{i \in I | s_i \neq e\}, \quad I_t := \{i \in I | t_i \neq e\}$$

halmazokat, amelyek a hipotézis szerint végesek. Ekkor az $I_* := I_s \cup I_t$ halmaz véges (8.1.12.), és két eset lehetséges.

1) $I_* = \emptyset$. Ekkor $I_s = \emptyset = I_t$, vagyis minden $i \in I$ esetén $s_i = e = t_i$, így $s_i \top t_i = e \top e = e$ teljesül, tehát 12.5.1. alapján

$$\mathop{\top}_{i\in I}(s_i \top t_i) = e = e \top e = \left(\mathop{\top}_{i\in I} s_i\right) \top \left(\mathop{\top}_{i\in I} t_i\right).$$

2) $I_* \neq \emptyset$. Ekkor I_* nem üres véges halmaz, így az 8.5.9. állításból következik, hogy

$$\mathop{\top}_{i\in I_*}(s_i \top t_i) = \left(\mathop{\top}_{i\in I_*} s_i\right) \top \left(\mathop{\top}_{i\in I_*} t_i\right). \tag{$*$}$$

Világos, hogy $I_s \subseteq I_*$ és $I_t \subseteq I_*$ és $\{i \in I | s_i \top t_i \neq e\} \subseteq I_*$, hiszen ha $i \in I \setminus I_*$, akkor $s_i = e = t_i$, tehát $s_i \top t_i = e \top e = e$. Ezért

$$\mathop{\top}_{i\in I} s_i = \mathop{\top}_{i\in I_*} s_i, \quad \mathop{\top}_{i\in I} t_i = \mathop{\top}_{i\in I_*} t_i, \quad \mathop{\top}_{i\in I}(s_i \top t_i) = \mathop{\top}_{i\in I_*}(s_i \top t_i),$$

amiből a $(*)$ egyenlőség alapján következik a bizonyítandó egyenlőség. ■

12.5.9. Tétel. (**A véges műveletek általános kommutativitása monoidban**) *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Legyen $(s_i)_{i\in I}$ olyan S-ben haladó rendszer, amelyre az $\{i \in I | s_i \neq e\}$ halmaz véges, és az $\{s_i | i \in I\}$ halmaz kommutatív a $\top$ művelet szerint. Ha J halmaz és $\sigma : J \to I$ bijekció, akkor a $\{j \in J | s_{\sigma(j)} \neq e\}$ halmaz véges, és az $\{s_{\sigma(j)} | j \in J\}$ halmaz kommutatív a $\top$ művelet szerint, valamint*

$$\mathop{\top}_{i\in I} s_i = \mathop{\top}_{j\in J} s_{\sigma(j)}.$$

Bizonyítás. Legyen $I_* := \{i \in I | s_i \neq e\}$ és $J_* := \{j \in J | s_{\sigma(j)} \neq e\}$. Világos, hogy $J_* = \overset{-1}{\sigma}\langle I_*\rangle = \sigma^{-1}\langle I_*\rangle$, ezért J_* véges halmaz (8.1.11.). Nyilvánvaló, hogy $\{s_{\sigma(j)} | j \in J\} = \{s_i | i \in I\}$, ezért az $\{s_{\sigma(j)} | j \in J\}$ halmaz is kommutatív a $\top$ művelet szerint.

Ha $I_* = \emptyset$, akkor $J_* = \emptyset$, így a definíció szerint

$$\mathop{\top}_{i\in I} s_i = e = \mathop{\top}_{j\in J} s_{\sigma(j)}.$$

Ha $I_* \neq \emptyset$, akkor $J_* \neq \emptyset$, így a definíció és 8.6.1. szerint

$$\mathop{\top}_{i\in I} s_i = \mathop{\top}_{i\in I_*} s_i = \mathop{\top}_{j\in J_*} s_{\sigma_*(j)} = \mathop{\top}_{j\in J} s_{\sigma(j)},$$

ahol σ_* jelöli a σ bijekció leszűkítését J_*, tehát $\sigma_* : J_* \to I_*$ bijekció. ■

12.5.10. Tétel. (**A véges műveletek általános asszociativitása monoidban I.**) *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Legyen I halmaz és $(I_j)_{j\in J}$ olyan diszjunkt halmazrendszer, hogy $I = \bigcup_{j\in J} I_j$. Legyen $(s_i)_{i\in I}$ olyan*

S-ben haladó rendszer, amelyre az $\{i \in I | s_i \neq e\}$ halmaz véges, és az $\{s_i | i \in I\}$ halmaz kommutatív a $\top$ művelet szerint. Ekkor

– minden $j \in J$ esetén az $\{i \in I_j | s_i \neq e\}$ halmaz véges, és az $\{s_i | i \in I_j\}$ halmaz kommutatív a $\top$ művelet szerint, így jól értelmezett a $\top_{i \in I_j} s_i$ elem;

– a $\left\{ j \in J \;\middle|\; \top_{i \in I_j} s_i \neq e \right\}$ halmaz véges, és a $\left\{ \top_{i \in I_j} s_i \;\middle|\; j \in J \right\}$ halmaz kommutatív a $\top$ művelet szerint, és

$$\top_{i \in I} s_i = \top_{j \in J} \left(\top_{i \in I_j} s_i \right).$$

Bizonyítás. Legyen $I_* := \{i \in I | s_i \neq e\}$, és minden $j \in J$ esetén $(I_j)_* := \{i \in I_j | s_i \neq e\}$. Mivel minden $j \in J$ esetén $I_j \subseteq I$, így $(I_j)_* \subseteq I_*$, tehát $(I_j)_*$ véges halmaz, továbbá $\{s_i | i \in I_j\} \subseteq \{s_i | i \in I\}$, tehát az $\{s_i | i \in I_j\}$ halmaz kommutatív a $\top$ művelet szerint.

Legyen $J_* := \left\{ j \in J \;\middle|\; \top_{i \in I_j} s_i \neq e \right\}$. Ha $j \in J_*$, akkor $\top_{i \in I_j} s_i \neq e$, következésképpen létezik olyan $i \in I_j$, amelyre $s_i \neq e$, tehát $I_j \cap I_* \neq \emptyset$. Ez azt jelenti, hogy ha $\tilde{J} := \{j \in J | I_j \cap I_* \neq \emptyset\}$, akkor $J_* \subseteq \tilde{J}$. Kiválasztva egy

$$f \in \prod_{j \in \tilde{J}} (I_j \cap I_*)$$

függvényt, azt kapjuk, hogy $f : \tilde{J} \to I_*$ *injekció*, mert az $(I_j)_{j \in J}$ halmazrendszer diszjunkt. Ezért az I_* halmaz végességéből következik, hogy $\tilde{J}$ véges, így J_* is véges.

Ha $j, j' \in J$ és $j \neq j'$, akkor az I_j és $I_{j'}$ indexhalmazok diszjunktak, ezért 12.5.6. alapján

$$\left(\top_{i \in I_j} s_i \right) \top \left(\top_{i \in I_{j'}} s_i \right) = \top_{i \in I_j \cup I_{j'}} s_i = \top_{i \in I_{j'} \cup I_j} s_i = \left(\top_{i \in I_{j'}} s_i \right) \top \left(\top_{i \in I_j} s_i \right),$$

tehát a $\left\{ \top_{i \in I_j} s_i \;\middle|\; j \in J \right\}$ halmaz kommutatív a $\top$ művelet szerint.

Az egyenlőség bizonyításához az imént bevezetett I_*, $(I_j)_*$, J_* és $\tilde{J}$ halmazokat alkalmazzuk, és először megjegyezzük, hogy a definíciók alapján nyilvánvalóan minden $j \in J$ indexre $I_j \cap I_* = (I_j)_*$, következésképpen $j \in \tilde{J}$ esetén

$$\top_{i \in I_j} s_i = \top_{i \in (I_j)_*} s_i = \top_{i \in I_j \cap I_*} s_i.$$

Ha $I_* = \emptyset$, akkor minden $j \in J$ esetén $I_j \cap I_* = \emptyset$, ezért $\tilde{J} = \emptyset$, így $J_* = \emptyset$. Ebből következik, hogy ha $I_* = \emptyset$, akkor

$$\top_{i \in I} s_i = e = \top_{j \in J} \left(\top_{i \in I_j} s_i \right).$$

Tegyük fel, hogy $I_* \neq \emptyset$. Világos, hogy $I_* = \bigcup_{i \in \tilde{J}} (I_j \cap I_*)$, tehát $(I_j \cap I_*)_{j \in \tilde{J}}$ nem üres véges partíciója az I_* nem üres véges halmaznak. Ebből 8.7.1. alapján kapjuk, hogy

$$\top_{i \in I} s_i = \top_{i \in I_*} s_i = \top_{j \in \tilde{J}} \left(\top_{i \in I_j \cap I_*} s_i \right) = \top_{j \in \tilde{J}} \left(\top_{i \in (I_j)_*} s_i \right) = \top_{j \in \tilde{J}} \left(\top_{i \in I_j} s_i \right).$$

A 12.5.6. állítás alapján

$$\top_{j\in\tilde J}\left(\top_{i\in I_j} s_i\right) = \left(\top_{j\in J_*}\left(\top_{i\in I_j} s_i\right)\right)\top\left(\top_{j\in\tilde J\setminus J_*}\left(\top_{i\in I_j} s_i\right)\right) =$$
$$= \left(\top_{j\in J_*}\left(\top_{i\in I_j} s_i\right)\right)\top e = \left(\top_{j\in J_*}\left(\top_{i\in I_j} s_i\right)\right) = \top_{j\in J}\left(\top_{i\in I_j} s_i\right),$$

mert minden $j \in \tilde J \setminus J_*$ esetén $\top_{i\in I_j} s_i = e$. (Itt $\tilde J \setminus J_* \neq \emptyset$ *lehetséges*, mert attól, hogy egy $j \in J$ esetén van olyan $i \in I_j$, hogy $s_i \neq e$ (azaz $j \in \tilde J$), még előfordulhat, hogy $\top_{i\in I_j} s_i = e$, vagyis $j \notin J_*$.) ■

12.5.11. Következmény. *Legyen $(S,\top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Legyenek I, J halmazok és $(s_{i,j})_{(i,j)\in I\times J}$ olyan S-ben haladó rendszer, amelyre az $\{(i,j) \in I \times J | s_{i,j} \neq e\}$ halmaz véges, és az $\{s_{i,j} | (i \in I) \wedge (j \in J)\}$ halmaz kommutatív a $\top$ művelet szerint. Ekkor*

a) *minden $i \in I$ esetén az $\{j \in J | s_{i,j} \neq e\}$ halmaz véges, és az $\{s_{i,j} | j \in J\}$ halmaz kommutatív a $\top$ művelet szerint, így jól értelmezett a $\top_{j\in J} s_{i,j}$ elem;*

b) *a $\left\{i \in I \,\middle|\, \top_{j\in J} s_{i,j} \neq e\right\}$ halmaz véges, és a $\left\{\top_{j\in J} s_{i,j} \,\middle|\, i \in I\right\}$ halmaz kommutatív a $\top$ művelet szerint;*

a′) *minden $j \in J$ esetén az $\{i \in I | s_{i,j} \neq e\}$ halmaz véges, és az $\{s_{i,j} | i \in I\}$ halmaz kommutatív a $\top$ művelet szerint, így jól értelmezett a $\top_{i\in I} s_{i,j}$ elem;*

b′) *a $\left\{j \in J \,\middle|\, \top_{i\in I} s_{i,j} \neq e\right\}$ halmaz véges, és a $\left\{\top_{i\in I} s_{i,j} \,\middle|\, j \in J\right\}$ halmaz kommutatív a $\top$ művelet szerint, továbbá fennállnak a*

$$\top_{i\in I}\left(\top_{j\in J} s_{i,j}\right) = \top_{(i,j)\in I\times J} s_{i,j} = \top_{j\in J}\left(\top_{i\in I} s_{i,j}\right)$$

egyenlőségek.

Bizonyítás. Legyen $S_* := \{s_{i,j} | (i \in I) \wedge (j \in J)\}$, amely a hipotézis szerint kommutatív halmaz a $\top$ művelet szerint, és $R := \{(i,j) \in I \times J | s_{i,j} \neq e\}$, amely a hipotézis szerint véges halmaz.

a) Ha $i \in I$, akkor $\{j \in J | s_{i,j} \neq e\} \subseteq \mathrm{pr}_2 R$, és a $\mathrm{pr}_2 R$ projekció véges halmaz, mert megegyezik az R véges reláció $R \to \mathrm{pr}_2 R$; $(i',j) \mapsto j$ függvény által létesített képével. Ezért minden $i \in I$ esetén az $\{j \in J | s_{i,j} \neq e\}$ halmaz véges. Ugyanakkor, minden $i \in I$ esetén $\{s_{i,j} | j \in J\} \subseteq S_*$, ezért az $\{s_{i,j} | j \in J\}$ halmaz is kommutatív a $\top$ művelet szerint.

b) Ha $i \in I$ olyan, hogy $\top_{j\in J} s_{i,j} \neq e$, akkor létezik olyan $j \in J$, hogy $s_{i,j} \neq e$, tehát $(i,j) \in R$, következésképpen $i \in \mathrm{pr}_1 R$. Ez azt jelenti, hogy $\left\{i \in I \,\middle|\, \top_{j\in J} s_{i,j} \neq e\right\} \subseteq \mathrm{pr}_1 R$, és a $\mathrm{pr}_1 R$ projekció véges halmaz, mert megegyezik az R véges reláció $R \to \mathrm{pr}_1 R$; $(i,j) \mapsto i$ függvény által létesített képével, ezért az $\left\{i \in I \,\middle|\, \top_{j\in J} s_{i,j} \neq e\right\}$ halmaz véges.

a′) Ha $j \in J$, akkor $\{i \in I | s_{i,j} \neq e\} \subseteq \mathrm{pr}_1 R$, és a $\mathrm{pr}_1 R$ projekció véges halmaz, ezért az $\{i \in I | s_{i,j} \neq e\}$ halmaz véges. Ugyanakkor, minden $j \in J$ esetén $\{s_{i,j} | i \in I\} \subseteq S_*$, ezért az $\{s_{i,j} | i \in I\}$ halmaz is kommutatív a $\top$ művelet szerint.

b′) Ha $j \in J$ olyan, hogy $\top_{i\in I} s_{i,j} \neq e$, akkor létezik olyan $i \in I$, hogy $s_{i,j} \neq e$, tehát $(i,j) \in R$, következésképpen $j \in \mathrm{pr}_2 R$. Ez azt jelenti, hogy $\left\{ j \in J \,\middle|\, \top_{i\in I} s_{i,j} \neq e \right\} \subseteq \mathrm{pr}_2 R$, és a $\mathrm{pr}_2 R$ projekció véges halmaz, ezért az $\left\{ j \in J \,\middle|\, \top_{i\in I} s_{i,j} \neq e \right\}$ halmaz véges.

Az $(\{i\} \times J)_{i\in I}$ rendszer diszjunkt és $\bigcup_{i\in I} (\{i\} \times J) = I \times J$, ezért a $\top$ művelet általános asszociativitása (12.5.10.) alapján

$$\top_{(i,j)\in I\times J} s_{i,j} = \top_{i\in I} \left(\top_{x\in\{i\}\times J} s_x \right) = \top_{i\in I} \left(\top_{j\in J} s_{i,j} \right),$$

ahol a második egyenlőségnél a $\top$ művelet általános kommutativitását (12.5.9.) alkalmazzuk minden $i \in I$ esetén a $J \to \{i\} \times J;\ j \mapsto (i,j)$ bijekcióra.

Az $(I \times \{j\})_{j\in J}$ rendszer diszjunkt és $\bigcup_{j\in J} (I \times \{j\}) = I \times J$, ezért a $\top$ művelet általános asszociativitása (12.5.10.) alapján

$$\top_{(i,j)\in I\times J} s_{i,j} = \top_{j\in J} \left(\top_{x\in I\times\{j\}} s_x \right) = \top_{j\in J} \left(\top_{i\in I} s_{i,j} \right),$$

ahol a második egyenlőségnél a $\top$ művelet általános kommutativitását (12.5.9.) alkalmazzuk minden $j \in J$ esetén az $I \to I \times \{j\};\ i \mapsto (i,j)$ bijekcióra. ∎

A 12.5.10. tételben az $(I_j)_{j\in J}$ halmazrendszer *diszjunkt*, és az uniója egyenlő I-vel, és I *egyenlő* az $(s_i)_{i\in I}$ rendszer indexhalmazával. Azonban sokszor előfordul, hogy az $(I_j)_{j\in J}$ halmazrendszer *nem diszjunkt*, és nem olyan rendszeren végezzük el a véges műveletet, amelynek indexhalmaza egyenlő $I := \bigcup_{j\in J} I_j$-vel. E helyett egy olyan $(s_j)_{j\in J}$ függvényrendszer áll a rendelkezésünkre, amelyre minden $j \in J$ esetén s_j olyan S-ben haladó rendszer, amelynek I_j indexhalmaza úgy függhet j-től, hogy az s_j rendszerek szükségképpen ragaszthatók össze, mert előfordulhat, hogy léteznek olyan $j, j' \in J$ indexek, amelyekre $s_j \neq s_{j'}$ a $I_j \cap I_{j'}$ halmazon. Ilyen esetre vonatkozik az általános asszociativitás tételének következő formája.

12.5.12. Tétel. (**A véges műveletek általános asszociativitása monoidban II.**) *Legyen $(S, \top)$ monoid, és jelölje $e \in S$ a $\top$ művelet szerinti neutrális elemet. Legyen $(s_j)_{j\in J}$ olyan rendszer, amelyre minden $j \in J$ esetén s_j egy S-ben haladó rendszer, amelyre $I_j := \mathrm{Dom}(s_j)$, és minden $i \in I_j$ esetén $s_{i,j} := s_j(i)$. Legyen $I := \bigcup_{j\in J} I_j$ és minden $i \in I$ esetén $J_i := \{j \in J | i \in I_j\}$. Ha az $\{(i,j) | (j \in J) \wedge (i \in I_j) \wedge (s_{i,j} \neq e)\}$ halmaz véges, és az $\{s_{i,j} | (j \in J) \wedge (i \in I_j)\}$ halmaz kommutatív a $\top$ művelet szerint, akkor:*

a) *minden $i \in I$ esetén a $\{j \in J_i | s_{i,j} \neq e\}$ halmaz véges, és az $\{s_{i,j} | j \in J_i\}$ halmaz kommutatív a $\top$ művelet szerint, így jól értelmezett a $\top_{j\in J_i} s_{i,j}$ elem;*

b) *az* $\left\{i\in I \;\middle|\; \top_{j\in J_i} s_{i,j}\neq e\right\}$ *halmaz véges, és a* $\left\{\top_{j\in J_i} s_{i,j} \;\middle|\; i\in I\right\}$ *halmaz kommutatív a* $\top$ *művelet szerint, így jól értelmezett a* $\top_{i\in I}\left(\top_{j\in J_i} s_{i,j}\right)$ *elem;*

a′) *minden* $j\in J$ *esetén az* $\{i\in I_j|s_{i,j}\neq e\}$ *halmaz véges, és az* $\{s_{i,j}|i\in I_j\}$ *halmaz kommutatív a* $\top$ *művelet szerint, így jól értelmezett a* $\top_{i\in I_j} s_{i,j}$ *elem;*

b′) *a* $\left\{j\in J \;\middle|\; \top_{i\in I_j} s_{i,j}\neq e\right\}$ *halmaz véges, és a* $\left\{\top_{i\in I_j} s_{i,j} \;\middle|\; j\in J\right\}$ *halmaz kommutatív a* $\top$ *művelet szerint, így jól értelmezett a* $\top_{j\in J}\left(\top_{i\in I_j} s_{i,j}\right)$ *elem;*

valamint fennáll a

$$\top_{j\in J}\left(\top_{i\in I_j} s_{i,j}\right)=\top_{i\in I}\left(\top_{j\in J_i} s_{i,j}\right).$$

egyenlőség.

Bizonyítás. Legyen $S_*:=\{s_{i,j}|(j\in J)\wedge(i\in I_j)\}$, amely a hipotézis szerint kommutatív halmaz a $\top$ művelet szerint, és $R:=\{(i,j)|(j\in J)\wedge(i\in I_j)\wedge(s_{i,j}\neq e)\}$, amely a hipotézis szerint véges halmaz.

Ha $i\in I$, akkor $\{j\in J_i|s_{i,j}\neq e\}\subseteq \mathrm{pr}_2R$, és a pr_2R projekció véges halmaz, mert megegyezik az R véges reláció $R\to\mathrm{pr}_2R;\ (i',j)\mapsto j$ függvény által létesített képével. Ezért minden $i\in I$ esetén az $\{j\in J_i|s_{i,j}\neq e\}$ halmaz véges. Ugyanakkor, minden $i\in I$ esetén $\{s_{i,j}|j\in J_i\}\subseteq S_*$, ezért az $\{s_{i,j}|j\in J_i\}$ halmaz is kommutatív a $\top$ művelet szerint.

b) Ha $i\in I$ olyan, hogy $\top_{j\in J_i} s_{i,j}\neq e$, akkor létezik olyan $j\in J_i$, hogy $s_{i,j}\neq e$, tehát $(i,j)\in R$, következésképpen $i\in\mathrm{pr}_1R$. Ez azt jelenti, hogy $\left\{i\in I \;\middle|\; \top_{j\in J_i} s_{i,j}\neq e\right\}\subseteq \mathrm{pr}_1R$, és a pr_1R projekció véges halmaz, mert megegyezik az R véges reláció $R\to\mathrm{pr}_1R;\ (i,j)\mapsto i$ függvény által létesített képével, ezért az $\left\{i\in I \;\middle|\; \top_{j\in J_i} s_{i,j}\neq e\right\}$ halmaz véges.

a′) Ha $j\in J$, akkor $\{i\in I_j|s_{i,j}\neq e\}\subseteq\mathrm{pr}_1R$, és a pr_1R projekció véges halmaz, ezért az $\{i\in I_j|s_{i,j}\neq e\}$ halmaz véges. Ugyanakkor, minden $j\in J$ esetén $\{s_{i,j}|i\in I_j\}\subseteq S_*$, ezért az $\{s_{i,j}|i\in I_j\}$ halmaz is kommutatív a $\top$ művelet szerint.

b′) Ha $j\in J$ olyan, hogy $\top_{i\in I_j} s_{i,j}\neq e$, akkor létezik olyan $i\in I_j$, hogy $s_{i,j}\neq e$, tehát $(i,j)\in R$, következésképpen $j\in\mathrm{pr}_2R$. Ez azt jelenti, hogy $\left\{j\in J \;\middle|\; \top_{i\in I_j} s_{i,j}\neq e\right\}\subseteq \mathrm{pr}_2R$, és a pr_2R projekció véges halmaz, ezért az $\left\{j\in J \;\middle|\; \top_{i\in I_j} s_{i,j}\neq e\right\}$ halmaz véges.

Most vezessük be a

$$I\times J\to S;\quad (i,j)\mapsto s'_{i,j}:=\begin{cases} s_{i,j} & ,\text{ ha } i\in I_j\\ e & ,\text{ ha } i\notin I_j\end{cases}$$

függvényt. Ekkor 12.5.11. alkalmazásával kapjuk, hogy

$$\top_{j\in J}\left(\top_{i\in I} s'_{i,j}\right)=\top_{i\in I}\left(\top_{j\in J} s'_{i,j}\right).$$

Legyen $i \in I$. Ekkor 12.5.6. alapján

$$\top_{j \in J} s'_{i,j} = \left(\top_{j \in J_i} s'_(i,j) \right) \top \left(\top_{j \in J \setminus J_i} s'_{i,j} \right),$$

és $j \in J_i$ esetén $i \in I_j$, tehát $s'_{i,j}) = s_{i,j}$, míg $j \in J \setminus J_i$ esetén $i \notin J_i$, tehát $s'_{i,j} = e$, ezért

$$\top_{j \in J_i} s'_{i,j} = \top_{j \in J_i} s_{i,j}, \qquad \top_{j \in J \setminus J_i} s'_{i,j} = e,$$

amiből következik, hogy

$$\top_{j \in J} s'_{i,j} = \left(\top_{j \in J_i} s_{i,j} \right) \top e = \top_{j \in J_i} s_{i,j}.$$

Legyen $j \in J$. Ekkor 12.5.6. alapján

$$\top_{i \in I} s'_{i,j} = \left(\top_{i \in I_j} s'_{i,j} \right) \top \left(\top_{i \in I \setminus I_j} s'_{i,j} \right),$$

és $i \in I_j$ esetén $s'_{i,j} = s_{i,j}$, míg $i \in I \setminus I_j$ esetén $s'_{i,j} = e$, tehát

$$\top_{i \in I_j} s'_{i,j} = \top_{i \in I_j} s_{i,j}, \qquad \top_{i \in I \setminus I_j} s'_{i,j} = e,$$

amiből következik, hogy

$$\top_{i \in I} s'_{i,j} = \left(\top_{i \in I_j} s_{i,j} \right) \top e = \top_{i \in I_j} s_{i,j}.$$

Ezzel megmutattuk, hogy

$$\top_{j \in J} \left(\top_{i \in I_j} s_{i,j} \right) = \top_{j \in J} \left(\top_{i \in I} s'_{i,j} \right) = \top_{i \in I} \left(\top_{j \in J} s'_{i,j} \right) = \top_{i \in I} \left(\top_{j \in J_i} s_{i,j} \right). \blacksquare$$

12.5.13. Lemma. *Legyen $(S, \top)$ félcsoport. Ha $n \in \mathbb{N}^*$, akkor minden S-ben haladó $(s_k)_{k \in [\![0,n]\!]}$ rendszerre és $m < n$ természetes számra*

$$\top_{k=0}^{n} s_k = \left(\top_{k=0}^{m} s_k \right) \top \left(\top_{k=m+1}^{n} s_k \right).$$

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk.

Ha $n = 1$, akkor $m = 0$, és 8.3.5. a) alkalmazásával

$$\top_{k=0}^{n} s_k = \top_{k=0}^{1} s_k = s_0 \top s_1 = \left(\top_{k=0}^{0} s_k \right) \top \left(\top_{k=1}^{1} s_k \right) = \left(\top_{k=0}^{m} s_k \right) \top \left(\top_{k=m+1}^{n} s_k \right),$$

adódik, tehát az állítás igaz.

Tegyük fel, hogy az állítás igaz az $n \in \mathbb{N}^*$ számra, és legyen $(s_i)_{i \in [\![0,n+1]\!]}$ tetszőleges S-ben haladó rendszer. Ekkor 8.3.5. b) alapján

$$\top_{k=0}^{n+1} s_k = \left(\top_{k=0}^{n} s_k \right) \top s_{n+1}. \tag{1}$$

Legyen $m < n+1$ természetes szám: ekkor két eset lehetséges.

Tegyük fel, hogy $m < n$. Ekkor

$$\mathop{\top}_{k=0}^{n+1} s_k \overset{(1)}{=} \left(\left(\mathop{\top}_{k=0}^{m} s_k\right) \top \left(\mathop{\top}_{k=m+1}^{n} s_k\right)\right) \top s_{n+1} \overset{(2)}{=}$$
$$\overset{(2)}{=} \left(\mathop{\top}_{k=0}^{m} s_k\right) \top \left(\left(\mathop{\top}_{k=m+1}^{n} s_k\right) \top s_{n+1}\right) \overset{(3)}{=} \left(\mathop{\top}_{k=0}^{m} s_k\right) \top \left(\mathop{\top}_{k=m+1}^{n+1} s_k\right),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél az (1) összefüggést és az indukciós hipotézist alkalmaztuk az $(s_k)_{k\in[\![0,n]\!]}$ rendszerre és $m < n$ természetes számra;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk a $\top$ művelet asszociativitását;

– a $\overset{(3)}{=}$ egyenlőségnél ismét 8.3.5. b)-t alkalmaztuk.

Tegyük fel, hogy $m = n$. Ekkor 8.3.5. a) szerint $s_{n+1} = \mathop{\top}_{k=m+1}^{n+1} s_k$, ezért (1) alapján

$$\mathop{\top}_{k=0}^{n+1} s_k = \left(\mathop{\top}_{k=0}^{n} s_k\right) \top s_{n+1} = \left(\mathop{\top}_{k=0}^{m} s_k\right) \top \left(\mathop{\top}_{k=m+1}^{n+1} s_k\right).$$

Tehát a bizonyítandó egyenlőség az $n+1$ természetes számra is igaz. ■

12.5.14. Állítás. *Legyen $(S, \top)$ monoid. Ha $n \in \mathbb{N}$ és $(s_k)_{k\in[\![0,n]\!]}$ olyan S-ben haladó rendszer, hogy minden $k \in [\![0,n]\!]$ esetén s_k invertálható a $\top$ művelet szerint, akkor $\mathop{\top}_{k=0}^{n} s_k$ is invertálható a $\top$ művelet szerint, és*

$$\left(\mathop{\top}_{k=0}^{n} s_k\right)^{-1} = \mathop{\top}_{k=0}^{n} s_{n-k}^{-1}.$$

Bizonyítás. Jelölje e az $(S, \top)$ monoid neutrális elemét. Az állítást n szerinti teljes indukcióval bizonyítjuk.

Ha $n = 0$, akkor az állítás 8.3.5. a) alapján triviálisan igaz, hiszen $\mathop{\top}_{k=0}^{0} s_k = s_0$ és $\mathop{\top}_{k=0}^{0} s_0^{-1} = s_0^{-1}$. Tegyük fel, hogy $n \in \mathbb{N}$ olyan szám, amelyre az állítás igaz, és legyen $(s_k)_{k\in[\![0,n+1]\!]}$ olyan S-ben haladó rendszer, hogy minden $k \in [\![0,n+1]\!]$ esetén s_k invertálható a $\top$ művelet szerint. Ekkor

$$\left(\mathop{\top}_{k=0}^{n+1} s_k\right) \top \left(\mathop{\top}_{k=0}^{n+1} s_{n+1-k}^{-1}\right) \overset{(1)}{=} \left(\left(\mathop{\top}_{k=0}^{n} s_k\right) \top s_{n+1}\right) \top \left(s_{n+1}^{-1} \top \left(\mathop{\top}_{k=1}^{n+1} s_{n+1-k}^{-1}\right)\right) \overset{(2)}{=}$$
$$\overset{(2)}{=} \left(\mathop{\top}_{k=0}^{n} s_k\right) \top \left(s_{n+1} \top s_{n+1}^{-1}\right) \top \left(\mathop{\top}_{k=1}^{n+1} s_{n+1-k}^{-1}\right) = \left(\mathop{\top}_{k=0}^{n} s_k\right) \top e \top \left(\mathop{\top}_{k=1}^{n+1} s_{n+1-k}^{-1}\right) \overset{(3)}{=}$$
$$\overset{(3)}{=} \left(\mathop{\top}_{k=0}^{n} s_k\right) \top \left(\mathop{\top}_{k=0}^{n} s_{n-k}^{-1}\right) \overset{(4)}{=} \left(\mathop{\top}_{k=0}^{n} s_k\right) \top \left(\mathop{\top}_{k=0}^{n} s_k\right)^{-1} = e,$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk a 8.3.5. a) és b) állítást, és az előző lemmát;

– a $\overset{(2)}{=}$ egyenlőségnél alkalmaztuk a $\top$ művelet asszociativitását;

– a $\overset{(3)}{=}$ egyenlőségnél a 8.3.4. állításra hivatkoztunk;

– a $\overset{(4)}{=}$ egyenlőségnél az indukciós hipotézist alkalmaztuk az $(s_k)_{k\in[\![0,n]\!]}$ rendszerre.

Hasonlóan kapjuk, hogy

$$\left(\mathop{\top}_{k=0}^{n+1} s_{n+1-k}^{-1}\right)\top\left(\mathop{\top}_{k=0}^{n+1} s_k\right)\overset{(5)}{=}\left(\left(\mathop{\top}_{k=0}^{n} s_{n+1-k}^{-1}\right)\top s_0^{-1}\right)\top\left(s_0\top\left(\mathop{\top}_{k=1}^{n+1} s_k\right)\right)\overset{(6)}{=}$$
$$\overset{(6)}{=}\left(\mathop{\top}_{k=0}^{n} s_{n+1-k}^{-1}\right)\top\left(s_0^{-1}\top s_0\right)\top\left(\mathop{\top}_{k=1}^{n+1} s_k\right)=\left(\mathop{\top}_{k=0}^{n} s_{n+1-k}^{-1}\right)\top e\top\left(\mathop{\top}_{k=1}^{n+1} s_k\right)\overset{(7)}{=}$$
$$\overset{(7)}{=}\left(\mathop{\top}_{k=0}^{n} s_{n-k+1}^{-1}\right)\top\left(\mathop{\top}_{k=0}^{n} s_{k+1}\right)\overset{(8)}{=}\left(\mathop{\top}_{k=0}^{n} s_{k+1}\right)^{-1}\top\left(\mathop{\top}_{k=0}^{n} s_{k+1}\right)=e,$$

ahol

– az $\overset{(5)}{=}$ egyenlőségnél felhasználtuk a 8.3.5. a) és b) állítást és az előző lemmát;

– a $\overset{(6)}{=}$ egyenlőségnél alkalmaztuk a $\top$ művelet asszociativitását;

– a $\overset{(7)}{=}$ egyenlőségnél a 8.3.4. állításra hivatkoztunk;

– a $\overset{(8)}{=}$ egyenlőségnél az indukciós hipotézist alkalmaztuk az $(s_{k+1})_{k\in[\![0,n]\!]}$ rendszerre. ■

12.5.15. Állítás. *Legyen S halmaz, és legyenek $\top$, $\perp$ olyan asszociatív műveletek S felett, hogy $\top$ disztributív $\perp$-ra nézve. Tegyük fel, hogy a $\perp$ művelet kommutatív és neutrális elemes (amelynek neutrális elemét $\mathbf{0}$ jelöli), továbbá tegyük fel, hogy $\mathbf{0}$ zéruselem a $\top$ műveletre nézve (vagyis minden $s\in S$ esetén $s\top\mathbf{0}=\mathbf{0}=\mathbf{0}\top s$). Ha $(s_j)_{j\in J}$ olyan S-ben haladó rendszer, hogy $\{j\in J|s_j\neq\mathbf{0}\}$ véges, akkor minden $s\in S$ esetén a $\{j\in J|s\top s_j\neq\mathbf{0}\}$ és $\{j\in J|s_j\top s\neq\mathbf{0}\}$ halmazok végesek és*

$$s\top\left(\mathop{\perp}_{j\in J} s_j\right)=\mathop{\perp}_{j\in J}(s\top s_j),$$
$$\left(\mathop{\perp}_{j\in J} s_j\right)\top s=\mathop{\perp}_{j\in J}(s_j\top s).$$

Bizonyítás. Legyen $(s_j)_{j\in J}$ olyan S-ben haladó rendszer, hogy $\{j\in J|s_j\neq\mathbf{0}\}$ véges halmaz. Mivel $\mathbf{0}$ zéruselem a $\top$ műveletre nézve, így $s\in S$ esetén $\{j\in J|s\top s_j\neq\mathbf{0}\}\subseteq\{j\in J|s_j\neq\mathbf{0}\}$ és $\{j\in J|s_j\top s\neq\mathbf{0}\}\subseteq\{j\in J|s_j\neq\mathbf{0}\}$, tehát a $\{j\in J|s\top s_j\neq\mathbf{0}\}$ és $\{j\in J|s_j\top s\neq\mathbf{0}\}$ halmazok végesek.

Legyen $s\in S$ rögzítve. Ha $J=\emptyset$, akkor $\mathop{\perp}_{j\in J} s_j=\mathbf{0}$, és $\mathop{\perp}_{j\in J}(s\top s_j)=\mathbf{0}=\mathop{\perp}_{j\in J}(s_j\top s)$, tehát a bizonyítandó egyenlőségek azért teljesülnek, mert $\mathbf{0}$ zéruselem a $\top$ műveletre nézve. Tegyük fel, hogy $J\neq\emptyset$ és legyen $J_*:=\{j\in J|s_j\neq\mathbf{0}\}$. Ekkor J_* nem üres véges halmaz, valamint $\{j\in J|s\top s_j\neq\mathbf{0}\}\subseteq J_*$ és $\{j\in J|s_j\top s\neq\mathbf{0}\}\subseteq J_*$, így az $(S,\perp)$ kommutatív monoidban értelmezett véges műveletek definíciója és 8.8.2. szerint teljesülnek az

$$s\top\left(\mathop{\perp}_{j\in J} s_j\right)=s\top\left(\mathop{\perp}_{j\in J_*} s_j\right)=\mathop{\perp}_{j\in J_*}(s\top s_j)=\mathop{\perp}_{j\in J}(s\top s_j),$$
$$\left(\mathop{\perp}_{j\in J} s_j\right)\top s=\left(\mathop{\perp}_{j\in J_*} s_j\right)\top s=\mathop{\perp}_{j\in J_*}(s_j\top s)=\mathop{\perp}_{j\in J}(s_j\top s)$$

egyenlőségek. ■

12.5.16. Állítás. *Legyenek* $(S, \perp)$ *és* $(S', \perp')$ *kommutatív monoidok, és jelölje* e *(illetve* e'*) az* $(S, \perp)$ *(illetve* $(S', \perp')$*) monoid neutrális elemét. Legyen* $\pi : S \to S'$ *olyan függvény, hogy minden* $s, t \in S$ *esetén* $\pi(s \perp t) = \pi(s) \perp' \pi(t)$*, valamint* $\pi(e) = e'$*. Ekkor minden* S*-ben haladó* $(s_i)_{i \in I}$ *rendszerre teljesül az, hogy ha* $\{i \in I | s_i \neq e\}$ *véges halmaz, akkor* $\{i \in I | \pi(s_i) \neq e'\}$ *is véges halmaz, és*

$$\pi\Big(\mathop{\perp}_{i \in I} s_i\Big) = \mathop{\perp'}_{i \in I} \pi(s_i).$$

Bizonyítás. Legyen $(s_i)_{i \in I}$ olyan S-ben haladó rendszer, hogy $I_* := \{i \in I | s_i \neq e\}$ véges halmaz.

Ha $I_* = \emptyset$, akkor minden $i \in I$ indexre $s_i = e$, tehát $\pi(s_i) = e'$, így $\{i \in I | \pi(s_i) \neq e'\} = \emptyset$, továbbá a monoidok véges műveleteinek definíciója szerint $\mathop{\perp}_{i \in I} s_i = e$ és $\mathop{\perp'}_{i \in I} \pi(s_i) = e'$, tehát

$$\pi\Big(\mathop{\perp}_{i \in I} s_i\Big) = \pi(e) = e' = \mathop{\perp'}_{i \in I} \pi(s_i),$$

tehát az állítás igaz.

Tegyük fel, hogy $I_* \neq \emptyset$. Ekkor I_* nem üres véges részhalmaza I-nek, így a monoidok véges műveleteinek definíciója szerint

$$\mathop{\perp}_{i \in I} s_i = \mathop{\perp}_{i \in I_*} s_i, \qquad \mathop{\perp'}_{i \in I} \pi(s_i) = \mathop{\perp'}_{i \in I_*} \pi(s_i),$$

következésképpen 8.8.1. alkalmazásával kapjuk, hogy

$$\pi\Big(\mathop{\perp}_{i \in I} s_i\Big) = \pi\Big(\mathop{\perp}_{i \in I_*} s_i\Big) = \mathop{\perp'}_{i \in I_*} \pi(s_i) = \mathop{\perp'}_{i \in I} \pi(s_i),$$

amit bizonyítani kellett. ■

12.6. Félcsoportok ábrázolásai és a Cayley-tétel

12.6.1. Definíció. *Ha* E *halmaz, akkor az* $(\mathscr{F}(E; E), \circ)$ *párt az* E *halmaz* **teljes transzformáció-félcsoportjának** *nevezzük, és ennek részfélcsoportjait az* E *halmaz* **transzformáció-félcsoportjainak** *nevezzük.*

12.6.2. Definíció. *Azt mondjuk, hogy* γ **ábrázolása az** $(S, \top)$ **félcsoportnak az** E **halmazban***, ha*

$$\gamma : S \to \mathscr{F}(E; E)$$

olyan függvény, amelyre minden $s, s' \in S$ *esetén*

$$\gamma(s \top s') = \gamma(s) \circ \gamma(s').$$

12.7. Generátorhalmazok és szabad félcsoportok

12.7.1. Definíció. *Legyen E halmaz. Ekkor*

$$\mathrm{Mon}(E) := \bigcup_{n\in\mathbb{N}} E^n,$$

valamint

$$\mathrm{in}_E : E \to \mathrm{Mon}(E)$$

az a függvény, amelyre minden $x \in E$ ponthoz azt az $(x_i)_{i\in 1} \in E^1 = E^{\{0\}}$ egy tagú rendszert rendeli, amelyre $x_0 = x$. Az in_E függvényt az E és $\mathrm{Mon}(E)$ halmazok közötti **kanonikus injekciónak** *nevezzük.*

Továbbá, minden $m, n \in \mathbb{N}^*$ és $(x_i)_{i\in m} \in E^m$ és $(y_i)_{i\in n} \in E^n$ esetén

$$(x_i)_{i\in m} \cdot (y_i)_{i\in n} := (z_i)_{i\in m+n} \in E^{m+n},$$

ahol minden $i \in m+n$ esetén

$$z_i := \begin{cases} x_i & , \textit{ha } i < m, \\ y_{i-m} & , \textit{ha } m \le i < m+n. \end{cases}$$

Végül, minden $\mathbf{x} \in \mathrm{Mon}(E)$ esetén

$$\emptyset \cdot \mathbf{x} := \mathbf{x} \cdot \emptyset := \mathbf{x}.$$

12.7.2. Állítás. *Ha E halmaz, akkor a $\mathrm{Mon}(E)$ halmaz a 12.7.1. definícióban bevezetett $\cdot$ művelettel ellátva olyan monoid, amelynek $\emptyset$ a neutrális eleme.*

Bizonyítás. A definíció szerint triviális, hogy $\emptyset \in \{\emptyset\} = E^0 \subseteq \mathrm{Mon}(E)$, és $\emptyset$ a neutrális elem a $\cdot$ műveletre nézve.

A $\cdot$ művelet asszociativitásának bizonyításához legyenek $m, n, p \in \mathbb{N}$ és $\mathbf{x} := (x_i)_{i\in m}$, $\mathbf{y} := (y_i)_{i\in n}$, $\mathbf{z} := (z_i)_{i\in p}$.

Ekkor a definíció szerint

– ha $\mathbf{x} = \emptyset$, akkor $\mathbf{x}\cdot(\mathbf{y}\cdot\mathbf{z}) = \emptyset\cdot(\mathbf{y}\cdot\mathbf{z}) = \mathbf{y}\cdot\mathbf{z} = (\emptyset\cdot\mathbf{y})\cdot\mathbf{z} = (\mathbf{x}\cdot\mathbf{y})\cdot\mathbf{z}$;

– ha $\mathbf{y} = \emptyset$, akkor $\mathbf{x}\cdot(\mathbf{y}\cdot\mathbf{z}) = \mathbf{x}\cdot(\emptyset\cdot\mathbf{z}) = \mathbf{x}\cdot\mathbf{z} = (\mathbf{x}\cdot\emptyset)\cdot\mathbf{z} = (\mathbf{x}\cdot\mathbf{y})\cdot\mathbf{z}$;

– ha $\mathbf{z} = \emptyset$, akkor $\mathbf{x}\cdot(\mathbf{y}\cdot\mathbf{z}) = \mathbf{x}\cdot(\mathbf{y}\cdot\emptyset) = \mathbf{x}\cdot\mathbf{y} = (\mathbf{x}\cdot\mathbf{y})\cdot\emptyset = (\mathbf{x}\cdot\mathbf{y})\cdot\mathbf{z}$.

Ezért az $\mathbf{x}\cdot(\mathbf{y}\cdot\mathbf{z}) = (\mathbf{x}\cdot\mathbf{y})\cdot\mathbf{z}$ egyenlőség bizonyításához feltehetjük az $\mathbf{x}$, $\mathbf{y}$ és $\mathbf{z}$ elemek egyike sem egyenlő az üres halmazzal, tehát $m, n, p \in \mathbb{N}^*$. Vezessük be az $(a_i)_{i\in n+p} \in E^{n+p}$, $(b_i)_{i\in n+p} \in E^{n+p}$, $(a'_i)_{i\in(m+n)+p} \in E^{(m+n)+p}$ és $(b'_i)_{i\in m+(n+p)} \in E^{m+(n+p)}$ rendszereket úgy, hogy $(a_i)_{i\in n+p} := \mathbf{y}\cdot\mathbf{z}$, $(b_i)_{i\in m+n} := \mathbf{x}\cdot\mathbf{y}$, $(a'_i)_{i\in m+(n+p)} := \mathbf{x}\cdot(\mathbf{y}\cdot\mathbf{z})$ és $(b'_i)_{i\in(m+n)+p} := (\mathbf{x}\cdot\mathbf{y})\cdot\mathbf{z}$. Azt kell igazolni, hogy $(a'_i)_{i\in(m+n)+p} = (b'_i)_{i\in m+(n+p)}$.

Mivel $(a'_i)_{i\in(m+n)+p} = \mathbf{x}\cdot(\mathbf{y}\cdot\mathbf{z}) = (x_i)_{i\in m}\cdot(a_i)_{i\in n+p}$, így $\cdot$ definíciója szerint minden $i \in m+(n+p)$ esetén

$$a'_i = \begin{cases} x_i & , \text{ha } i < m, \\ a_{i-m} & , \text{ha } m \le i < m+n+p, \end{cases}$$

és minden $m \le i < m+n+p$ indexre $i - m \in n+p$, tehát $\cdot$ definíciója szerint

$$a_{i-m} = \begin{cases} y_{i-m} & , \text{ha } i-m < n, \\ z_{i-m-n} & , \text{ha } n \le i-m < n+p, \end{cases}$$

ami azt jelenti, hogy

$$a'_i = \begin{cases} x_i & \text{, ha } i < m, \\ y_{i-m} & \text{, ha } m \leq i < m+n, \\ z_{i-m-n} & \text{, ha } m+n \leq i < m+n+p. \end{cases} \tag{1}$$

Mivel $(b'_i)_{i \in (m+n)+p} = (\mathbf{x} \cdot \mathbf{y}) \cdot \mathbf{z} = (b_i)_{i \in m+n} \cdot (z_i)_{i \in p}$, így $\cdot$ definíciója szerint minden $i \in (m+n)+p$ esetén

$$b'_i = \begin{cases} b_i & \text{, ha } i < m+n, \\ z_{i-m-n} & \text{, ha } m+n \leq i < m+n+p, \end{cases}$$

és $\cdot$ definíciója szerint

$$b_i = \begin{cases} x_i & \text{, ha } i < m, \\ y_{i-m} & \text{, ha } m \leq i < m+n, \end{cases}$$

ami azt jelenti, hogy

$$b'_i = \begin{cases} x_i & \text{, ha } i < m, \\ y_{i-m} & \text{, ha } m \leq i < m+n, \\ z_{i-m-n} & \text{, ha } m+n \leq i < m+n+p. \end{cases} \tag{2}$$

Az (1) és (2) kifejezések összehasonlításával nyerjük, hogy $(a'_i)_{i \in (m+n)+p} = (b'_i)_{i \in m+(n+p)}$, amit bizonyítani kellett. ■

12.7.3. Definíció. *Ha E halmaz, és $\cdot$ jelöli a 12.7.1. definícióban bevezetett* $\mathrm{Mon}(E)$ *feletti műveletet, akkor a* $(\mathrm{Mon}(E), \cdot)$ *párt az E halmaz által generált* **szabad monoidnak** *nevezzük.*

12.7.4. Tétel. *Legyen E halmaz.*

a) *Minden $(S, \top)$ monoidhoz és $f : E \to S$ függvényhez létezik egyetlen olyan $\widetilde{f} : \mathrm{Mon}(E) \to S$ morfizmus a $(\mathrm{Mon}(E), \cdot)$ és $(S, \top)$ monoidok között, hogy $\widetilde{f} \circ \mathrm{in}_E = f$, vagyis a következő diagram kommutatív:*

$$\begin{tikzcd} E \arrow[r, "\mathrm{in}_E"] \arrow[dr, "f"'] & \mathrm{Mon}(E) \arrow[d, "\widetilde{f}"] \\ & S \end{tikzcd}$$

b) *Legyen $((S', \top'), \mathrm{i})$ olyan pár, hogy $(S', \top')$ monoid, és $\mathrm{i} : E \to S'$ függvény, és minden $(S, \top)$ monoidhoz és $f : E \to S$ függvényhez létezik egyetlen olyan $\widetilde{f} : S' \to S$ morfizmus a $(S', \top')$ és $(S, \top)$ monoidok között, hogy $\widetilde{f} \circ \mathrm{i} = f$. Ekkor létezik egyetlen olyan $g : \mathrm{Mon}(E) \to S'$ izomorfizmus a $(\mathrm{Mon}(E), \cdot)$ és $(S', \top')$ monoidok között, amelyre $g \circ \mathrm{in}_E = \mathrm{i}$.*

Bizonyítás. a) Legyen $(S, \top)$ monoid és $f : E \to S$ függvény.

(*Unicitás.*) Az előírt tulajdonságú $\widetilde{f}$ függvény egyértelműségéhez elegendő azt igazolni, hogy $\{\emptyset\} \cup \mathrm{Im}\,(\mathrm{in}_E)$ generátorhalmaz az $(\mathrm{Mon}(E), \cdot)$ félcsoportban. Ehhez elegendő azt belátni, hogy minden $n \in \mathbb{N}$ és $(x_i)_{i \in n+1} \in E^{n+1}$ esetén

$$(x_i)_{i \in n+1} = \mathop{\mathrm{P}}_{i=0}^{n} \mathrm{in}_E(x_i).$$

Ezt n szerinti teljes indukcióval igazoljuk.

Ha $n = 0$, akkor minden $(x_i)_{i\in 1} \in E^1$ esetén in_E definíciója szerint

$$(x_i)_{i\in 1} = \mathrm{in}_E(x_0) = \mathop{\mathrm{P}}\limits_{i=0}^{0} \mathrm{in}_E(x_i).$$

Tegyük fel, hogy az állítás igaz az $n \in \mathbb{N}$ számra, és legyen $(x_i)_{i\in n+2} \in E^{n+2}$ tetszőleges, valamint $y_0 := x_{n+1}$. Ekkor in_E definíciója szerint $(y_i)_{i\in 1} = \mathrm{in}_E(x_{n+1})$, tehát

$$\mathop{\mathrm{P}}\limits_{i=0}^{n+1} \mathrm{in}_E(x_i) = \left(\mathop{\mathrm{P}}\limits_{i=0}^{n} \mathrm{in}_E(x_i) \right) \cdot \mathrm{in}_E(x_{n+1}) \overset{(*)}{=} (x_i)_{i\in n+1} \cdot \mathrm{in}_E(x_{n+1}) = (x_i)_{i\in n+1} \cdot (y_i)_{i\in 1},$$

ahol a $\overset{(*)}{=}$ egyenlőségnél az indukciós hipotézist alkalmaztuk az $(x_i)_{i\in n+1} \in E^{n+1}$ rendszerre. A $\cdot$ művelet definícióját alkalmazva kapjuk, az $(a_i)_{i\in n+2} := (x_i)_{i\in n+1} \cdot (y_i)_{i\in 1} \in E^{n+2}$ rendszerre teljesül az, hogy minden $i \in n+2$ esetén

$$a_i := \begin{cases} x_i & \text{, ha } i < n+1, \\ y_{n+1-i} & \text{, ha } n+1 \le i < n+2. \end{cases} = \begin{cases} x_i & \text{, ha } i < n+1, \\ x_{n+1} & \text{, ha } n+1 \le i < n+2. \end{cases} = x_i,$$

tehát $(x_i)_{i\in n+1} \cdot (y_i)_{i\in 1} = (x_i)_{i\in n+2}$. Ez azt jelenti, hogy az állítás igaz az $n+1$ számra is.

(*Egzisztencia.*) Az előírt tulajdonságú $\widetilde{f}$ függvény létezésének bizonyításához értelmezzük az $\widetilde{f} : \mathrm{Mon}(E) \to S$ függvényt úgy, hogy $\widetilde{f}(\emptyset) := e$, ahol e jelöli az $(S, \top)$ monoid neutrális elemét, továbbá minden $n \in \mathbb{N}^*$ és $(x_i)_{i\in \mathbb{N}} \in E^n$ esetén

$$\widetilde{f}\left((x_i)_{i\in \mathbb{N}}\right) := \mathop{\top}\limits_{i=0}^{n-1} f(x_i).$$

Megmutatjuk, hogy $\widetilde{f} : \mathrm{Mon}(E) \to S$ az a monoid-morfizmus a $(\mathrm{Mon}(E), \cdot)$ és $(S, \top)$ monoidok között, amelyre $\widetilde{f} \circ \mathrm{in}_E = f$.

Ha $x \in E$ és $(x_i)_{i\in 1} \in E^1$ az a rendszer, amelyre $x_0 = x$, akkor in_E definíciója szerint $\mathrm{in}_E(x) = (x_i)_{i\in 1}$, következésképpen

$$(\widetilde{f} \circ \mathrm{in}_E)(x) = \widetilde{f}((x_i)_{i\in 1}) = \mathop{\top}\limits_{i=0}^{0} f(x_i) = f(x_0) = f(x),$$

tehát $\widetilde{f} \circ \mathrm{in}_E = f$.

A $\widetilde{f}$ függvény morfikusságának bizonyításához legyenek $m, n \in \mathbb{N}$ és $\mathbf{x} = (x_i)_{i\in m} \in E^m$ és $\mathbf{y} = (y_i)_{i\in n} \in E^n$.

Ekkor $\widehat{f}(\emptyset) := e$ és $\cdot$ definíciója szerint

– ha $\mathbf{x} = \emptyset$, akkor $\widetilde{f}(\mathbf{x} \cdot \mathbf{y}) = \widetilde{f}(\emptyset \cdot \mathbf{y}) = \widetilde{f}(\mathbf{y}) = e \top \widetilde{f}(\mathbf{y}) = \widetilde{f}(\emptyset) \top \widetilde{f}(\mathbf{y}) = \widetilde{f}(\mathbf{x}) \top \widetilde{f}(\mathbf{y})$;

– ha $\mathbf{y} = \emptyset$, akkor $\widetilde{f}(\mathbf{x} \cdot \mathbf{y}) = \widetilde{f}(\mathbf{x} \cdot \emptyset) = \widetilde{f}(\mathbf{x}) = \widetilde{f}(\mathbf{x}) \top e = \widetilde{f}(\mathbf{x}) \top \widetilde{f}(\emptyset) = \widetilde{f}(\mathbf{x}) \top \widetilde{f}(\mathbf{y})$.

Ezért az $\widetilde{f}(\mathbf{x} \cdot \mathbf{y}) = \widetilde{f}(\mathbf{x}) \top \widetilde{f}(\mathbf{y})$ egyenlőség bizonyításához feltehetjük, hogy az $\mathbf{x}$ és $\mathbf{y}$ elemek egyike sem egyenlő az üres halmazzal, tehát $m, n \in \mathbb{N}^*$. Vezessük be a $(z_i)_{i\in m+n} := \mathbf{x} \cdot \mathbf{y}$ rendszert, tehát minden $i \in m+n$ esetén

$$z_i := \begin{cases} x_i & \text{, ha } i < m, \\ y_{i-m} & \text{, ha } m \le i < m+n \end{cases}.$$

Ekkor

$$\widehat{f}\,(\mathbf{x}\cdot\mathbf{y})=\widehat{f}\,((z_i)_{i\in m+n})=\mathop{\top}_{i=0}^{m+n-1} f(z_i)\overset{(**)}{=}\left(\mathop{\top}_{i=0}^{m-1} f(z_i)\right)\top\left(\mathop{\top}_{i=m}^{m+n-1} f(z_i)\right)=$$
$$=\left(\mathop{\top}_{i=0}^{m-1} f(x_i)\right)\top\left(\mathop{\top}_{i=m}^{m+n-1} f(y_{i-m})\right)=\left(\mathop{\top}_{i=0}^{m-1} f(x_i)\right)\top\left(\mathop{\top}_{i=0}^{n-1} f(y_i)\right)=\widetilde{f}(\mathbf{x})\top\widetilde{f}(\mathbf{y}),$$

ahol a $\overset{(**)}{=}$ egyenlőségnél a 12.5.13. állítást alkalmaztuk.

b) Az a) állítás alapján az $(S',\top')$ monoidhoz és $\mathrm{i}:E\to S'$ függvényhez létezik egyetlen olyan $\widetilde{\mathrm{i}}:\mathrm{Mon}(E)\to S'$ morfizmus a $(\mathrm{Mon}(E),\cdot)$ és $(S',\top')$ monoidok között, hogy $\widetilde{\mathrm{i}}\circ\mathrm{in}_E=\mathrm{i}$. Ugyanakkor az $((S',\top'),\mathrm{i})$ párra b)-ben előírt feltétel alapján a $(\mathrm{Mon}(E),\cdot)$ monoidhoz és $\mathrm{in}_E:E\to\mathrm{Mon}(E)$ függvényhez létezik egyetlen olyan $\widetilde{\mathrm{in}_E}:S'\to\mathrm{Mon}(E)$ morfizmus az $(S',\top')$ és $(\mathrm{Mon}(E),\cdot)$ monoidok között, hogy $\widetilde{\mathrm{in}_E}\circ\mathrm{i}=\mathrm{in}_E$.

Világos, hogy ekkor

$$\left(\widetilde{\mathrm{in}_E}\circ\widetilde{\mathrm{i}}\right)\circ\mathrm{in}_E=\widetilde{\mathrm{in}_E}\circ\left(\widetilde{\mathrm{i}}\circ\mathrm{in}_E\right)=\widetilde{\mathrm{in}_E}\circ\mathrm{i}=\mathrm{in}_E,$$

és $\widetilde{\mathrm{in}_E}\circ\widetilde{\mathrm{i}}:\mathrm{Mon}(E)\to\mathrm{Mon}(E)$ morfizmus a $(\mathrm{Mon}(E),\cdot)$ és $(\mathrm{Mon}(E),\cdot)$ monoidok között. Ugyanakkor triviális, hogy $\mathrm{id}_{\mathrm{Mon}(E)}$ is morfizmus a $(\mathrm{Mon}(E),\cdot)$ és $(\mathrm{Mon}(E),\cdot)$ monoidok között, és természetesen $\mathrm{id}_{\mathrm{Mon}(E)}\circ\mathrm{in}_E=\mathrm{in}_E$. Ezért az a) állításban szereplő egyértelműségi feltétel szerint $\widetilde{\mathrm{in}_E}\circ\widetilde{\mathrm{i}}=\mathrm{id}_{\mathrm{Mon}(E)}$.

Továbbá, világos, hogy

$$\left(\widetilde{\mathrm{i}}\circ\widetilde{\mathrm{in}_E}\right)\circ\mathrm{i}=\widetilde{\mathrm{i}}\circ\left(\widetilde{\mathrm{in}_E}\circ\mathrm{i}\right)=\widetilde{\mathrm{i}}\circ\mathrm{in}_E=\mathrm{i},$$

és $\widetilde{\mathrm{i}}\circ\widetilde{\mathrm{in}_E}:S'\to S'$ morfizmus az $(S',\top')$ és $(S',\top')$ monoidok között. Ugyanakkor triviális, hogy $\mathrm{id}_{S'}$ is morfizmus az $(S',\top')$ és $(S',\top')$ monoidok között, és természetesen $\mathrm{id}_{S'}\circ\mathrm{i}=\mathrm{i}$. Ezért az $((S',\top'),\mathrm{i})$ párra előírt egyértelműségi feltételből következik, hogy $\widetilde{\mathrm{i}}\circ\widetilde{\mathrm{in}_E}=\mathrm{id}_{S'}$.

Ezzel bebizonyítottuk, hogy $\widetilde{\mathrm{i}}:\mathrm{Mon}(E)\to S'$ bijekció és $\widetilde{\mathrm{i}}^{-1}=\widetilde{\mathrm{in}_E}$. Tehát $\widetilde{\mathrm{i}}$ olyan izomorfizmus a $(\mathrm{Mon}(E),\cdot)$ és $(S',\top')$ monoidok között, amelyre $\widetilde{\mathrm{i}}\circ\mathrm{in}_E=\mathrm{i}$.

Ha $g:\mathrm{Mon}(E)\to S'$ olyan morfizmus a $(\mathrm{Mon}(E),\cdot)$ és $(S',\top')$ monoidok között, amelyre $g\circ\mathrm{in}_E=\mathrm{i}$, akkor $g=\widetilde{\mathrm{i}}$ az $\{\emptyset\}\cup\mathrm{Im}\,(\mathrm{in}_E)$ halmazon, amelyről a) bizonyításában láttuk, hogy generátorhalmaz az $(\mathrm{Mon}(E),\cdot)$ monoidban, ezért $g=\widetilde{\mathrm{i}}$. Ez azt jelenti, hogy még az $\mathrm{Mon}(E)\to S'$ monoid-morfizmusok halmazában is csak legfeljebb egy olyan g elem létezhet, amelyre $g\circ\mathrm{in}_E=\mathrm{i}$. ■

13. fejezet

Csoportok

13.1. Csoportok és csoport-morfizmusok

Emlékeztetünk arra, hogy a $(G, \top)$ párt *csoportnak* nevezzük, ha $\top$ asszociatív, neutráliselemes és inverzelemes művelet a G halmaz felett. (6.6.5.) A G halmaz feletti *csoportműveletnek* nevezünk minden olyan G feletti $\top$ műveletet, amelyre a $(G, \top)$ pár csoport. A következő állítás jellemzést ad a csoportműveletekre, az asszociatív műveletek körében.

13.1.1. Állítás. *A $(G, \top)$ félcsoport pontosan akkor csoport, ha létezik olyan $e \in G$, amelyre teljesülnek a következők:*

– minden $s \in G$ esetén $e \top s = s$;

– minden $s \in G$ esetén létezik olyan $s' \in G$, hogy $s' \top s = e$.

Bizonyítás. Világos, hogy ha $(G, \top)$ csoport, akkor az $e := e_G$ neutrális elem olyan, amely eleget tesz a feltételeknek. Megfordítva, legyen $e \in G$ olyan elem, amelyre a feltételek teljesülnek. Legyen $s \in G$ és legyenek $s' \in G$ és $s'' \in G$ olyan elemek, amelyekre $s' \top s = e$ és $s'' \top s' = e$. Ekkor kihasználva e tulajdonságait, az s' és s'' elemek definícióját, valamint a $\top$ művelet asszociativitását kapjuk, hogy

$$\begin{gathered} e = s'' \top s' = s'' \top (e \top s') = s'' \top ((s' \top s) \top s') = \\ = (s'' \top (s' \top s)) \top s' = ((s'' \top s') \top s) \top s' = (e \top s) \top s' = s \top s', \end{gathered}$$

tehát $s \top s' = e$ is teljesül. Ebből, és a $\top$ művelet asszociativitásából következik, hogy ha $s \in G$ és $s' \in G$ olyan elem, hogy $s' \top s = e$, akkor

$$s \top e = s \top (s' \top s) = (s \top s') \top s = e \top s = s,$$

ami azt jelenti, hogy e a $\top$ műveletnek neutrális eleme. Továbbá, az előzőek szerint, ha $s \in G$ és $s' \in G$ olyan elem, hogy $s' \top s = e$, akkor $s \top s' = e$ is teljesül, tehát s' az s elem inverze a $\top$ művelet szerint, így $\top$ csoportművelet G felett. ■

Jelölések. Legyen G csoport.

– A G neutrális elemét e_G jelöli, vagy ha világos, hogy melyik csoport neutrális eleméről van szó, akkor az e jelet alkalmazzuk.

– A G csoport műveletét rendszerint szorzással (kommutatív esetben összeadással) jelöljük. Előfordul, hogy a $G \times G \to G; (s, t) \mapsto st$ csoportműveletet a p_G, és a

$G \to G;\ s \mapsto s^{-1}$ csoport-inverziót az i_G szimbólummal jelöljük.

– Minden $s \in G$ esetén a következő függvény-jelöléseket alkalmazzuk.

$$\begin{aligned}\gamma_G(s) : G \to G; &\quad t \mapsto st,\\ \delta_G(s) : G \to G; &\quad t \mapsto ts^{-1},\\ \mathrm{Int}_G(s) : G \to G; &\quad t \mapsto sts^{-1},\end{aligned}$$

tehát $\mathrm{Int}_G(s) = \gamma_G(s) \circ \delta_G(s) = \delta_G(s) \circ \gamma_G(s)$.

13.1.2. Definíció. *Legyenek G és H csoportok. Azt mondjuk, hogy a $\pi : G \to H$ függvény* **csoport-morfizmus**, *ha minden $s, s' \in G$ esetén $\pi(ss') = \pi(s)\pi(s')$. Azt mondjuk, hogy a $\pi : G \to H$ függvény* **csoport-izomorfizmus**, *ha π bijektív csoport-morfizmus. Azt mondjuk, hogy a G és H csoportok* **izomorfak**, *ha létezik $G \to H$ csoport-izomorfizmus.*

13.1.3. Állítás. *Legyenek G és H csoportok. Ha a $\pi : G \to H$ függvény csoport-morfizmus, akkor $\pi(e_G) = e_H$ és minden $s \in G$ esetén $\pi(s^{-1}) = (\pi(s))^{-1}$. Ha a $\pi : G \to H$ függvény csoport-izomorfizmus, akkor a $\pi^{-1} : H \to G$ függvény csoport-izomorfizmus.*

Bizonyítás. Ha $\pi : G \to H$ csoport-morfizmus, akkor $e_G e_G = e_G$ miatt $\pi(e_G)\pi(e_G) = \pi(e_G e_G) = \pi(e_G)$, amiből H csoportműveletének tulajdonságai alapján kapjuk, hogy

$$\begin{aligned}\pi(e_G) &= \pi(e_G)\, e_H = \pi(e_G)\left(\pi(e_G)(\pi(e_G))^{-1}\right) =\\ &= (\pi(e_G)\pi(e_G))(\pi(e_G))^{-1} = \pi(e_G)(\pi(e_G))^{-1} = e_H.\end{aligned}$$

Ebből következik, hogy ha $\pi : G \to H$ csoport-morfizmus, akkor minden $s \in G$ esetén $\pi(s)\pi(s^{-1}) = \pi(ss^{-1}) = \pi(e_G) = e_H$, amiből H csoportműveletének tulajdonságai alapján kapjuk, hogy

$$\begin{aligned}(\pi(s))^{-1} &= (\pi(s))^{-1}e_H = (\pi(s))^{-1}\left(\pi(s)\pi\left(s^{-1}\right)\right) =\\ &= \left((\pi(s))^{-1}\pi(s)\right)\pi\left(s^{-1}\right) = e_H\pi\left(s^{-1}\right) = \pi\left(s^{-1}\right).\end{aligned}$$

Ha $\pi : G \to H$ csoport-izomorfizmus, akkor $\pi^{-1} : H \to G$ bijekció, és π csoport-morfizmus, tehát minden $t, t' \in H$ esetén

$$\pi\left(\pi^{-1}(t)\pi^{-1}(t')\right) = \pi\left(\pi^{-1}(t)\right)\pi\left(\pi^{-1}(t')\right) = tt' = \pi\left(\pi^{-1}(tt')\right),$$

így π injektivitása miatt $\pi^{-1}(t)\pi^{-1}(t') = \pi^{-1}(tt')$, vagyis a $\pi^{-1} : G \to H$ függvény csoport-morfizmus is. Ezért a $\pi^{-1} : H \to G$ függvény csoport-izomorfizmus. ∎

13.1.4. Következmény. *Ha G és H csoportok és $\pi : G \to H$ csoport-morfizmus, akkor minden $s, t \in G$ esetén $\pi(st^{-1}) = \pi(s)(\pi(t))^{-1}$.* ∎

13.1.5. Definíció. *Ha G csoport, akkor* $\mathbf{Aut}(G)$ *jelöli a $G \to G$ csoport-izomorfizmusok halmazát, és* $\mathbf{Int}(G) := \{\mathrm{Int}_G(s) | s \in G\}$.

13.1.6. Állítás. *Ha G csoport, akkor az $\mathbf{Aut}(G)$ halmaz felett a függvénykompozíció csoport-művelet, és $\mathbf{Int}(G) \subseteq \mathbf{Aut}(G)$, és ha $\mathbf{Aut}(G)$-t ellátjuk a függvénykompozícióval, akkor a*

$$G \to \mathbf{Aut}(G); \quad s \mapsto \mathrm{Int}_G(s)$$

leképezés csoport-morfizmus.

Bizonyítás. Ha $\pi, \pi' \in \mathbf{Aut}(G)$, akkor $\pi' \circ \pi : G \to G$ bijekció, mert bijekciók kompozíciója, és $\pi' \circ \pi$ csoport-morfizmus is, mert minden $s, s' \in G$ esetén $(\pi' \circ \pi)(ss') = \pi'(\pi(ss')) = \pi'(\pi(s)\pi(s')) = \pi'(\pi(s))\pi'(\pi(s')) = (\pi' \circ \pi)(s)(\pi' \circ \pi)(s')$. Ezért a függvénykompozíció az $\mathbf{Aut}(G)$ halmaz felett asszociatív művelet. Nyilvánvaló, hogy $\mathrm{id}_G \in \mathbf{Aut}(G)$ a neutrális elem erre a műveletre nézve, és az előző állítás szerint minden $\pi \in \mathbf{Aut}(G)$ a π függvény inverze eleme $\mathbf{Aut}(G)$-nek, tehát π-nek létezik inverze a függvénykompozíció szerint. Ezért az $\mathbf{Aut}(G)$ halmaz felett a függvénykompozíció csoport-művelet.

Legyen $s \in G$. Ekkor az $\mathrm{Int}_G(s) : G \to G$ függvény bijekció, hiszen $\mathrm{Int}_G(s) = \gamma_G(s) \circ \delta_G(s)$ és a $\gamma_G(s) : G \to G$ és a $\delta_G(s) : G \to G$ függvények bijekciók. Továbbá, minden $t, t' \in G$ esetén

$$\mathrm{Int}_G(s)(t)\mathrm{Int}_G(s)(t') = \left(sts^{-1}\right)\left(st's^{-1}\right) = s\,(tt')\,s^{-1} = \mathrm{Int}_G(s)(tt'),$$

így az $\mathrm{Int}_G(s) : G \to G$ függvény csoport-izomorfizmus, vagyis $\mathrm{Int}_G(s) \in \mathbf{Aut}(G)$.

Legyenek $s, \tilde{s} \in G$. Ekkor minden $t \in G$ esetén

$$\mathrm{Int}_G(s)\left(\mathrm{Int}_G(\tilde{s})(t)\right) = s\left(\tilde{s}t\tilde{s}^{-1}\right)s^{-1} = (s\tilde{s})t(s\tilde{s})^{-1} = \mathrm{Int}_G(s\tilde{s})(t),$$

tehát $\mathrm{Int}_G(s) \circ \mathrm{Int}_G(\tilde{s}) = \mathrm{Int}_G(s\tilde{s})$. Ez azt jelenti, hogy a $G \to \mathbf{Aut}(G);\ s \mapsto \mathrm{Int}_G(s)$ leképezés csoport-morfizmus. ■

13.1.7. Definíció. *Ha G és H csoportok és $\pi : G \to H$ csoport-morfizmus, akkor*

$$\mathrm{Ker}(\pi) := \{\ s \in G \mid \pi(s) = e_H\ \},$$

és a $\mathrm{Ker}(\pi)$ *halmazt a π csoport-morfizmus* **magjának** *nevezzük.*

13.1.8. Állítás. *Legyenek G és H csoportok. A $\pi : G \to H$ csoport-morfizmus pontosan akkor injektív, ha* $\mathrm{Ker}(\pi) = \{e_G\}$.

Bizonyítás. Világos, hogy $\pi(e_G) = e_H$ miatt $\{e_G\} \subseteq \mathrm{Ker}(\pi)$. Ha π injektív és $s \in \mathrm{Ker}(\pi)$, akkor $\pi(s) = e_H = \pi(e_G)$, tehát $s = e_G$, így $\mathrm{Ker}(\pi) \subseteq \{e_G\}$.

Tegyük fel, hogy $\mathrm{Ker}(\pi) = \{e_G\}$, és legyenek $s, s' \in G$ olyanok, hogy $\pi(s) = \pi(s')$. Ekkor G szorzásának asszociativitása miatt $\pi(s') = \pi\left(s'\left(s^{-1}s\right)\right) = \pi\left(\left(s's^{-1}\right)s\right) = \pi\left(s's^{-1}\right)\pi(s)$, és ezt az egyenlőséget jobbról szorozva $(\pi(s))^{-1}$-gyel és felhasználva a $\pi(s) = \pi(s')$ egyenlőséget kapjuk, hogy $e_H = \pi\left(s's^{-1}\right)$, tehát $s's^{-1} \in \mathrm{Ker}(\pi)$, így $s's^{-1} = e_G$. Ezt az egyenlőséget jobbról szorozva s-sel kapjuk, hogy $s' = s$. Ez azt jelenti, hogy π injektív. ■

13.1.9. Lemma. *Ha G csoport és $X \subseteq G$ kommutatív halmaz (vagyis minden $s, t \in X$ esetén $st = ts$), akkor az $X \cup X^{-1}$ halmaz is kommutatív.*

Bizonyítás. Ha $s, t \in X$, akkor 12.5.14. szerint $t^{-1}s^{-1} = (st)^{-1} = (ts)^{-1} = s^{-1}t^{-1}$, továbbá a csoportművelet asszociativitása miatt $t(st^{-1}) = (ts)t^{-1} = (st)t^{-1} = s(tt^{-1}) = se_G = s$, amiből t^{-1}-gyel balról szorozva kapjuk, hogy $st^{-1} = e_G(st^{-1}) = (t^{-1}t)(st^{-1}) = t^{-1}(t(st^{-1})) = t^{-1}s$. Ebből következik, hogy minden $s, t \in X \cup X^{-1}$ esetén $st = ts$. ■

13.1.10. Állítás. *Legyen G csoport és $\mathbf{s} : \mathbb{N} \to G$ függvény. Legfeljebb egy olyan $\mathbb{Z} \to G$ csoport-morfizmus létezik $\mathbb{Z}$ additív csoportja és G között, amely $\mathbf{s}$-nek kiterjesztése. Akkor és csak akkor létezik olyan $\mathbb{Z} \to G$ csoport-morfizmus $\mathbb{Z}$ additív csoportja és G között, amely kiterjesztése $\mathbf{s}$-nek, ha minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}(m+n) = \mathbf{s}(m)\mathbf{s}(n)$.*

Bizonyítás. (*Unicitás.*) Ha $\widetilde{\mathbf{s}} : \mathbb{Z} \to G$ olyan csoport-morfizmus, amelyek kiterjesztése $\mathbf{s}$-nek, akkor minden $m, n \in \mathbb{Z}$ esetén

$$\widetilde{\mathbf{s}}(m-n) = \widetilde{\mathbf{s}}(m+(-n)) = \widetilde{\mathbf{s}}(m)\widetilde{\mathbf{s}}(-n) = \widetilde{\mathbf{s}}(m)(\widetilde{\mathbf{s}}(n))^{-1} = \mathbf{s}(m)(\mathbf{s}(n))^{-1},$$

amiből látható, hogy $\widetilde{\mathbf{s}}$ egyértelműen van meghatározva, hiszen minden $a \in \mathbb{Z}$ esetén léteznek olyan $m, n \in \mathbb{N}$, hogy $a = m - n$.

(*Egzisztencia.*) A feltétel nyilvánvalóan szükséges. Az elégségesség bizonyításához először megjegyezzük, hogy az $\mathrm{Im}(\mathbf{s}) \subseteq G$ halmaz kommutatív, mert az $\mathbf{s}$ sorozatra vonatkozó hipotézis és a $\mathbb{Z}$ feletti összeadás kommutativitása szerint minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}(m)\mathbf{s}(n) = \mathbf{s}(m+n) = \mathbf{s}(n+m) = \mathbf{s}(n)\mathbf{s}(m)$. Ezért 13.1.9. alapján az $\mathrm{Im}(\mathbf{s}) \cup (\mathrm{Im}(\mathbf{s}))^{-1} \subseteq G$ halmaz is kommutatív. Továbbá, a feltevés szerint $\mathbf{s}(0) = \mathbf{s}(0+0) = \mathbf{s}(0)\mathbf{s}(0)$, amiből balról (vagy jobbról) szorozva az $(\mathbf{s}(0))^{-1}$ elemmel $\mathbf{s}(0) = e_G$ adódik.

Legyenek $m, n, m', n' \in \mathbb{N}$ olyanok, hogy $m + n' = m' + n$. Ekkor az $\mathbf{s}$ sorozatra vonatkozó hipotézis alapján $\mathbf{s}(m)\mathbf{s}(n') = \mathbf{s}(m+n') = \mathbf{s}(m'+n) = \mathbf{s}(m')\mathbf{s}(n)$, amiből az $\mathrm{Im}(\mathbf{s}) \cup (\mathrm{Im}(\mathbf{s}))^{-1}$ halmaz kommutativitását kihasználva kapjuk, hogy $\mathbf{s}(m)(\mathbf{s}(n))^{-1} = \mathbf{s}(m')(\mathbf{s}(n'))^{-1}$. Ezért $\mathbb{Z}$ definíciója szerint létezik egyetlen olyan $\widetilde{\mathbf{s}} : \mathbb{Z} \to G$ függvény, hogy minden $m, n \in \mathbb{N}$ esetén $\widetilde{\mathbf{s}}(m-n) = \mathbf{s}(m)(\mathbf{s}(n))^{-1}$. Ekkor nyilvánvalóan minden $m \in \mathbb{N}$ számra $\widetilde{\mathbf{s}}(m) = \widetilde{\mathbf{s}}(m-0) = \mathbf{s}(m)(\mathbf{s}(0))^{-1} = \mathbf{s}(m)(e_G)^{-1} = \mathbf{s}(m)e_G = \mathbf{s}(m)$, vagyis $\widetilde{\mathbf{s}}$ kiterjesztése $\mathbf{s}$-nek. Továbbá, az $\widetilde{\mathbf{s}} : \mathbb{Z} \to G$ függvény csoport-morfizmus, mert minden $m, n, m', n' \in \mathbb{N}$ esetén

$$\begin{aligned}\widetilde{\mathbf{s}}((m-n)+(m'-n')) &= \widetilde{\mathbf{s}}((m+m')-(n+n')) = \mathbf{s}(m+m')(\mathbf{s}(n+n'))^{-1} = \\ &= \mathbf{s}(m)\mathbf{s}(m')\left(\mathbf{s}(n)\mathbf{s}(n')\right)^{-1} = \mathbf{s}(m)\mathbf{s}(m')(\mathbf{s}(n'))^{-1}(\mathbf{s}(n))^{-1} = \\ &= (\mathbf{s}(m)(\mathbf{s}(n))^{-1})(\mathbf{s}(m')(\mathbf{s}(n'))^{-1}) = \widetilde{\mathbf{s}}(m-n)\widetilde{\mathbf{s}}(m'-n'),\end{aligned}$$

ahol felhasználtuk a $\mathbb{Z}$-beli összeadás és a $\widetilde{\mathbf{s}}$ függvény definícióját, valamint a G-beli szorzás asszociativitását, és az $\mathrm{Im}(\mathbf{s}) \cup (\mathrm{Im}(\mathbf{s}))^{-1}$ halmaz kommutativitását. ■

13.2. Permutációcsoportok és csoportábrázolások

13.2.1. Definíció. *Ha E halmaz, akkor $\mathfrak{S}(E)$ vagy $\mathfrak{S}_E$ jelöli azt a csoportot, amelynek alaphalmaza az $E \to E$ bijekciók halmaza, és művelete a függvénykompozíció. Az $\mathfrak{S}(E)$ csoportot az E halmaz* **teljes permutációcsoportjának** *nevezzük.*

Ha $n \in \mathbb{N}$, akkor n halmaz teljes permutációcsoportjára szinte mindig az $\mathfrak{S}_n$ jelölést alkalmazzuk $\mathfrak{S}(n)$ helyett.

13.2.2. Állítás. *Legyen I véges halmaz és $j, k \in I$ olyan elemek, hogy $j \neq k$. Jelölje $\tau_{j,k} \in \mathfrak{S}(I)$ azt a permutációt, amelyre $\tau_{j,k}(j) = k$ és $\tau_{j,k}(k) = j$ és minden $i \in I$ esetén, ha $i \neq j$ és $i \neq k$, akkor $\tau_{j,k}(i) = i$. Ha $(S, \top)$ neutráliselemes kommutatív félcsoport, amelynek a neutrális elemét $\mathbf{e}$ jelöli, és $f : \mathfrak{S}(I) \to S$ olyan függvény, hogy minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma) \top f(\sigma \circ \tau_{j,k}) = \mathbf{e}$, vagy minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma) \top f(\tau_{j,k} \circ \sigma) = \mathbf{e}$, akkor*

$$\mathop{\top}_{\sigma \in \mathfrak{S}(I)} f(\sigma) = \mathbf{e}.$$

Bizonyítás. (I) Először arra az esetre bizonyítunk, amikor minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma) \top f(\sigma \circ \tau_{j,k}) = \mathbf{e}$.

Jelöljön $\leq$ egy lineáris rendezést az I véges halmaz felett (8.2.1.), és vezessük be a következő halmazokat:

$$\mathfrak{S}^+(I) := \{\sigma \in \mathfrak{S}(I) | \sigma(j) < \sigma(k)\},$$

$$\mathfrak{S}^-(I) := \{\sigma \in \mathfrak{S}(I) | \sigma(j) > \sigma(k)\}.$$

Ekkor a $\leq$ rendezés trichotómiája miatt $\mathfrak{S}(I) = \mathfrak{S}^+(I) \cup \mathfrak{S}^-(I)$ és természetesen $\mathfrak{S}^+(I) \cap \mathfrak{S}^-(I) = \emptyset$. Nyilvánvaló, hogy minden $\sigma \in \mathfrak{S}^+(I)$ esetén $\sigma \circ \tau_{j,k} \in \mathfrak{S}^-(I)$, hiszen $(\sigma \circ \tau_{j,k})(j) = \sigma(k) > \sigma(j) = (\sigma \circ \tau_{j,k})(k)$. Hasonlóan, minden $\sigma \in \mathfrak{S}^-(I)$ esetén $\sigma \circ \tau_{j,k} \in \mathfrak{S}^+(I)$, hiszen $(\sigma \circ \tau_{j,k})(j) = \sigma(k) < \sigma(j) = (\sigma \circ \tau_{j,k})(k)$. Mivel nyilvánvalóan $\tau_{j,k} \circ \tau_{j,k} = \mathrm{id}_I$, így az

$$\mathfrak{S}^+(I) \to \mathfrak{S}^-(I); \quad \sigma \mapsto \sigma \circ \tau_{j,k}$$

leképezés bijekció, amelynek inverze egyenlő a

$$\mathfrak{S}^-(I) \to \mathfrak{S}^+(I); \quad \sigma \mapsto \sigma \circ \tau_{j,k}$$

leképezéssel. Ha $j < k$, akkor $\mathrm{id}_I \in \mathfrak{S}^+(I)$ és $\tau_{j,k} \in \mathfrak{S}^-(I)$. Ha $k < j$, akkor $\mathrm{id}_I \in \mathfrak{S}^-(I)$ és $\tau_{j,k} \in \mathfrak{S}^+(I)$. Ebből látható, hogy $\mathfrak{S}^+(I) \neq \emptyset$ és $\mathfrak{S}^-(I) \neq \emptyset$. Tehát

$$\top_{\sigma \in \mathfrak{S}(I)} f(\sigma) \overset{(1)}{=} \left(\top_{\sigma \in \mathfrak{S}^+(I)} f(\sigma) \right) \top \left(\top_{\sigma \in \mathfrak{S}^-(I)} f(\sigma) \right) \overset{(2)}{=}$$

$$\overset{(2)}{=} \left(\top_{\sigma \in \mathfrak{S}^+(I)} f(\sigma) \right) \top \left(\top_{\sigma \in \mathfrak{S}^+(I)} f(\sigma \circ \tau_{j,k}) \right) \overset{(3)}{=} \top_{\sigma \in \mathfrak{S}^+(I)} (f(\sigma) \top f(\sigma \circ \tau_{j,k})) \overset{(4)}{=} \mathbf{e},$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 8.5.5. állítást alkalmaztuk;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk az általános kommutatvitás tételét (8.6.1.);

– a $\overset{(3)}{=}$ egyenlőségnél a 8.5.9. állításra hivatkozunk;

– a $\overset{(4)}{=}$ egyenlőségnél a 12.5.2. állítást alkalmaztuk.

(II) Most tegyük fel, hogy minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma) \top f(\tau_{j,k} \circ \sigma) = \mathbf{e}$, és vezessük be az

$$\check{f} : \mathfrak{S}(I) \to S; \quad \sigma \mapsto f(\sigma^{-1})$$

függvényt. Mivel $\tau_{j,k}^{-1} = \tau_{j,k}$, így minden $\sigma \in \mathfrak{S}(I)$ permutációra, az f függvényre vonatkozó hipotézis miatt

$$\check{f}(\sigma) \top \check{f}(\sigma \circ \tau_{j,k}) = f\left(\sigma^{-1}\right) \top f\left(\tau_{j,k}^{-1} \circ \sigma^{-1}\right) = f\left(\sigma^{-1}\right) \top f\left(\tau_{j,k} \circ \sigma^{-1}\right) = \mathbf{e}.$$

Ezért alkalmazhatjuk az (I) állítást az f függvény helyett $\check{f}$-ra. Azt kapjuk, hogy

$$\mathbf{e} = \top_{\sigma \in \mathfrak{S}(I)} \check{f}(\sigma) = \top_{\sigma \in \mathfrak{S}(I)} f\left(\sigma^{-1}\right) = \top_{\sigma \in \mathfrak{S}(I)} f(\sigma),$$

ahol az utolsó egyenlőségnél felhasználtuk azt, hogy az $\mathfrak{S}(I) \to \mathfrak{S}(I)$; $\sigma \mapsto \sigma^{-1}$ leképezés bijekció, így a $\top$ műveletre alkalmazható az általános kommutatvitás tétele (8.6.1.). ■

13.2.3. Definíció. *Azt mondjuk, hogy γ* **ábrázolása a** G **csoportnak az** E **halmazban**, *ha $\gamma : G \to \mathfrak{S}(E)$ csoport-morfizmus. Ekkor E-t a γ* **ábrázolás terének** *nevezzük, és minden $s \in G$ esetén a $\gamma(s) : E \to E$ bijekciót az $s \in G$* **csoportelemet ábrázoló** *vagy* **reprezentáló operátornak** *nevezzük.*

Tehát ha γ ábrázolása a G csoportnak az E halmazban, akkor $\gamma : G \to \mathfrak{S}(E)$ olyan függvény, hogy minden $s, t \in G$ esetén $\gamma(st) = \gamma(s) \circ \gamma(t)$. Ekkor automatikusan teljesül az, hogy $\gamma\left(e_G\right) = \mathrm{id}_E$ és minden $s \in G$ elemre $\gamma\left(s^{-1}\right) = (\gamma(s))^{-1}$ (13.1.3.).

13.2.4. Definíció. *Legyen γ (illetve γ') ábrázolása a G csoportnak az E (illetve E') halmazban. Azt mondjuk, hogy γ és γ'* **ekvivalensek**, *ha létezik olyan $\sigma : E \to E'$ bijekció, amelyre minden $s \in G$ esetén $\sigma \circ \gamma(s) = \gamma'(s) \circ \sigma$, vagyis a következő diagram kommutatív.*

$$\begin{tikzcd} E \arrow[r, "\gamma(s)"] \arrow[d, "\sigma"'] & E \arrow[d, "\sigma"] \\ E' \arrow[r, "\gamma'(s)"'] & E' \end{tikzcd}$$

13.2.5. Állítás. *Legyen G csoport és $\mathscr{R}$ a G csoport ábrázolásainak tetszőleges halmaza. Ekkor a*

$$\{\ (\gamma, \gamma') \in \mathscr{R} \times \mathscr{R} \mid \text{"a } \gamma \text{ és } \gamma' \text{ ábrázolások ekvivalensek"}\ \}$$

reláció ekvivalencia az $\mathscr{R}$ halmaz felett.

Bizonyítás. Jelölje R az állításban értelmezett $\mathscr{R}$ feletti relációt.

Ha $\gamma \in \mathscr{R}$ és E a γ ábrázolás tere, akkor $\mathrm{id}_E : E \to E$ olyan bijekció, amelyre $\mathrm{id}_E \circ \gamma(s) = \gamma(s) \circ \mathrm{id}_E$, tehát $(\gamma, \gamma) \in R$, vagyis az R reláció reflexív az $\mathscr{R}$ halmaz felett.

Legyen $(\gamma, \gamma') \in R$, és jelölje E (illetve E') a γ (illetve γ') ábrázolás terét. Vegyünk olyan $\sigma : E \to E'$ bijekciót, amelyre minden $s \in G$ esetén $\sigma \circ \gamma(s) = \gamma'(s) \circ \sigma$. Ekkor $\sigma^{-1} : E' \to E$ olyan bijekció, amelyre minden $s \in G$ esetén $\sigma^{-1} \circ \gamma'(s) = \gamma(s) \circ \sigma^{-1}$, ezért $(\gamma', \gamma) \in R$. Tehát az R reláció szimmetrikus.

Legyenek $(\gamma, \gamma') \in R$ és $(\gamma', \gamma'') \in R$, továbbá jelölje E a γ, és E' a γ', és E'' a γ'' ábrázolás terét. Legyen $\sigma : E \to E'$ olyan bijekció, amelyre minden $s \in G$ esetén $\sigma \circ \gamma(s) = \gamma'(s) \circ \sigma$, és legyen $\sigma' : E' \to E''$ olyan bijekció, amelyre minden $s \in G$ esetén $\sigma' \circ \gamma'(s) = \gamma''(s) \circ \sigma'$. Ekkor $\sigma' \circ \sigma : E \to E''$ olyan bijekció, amelyre minden $s \in G$ esetén $(\sigma' \circ \sigma) \circ \gamma(s) = \gamma''(s) \circ (\sigma' \circ \sigma)$, ezért $(\gamma, \gamma'') \in R$. Tehát az R reláció tranzitív. ∎

13.2.6. Definíció. *Ha γ ábrázolása a G csoportnak az E halmazban, akkor*

$$\mathrm{R}_\gamma := \{\ (x, y) \in E \times E \mid (\exists s \in G)\ y = \gamma(s)x\ \}.$$

13.2.7. Állítás. *Ha γ ábrázolása a G csoportnak az E halmazban, akkor az R_γ reláció ekvivalencia az E halmaz felett.*

Bizonyítás. Ha $x \in E$, akkor $e_G \in G$ olyan, hogy $x = \gamma\left(e_G\right)x$, ezért $(x, x) \in \mathrm{R}_\gamma$. Tehát az R_γ reláció reflexív az E halmazon.

Legyen $(x, y) \in \mathrm{R}_\gamma$, és vegyünk olyan $s \in G$ elemet, amelyre $y = \gamma(s)x$. Ekkor

$$\gamma\left(s^{-1}\right)y = \gamma\left(s^{-1}\right)(\gamma(s)x) = \left(\gamma\left(s^{-1}\right) \circ \gamma(s)\right)x = \gamma\left(s^{-1}s\right)x = \gamma\left(e_G\right)x = x,$$

ezért $(y, x) \in \mathrm{R}_\gamma$. Tehát az R_γ reláció szimmetrikus.

Legyenek $(x, y) \in \mathrm{R}_\gamma$ és $(y, z) \in \mathrm{R}_\gamma$, továbbá vegyünk olyan $s, t \in G$ elemeket, amelyekre $y = \gamma(s)x$ és $z = \gamma(t)y$. Ekkor $ts \in G$ olyan elem, amelyre

$$\gamma(ts)x = (\gamma(t) \circ \gamma(s))x = \gamma(t)(\gamma(s)x) = \gamma(t)y = z,$$

ezért $(x, z) \in \mathrm{R}_\gamma$. Tehát az R_γ reláció tranzitív. ∎

13.2.8. Állítás. *Ha γ ábrázolása a G csoportnak az $E \neq \emptyset$ halmazban, akkor a következő állítások ekvivalensek.*

(i) *Minden $x, y \in E$ esetén van olyan $s \in G$, amelyre $y = \gamma(s)x$.*

(ii) *Létezik olyan $x \in E$, hogy minden $y \in E$ elemhez van olyan $s \in G$, amelyre $y = \gamma(s)x$.*

(iii) $\mathrm{R}_\gamma = E \times E$.

Bizonyítás. (i)⇒(ii) Nyilvánvaló, mert $E \neq \emptyset$.

(ii)⇒(iii) Legyen $x \in E$ olyan, hogy minden $y \in E$ elemhez van olyan $s \in G$, amelyre $y = \gamma(s)x$. Vegyünk tetszőleges $(y, z) \in E \times E$ párt. Legyenek $s, t \in G$ olyan csoportelemek, amelyekre $y = \gamma(s)x$ és $z = \gamma(t)x$. Ekkor

$$z = \gamma(t)x = \gamma\left(\left(ts^{-1}\right)s\right)x = \gamma\left(ts^{-1}\right)(\gamma(s)x) = \gamma\left(ts^{-1}\right)y,$$

tehát $(y, z) \in \mathrm{R}_\gamma$, ezért $E \times E \subseteq \mathrm{R}_\gamma$.

(iii)⇒(i) Triviális. ■

13.2.9. Definíció. *Legyen γ ábrázolása a G csoportnak az E halmazban.*

– *Minden $x \in E$ esetén a $\{\gamma(s)x | s \in G\}$ halmazt, tehát az x pont R_γ szerinti ekvivalencia-osztályát az x pont* **γ-pályájának**, *vagy* **γ-orbitjának** *nevezzük;*

– *Azt mondjuk, hogy a γ* **ábrázolás tranzitív**, *ha teljesül rá az előző állítás* (i) *feltétele.*

13.3. Véges permutációcsoport előjel-függvénye

Jelölés. Minden $n \in \mathbb{N}$ esetén $\mathfrak{S}_n$ jelöli az $n \to n$ bijekciók halmazát. Továbbá, $n \in \mathbb{N}$ esetén az $\mathfrak{S}_n$ felett értelmezett függvénykompozíció műveletet a $\circ$ szimbólummal jelöljük.

Ha $n \in \mathbb{N}$, akkor az $(\mathfrak{S}_n, \circ)$ pár *csoport*, ezt nevezzük az n természetes szám **teljes permutációcsoportjának**, és ha $m \in \mathbb{N}$ és $(\sigma_k)_{k \in [\![0,m]\!]}$ tetszőleges $\mathfrak{S}_n$-ben haladó rendszer, akkor értelmezve van az $\mathop{\bigcirc}\limits_{k=0}^{m} \sigma_k$ objektum, amely eleme $\mathfrak{S}_n$-nek. Azonban $n \geq 2$ esetén a függvénykompozíció-művelet nem kommutatív $\mathfrak{S}_n$ felett, ezért ha I nem üres véges halmaz és $(\sigma_i)_{i \in I}$ egy $\mathfrak{S}_n$-ben haladó rendszer, akkor a $\mathop{\bigcirc}\limits_{i \in I} \sigma_i$ objektum csak akkor van értelmezve, ha minden $i, j \in I$ esetén $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$.

13.3.1. Definíció. *Ha $n \in \mathbb{N}$, akkor egy $\sigma \in \mathfrak{S}_n$ permutációt* **transzpozíciónak** *nevezünk, ha léteznek olyan $i, j \in n$ elemek, hogy $i \neq j$ és $\sigma(i) = j$, és $\sigma(j) = i$, valamint minden $k \in n$ esetén, ha $k \neq i$ és $k \neq j$, akkor $\sigma(k) = k$.*

13.3.2. Lemma. *Legyen $n \in \mathbb{N}$. Ekkor minden $m \in \mathbb{N}$ esetén, ha $(\sigma_k)_{k \in [\![0,m]\!]}$ olyan $\mathfrak{S}_{n+1}$-ben haladó rendszer, amelyre minden $k \in [\![0, m]\!]$ esetén $\sigma_k(n) = n$, akkor*

$$\left(\mathop{\bigcirc}\limits_{k=0}^{m} \sigma_k\right)(n) = n,$$

és minden $j \in n$ esetén

$$\left(\mathop{\bigcirc}\limits_{k=0}^{m} \sigma_k\right)(j) = \left(\mathop{\bigcirc}\limits_{k=0}^{m} (\sigma_k|_n)\right)(j).$$

Bizonyítás. Adott $n \in \mathbb{N}$ esetén az állítást m szerinti teljes indukcióval bizonyítjuk. A 8.3.5. a) állítás szerint

$$\left(\mathop{\bigcirc}_{k=0}^{0} \sigma_k\right)(n) = \sigma_0(n) = n,$$

továbbá minden $j \in n$ esetén

$$\left(\mathop{\bigcirc}_{k=0}^{0} \sigma_k\right)(j) = \sigma_0(j) = (\sigma_0|_n)(j) = \left(\mathop{\bigcirc}_{k=0}^{0} (\sigma_k|_n)\right)(j),$$

ezért az állítás igaz, ha $m = 0$.

Tegyük fel, hogy az állítás teljesül a $m \in \mathbb{N}$ számra, és legyen $(\sigma_k)_{k\in[\![0,m+1]\!]}$ olyan $\mathfrak{S}_{n+1}$-ben haladó rendszer, amelyre minden $k \in [\![0, m+1]\!]$ esetén $\sigma_k(n) = n$. Ekkor a 8.3.5. a) állítás és az indukciós hipotézis szerint

$$\left(\mathop{\bigcirc}_{k=0}^{m+1} \sigma_k\right)(n) = \left(\left(\mathop{\bigcirc}_{k=0}^{m} \sigma_k\right) \circ \sigma_{m+1}\right)(n) = \left(\mathop{\bigcirc}_{k=0}^{m} \sigma_k\right)(\sigma_{m+1}(n)) = \left(\mathop{\bigcirc}_{k=0}^{m} \sigma_k\right)(n) = n,$$

továbbá minden $j \in n$ esetén az indukciós hipoztézis alkalmazásával

$$\left(\mathop{\bigcirc}_{k=0}^{m+1} \sigma_k\right)(j) = \left(\left(\mathop{\bigcirc}_{k=0}^{m} \sigma_k\right) \circ \sigma_{m+1}\right)(j) = \left(\mathop{\bigcirc}_{k=0}^{m} \sigma_k\right)((\sigma_{m+1})|_n(j)) =$$
$$= \left(\mathop{\bigcirc}_{k=0}^{m} (\sigma_k|_n)\right)((\sigma_{m+1})|_n(j)) = \left(\mathop{\bigcirc}_{k=0}^{m+1} (\sigma_k|_n)\right)(j),$$

ezért az állítás teljesül az $m + 1$ számra is. ■

13.3.3. Állítás. *Ha $n \in \mathbb{N}$ és $n \geq 2$, akkor minden $\sigma \in \mathfrak{S}_n$ permutációhoz létezik olyan $m \in \mathbb{N}$ és olyan $\mathfrak{S}_n$-ben haladó $(\sigma_k)_{k\in[\![0,m]\!]}$ rendszer, hogy minden $k \in [\![0, m]\!]$ esetén σ_k transzpozíció és*

$$\sigma = \mathop{\bigcirc}_{k=0}^{m} \sigma_k.$$

(*Minden véges permutáció előáll véges sok transzpozíció kompozíciójaként.*)

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk.

Ha $\sigma \in \mathfrak{S}_2$ az a permutáció, amelyre $\sigma(0) := 1$ és $\sigma(1) := 0$, akkor σ transzpozíció és nyilvánvaló, hogy $\mathrm{id}_2 = \sigma \circ \sigma$, ezért az állítás $n = 2$ esetén igaz.

Legyen $n \geq 2$ olyan természetes szám, amelyre az állítás igaz, és legyen S azon $\sigma \in \mathfrak{S}_{n+1}$ permutációk halmaza, amelyekhez létezik olyan $m \in \mathbb{N}$ és olyan $\mathfrak{S}_{n+1}$-ben haladó $(\sigma_k)_{k\in[\![0,m]\!]}$ rendszer, hogy minden $k \in [\![0, m]\!]$ esetén σ_k transzpozíció és $\sigma = \mathop{\bigcirc}_{k=0}^{m} \sigma_k$. Azt kell igazolni, hogy $S = \mathfrak{S}_{n+1}$.

Ha $\sigma, \sigma' \in S$, akkor $\sigma \circ \sigma' \in S$. Valóban, ekkor léteznek olyan $m, m' \in \mathbb{N}$ számok és olyan $\mathfrak{S}_{n+1}$-ben haladó $(\sigma_k)_{k\in[\![0,m]\!]}$ és $(\sigma'_k)_{k\in[\![0,m']\!]}$ rendszerek, hogy minden $k \in [\![0, m]\!]$ esetén σ_k transzpozíció, és minden $k \in [\![0, m']\!]$ esetén σ'_k transzpozíció, valamint $\sigma = \mathop{\bigcirc}_{k=0}^{m} \sigma_k$ és $\sigma' = \mathop{\bigcirc}_{k=0}^{m'} \sigma'_k$. Legyen $(\sigma''_k)_{k\in[\![0,m+m'+1]\!]}$ az a rendszer, amelyre minden $k \in [\![0, m + m' + 1]\!]$ esetén

$$\sigma''_k := \begin{cases} \sigma_k & , \text{ha } 0 \leq k \leq m; \\ \sigma'(k - (m+1)) & , \text{ha } m + 1 \leq k \leq m + m' + 1. \end{cases}$$

Ekkor 8.3.5. d) szerint

$$\sigma \circ \sigma' = \left(\bigcirc_{k=0}^{m} \sigma_k \right) \circ \left(\bigcirc_{k=0}^{m'} \sigma'_k \right) = \bigcirc_{k=0}^{m+m'+1} \sigma''_k,$$

és természetesen minden $k \in [\![0, m + m' + 1]\!]$ esetén $\sigma''_k \in \mathfrak{S}_{n+1}$ transzpozíció, ezért $\sigma \circ \sigma' \in S$.

Most megmutatjuk, hogy ha $\sigma \in \mathfrak{S}_{n+1}$ olyan, hogy $\sigma(n) = n$, akkor $\sigma \in S$. Valóban, ekkor $\sigma|_n \in \mathfrak{S}_n$, így az indukciós hipotézis szerint létezik olyan $m \in \mathbb{N}$ és olyan $\mathfrak{S}_n$-ben haladó $(\sigma'_k)_{k \in [\![0,m]\!]}$ rendszer, hogy minden $k \in [\![0, m]\!]$ esetén σ'_k transzpozíció és $\sigma|_n = \bigcirc_{k=0}^{m} \sigma'_k$. Minden $k \in [\![0, m]\!]$ esetén legyen $\sigma_k : n+1 \to n+1$ az a függvény, amelyre minden $j \in n + 1$ esetén

$$\sigma_k(j) := \begin{cases} \sigma'_k(j) & \text{, ha } j \neq n; \\ n & \text{, ha } j = n, \end{cases}$$

tehát $\sigma_k|_n = \sigma'_k$ és $\sigma_k(n) := n$. Világos, hogy minden $k \in [\![0, m]\!]$ számra $\sigma_k \in \mathfrak{S}_{n+1}$ és σ_k transzpozíció, továbbá az előző lemma szerint

$$\left(\bigcirc_{k=0}^{m} \sigma_k \right)(n) = n = \sigma(n),$$

és minden $j \in n$ esetén

$$\left(\bigcirc_{k=0}^{m} \sigma_k \right)(j) = \left(\bigcirc_{k=0}^{m} (\sigma_k|_n) \right)(j) = \left(\bigcirc_{k=0}^{m} \sigma'_k \right)(j) = \sigma|_n(j) = \sigma(j),$$

tehát $\bigcirc_{k=0}^{m} \sigma_k = \sigma$, vagyis $\sigma \in S$.

Végül, legyen $\sigma \in \mathfrak{S}_{n+1}$ tetszőleges. Megmutatjuk, hogy $\sigma \in S$. Ha $\sigma(n) = n$, akkor az előző bekezdés alapján $\sigma \in S$, ezért feltehetjük, hogy $\sigma(n) \neq n$. Legyen $\sigma_* : n+1 \to n+1$ az a függvény, amelyre $\sigma_*(\sigma(n)) := n$ és $\sigma_*(n) := \sigma(n)$ és minden $k \in n + 1$ esetén, ha $n \neq k \neq \sigma(n)$, akkor $\sigma_*(k) = k$. Ekkor $\sigma_* \in \mathfrak{S}_{n+1}$ és σ_* transzpozíció, tehát $\sigma_* \in S$. Továbbá, $(\sigma_* \circ \sigma)(n) = n$, ezért $\sigma_* \circ \sigma \in S$. Mivel $\sigma_*^{-1} = \sigma_*$, ebből következik, hogy $\sigma = \sigma_*^{-1} \circ (\sigma_* \circ \sigma) \in S$, amit bizonyítani kellett. ■

13.3.4. Tétel. *Legyen $n \in \mathbb{N}^*$, és minden $\sigma \in \mathfrak{S}_n$ esetén*

$$\mathrm{T}_n(\sigma) := \{ \ (i, j) \ \in \ n \times n \mid (i < j) \wedge (\sigma(i) > \sigma(j)) \ \}.$$

Ekkor minden $\sigma \in \mathfrak{S}_n$ esetén $\mathrm{Card}(\mathrm{T}_n(\sigma)) = \mathrm{Card}(\mathrm{T}_n(\sigma^{-1}))$, és az

$$\varepsilon_n : \mathfrak{S}_n \to \{-1, 1\}; \quad \sigma \mapsto (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))}$$

leképezés az egyetlen olyan $\mathfrak{S}_n \to \{-1, 1\}$ függvény, amelyre teljesülnek a következők:

a) $\varepsilon_n(\mathrm{id}_n) = 1$.

b) *Minden $\sigma, \tau \in \mathfrak{S}_n$ esetén $\varepsilon_n(\tau \circ \sigma) = \varepsilon_n(\tau) \cdot \varepsilon_n(\sigma)$.*

c) *Minden $\sigma \in \mathfrak{S}_n$ transzpozícióra $\varepsilon_n(\sigma) = -1$.*

Bizonyítás. (*Egzisztencia.*) Feltehetjük, hogy $n \geq 2$, mert $n = 1$ esetén $\mathfrak{S}_n$ egy elemű, így ε_n létezése nyilvánvaló.

Ha $\sigma \in \mathfrak{S}_n$, akkor könnyen látható, hogy a

$$\begin{aligned} \mathrm{T}_n(\sigma) \to \mathrm{T}_n(\sigma^{-1}); &\quad (i,j) \mapsto (\sigma(j), \sigma(i)), \\ \mathrm{T}_n(\sigma^{-1}) \to \mathrm{T}_n(\sigma); &\quad (i,j) \mapsto (\sigma^{-1}(j), \sigma^{-1}(i)) \end{aligned}$$

leképezések egymás inverzei, tehát $\mathrm{T}_n(\sigma)$ és $\mathrm{T}_n(\sigma^{-1})$ ekvipotensek, így $\mathrm{Card}(\mathrm{T}_n(\sigma)) = \mathrm{Card}(\mathrm{T}_n(\sigma^{-1}))$.

Vezessük be a

$$\mathrm{P}_n : \mathfrak{S}_n \to \mathbb{Z}; \quad \sigma \mapsto \prod_{\substack{(i,j) \,\in\, n\times n \\ i<j}} (\sigma(j) - \sigma(i))$$

függvényt. Megmutatjuk, hogy minden $\tau, \sigma \in \mathfrak{S}_n$ esetén

$$\mathrm{P}_n(\tau \circ \sigma) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \mathrm{P}_n(\tau).$$

Ehhez először értelmezzük a

$$\mathrm{H}_n := \{\ (i,j) \ \in\ n \times n \mid (i < j)\ \},$$

halmazt. Legyenek $\tau, \sigma \in \mathfrak{S}_n$ rögzítve. Világos, hogy a

$$f : \mathrm{H}_n \ \to\ \mathrm{H}_n; \quad (i,j) \mapsto \begin{cases} (\sigma^{-1}(i), \sigma^{-1}(j)) & \text{, ha } \sigma^{-1}(i) < \sigma^{-1}(j); \\ (\sigma^{-1}(j), \sigma^{-1}(i)) & \text{, ha } \sigma^{-1}(j) < \sigma^{-1}(i), \end{cases}$$

$$g : \mathrm{H}_n \ \to\ \mathrm{H}_n; \quad (i,j) \mapsto \begin{cases} (\sigma(i), \sigma(j)) & \text{, ha } \sigma(i) < \sigma(j); \\ (\sigma(j), \sigma(i)) & \text{, ha } \sigma(j) < \sigma(i) \end{cases}$$

leképezések egymás inverzei, tehát mindkét függvény permutációja H_n-nek. Ebből a véges műveletek általános kommutativitása alapján kapjuk, hogy

$$\begin{aligned} \mathrm{P}_n(\tau \circ \sigma) &= \prod_{(i,j)\in \mathrm{H}_n} ((\tau\circ\sigma)(j) - (\tau\circ\sigma)(i)) = \prod_{(i,j)\in \mathrm{H}_n} ((\tau\circ\sigma)(\mathrm{pr}_2(i,j)) - (\tau\circ\sigma)(\mathrm{pr}_1(i,j))) = \\ &= \prod_{(i,j)\in \mathrm{H}_n} ((\tau\circ\sigma)(\mathrm{pr}_2(f(i,j))) - (\tau\circ\sigma)(\mathrm{pr}_1(f(i,j)))). \end{aligned}$$

Három eset lehetséges.

1) $\mathrm{T}_n(\sigma^{-1}) = \emptyset$, vagyis $\sigma^{-1} : n \to n$ *szigorúan monoton növő* függvény, így $\sigma^{-1} = \mathrm{id}_n$, tehát $\sigma = \mathrm{id}_n$. Ekkor $\mathrm{Card}(\mathrm{T}_n(\sigma)) = 0$ miatt

$$\mathrm{P}_n(\tau\circ\sigma) = \mathrm{P}_n(\tau) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \mathrm{P}_n(\tau).$$

2) $\mathrm{H}_n \setminus \mathrm{T}_n(\sigma^{-1}) = \emptyset$, vagyis $\mathrm{H}_n = \mathrm{T}_n(\sigma^{-1})$. Ekkor minden $(i,j) \in \mathrm{H}_n$ esetén $\sigma^{-1}(j) < \sigma^{-1}(i)$, tehát $f(i,j) = (\sigma^{-1}(j), \sigma^{-1}(i))$, következésképpen

$$\begin{aligned} \mathrm{P}_n(\tau\circ\sigma) &= \prod_{(i,j)\in \mathrm{H}_n} ((\tau\circ\sigma)(\sigma^{-1}(i)) - (\tau\circ\sigma)(\sigma^{-1}(j))) = \prod_{(i,j)\in \mathrm{H}_n} (\tau(i) - \tau(j)) = \\ &= \prod_{(i,j)\in \mathrm{H}_n} ((-1)(\tau(j) - \tau(i))) \overset{(1)}{=} \Big(\prod_{(i,j)\in \mathrm{H}_n} (-1)\Big)\Big(\prod_{(i,j)\in \mathrm{H}_n} (\tau(j) - \tau(i))\Big) \overset{(2)}{=} \\ &\overset{(2)}{=} (-1)^{\mathrm{Card}(\mathrm{H}_n)} \mathrm{P}_n(\tau) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma^{-1}))} \mathrm{P}_n(\tau) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \mathrm{P}_n(\tau), \end{aligned}$$

ahol az $\overset{(1)}{=}$ egyenlőségnél a 8.5.9. állítást alkalmaztuk, és a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk a 9.1.1. állítást.

3) $\mathrm{T}_n(\sigma^{-1}) \neq \emptyset$ és $\mathrm{H}_n \setminus \mathrm{T}_n(\sigma^{-1}) \neq \emptyset$. Ekkor a $\mathbb{Z}$ feletti szorzásra alkalmazhatjuk a 8.5.4. állítást, ezért az f függvény definíciója alapján

$$\mathrm{P}_n(\tau \circ \sigma) = A \cdot B,$$

ahol

$$A := \prod_{(i,j)\in \mathrm{T}_n(\sigma^{-1})} ((\tau\circ\sigma)(\sigma^{-1}(i)) - (\tau\circ\sigma)(\sigma^{-1}(j))) = \prod_{(i,j)\in \mathrm{T}_n(\sigma^{-1})} (\tau(i) - \tau(j)),$$
$$B := \prod_{(i,j)\in \mathrm{H}_n\setminus \mathrm{T}_n(\sigma^{-1})} ((\tau\circ\sigma)(\sigma^{-1}(j)) - (\tau\circ\sigma)(\sigma^{-1}(i))) = \prod_{(i,j)\in \mathrm{H}_n\setminus \mathrm{T}_n(\sigma^{-1})} (\tau(j) - \tau(i)).$$

Ekkor

$$A = \prod_{(i,j)\in \mathrm{T}_n(\sigma^{-1})} ((-1)(\tau(j) - \tau(i))) = \Bigg(\prod_{(i,j)\in \mathrm{T}_n(\sigma^{-1})} (-1) \Bigg) \Bigg(\prod_{(i,j)\in \mathrm{T}_n(\sigma^{-1})} (\tau(j) - \tau(i)) \Bigg) =$$
$$= (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \Bigg(\prod_{(i,j)\in \mathrm{T}_n(\sigma^{-1})} (\tau(j) - \tau(i)) \Bigg),$$

ahol ismét a 8.5.9. és 9.1.1. állításokat alkalmaztuk. Ez azt jelenti, hogy

$$\mathrm{P}_n(\tau\circ\sigma) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \Bigg(\prod_{(i,j)\in \mathrm{T}_n(\sigma^{-1})} (\tau(j) - \tau(i)) \Bigg) \Bigg(\prod_{(i,j)\in \mathrm{H}_n\setminus \mathrm{T}_n(\sigma^{-1})} (\tau(j) - \tau(i)) \Bigg) \overset{(3)}{=}$$
$$\overset{(3)}{=} (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \Bigg(\prod_{(i,j)\in \mathrm{H}_n} (\tau(j) - \tau(i)) \Bigg) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \mathrm{P}_n(\tau),$$

ahol az $\overset{(3)}{=}$ egyenlőségnél ismét a 8.5.4. állításra hivatkozhatunk.
Ezzel megmutattuk, hogy minden $\tau, \sigma \in \mathfrak{S}_n$ esetén

$$\mathrm{P}_n(\tau\circ\sigma) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \mathrm{P}_n(\tau).$$

Ide $\sigma \in \mathfrak{S}_n$ esetén a $\tau := \mathrm{id}_n$ permutációt helyettesítve kapjuk, hogy

$$\mathrm{P}_n(\sigma) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \mathrm{P}_n(\mathrm{id}_n).$$

Ebből következik, hogy minden $\tau, \sigma \in \mathfrak{S}_n$ esetén

$$(-1)^{\mathrm{Card}(\mathrm{T}_n(\tau\circ\sigma))} \mathrm{P}_n(\mathrm{id}_n) = \mathrm{P}_n(\tau\circ\sigma) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} \mathrm{P}_n(\tau) =$$
$$= (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} (-1)^{\mathrm{Card}(\mathrm{T}_n(\tau))} \mathrm{P}_n(\mathrm{id}_n).$$

Nyilvánvaló, hogy $\mathrm{P}_n(\mathrm{id}_n) \in \mathbb{N}^*$, sőt teljes indukcióval könnyen igazolható, hogy $\mathrm{P}_n(\mathrm{id}_n) = \prod_{k=1}^{n-1} k!$, ezért ebből a $\mathbb{Z}$ feletti szorzás kancellativitása alapján következik, hogy minden $\tau, \sigma \in \mathfrak{S}_n$ esetén

$$\varepsilon_n(\tau\circ\sigma) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\tau\circ\sigma))} = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} (-1)^{\mathrm{Card}(\mathrm{T}_n(\tau))} = \varepsilon_n(\tau) \cdot \varepsilon_n(\sigma),$$

tehát ε_n-re b) teljesül. Ugyanakkor ε_n-re a) nyilvánvalóan igaz, mert $\mathrm{T}_n(\mathrm{id}_n) = \emptyset$.
Végül bebizonyítjuk, hogy ε_n-re c) is teljesül. Ehhez legyen $\sigma \in \mathfrak{S}_n$ transzpozíció, és legyenek $i_0, j_0 \in n$ olyanok, hogy $i_0 \neq j_0$ és $\sigma(i_0) = j_0$ és $\sigma(j_0) = i_0$, valamint minden

$k \in n$ esetén, ha $k \neq i_0$ és $k \neq j_0$, akkor $\sigma(k) = k$. Nyilvánvaló, hogy az általánosság korlátozása nélkül feltehetjük, hogy $i_0 < j_0$. Ekkor

$$\begin{gathered}\mathrm{T}_n(\sigma) = \{(i,j) \in n \times n | (i<j) \wedge (\sigma(i) > \sigma(j))\} = \\ =\{(i_0,j) \in n \times n | (i_0 < j) \wedge (j_0 > \sigma(j))\} \cup \{(i,j) \in n \times n | (i \neq i_0) \wedge (i<j) \wedge (\sigma(i) > \sigma(j))\}= \\ = \{(i_0,j) \in n \times n | (i_0 < j) \wedge (j_0 > \sigma(j))\} \cup \{(i,j_0) \in n \times n | (i \neq i_0) \wedge (i<j_0) \wedge (\sigma(i) > i_0)\} \cup \\ \cup \{(i,j) \in n \times n | (i \neq i_0) \wedge (j \neq j_0) \wedge (i<j) \wedge (\sigma(i) > \sigma(j))\}.\end{gathered}$$

Ha $(i,j) \in n \times n$ és $i \neq i_0$ és $j \neq j_0$ és $i < j$, akkor $\sigma(i) = i < j = \sigma(j)$, ezért

$$\{(i,j) \in n \times n | (i \neq i_0) \wedge (j \neq j_0) \wedge (i<j) \wedge (\sigma(i) > \sigma(j))\} = \emptyset.$$

Ugyanakkor $(i_0, j_0) \in \{(i_0,j) \in n \times n | (i_0 < j) \wedge (j_0 > \sigma(j))\}$, és ha $j \in n$ olyan, hogy $i_0 < j$ és $j \neq j_0$, akkor $\sigma(j) = j$. Ez azt jelenti, hogy

$$\begin{gathered}\{(i_0,j) \in n \times n | (i_0 < j) \wedge (j_0 > \sigma(j))\} = \\ = \{(i_0,j_0)\} \cup \{(i_0,j) \in n \times n | (i_0 < j) \wedge (j \neq j_0) \wedge (j_0 > j)\} = \{(i_0,j_0)\} \cup (\{i_0\} \times]\!]i_0, j_0[\![) \, .\end{gathered}$$

Továbbá, ha $i \in n$ és $i \neq i_0$ és $i < j_0$, akkor $\sigma(i) = i$, ezért

$$\begin{gathered}\{(i,j_0) \in n \times n | (i \neq i_0) \wedge (i < j_0) \wedge (\sigma(i) > i_0)\} = \\ = \{(i,j_0) \in n \times n | (i \neq i_0) \wedge (i < j_0) \wedge (i > i_0)\} =]\!]i_0, j_0[\![\times \{j_0\}.\end{gathered}$$

Ezzel megmutattuk, hogy

$$\mathrm{T}_n(\sigma) = \{(i_0,j_0)\} \cup (\{i_0\} \times]\!]i_0, j_0[\![) \cup (]\!]i_0, j_0[\![\times \{j_0\}) \, ,$$

és itt a jobb oldalon három diszjunkt halmaz áll, tehát 9.1.4. alapján

$$\mathrm{Card}(\mathrm{T}_n(\sigma)) = 1 + \mathrm{Card}\,(\{i_0\} \times]\!]i_0, j_0[\![) + \mathrm{Card}\,(]\!]i_0, j_0[\![\times \{j_0\}) \, .$$

Végül, nyilvánvaló, hogy a

$$\{i_0\} \times]\!]i_0, j_0[\![\ \rightarrow \ ]\!]i_0, j_0[\![\times \{j_0\}; \quad (i_0, k) \mapsto (k, j_0)$$

leképezés bijekció, ezért

$$m := \mathrm{Card}\,(\{i_0\} \times]\!]i_0, j_0[\![) = \mathrm{Card}\,(]\!]i_0, j_0[\![\times \{j_0\}) \, .$$

Ebből következik, hogy $\mathrm{Card}(\mathrm{T}_n(\sigma)) = 2m+1$, tehát $\varepsilon_n(\sigma) = (-1)^{\mathrm{Card}(\mathrm{T}_n(\sigma))} = -1$, amit bizonyítani kellett.

(*Unicitás.*) Legyenek $\varepsilon, \varepsilon' : \mathfrak{S}_n \rightarrow \{-1, 1\}$ olyan függvények, amelyekre a), b) és c) teljesül, ε_n helyére ε-t és ε'-t helyettesítve. Ekkor az $S := \{\sigma \in \mathfrak{S}_n | \varepsilon(\sigma) = \varepsilon'(\sigma)\}$ halmazra a) miatt $\mathrm{id}_n \in S$ teljesül, és c)-ből következik, hogy $\mathfrak{S}_n$ minden transzpozíciója eleme S-nek.

Most m szerinti teljes indukcióval igazoljuk, hogy minden $m \in \mathbb{N}$ esetén, minden S-ben haladó $(\sigma_k)_{k \in [\![0,m]\!]}$ rendszerre $\bigcirc_{k=0}^{m} \sigma_k \in S$. Ez 8.3.5. a) szerint nyilvánvalóan igaz, ha $m = 0$. Ha $m \in \mathbb{N}$ olyan, hogy m-re teljesül az állítás, és $(\sigma_k)_{k \in [\![0,m+1]\!]}$ egy S-ben haladó rendszer, akkor 8.3.5. b) alapján

$$\bigcirc_{k=0}^{m+1} \sigma_k = \left(\bigcirc_{k=0}^{m} \sigma_k \right) \circ \sigma_{m+1} \in S,$$

mert az indukciós hipotézis szerint $\mathop{\circ}\limits_{k=0}^{m} \sigma_k \in S$, továbbá a hipotézis szerint $\sigma_{m+1} \in S$, valamint a b) feltételből következik, hogy minden $\sigma, \tau \in S$ esetén $\sigma \circ \tau \in S$.

Ha $n = 1$, akkor $\mathfrak{S}_n$ egy elemű, tehát $S = \mathfrak{S}_n$. Ha $n \geq 2$, akkor az előző állítás szerint $\mathfrak{S}_n$ minden eleme előáll véges sok transzpozíció, tehát véges egy véges S-beli rendszer kompozíciójaként, tehát az előzőek szerint $S = \mathfrak{S}_n$. Ez azt jelenti, hogy $\varepsilon = \varepsilon'$. ■

13.3.5. Definíció. *Ha $n \in \mathbb{N}^*$ és $\sigma \in \mathfrak{S}_n$, akkor az előző tételben értelmezett $\varepsilon_n(\sigma) \in \{-1, 1\}$ számot a σ permutáció* **előjelének** *nevezzük, és az $\varepsilon_n : \mathfrak{S}_n \to \{-1, 1\}$ függvényt az $\mathfrak{S}_n$ permutációcsoport* **előjel-függvényének** *nevezzük.*

13.3.6. Definíció. *Az E halmaz* **transzpozíciójának** *nevezünk minden olyan $\tau : E \to E$ bijekciót, amelyhez léteznek olyan $x, y \in E$ elemek, hogy $x \neq y$ és $\tau(x) = y$, $\tau(y) = x$, és minden $z \in E \setminus \{x, y\}$ elemre $\tau(z) = z$.*

13.3.7. Állítás. *Ha E és F halmazok, és $f : E \to F$ bijekció, akkor minden $\sigma \in \mathfrak{S}(E)$ esetén $f \circ \sigma \circ f^{-1} \in \mathfrak{S}(F)$, és az*

$$\widehat{f} : \mathfrak{S}(E) \to \mathfrak{S}(F); \quad \sigma \mapsto f \circ \sigma \circ f^{-1}$$

leképezés olyan izomorfizmus az $\mathfrak{S}(E)$ és $\mathfrak{S}(F)$ permutációcsoportok között, hogy

$$\widehat{f}^{-1} = \widehat{f^{-1}},$$

és az E halmaz minden τ transzpozíciójára $\widehat{f}(\tau)$transzpozíciója az F halmaznak.

Bizonyítás. Ha $\sigma, \sigma' \in \mathfrak{S}(E)$, akkor $\mathrm{id}_E = f^{-1} \circ f$ miatt

$$\begin{aligned} f \circ (\sigma \circ \sigma') \circ f^{-1} &= f \circ (\sigma \circ \mathrm{id}_E \circ \sigma') \circ f^{-1} = \\ = f \circ (\sigma \circ f^{-1} \circ f \circ \sigma') \circ f^{-1} &= \left(f \circ \sigma \circ f^{-1}\right) \circ \left(f \circ \sigma' \circ f^{-1}\right), \end{aligned}$$

ezért a szóban forgó leképezés csoport-morfizmus.

A definíció alkalmazásával könnyen ellenőrizhető, hogy $\widehat{f^{-1}} \circ \widehat{f} = \mathrm{id}_{\mathfrak{S}(E)}$ és $\widehat{f} \circ \widehat{f^{-1}} = \mathrm{id}_{\mathfrak{S}(F)}$, tehát $\widehat{f} : \mathfrak{S}(E) \to \mathfrak{S}(F)$ bijekció és $\widehat{f}^{-1} = \widehat{f^{-1}}$.

Legyen τ transzpozíciója az E halmaznak, és legyenek $x, y \in E$ olyan elemek, hogy $x \neq y$ és $\tau(x) = y$, $\tau(y) = x$, és minden $z \in E \setminus \{x, y\}$ elemre $\tau(z) = z$. Ekkor $f(x),\ f(y) \in F$ olyan elemek, hogy $f(x) \neq f(y)$, hiszen f injektív, továbbá a definíció szerint

$$\begin{aligned} \left(\widehat{f}(\tau)\right)(f(x)) &= (f \circ \tau \circ f^{-1})(f(x)) = f(\tau(x)) = f(y), \\ \left(\widehat{f}(\tau)\right)(f(y)) &= (f \circ \tau \circ f^{-1})(f(y)) = f(\tau(y)) = f(x), \end{aligned}$$

és ha $v \in F \setminus \{f(x), f(y)\}$, akkor $f^{-1}(v) \in E$ olyan, hogy $f^{-1}(v) \neq x$ és $f^{-1}(v) \neq y$, ezért $\tau(f^{-1}(v)) = f^{-1}(v)$, így

$$\left(\widehat{f}(\tau)\right)(v) = (f \circ \tau \circ f^{-1})(v) = f(f^{-1}(v)) = v.$$

Ez azt jelenti, hogy $\widehat{f}(\tau)$ transzpozíciója az F halmaznak. ■

13.3.8. Tétel. *Ha E véges halmaz, akkor létezik egyetlen olyan $\varepsilon : \mathfrak{S}(E) \to \{-1, 1\}$ leképezés, amely csoport-morfizmus az $\mathfrak{S}(E)$ permutációcsoport és a $\{-1, 1\}$ multiplikatív csoport között, és amelyre teljesül az, hogy minden $\tau : E \to E$ transzpozícióra fennáll az $\varepsilon(\tau) = -1$ egyenlőség.*

Bizonyítás. Ha $E = \emptyset$, akkor $\mathfrak{S}(E)$ egy elemű csoport, így ε_E egzisztenciája és unicitása triviális. A továbbiakban feltesszük, hogy $E \neq \emptyset$ véges halmaz és $n := \mathrm{Card}(E)$.

Rögzítsünk egy $f : E \to n$ bijekciót és vezessük be az

$$\widehat{f} : \mathfrak{S}(E) \to \mathfrak{S}_n; \quad \sigma \mapsto f \circ \sigma \circ f^{-1}$$

leképezést, amely az előző állítás szerint olyan izomorfizmus az $\mathfrak{S}(E)$ és $\mathfrak{S}_n$ permutációcsoportok között, hogy az E halmaz minden τ transzpozíciójára $\widehat{f}(\tau)$ transzpozíciója az n halmaznak. Ugyanakkor az $\varepsilon_n : \mathfrak{S}_n \to \{0,1\}$ előjelfüggvény olyan olyan csoport-morfizmus az $\mathfrak{S}_n$ permutációcsoport és a $\{-1,1\}$ multiplikatív csoport között, hogy n minden τ transzpozíciójára $\varepsilon_n(\tau) = -1$. Ezért az $\varepsilon_n \circ \widehat{f} : \mathfrak{S}(E) \to \{-1,1\}$ leképezés olyan csoport-morfizmus az $\mathfrak{S}(E)$ permutációcsoport és a $\{-1,1\}$ multiplikatív csoport között, hogy az E halmaz minden τ transzpozíciójára $(\varepsilon_n \circ \widehat{f})(\tau) = -1$, amivel az előírt tulajdonságú leképezés létezését igazoltuk.

Az unicitás bizonyításához legyenek $\varepsilon, \varepsilon' : \mathfrak{S}(E) \to \{-1,1\}$ olyan csoport-morfizmusok, hogy az E halmaz minden τ transzpozíciójára $\varepsilon(\tau) = -1 = \varepsilon'(\tau)$. Rögzítsünk egy $g : n \to E$ bijekciót és vezessük be az

$$\widehat{g} : \mathfrak{S}_n \to \mathfrak{S}(E); \quad \sigma \mapsto g \circ \sigma \circ g^{-1}$$

leképezést, amely az előző állítás szerint olyan izomorfizmus az $\mathfrak{S}_n$ és $\mathfrak{S}(E)$ permutációcsoportok között, hogy az n halmaz minden τ transzpozíciójára $\widehat{g}(\tau)$ transzpozíciója az E halmaznak. Ekkor $\varepsilon \circ \widehat{g}$ és $\varepsilon' \circ \widehat{g}$ olyan csoport-morfizmusok a $\mathfrak{S}_n$ permutációcsoport és a $\{-1,1\}$ multiplikatív csoport között, amely az n halmaz minden transzpozíciójához a -1 értéket rendelik, így az n halmaz előjel-függvényének egyértelműsége folytán $\varepsilon \circ \widehat{g} = \varepsilon_n = \varepsilon' \circ \widehat{g}$, amiből a $\widehat{g} : \mathfrak{S}_n \to \mathfrak{S}(E)$ függvény bijektivitása alapján $\varepsilon = \varepsilon'$ következik. ■

13.3.9. Definíció. *Ha E véges halmaz, akkor ε_E jelöli azt az egyértelműen meghatározott csoport-morfizmust az $\mathfrak{S}(E)$ permutációcsoport és a $\{-1,1\}$ multiplikatív csoport között, amelyre teljesül az, hogy minden $\tau : E \to E$ transzpozícióra $\varepsilon_E(\tau) = -1$; és ezt az $\varepsilon_E : \mathfrak{S}(E) \to \{-1,1\}$ leképezést az $\mathfrak{S}(E)$ permutációcsoport* **előjel-függvényének** *nevezzük.*

13.3.10. Állítás. *Legyen E véges halmaz, $X \subseteq E$, és minden $\tau \in \mathfrak{S}(X)$ esetén jelölje $\widehat{\tau}$ az*

$$E \to E; \quad x \mapsto \begin{cases} \tau(x) & , \text{ha } x \in X, \\ x & , \text{ha } x \in E \setminus X \end{cases}$$

leképezést. Ekkor minden $\tau \in \mathfrak{S}(X)$ permutációra $\widehat{\tau} \in \mathfrak{S}(E)$ és a

$$\mathfrak{S}(X) \to \mathfrak{S}(E); \quad \tau \mapsto \widehat{\tau}$$

leképezés olyan csoport-morfizmus, amelyre minden $\tau \in \mathfrak{S}(X)$ esetén

$$\varepsilon_E(\widehat{\tau}) = \varepsilon_X(\tau).$$

Bizonyítás. Ha $\tau \in \mathfrak{S}(X)$, akkor $\widehat{\tau}$ nyilvánvalóan injektív az X és az $E \setminus X$ halmazon, továbbá $x \in X$ és $y \in E \setminus X$ esetén a definíció alapján $\widehat{\tau}(x) = \tau(x) \neq y = \widehat{\tau}(y)$, hiszen $\tau(x) \in X$ és $y \in E \setminus X$, tehát a $\widehat{\tau} : E \to E$ függvény injekció, így $\widehat{\tau} \in \mathfrak{S}(E)$ (8.1.16.).

Ha $\sigma, \tau \in \mathfrak{S}(X)$, akkor a definíció szerint

– $x \in X$ esetén $\widehat{\sigma}(\tau(x)) = \sigma(\tau(x))$ és $\widehat{\tau}(x) = \tau(x)$, így $\widehat{(\sigma \circ \tau)}(x) = (\sigma \circ \tau)(x) = \sigma(\tau(x)) = \widehat{\sigma}(\tau(x)) = \widehat{\sigma}(\widehat{\tau}(x)) = (\widehat{\sigma} \circ \widehat{\tau})(x)$,

– $x \in E \setminus X$ esetén $\widehat{\sigma}(x) = x = \widehat{\tau}(x)$, így $\widehat{(\sigma \circ \tau)}(x) = x = (\widehat{\sigma} \circ \widehat{\tau})(x)$.

Ez azt jelenti, hogy minden $\sigma, \tau \in \mathfrak{S}(X)$ esetén $\widehat{(\sigma \circ \tau)} = \widehat{\sigma} \circ \widehat{\tau}$, tehát az $\mathfrak{S}(X) \to \mathfrak{S}(E)$; $\tau \mapsto \widehat{\tau}$ leképezés csoport-morfizmus.

Végül, tekintsük az
$$\varepsilon : \mathfrak{S}(X) \to \{-1, 1\}; \quad \tau \mapsto \varepsilon_E(\widehat{\tau})$$
leképezést, amely az előzőek szerint csoport-morfizmus. Ha τ transzpozíciója X-nek és $x, y \in X$ olyan pontok, hogy $x \neq y$, és $\tau(x) = y$, $\tau(y) = x$, valamint minden $z \in X \setminus \{x, y\}$ esetén $\tau(z) = z$, akkor a definíció szerint $\widehat{\tau}(x) = \tau(x) = y$ és $\widehat{\tau}(y) = \tau(y) = x$, valamint minden $z \in E \setminus \{x, y\}$ esetén, ha $z \in X$, akkor $\widehat{\tau}(z) = \tau(z) = z$, és ha $z \notin X$, akkor $\widehat{\tau}(z) = z$, vagyis $\widehat{\tau}$ transzpozíciója E-nek, tehát $\varepsilon(\tau) = \varepsilon_E(\widehat{\tau}) = -1$. Ezért az előjelfüggvény egyértelműsége miatt $\varepsilon = \varepsilon_X$, ami pontosan azt jelenti, hogy minden $\tau \in \mathfrak{S}(X)$ esetén $\varepsilon_E(\widehat{\tau}) = \varepsilon_X(\tau)$. ■

13.4. Részcsoportok és tranzitív ábrázolások

13.4.1. Definíció. *A G csoport* **részcsoportjának** *nevezünk minden olyan $H \subseteq G$ halmazt, melyre*
$$H \neq \emptyset; \quad HH \subseteq H; \quad H^{-1} \subseteq H.$$

Vigyázzunk arra, hogy ha G csoport, akkor $H := \emptyset$ nyilvánvalóan olyan, hogy $HH = H$ és $H^{-1} = H$, de H *nem részcsoport.*

13.4.2. Állítás. *Ha G csoport és $H \subseteq G$, akkor a következő állítások ekvivalensek.*

(i) *H részcsoportja G-nek.*

(ii) *$e_G \in H$ és $HH = H = H^{-1}$.*

(iii) *$H \neq \emptyset$ és $HH^{-1} \subseteq H$.*

Bizonyítás. (i)⇒(ii) $H \neq \emptyset$, így vehetünk egy $s \in H$ elemet, és akkor $e_G = ss^{-1} \in HH^{-1} \subseteq HH \subseteq H$, tehát $e_G \in H$. Ezért $s \in H$ esetén $s = e_G s \in HH$, így $H \subseteq HH$, vagyis $H = HH$. Ha $s \in H$, akkor $s^{-1} \in H^{-1} \subseteq H$, azaz $s^{-1} \in H$, következésképpen $s = (s^{-1})^{-1} \in H^{-1}$, így $H \subseteq H^{-1}$, vagyis $H = H^{-1}$.

(i)⇒(iii) Triviális.

(iii)⇒(i) Ha $s \in H$, akkor $e_G = ss^{-1} \in HH^{-1} \subseteq H$, vagyis $e_G \in H$. Ebből következik, hogy minden $s \in H$ esetén $s^{-1} = e_G s^{-1} \in HH^{-1} \subseteq H$, tehát $H^{-1} \subseteq H$. Végül, ha $s, t \in H$, akkor $t^{-1} \in H$, ezért $st = s(t^{-1})^{-1} \in HH^{-1} \subseteq H$, tehát $HH \subseteq H$. ■

13.4.3. Állítás. *Ha H olyan nem üres véges részhalmaza a G csoportnak, hogy $HH \subseteq H$, akkor H részcsoportja G-nek.*

Bizonyítás. Legyen $s \in H$. A $HH \subseteq H$ feltételből teljes indukcióval következik, hogy minden $n \in \mathbb{N}^*$ esetén $s^n \in H$. Ugyanakkor H végessége miatt az $\mathbb{N}^* \to H$; $n \mapsto s^n$ függvény nem lehet injektív, tehát léteznek olyan $j, k \in \mathbb{N}^*$ számok, hogy $j < k$ és $s^j = s^k$. Ekkor $n := k - j \in \mathbb{N}^*$ olyan, hogy $s^n = e_G$. Ha $n = 1$, akkor $s = e_G$, tehát $s^{-1} = s \in H$. Ha $n > 1$, akkor $s^{n-1}s = s^n = e_G$ miatt $s^{-1} = s^{n-1} \in H$. Tehát $H^{-1} \subseteq H$ is teljesül, így H részcsoportja G-nek. ■

13.4.4. Állítás. *Legyen G csoport és jelölje $\cdot$ a G műveletét. Legyen $H \subseteq G$ és jelölje $*$ a $\cdot$ csoportművelet leszűkítését $H \times H$-ra. A H halmaz pontosan akkor részcsoportja G-nek, ha $*$ csoportművelet a H halmaz felett. Továbbá, ha H részcsoportja G-nek, akkor $(G, \cdot)$ és a $(H, *)$ csoportok neutrális elemei egyenlőek, és H minden elemének az inverze ugyanaz a $\cdot$ és $*$ csoportműveletek szerint.*

Bizonyítás. Legyen H részcsoportja G-nek. A $H \cdot H \subseteq H$ feltétel miatt $\mathrm{Im}(*) \subseteq H$, tehát a $*$ függvény művelet a H halmaz felett. A $\cdot$ művelet asszociativitásából nyilvánvalóan következik a $*$ művelet asszociativitása. Továbbá, e_G neutrális elem a $\cdot$ műveletre nézve, ezért a $*$ művelet szerint még inkább neutrális elem. Ha $s \in H$, akkor a $H^{-1} \subseteq H$ feltétel miatt $s^{-1} \in H$ olyan, hogy $s * s^{-1} = s \cdot s^{-1} = e_G$ és $s^{-1} * s = s^{-1} \cdot s = e_G$, továbbá e_G a neutrális elem a $*$ művelet szerint, ezért s-nek s^{-1} az inverze a mind a $\cdot$, mind a $*$ művelet szerint. Ezzel beláttuk, hogy $*$ csoportművelet a H halmaz felett, valamint a $(G, \cdot)$ és $(H, *)$ csoportok neutrális elemei egyenlőek, és H minden elemének az inverze ugyanaz a $\cdot$ és $*$ csoportműveletek szerint.

Megfordítva, tegyük fel, hogy $H \subseteq G$ olyan halmaz, amelyre $*$ csoportművelet a H halmaz felett. Ekkor $H \cdot H = H * H \subseteq H$, és van olyan $e_H \in H$, amely neutrális elem a $*$ művelet szerint. Ekkor $e_H \cdot e_H = e_H * e_H = e_H$, amiből e_H^{-1}-gyel jobbról szorozva, hogy $e_H = e_G$. Ha $s \in H$, és s^* az s elem inverze $*$ szerint, akkor $ss^* = s * s^* = e_H = e_G$ és ezt az egyenlőséget balról szorozra s^{-1}-gyel kapjuk, hogy $s^* = s^{-1}$, tehát $s^{-1} \in H$. Ez azt jelenti, hogy $H^{-1} \subseteq H$ is teljesül, vagyis H részcsoportja G-nek. ■

13.4.5. Állítás. *Ha G és H csoportok, valamint $\pi : G \to H$ csoport-morfizmus, akkor* $\mathrm{Im}(\pi)$ *részcsoportja H-nak és* $\mathrm{Ker}(\pi)$ *részcsoportja G-nek.*

Bizonyítás. Világos, hogy $\pi(e_G) = e_H$ miatt $e_G \in \mathrm{Ker}(\pi)$ és $e_H \in \mathrm{Im}(\pi)$, tehát $\mathrm{Ker}(\pi) \neq \emptyset$ és $\mathrm{Im}(\pi) \neq \emptyset$.

Ha $t, t' \in \mathrm{Im}(\pi)$, akkor léteznek olyan $s, s' \in G$, hogy $\pi(s) = t$ és $\pi(s') = t'$, ezért $tt' = \pi(s)\pi(s') = \pi(ss') \in \mathrm{Im}(\pi)$, következésképpen $\mathrm{Im}(\pi)\mathrm{Im}(\pi) \subseteq \mathrm{Im}(\pi)$. Ha $t \in \mathrm{Im}(\pi)$, akkor létezik olyan $s \in G$, hogy $\pi(s) = t$, ezért $t^{-1} = (\pi(s))^{-1} = \pi(s^{-1}) \in \mathrm{Im}(\pi)$, következésképpen $(\mathrm{Im}(\pi))^{-1} \subseteq \mathrm{Im}(\pi)$. Ezért $\mathrm{Im}(\pi)$ részcsoportja H-nak.

Ha $s, s' \in \mathrm{Ker}(\pi)$, akkor $\pi(s) = e_H$ és $\pi(s') = e_H$, ezért $\pi(ss') = \pi(s)\pi(s') = e_H e_H = e_H$, vagyis $ss' \in \mathrm{Ker}(\pi)$, következésképpen $\mathrm{Ker}(\pi)\mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(\pi)$. Ha $s \in \mathrm{Ker}(\pi)$, akkor $\pi(s) = e_H$, ezért $\pi(s^{-1}) = (\pi(s))^{-1} = (e_H)^{-1} = e_H$, vagyis $s^{-1} \in \mathrm{Ker}(\pi)$, következésképpen $(\mathrm{Ker}(\pi))^{-1} \subseteq \mathrm{Ker}(\pi)$. Ezért $\mathrm{Ker}(\pi)$ részcsoportja G-nek. ■

13.4.6. Következmény. *Ha G csoport, akkor* $\mathbf{Int}(G)$ *részcsoportja az* $\mathbf{Aut}(G)$ *automorfizmuscsoportnak.*

Bizonyítás. A 13.1.6. állításban láttuk, hogy a $\pi : G \to \mathbf{Aut}(G);\ s \mapsto \mathrm{Int}_G(s)$ leképezés csoport-morfizmus, és a definíció szerint $\mathbf{Int}(G) = \mathrm{Im}(\pi)$, ezért elég hivatkozni az előző állításra. ■

13.4.7. Definíció. *Legyen G csoport és $N \subseteq G$. Ekkor*

$$\begin{aligned} L_N &:= \{\ (s,t) \in G \times G \mid s^{-1}t \in N\ \}, \\ R_N &:= \{\ (s,t) \in G \times G \mid ts^{-1} \in N\ \}. \end{aligned}$$

13.4.8. Állítás. *Ha G csoport és H részcsoportja G-nek, akkor az L_H és R_H relációk elvivalenciák a G halmaz felett.*

Bizonyítás. Ha $s \in G$, akkor $ss^{-1} = s^{-1}s = e_{G} \in H$, így az L_H és R_H relációk reflexívek G felett. Ha $(s,t) \in L_H$ (illetve $(s,t) \in R_H$), akkor $s^{-1}t \in H$ (illetve $ts^{-1} \in H$), ezért $t^{-1}s = (s^{-1}t)^{-1} \in H^{-1} \subseteq H$ (illetve $st^{-1} = (ts^{-1})^{-1} \in H^{-1} \subseteq H$), tehát $(t,s) \in L_H$ (illetve $(t,s) \in R_H$), tehát az L_H és R_H relációk szimmetrikusak. Végül, ha $(r,s) \in L_H$ és $(s,t) \in L_H$ (illetve $(r,s) \in R_H$ és $(s,t) \in R_H$), akkor $r^{-1}s \in H$ és $s^{-1}t \in H$ (illetve $(sr^{-1} \in H$ és $ts^{-1} \in H)$, ezért $r^{-1}t = (r^{-1}s)(s^{-1}t) \in HH \subseteq H$ (illetve $tr^{-1} = (ts^{-1})(sr^{-1}) \in HH \subseteq H)$, tehát $(r,t) \in L_H$ (illetve $(r,t) \in R_H$), vagyis az L_H és R_H relációk tranzitívak. ■

13.4.9. Definíció. *Legyen G csoport és H részcsoportja G-nek. Ekkor az L_H (illetve R_H) G feletti ekvivalenciát a H részcsoport által meghatározott* **baloldali** (*illetve* **jobboldali**) **ekvivalenciának** *nevezzük, és a G/L_H (illetve G/R_H) faktorhalmazt a G/H (illetve $H \setminus G$) szimbólummal jelöljük. A G/H (illetve $H \setminus G$) halmaz elemeit H szerinti* **baloldali** (*illetve* **jobboldali**) **mellékosztályoknak** *nevezzük.*

Ebben az összefüggésben a $H \setminus G$ jelölés nem vezet félreértésre, mert ha ezt a H és G halmazok halmazkülönbségének tekintenénk, akkor $H \subseteq G$ miatt triviálisan $H \setminus G = \emptyset$ teljesülne, ugyakkor a G/R_H faktorhalmaz soha nem üres, mert $G \neq \emptyset$. Ezért ilyen kontextusban a $H \setminus G$ szimbólum a G/R_H faktorhalmazt jelöli. Mindazonáltal a $H \setminus G$ jelölést lehetőség szerint kerülni fogjuk.

13.4.10. Állítás. *Legyen G csoport és H részcsoportja G-nek.*

a) *Minden $s \in G$ esetén létezik egyetlen olyan $\gamma_{G/H}(s) : G/H \to G/H$ függvény, amelyre $\pi_{G/H} \circ \gamma_{G}(s) = \gamma_{G/H}(s) \circ \pi_{G/H}$, vagyis a következő diagram kommutatív:*

$$\begin{tikzcd} G \arrow[r, "\gamma_G(s)"] \arrow[d, "\pi_{G/H}"'] & G \arrow[d, "\pi_{G/H}"] \\ G/H \arrow[r, "\gamma_{G/H}(s)"'] & G/H \end{tikzcd}$$

Minden $s \in G$ esetén $\gamma_{G/H}(s)$ permutációja a G/H halmaznak, és a

$$\gamma_{G/H} : G \to \mathfrak{S}(G/H); \quad s \mapsto \gamma_{G/H}(s)$$

leképezés tranzitív ábrázolása a G csoportnak a G/H halmazban.

b) *Minden $s \in G$ esetén létezik egyetlen olyan $\delta_{G/H}(s) : H \setminus G \to H \setminus G$ függvény, amelyre $\pi_{H\setminus G} \circ \delta_{G}(s) = \delta_{H\setminus G}(s) \circ \pi_{H\setminus G}$, vagyis a következő diagram kommutatív:*

$$\begin{tikzcd} G \arrow[r, "\delta_G(s)"] \arrow[d, "\pi_{H\setminus G}"'] & G \arrow[d, "\pi_{H\setminus G}"] \\ H \setminus G \arrow[r, "\delta_{H\setminus G}(s)"'] & H \setminus G \end{tikzcd}$$

Minden $s \in G$ esetén $\delta_{H\setminus G}(s)$ permutációja a $H \setminus G$ halmaznak, és a

$$\delta_{H\setminus G} : G \to \mathfrak{S}(H \setminus G); \quad s \mapsto \delta_{H\setminus G}(s)$$

leképezés tranzitív ábrázolása a G csoportnak a $H \setminus G$ halmazban.

Bizonyítás. a) Legyen $s \in G$. Azt kell igazolni, hogy a $\gamma_{G}(s) : G \to G;\ t \mapsto st$ leképezés $L_H - L_H$ faktorizálható, vagyis $(t,t') \in L_H$ esetén $(st, st') = (\gamma_{G}(s)(t), \gamma_{G}(s)(t')) \in L_H$. Ez viszont nyilvánvalóan igaz, mert $(t,t') \in L_H$ esetén $t^{-1}t' \in H$, ezért $(st)^{-1}(st') = t^{-1}s^{-1}st' = t^{-1}t' \in H$, vagyis $(st, st') \in L_H$. Ezért vehetjük a $\gamma_{G}(s)$ függvény $L_H - L_H$ faktorizáltját, vagyis azt $\gamma_{G/H}(s) : G/H \to G/H$ függvényt, amelyre $\pi_{G/H} \circ \gamma_{G}(s) = \gamma_{G/H}(s) \circ \pi_{G/H}$.

A definíció és $\gamma_{G}(e_{G}) = \mathrm{id}_{G}$ alapján

$$\gamma_{G/H}(e_{G}) \circ \pi_{G/H} = \pi_{G/H} \circ \gamma_{G}(e_{G}) = \pi_{G/H} \circ \mathrm{id}_{G} = \mathrm{id}_{G/H} \circ \pi_{G/H},$$

amiből a $\pi_{G/H} : G \to G/H$ függvény szürjektivitása szerint következik, hogy

$$\gamma_{G/H}(e_{G}) = \mathrm{id}_{G/H}. \tag{1}$$

Ha $s, t \in G$, akkor a definíciók alapján

$$\begin{aligned}\left(\gamma_{G/H}(s) \circ \gamma_{G/H}(t)\right) \circ \pi_{G/H} &= \gamma_{G/H}(s) \circ \left(\gamma_{G/H}(t) \circ \pi_{G/H}\right) = \gamma_{G/H}(s) \circ \left(\pi_{G/H} \circ \gamma_{G}(t)\right) = \\ &= \left(\gamma_{G/H}(s) \circ \pi_{G/H}\right) \circ \gamma_{G}(t) = \left(\pi_{G/H} \circ \gamma_{G}(s)\right) \circ \gamma_{G}(t) = \pi_{G/H} \circ (\gamma_{G}(s) \circ \gamma_{G}(t)) \overset{(*)}{=} \\ &\overset{(*)}{=} \pi_{G/H} \circ \gamma_{G}(st) = \gamma_{G/H}(st) \circ \pi_{G/H},\end{aligned}$$

ahol a $\overset{(*)}{=}$ egyenlőségnél azt használtuk ki, hogy $\gamma_{G}(s) \circ \gamma_{G}(t) = \gamma_{G}(st)$, ami G csoportműveletének asszociativitása alapján nyilvánvaló. Ezért a $\pi_{G/H} : G \to G/H$ függvény szürjektivitása miatt

$$\gamma_{G/H}(s) \circ \gamma_{G/H}(t) = \gamma_{G/H}(st). \tag{2}$$

Ha $s \in G$, akkor (2) és (1) alkalmazásával kapjuk, hogy

$$\begin{aligned}\gamma_{G/H}(s) \circ \gamma_{G/H}\left(s^{-1}\right) &= \gamma_{G/H}\left(ss^{-1}\right) = \gamma_{G/H}(e_{G}) = \mathrm{id}_{G/H}, \\ \gamma_{G/H}\left(s^{-1}\right) \circ \gamma_{G/H}(s) &= \gamma_{G/H}\left(s^{-1}s\right) = \gamma_{G/H}(e_{G}) = \mathrm{id}_{G/H},\end{aligned}$$

tehát a $\gamma_{G/H}(s) : G/H \to G/H$ függvény bijekció, vagyis permutációja G/H-nak, és

$$\gamma_{G/H}\left(s^{-1}\right) = \left(\gamma_{G/H}(s)\right)^{-1}. \tag{3}$$

Az (1), (2) és (3) egyenlőségek alapján a $\gamma_{G/H} : G \to \mathfrak{S}(G/H);\ s \mapsto \gamma_{G/H}(s)$ leképezés csoport-morfizmus, vagyis $\gamma_{G/H}$ ábrázolása a G csoportnak a G/H halmazban.

Ha $\xi \in G/H$ és $s \in G$ olyan, hogy $\pi_{G/H}(s) = \xi$, akkor

$$\begin{aligned}\xi = \pi_{G/H}(s) = \pi_{G/H}(se_{G}) &= \left(\pi_{G/H} \circ \gamma_{G/H}(s)\right)(e_{G}) = \\ &= \left(\gamma_{G/H}(s) \circ \pi_{G/H}\right)(e_{G}) = \gamma_{G/H}(s)\left(\pi_{G/H}(e_{G})\right),\end{aligned}$$

vagyis $\dot{e} := \pi_{G/H}(e_{G}) \in G/H$ olyan pont, amelyre $G/H = \{\gamma_{G/H}(s)\dot{e} | s \in G\}$, így a $\gamma_{G/H}$ ábrázolás tranzitív.

b) Legyen $s \in G$. Azt kell igazolni, hogy a $\delta_{G}(s) : G \to G;\ t \mapsto ts^{-1}$ leképezés $R_H - R_H$ faktorizálható, vagyis $(t,t') \in R_H$ esetén $(ts^{-1}, t's^{-1}) = (\delta_{G}(s)(t), \delta_{G}(s)(t')) \in R_H$. Ez viszont nyilvánvalóan igaz, mert $(t,t') \in R_H$ esetén $t't^{-1} \in H$, ezért $(t's^{-1})(ts^{-1})^{-1} = t's^{-1}st^{-1} = t't^{-1} \in H$, vagyis $(ts^{-1}, t's^{-1}) \in R_H$. Ezért vehetjük a $\delta_{G}(s)$ függvény

$R_H - R_H$ faktorizáltját, vagyis azt $\delta_{H\backslash G}(s) : H \setminus G \to H \setminus G$ függvényt, amelyre $\pi_{H\backslash G} \circ \delta_G(s) = \delta_{H\backslash G}(s) \circ \pi_{H\backslash G}$.
A definíció és $\delta_G(e_G) = \mathrm{id}_G$ alapján

$$\delta_{H\backslash G}(e_G) \circ \pi_{H\backslash G} = \pi_{H\backslash G} \circ \delta_G(e_G) = \pi_{H\backslash G} \circ \mathrm{id}_G = \mathrm{id}_{H\backslash G} \circ \pi_{H\backslash G},$$

amiből a $\pi_{H\backslash G} : G \to H \setminus G$ függvény szürjektivitása szerint következik, hogy

$$\delta_{H\backslash G}(e_G) = \mathrm{id}_{H\backslash G}. \tag{3}$$

Ha $s, t \in G$, akkor a definíciók alapján

$$\begin{aligned}\left(\delta_{H\backslash G}(s) \circ \delta_{H\backslash G}(t)\right) \circ \pi_{H\backslash G} &= \delta_{H\backslash G}(s) \circ \left(\delta_{H\backslash G}(t) \circ \pi_{H\backslash G}\right) = \delta_{H\backslash G}(s) \circ \left(\pi_{H\backslash G} \circ \delta_G(t)\right) = \\ = \left(\delta_{H\backslash G}(s) \circ \pi_{H\backslash G}\right) \circ \delta_G(t) &= \left(\pi_{H\backslash G} \circ \delta_G(s)\right) \circ \delta_G(t) = \pi_{H\backslash G} \circ (\delta_G(s) \circ \delta_G(t)) \overset{(**)}{=} \\ &\overset{(**)}{=} \pi_{H\backslash G} \circ \delta_G(st) = \delta_{H\backslash G}(st) \circ \pi_{H\backslash G},\end{aligned}$$

ahol a $\overset{(**)}{=}$ egyenlőségnél azt használtuk ki, hogy $\delta_G(s) \circ \delta_G(t) = \delta_G(st)$, ami nyilvánvaló, mert minden $x \in G$ esetén

$$(\delta_G(s) \circ \delta_G(t))(x) = \left(xt^{-1}\right)s^{-1} = x(t^{-1}s^{-1}) = x(st)^{-1} = \delta_G(st)(x).$$

Ezért a $\pi_{H\backslash G} : G \to H \setminus G$ függvény szürjektivitása miatt

$$\delta_{H\backslash G}(s) \circ \delta_{H\backslash G}(t) = \delta_{H\backslash G}(st). \tag{4}$$

Ha $s \in G$, akkor (4) és (3) alkalmazásával kapjuk, hogy

$$\begin{aligned}\delta_{H\backslash G}(s) \circ \delta_{H\backslash G}\left(s^{-1}\right) &= \delta_{H\backslash G}\left(ss^{-1}\right) = \delta_{H\backslash G}(e_G) = \mathrm{id}_{H\backslash G}, \\ \delta_{H\backslash G}\left(s^{-1}\right) \circ \delta_{H\backslash G}(s) &= \delta_{H\backslash G}\left(s^{-1}s\right) = \delta_{H\backslash G}(e_G) = \mathrm{id}_{H\backslash G},\end{aligned}$$

tehát a $\delta_{H\backslash G}(s) : H \setminus G \to H \setminus G$ függvény bijekció, vagyis permutációja $H \setminus G$-nak, és

$$\delta_{H\backslash G}\left(s^{-1}\right) = \left(\delta_{H\backslash G}(s)\right)^{-1}. \tag{5}$$

A (3), (4) és (5) egyenlőségek alapján a $\delta_{H\backslash G} : G \to \mathfrak{S}(H \setminus G);\ s \mapsto \delta_{H\backslash G}(s)$ leképezés csoport-morfizmus, vagyis $\delta_{H\backslash G}$ ábrázolása a G csoportnak a $H \setminus G$ halmazban.
Ha $\xi \in H \setminus G$ és $s \in G$ olyan, hogy $\pi_{H\backslash G}(s) = \xi$, akkor

$$\begin{aligned}\xi = \pi_{H\backslash G}(s) &= \pi_{H\backslash G}\left(e_G\left(s^{-1}\right)^{-1}\right) = \left(\pi_{H\backslash G} \circ \delta_{H\backslash G}\left(s^{-1}\right)\right)(e_G) = \\ &= \left(\delta_{H\backslash G}\left(s^{-1}\right) \circ \pi_{H\backslash G}\right)(e_G) = \delta_{H\backslash G}\left(s^{-1}\right)\left(\pi_{H\backslash G}(e_G)\right),\end{aligned}$$

vagyis $\overset{\circ}{e} := \pi_{H\backslash G}(e_G) \in H \setminus G$ olyan pont, amelyre $H \setminus G = \{\delta_{H\backslash G}(s) overset \circ e | s \in G\}$, így a $\delta_{H\backslash G}$ ábrázolás tranzitív. ■

13.4.11. Állítás. *Legyen γ tranzitív ábrázolása a G csoportnak az $E \neq \emptyset$ halmazban. Ekkor létezik G-nek olyan H részcsoportja, amelyre a γ és $\gamma_{G/H}$ ábrázolások ekvivalensek.*

Bizonyítás. Legyen $x_0 \in E$ rögzített pont, és $H := \{s \in G | \gamma(s)x_0 = x_0\}$. Világos, hogy H részcsoportja G-nek, mert

– $e_G \in H$, hiszen $\gamma(e_G)\, x_0 = \mathrm{id}_E(x_0) = x_0$, tehát H nem üres;

– minden $t, t' \in H$ esetén $\gamma(tt')x_0 = \gamma(t)(\gamma(t')x_0) = \gamma(t)x_0 = x_0$, vagyis $tt' \in H$, ezért $HH \subseteq H$;

– minden $t \in H$ esetén $\gamma(t^{-1})\, x_0 = \gamma(t^{-1})\,(\gamma(t)x_0) = \gamma(t^{-1}t)\, x_0 = x_0$, vagyis $t^{-1} \in H$, ezért $H^{-1} \subseteq H$.

Megmutatjuk, hogy a $\gamma_{G/H}$ és γ ábrázolások ekvivalensek. Ehhez először megjegyezzük, hogy a

$$G \to E; \quad s \mapsto \gamma(s)x$$

függvény faktorizálható a G feletti L_H ekvivalencia szerint. Valóban, ha $s, s' \in G$ olyanok, hogy $(s, s') \in L_H$, akkor $s^{-1}s' \in H$, tehát $\gamma(s^{-1}s')\, x_0 = x_0$, amiből következik, hogy

$$\gamma(s)x_0 = \gamma(s)\left(\gamma\left(s^{-1}s'\right) x_0\right) = \gamma\left(s\left(s^{-1}s'\right)\right) x_0 = \gamma(s')x_0.$$

Ezért egyértelműen létezik az a $\sigma : G/H \to E$ függvény, amelyre minden $s \in G$ esetén

$$\sigma\left(\pi_{G/H}(s)\right) = \gamma(s)x_0.$$

Ez a σ függvény injektív. Valóban, legyenek $\xi, \xi' \in G/H$ olyanok, hogy $\sigma(\xi) = \sigma(\xi')$. Vegyünk olyan $s, s' \in G$ elemeket, amelyekre $\xi = \pi_{G/H}(s)$ és $\xi' = \pi_{G/H}(s')$. Ekkor

$$\gamma(s)x_0 = \sigma\left(\pi_{G/H}(s)\right) = \sigma(\xi) = \sigma(\xi') = \sigma\left(\pi_{G/H}(s')\right) = \gamma(s')x_0,$$

amiből $\gamma(s^{-1}) = (\gamma(s))^{-1}$ alapján következik, hogy

$$x_0 = \gamma\left(s^{-1}\right)(\gamma(s)x_0) = \gamma\left(s^{-1}\right)(\gamma(s')x_0) = \gamma\left(s^{-1}s'\right) x_0,$$

tehát $s^{-1}s' \in H$, azaz $(s, s') \in L_H$, így $\xi = \pi_{G/H}(s) = \pi_{G/H}(s') = \xi'$.

A $\sigma : G/H \to E$ függvény szürjektív is, mert $x \in E$ esetén a γ ábrázolás tranzitivitása folytán van olyan $s \in G$, amelyre $\gamma(s)x_0 = x$, ezért $\xi := \pi_{G/H}(s) \in G/H$ olyan pont, amelyre $\sigma(\xi) = \sigma\left(\pi_{G/H}(s)\right) = \gamma(s)x_0 = x$.

Tehát a $\sigma : G/H \to E$ függvény bijekció. Legyen $s \in G$ és $\xi \in G/H$. Rögzítsünk olyan $t \in G$ elemet, amelyre $\xi = \pi_{G/H}(t)$. Ekkor

$$\begin{aligned}(\gamma(s) \circ \sigma)(\xi) &= \gamma(s)\left(\sigma\left(\pi_{G/H}(t)\right)\right) = \gamma(s)(\gamma(t)x_0) = \gamma(st)x_0 = \sigma\left(\pi_{G/H}(st)\right) = \\ &= \sigma\left(\gamma_{G(H}(s)\pi_{G/H}(t)\right) = \left(\sigma \circ \gamma_{G(H}(s)\right)\left(\pi_{G/H}(t)\right) = \left(\sigma \circ \gamma_{G(H}(s)\right)(\xi).\end{aligned}$$

Ez azt jelenti, hogy minden $s \in G$ esetén $\gamma(s) \circ \sigma = \sigma \circ \gamma_{G(H}(s)$, tehát a $\gamma_{G/H}$ és γ ábrázolások ekvivalensek. ■

13.4.12. Állítás. *Legyenek H és H' részcsoportjai a G csoportnak. A $\gamma_{G/H}$ és $\gamma_{G/H'}$ ábrázolások pontosan akkor ekvivalensek, ha létezik olyan $s_0 \in G$, amelyre $s_0 H s_0^{-1} = H'$.*

Bizonyítás. (I) Tegyük fel, hogy $s_0 \in G$ olyan csoportelem, amelyre $s_0 H s_0^{-1} = H'$. Megmutatjuk, hogy a $\gamma_{G/H}$ és $\gamma_{G/H'}$ ábrázolások ekvivalensek. Ehhez először megjegyezzük, hogy a $\delta_G(s_0) : G \to G$ függvény $L_H - L_{H'}$ faktorizálható. Valóban, ha $s, s' \in G$ olyanok, hogy $(s, s') \in L_H$, akkor $s^{-1}s' \in H$, tehát $s_0\,(s^{-1}s')\, s_0^{-1} \in$

$s_0Hs_0^{-1} = H'$, következésképpen $\left(ss_0^{-1}\right)^{-1}\left(s's_0^{-1}\right) \in H'$, tehát $(\delta_G(s_0)(s), \delta_G(s_0)(s')) = \left(ss_0^{-1}, s's_0^{-1}\right) \in L_{H'}$. Ezért egyértelműen létezik az a $\sigma : G/H \to G/H'$ függvény, amelyre

$$\sigma \circ \pi_{G/H} = \pi_{G/H'} \circ \delta_G(s_0). \tag{1}$$

A σ függvény injektív. Valóban, legyenek $\xi, \eta \in G/H$ olyanok, hogy $\sigma(\xi) = \sigma(\eta)$. Vegyünk olyan $s, t \in G$ csoportelemeket, amelyekre $\xi = \pi_{G/H}(s)$ és $\eta = \pi_{G/H}(t)$. Ekkor (1) alapján

$$\begin{aligned}\pi_{G/H'}\left(ss_0^{-1}\right) &= \left(\pi_{G/H'} \circ \delta_G(s_0)\right)(s) = \left(\sigma \circ \pi_{G/H}\right)(s) = \sigma(\xi) = \\ &= \sigma(\eta) = \left(\sigma \circ \pi_{G/H}\right)(t) = \left(\pi_{G/H'} \circ \delta_G(s_0)\right)(t) = \pi_{G/H'}\left(ts_0^{-1}\right),\end{aligned}$$

tehát $\left(ss_0^{-1}, ts_0^{-1}\right) \in L_{H'}$, vagyis $\left(ss_0^{-1}\right)^{-1}\left(ts_0^{-1}\right) \in H'$, azaz $s_0\left(s^{-1}t\right)s_0^{-1} \in H' = s_0Hs_0^{-1}$, így $s^{-1}t \in H$, következésképpen $\xi = \pi_{G/H}(s) = \pi_{G/H}(t) = \eta$.

A $\sigma : G/H \to G/H'$ függvény szürjektív. Valóban, legyen $\xi' \in G/H'$, és vegyünk olyan $s \in G$ elemet, amelyre $\xi' = \pi_{G/H'}(s)$. Ekkor (1) alapján

$$\xi' = \pi_{G/H'}(s) = \pi_{G/H'}\left(ss_0s_0^{-1}\right) = \left(\pi_{G/H'} \circ \delta_G(s_0)\right)(ss_0) = \left(\sigma \circ \pi_{G/H}\right)(ss_0),$$

tehát $\xi := \pi_{G/H}(ss_0) \in G/H$ olyan pont, hogy $\xi' = \sigma(\xi)$.

Tehát a $\sigma : G/H \to G/H'$ függvény bijekció. Megmutatjuk, hogy minden $s \in G$ esetén $\gamma_{G/H'}(s) \circ \sigma = \sigma \circ \gamma_{G/H}(s)$, ami már azt jelenti, hogy a $\gamma_{G/H}$ és $\gamma_{G/H'}$ ábrázolások ekvivalensek. Valóban, legyen $s \in G$ rögzítve. Ekkor (1) alapján

$$\begin{aligned}\left(\gamma_{G/H'}(s) \circ \sigma\right) \circ \pi_{G/H} &= \gamma_{G/H'}(s) \circ \left(\sigma \circ \pi_{G/H}\right) = \gamma_{G/H'}(s) \circ \left(\pi_{G/H'} \circ \delta_G(s_0)\right) = \\ &= \left(\gamma_{G/H'}(s) \circ \pi_{G/H'}\right) \circ \delta_G(s_0) = \left(\pi_{G/H'} \circ \gamma_G(s)\right) \circ \delta_G(s_0) \overset{(*)}{=} \\ &\overset{(*)}{=} \left(\pi_{G/H'} \circ \delta_G(s_0)\right) \circ \gamma_G(s) = \left(\sigma \circ \pi_{G/H}\right) \circ \gamma_G(s) = \sigma \circ \left(\pi_{G/H} \circ \gamma_G(s)\right) = \\ &= \sigma \circ \left(\gamma_{G/H}(s) \circ \pi_{G/H}\right) = \left(\sigma \circ \gamma_{G/H}(s)\right) \circ \pi_{G/H},\end{aligned}$$

ahol a $\overset{(*)}{=}$ egyenlőségnél felhasználtuk, hogy G szorzásának asszociativitása miatt $\gamma_G(s) \circ \delta_G(s_0) = \delta_G(s_0) \circ \gamma_G(s)$. Mivel a $\pi_{G/H} : G \to G/H$ függvény szürjektív, ebből következik, hogy $\gamma_{G/H'}(s) \circ \sigma = \sigma \circ \gamma_{G/H}(s)$.

(II) Tegyük fel, hogy a $\gamma_{G/H}$ és $\gamma_{G/H'}$ ábrázolások ekvivalensek, és $\sigma : G/H \to G/H'$ olyan bijekció, amelyre minden $s \in G$ esetén $\gamma_{G/H'}(s) \circ \sigma = \sigma \circ \gamma_{G/H}(s)$. Olyan $s_0 \in G$ elemet keresünk, amelyre $s_0Hs_0^{-1} = H'$.

Mivel a $\pi_{G/H'} : G \to G/H'$ függvény szürjektív és $\sigma\left(\pi_{G/H}(e_G)\right) \in G/H'$, így vehetünk olyan $s_0 \in G$ elemet, hogy

$$\sigma\left(\pi_{G/H}(e_G)\right) = \pi_{G/H'}\left(s_0^{-1}\right). \tag{2}$$

Ekkor minden $s \in G$ esetén

$$\begin{aligned}\left(\sigma \circ \pi_{G/H}\right)(s) &= \sigma\left(\pi_{G/H}(se_G)\right) = \sigma\left(\gamma_{G/H}(s)\left(\pi_{G/H}(e_G)\right)\right) = \gamma_{G/H'}(s)\left(\sigma\left(\pi_{G/H}(e_G)\right)\right) = \\ &= \gamma_{G/H'}(s)\left(\pi_{G/H'}\left(s_0^{-1}\right)\right) = \pi_{G/H'}\left(\gamma_{G/H}(s)\left(s_0^{-1}\right)\right) = \pi_{G/H'}\left(ss_0^{-1}\right) = \left(\pi_{G/H'} \circ \delta_G(s_0)\right)(s),\end{aligned}$$

vagyis σ-ra és s_0-ra fennáll az (1) egyenlőség. Bebizonyítjuk, hogy $s_0Hs_0^{-1} = H'$.

Legyen $t \in H$. Ekkor $\pi_{G/H}(t) = \pi_{G/H}(e_G)$, így (1) és (2) alkalmazásával kapjuk, hogy

$$\begin{aligned}\pi_{G/H'}\left(s_0ts_0^{-1}\right) &= \left(\pi_{G/H'} \circ \delta_G(s_0)\right)(s_0t) = \left(\sigma \circ \pi_{G/H}\right)(s_0t) = \sigma\left(\pi_{G/H}(s_0t)\right) = \\ &= \sigma\left(\gamma_{G/H}(s_0)\left(\pi_{G/H}(t)\right)\right) = \sigma\left(\gamma_{G/H}(s_0)\left(\pi_{G/H}(e_G)\right)\right) = \gamma_{G/H'}(s_0)\left(\sigma\left(\pi_{G/H}(e_G)\right)\right) = \\ &= \gamma_{G/H'}(s_0)\left(\pi_{G/H'}\left(s_0^{-1}\right)\right) = \pi_{G/H'}\left(\gamma_G(s_0)\left(s_0^{-1}\right)\right) = \pi_{G/H'}(e_G),\end{aligned}$$

ezért $s_0ts_0^{-1} \in H'$. Ez azt jelenti, hogy $s_0Hs_0^{-1} \subseteq H'$.

Megfordítva, legyen $t \in H'$. Ekkor $\pi_{G/H'}(t) = \pi_{G/H'}(e_G)$, így (1) és (2) alkalmazásával kapjuk, hogy

$$\begin{aligned}\sigma\left(\pi_{G/H}\left(s_0^{-1}ts_0\right)\right) &= \left(\sigma \circ \pi_{G/H}\right)\left(s_0^{-1}ts_0\right) = \left(\pi_{G/H'} \circ \delta_G(s_0)\right)\left(s_0^{-1}ts_0\right) = \pi_{G/H'}\left(s_0^{-1}t\right) = \\ &= \left(\pi_{G/H'} \circ \gamma_G\left(s_0^{-1}\right)\right)(t) = \left(\gamma_{G/H'}\left(s_0^{-1}\right) \circ \pi_{G/H'}\right)(t) = \gamma_{G/H'}\left(s_0^{-1}\right)\left(\pi_{G/H'}(t)\right) = \\ &= \gamma_{G/H'}\left(s_0^{-1}\right)\left(\pi_{G/H'}(e_G)\right) = \pi_{G/H'}\left(s_0^{-1}\right) = \sigma\left(\pi_{G/H}(e_G)\right).\end{aligned}$$

A σ függvény injektivitása miatt ebből következik, hogy $\pi_{G/H}\left(s_0^{-1}ts_0\right) = \pi_{G/H}(e_G)$, tehát $s_0^{-1}ts_0 \in H$. Ezért $t = s_0\left(s_0^{-1}ts_0\right)s_0^{-1} \in s_0Hs_0^{-1}$, ami azt jelenti, hogy $H' \subseteq s_0Hs_0^{-1}$. ■

13.5. Invariáns részcsoportok és faktorcsoportok

13.5.1. Állítás. *Ha G csoport és $N \subseteq G$, akkor a következő állítások ekvivalensek.*

(i) *Minden $s \in G$ esetén $sNs^{-1} \subseteq N$.*

(ii) *Minden $s \in G$ esetén $sNs^{-1} = N$.*

(iii) $L_N = R_N$.

(iv) $R_N \subseteq L_N$.

(v) $L_N \subseteq R_N$.

Bizonyítás. (i)⇒(ii) Ha $s \in G$, akkor (i) alapján $N = s^{-1}(sNs^{-1})(s^{-1})^{-1} \subseteq s^{-1}Ns$. Ezért minden $s \in G$ elemre $N \subseteq (s^{-1})^{-1}Ns^{-1} = sNs^{-1}$ is teljesül, így $N = sNs^{-1}$.

(ii)⇒(iii) Legyen $(s,t) \in G \times G$. Ekkor

$$(s,t) \in L_N \Leftrightarrow s^{-1}t \in N \overset{(*)}{\Leftrightarrow} s(s^{-1}t)s^{-1} \in N \Leftrightarrow ts^{-1} \in N \Leftrightarrow (s,t) \in R_N,$$

ahol az $\overset{(*)}{\Leftrightarrow}$ ekvivalenciánál alkalmaztuk (ii)-t.

(iii)⇒(iv) Triviális.

(iv)⇒(v) Legyen $(s,t) \in L_N$, vagyis $s^{-1}t \in N$. Ekkor $s^{-1}(t^{-1})^{-1} \in N$, vagyis $(t^{-1}, s^{-1}) \in R_N$, amiből (iv) alapján következik, hogy $(t^{-1}, s^{-1}) \in L_N$, vagyis $ts^{-1} = (t^{-1})^{-1}s^{-1} \in N$, tehát $(s,t) \in R_N$.

(v)⇒(i) Legyen $s \in G$ és $t \in N$. Ekkor $s^{-1}(st) = t \in N$, vagyis $(s, st) \in L_N$, amiből (v) alapján következik, hogy $(s, st) \in R_N$, azaz $(st)s^{-1} \in N$. ■

13.5.2. Definíció. *Ha G csoport, akkor az $N \subseteq G$ részcsoportot* **invariáns részcsoportnak** *vagy* **normálosztónak** *nevezzük, ha minden $s \in G$ esetén $sNs^{-1} \subseteq N$ (vagyis $\mathrm{Int}_G(s)\langle N\rangle \subseteq N$).*

Nyilvánvaló, hogy ha G csoport, akkor az $\{e_G\}$ *neutrális részcsoport* és G invariáns részcsoportja G-nek. Kevésbé triviális példa a következő.

13.5.3. Állítás. *Ha G csoport, akkor* $\mathbf{Int}(G)$ *invariáns részcsoportja az* $\mathbf{Aut}(G)$ *automorfizmuscsoportnak.*

Bizonyítás. Legyen $s \in G$ és $\pi \in \mathbf{Aut}(G)$. Ekkor minden $s' \in G$ esetén

$$\left(\pi \circ \mathrm{Int}_G(s) \circ \pi^{-1}\right)(s') = \pi\left(s\pi^{-1}(s')s^{-1}\right) = \pi(s)\pi\left(\pi^{-1}(s')\right)\pi\left(s^{-1}\right) = \\ = \pi(s)s'\left(\pi(s)\right)^{-1} = \mathrm{Int}_G(\pi(s))(s'),$$

tehát $\pi \circ \mathrm{Int}_G(s) \circ \pi^{-1} = \mathrm{Int}_G(\pi(s)) \in \mathbf{Int}(G)$. ■

13.5.4. Tétel. *Legyen G csoport.*

a) *Ha $N \subseteq G$ invariáns részcsoport, akkor R_N olyan ekvivalencia-reláció G felett, amely szerint G csoportművelete faktorizálható és $N = \{s \in G | (e_G, s) \in R_N\}$.*

b) *Ha R olyan ekvivalencia-reláció G felett, amely szerint G csoportművelete faktorizálható, akkor $N := \{s \in G | (e_G, s) \in R\}$ (vagyis G neutrális elemének R szerinti ekvivalencia-osztálya) olyan invariáns részcsoport G-ben, amelyre $R_N = R$.*

c) *Ha $\mathscr{N}$ jelöli G invariáns részcsoportjainak halmazát és $\mathscr{R}$ jelöli azon G feletti ekvivalencia-relációk halmazát amelyek szerint G csoportművelete faktorizálható, akkor az*

$$\mathscr{N} \to \mathscr{R}; \quad N \mapsto R_N$$

leképezés bijekció.

Bizonyítás. a) Ha $s \in G$, akkor $ss^{-1} = e_G \in N$, tehát $(s,s) \in R_N$, ezért az R_N reláció reflexív G felett. Ha $(s,t) \in G \times G$, akkor

$$(s,t) \in R_N \Leftrightarrow ts^{-1} \in N \Leftrightarrow st^{-1} = (ts^{-1})^{-1} \in N^{-1} = N \Leftrightarrow (t,s) \in R_N,$$

vagyis $\overset{-1}{R_N} = R_N$, tehát az R_N reláció szimmetrikus. Ha $(r,s) \in R_N$ és $(s,t) \in R_N$, akkor $sr^{-1} \in N$ és $ts^{-1} \in N$, ezért $tr^{-1} = (ts^{-1})(sr^{-1}) \in NN \subseteq N$, vagyis $(r,t) \in R_N$, tehát az R_N reláció tranzitív. Ez azt jelenti, hogy R_N ekvivalenciareláció G felett.

Legyenek $(s,t) \in R_N$ és $(\tilde{s},\tilde{t}) \in R_N$, vagyis $ts^{-1} \in N$ és $\tilde{t}\tilde{s}^{-1} \in N$. Ekkor

$$(t\tilde{t})(s\tilde{s})^{-1} = (t(\tilde{t}\tilde{s}^{-1})t^{-1})(ts^{-1}) \in (tNt^{-1})N \subseteq NN \subseteq N,$$

mert $tNt^{-1} \subseteq N$, hiszen N invariáns részcsoport G-ben. Ez azt jelenti, hogy G csoportművelete faktorizálható az R_N ekvivalenciareláció szerint. Világos, hogy $s \in G$ esetén $(e_G, s) \in R_N$ azzal ekvivalens, hogy $s = s{e_G}^{-1} \in N$, így $N = \{s \in G | (e_G, s) \in R_N\}$.

b) Legyen R olyan ekvivalencia-reláció G felett, amely szerint G csoportművelete faktorizálható, és legyen $N := \{s \in G | (e_G, s) \in R\}$.

Az N halmaz nem üres, mert R reflexív G felett, így $(e_G, e_G) \in R$, vagyis $e_G \in N$. Ha $s \in N$, vagyis $(e_G, s) \in R$, akkor $(s^{-1}, s^{-1}) \in R$ és G csoportműveletének faktorizálhatósága miatt $(s^{-1}, e_G) = (e_G s^{-1}, ss^{-1}) \in R$, tehát R szimmetrikussága alapján $(e_G, s^{-1}) \in R$, vagyis $s^{-1} \in N$, ami azt jelenti, hogy $N^{-1} \subseteq N$. Ha $s,t \in N$, akkor $(e_G, s) \in R$ és $(e_G, t) \in R$, ezért G csoportműveletének faktorizálhatósága miatt $(e_G, st) = (e_G e_G, st) \in R$, vagyis $st \in N$, ami azt jelenti, hogy $NN \subseteq N$. Ezzel beláttuk, hogy N részcsoportja G-nek.

Legyen $s \in G$ és $t \in N$. Ekkor $(e_G, t) \in R$ és $(s^{-1}, s^{-1}) \in R$, így G csoportműveletének faktorizálhatósága miatt $(s^{-1}, ts^{-1}) = (e_G s^{-1}, ts^{-1}) \in R$. Ugyanakkor $(s,s) \in R$

is teljseül, ezért ismét G csoportműveletének faktorizálhatósága miatt $(e_G, sts^{-1}) = (ss^{-1}, s(ts^{-1})) \in R$, vagyis $sts^{-1} \in N$. Ez azt jelenti, hogy N invariáns részcsoportja G-nek.

Ha $(s,t) \in R$, akkor $(s^{-1}, s^{-1}) \in R$ és G csoportműveletének faktorizálhatósága miatt $(e_G, ts^{-1}) = (ss^{-1}, ts^{-1}) \in R$, tehát $ts^{-1}) \in N$, azaz $(s,t) \in R_N$. Megfordítva, ha $(s,t) \in R_N$, vagyis $ts^{-1}) \in N$, akkor $(e_G, ts^{-1}) \in R$, ugyanakkor $(s,s) \in R$, így G csoportműveletének faktorizálhatósága miatt $(s,t) = (e_G s, (ts^{-1})s) \in R$. Ez azt jelenti, hogy $R = R_N$.

c) Az $\mathscr{N} \to \mathscr{R}$; $N \mapsto R_N$ leképezés injektív, mert ha $N, N' \in \mathscr{N}$ és $R_N = R_{N'}$, akkor az a) állítás szerint $N = \{s \in G | (e_G, s) \in R_N\} = \{s \in G | (e_G, s) \in R_{N'}\} = N'$. A b) állítás szerint ez a leképezés szürjektív. ■

13.5.5. Definíció. *Ha G csoport és $N \subseteq G$ invariáns részcsoport, akkor a G/R_N faktorhalmazt a G csoportműveletének R_N szerinti faktorizáltjával ellátva a G csoport N szerinti* **faktorcsoportjának** *nevezzük és a G/N szimbólummal jelöljük.*

A G/N jelölés összhangban van a baloldali mellékosztályok halmazának jelölésével, mert a korábbi jelölés szerint $G/N := G/L_N$ és $L_N = R_N$, mivel N invariáns részcsoportja G-nek. Továbbá, 11.5.1. és az előző tétel szerint $\pi_{G/N} : G \to G/N$ kanonikus szürjekció csoport-morfizmus a G csoport és a G/N faktorcsoport között.

13.5.6. Állítás. *Ha G és H csoportok, valamint $\pi : G \to H$ csoport-morfizmus, akkor* $\mathrm{Ker}(\pi)$ *invariáns részcsoportja G-nek, és a π függvény kanonikus faktorizáltja csoport-izomorfizmus a* $G/\mathrm{Ker}(\pi)$ *faktorcsoport és az* $\mathrm{Im}(\pi)$ *részcsoport között.*

Bizonyítás. A 13.4.5. állítás szerint $\mathrm{Ker}(\pi)$ részcsoportja G-nek, és ha $s \in G$, akkor minden $s' \in \mathrm{Ker}(\pi)$ esetén $\pi(ss's^{-1}) = \pi(s)\pi(s')(\pi(s))^{-1} = \pi(s)e_H\pi(s^{-1}) = e_H$, tehát $ss's^{-1} \in \mathrm{Ker}(\pi)$, ezért $\mathrm{Ker}(\pi)$ invariáns részcsoportja G-nek. Tehát elkészíthető a $G/\mathrm{Ker}(\pi)$ faktorcsoport és 13.4.5. szerint az $\mathrm{Im}(\pi)$ részcsoport is.

Jelölje $\dot{\pi} : G/\mathrm{R}_\pi \to \mathrm{Im}(\pi)$ kanonikus faktorizált függvény, tehát $\mathrm{R}_\pi := \{(s,s') \in G \times G | \pi(s) = \pi(s')\}$. Nyilvánvaló, hogy minden $(s,s') \in G \times G$ esetén

$$(s,s') \in \mathrm{R}_\pi \Leftrightarrow \pi(s) = \pi(s') \Leftrightarrow \pi\left(s^{-1}s'\right) = e_H \Leftrightarrow s^{-1}s' \in \mathrm{Ker}(\pi) \Leftrightarrow (s,s') \in L_{\mathrm{Ker}(\pi)},$$

vagyis $\mathrm{R}_\pi = L_{\mathrm{Ker}(\pi)}$, így $G/\mathrm{R}_\pi = G/\mathrm{Ker}(\pi)$. Ezért 11.5.1. és az előző tétel szerint $\dot{\pi}$ csoport-morfizmus a $G/\mathrm{Ker}(\pi)$ faktorcsoport és az $\mathrm{Im}(\pi)$ részcsoport között, és mivel bijekció is, így csoport-izomorfizmus is. ■

13.5.7. Állítás. *Ha N invariáns részcsoportja a G csoportnak, akkor létezik olyan H csoport és olyan $\pi : G \to H$ szürjektív csoport-morfizmus, amelyre* $N = \mathrm{Ker}(\pi)$.

Bizonyítás. Világos, hogy $H := G/N$ és $\pi := \pi_{G/N}$ megfelelő választás. ■

13.6. Csoportok szorzata és féldirekt szorzata

13.6.1. Állítás. *Ha $(G_i)_{i \in I}$ csoportok tetszőleges rendszere, akkor a $G := \prod_{i \in I} G_i$ halmaz a*

$$G \times G \to G; \quad ((s_i)_{i \in I}, (s'_i)_{i \in I}) \mapsto (s_i s'_i)_{i \in I}$$

szorzatművelettel ellátva olyan csoport, amelyre teljesülnek a következők.

a) *Minden* $i \in I$ *esetén a* $\mathrm{pr}_i : G \to G_i$ *projekció szürjektív csoport-morfizmus.*

b) *Az* $e := \left(e_{G_i}\right)_{i\in I} \in G$ *elem egyenlő a* G *csoport neutrális elemével, és minden* $i \in I$ *esetén az* $\mathrm{in}_{i,e} : G_i \to G$ *függvény injektív csoport-morfizmus. Továbbá, minden* $(s_i)_{i\in I} \in G$ *esetén az* $\left(s_i^{-1}\right)_{i\in I}$ *rendszer egyenlő az* $(s_i)_{i\in I}$ *rendszer inverzével a* G *csoportban.*

c) *Ha minden* $i \in I$ *esetén* $\widetilde{G_i} := \mathrm{Im}\,(\mathrm{in}_{i,e})$ *és* C_i *az* $\bigcup\limits_{k\in I\setminus\{i\}} \widetilde{G_k}$ *halmaz által generált részcsoport* G*-ben, akkor* $\left(\widetilde{G_i}\right)_{i\in I}$ *a* G *csoport részcsoportjainak olyan rendszere, hogy minden* $j, k \in I$*,* $j \neq k$ *indexre* $\widetilde{G_j}\widetilde{G_k} = \widetilde{G_k}\widetilde{G_j}$ *és minden* $i \in I$ *esetén* $\widetilde{G_i} \cap C_i = \{e\}$*.*

Bizonyítás. Minden $i \in I$ esetén G_i művelete asszociatív, neutrális elemes és inverzelemes, így 11.4.2. szerint G felett a szorzatművelet szintén asszociatív, neutrális elemes és inverzelemes, tehát csoportművelet.

a) A szorzatművelet *definíciója* szerint minden minden $i \in I$ és $s, s' \in G$ esetén $\mathrm{pr}_i(ss') = \mathrm{pr}_i(s)\mathrm{pr}_i(s')$, tehát a $\mathrm{pr}_i : G \to G_i$ projekció csoport-morfizmus, és mivel minden $k \in I$ indexre $G_k \neq \emptyset$ (hiszen G_k-ban létezik neutrális elem), így pr_i szürjektív.

b) A 11.4.2. tétel bizonyítása szerint az $e := \left(e_{G_i}\right)_{i\in I} \in G$ elem egyenlő a G csoport neutrális elemével, és minden $(s_i)_{i\in I} \in G$ esetén az $\left(s_i^{-1}\right)_{i\in I}$ rendszer egyenlő az $(s_i)_{i\in I}$ rendszer inverzével a G csoportban. Ha $i \in I$ és $s, s' \in G_i$, akkor minden $k \in I$ esetén

$$(\mathrm{in}_{i,e}(s))_k = \begin{cases} s & \text{, ha } k = i, \\ e_{G_k} & \text{, ha } k \neq i, \end{cases} \qquad (\mathrm{in}_{i,e}(s'))_k = \begin{cases} s' & \text{, ha } k = i, \\ e_{G_k} & \text{, ha } k \neq i, \end{cases}$$

következésképpen

$$(\mathrm{in}_{i,e}(s)\mathrm{in}_{i,e}(s'))_k = (\mathrm{in}_{i,e}(s))_k\,(\mathrm{in}_{i,e}(s'))_k = \begin{cases} ss' & \text{, ha } k = i, \\ e_{G_k} & \text{, ha } k \neq i, \end{cases}$$

amiből következik, hogy $(\mathrm{in}_{i,e}(ss'))_k = (\mathrm{in}_{i,e}(s)\mathrm{in}_{i,e}(s'))_k$, így $\mathrm{in}_{i,e}(ss') = (\mathrm{in}_{i,e}(s)\mathrm{in}_{i,e}(s')$. Tehát minden $i \in I$ esetén az $\mathrm{in}_{i,e} : G_i \to G$ függvény csoport-morfizmus, amelynek injektivitása nyilvánvaló.

c)

■

13.6.2. Állítás. *Ha* N *és* H *csoportok, valamint* $\tau : H \to \mathbf{Aut}(N)$ *csoport-morfizmus, akkor az*

$$(N \times H) \times (N \times H) \to N \times H; \quad ((n, h), (n', h')) \mapsto (n, h) \cdot (n', h') := (n\tau_h(n'), hh')$$

leképezés csoportművelet az $N \times H$ *halmaz felett.*

Bizonyítás. A $\cdot$ művelet asszociatív, mert (n, h), (n', h'), $(n'', h'') \in N \times H$ esetén

$$(n, h) \cdot ((n', h') \cdot (n'', h'')) = (n, h) \cdot (n'\tau_{h'}(n''), h'h'') = (n\tau_h(n'\tau_{h'}(n'')), h(h'h'')) \overset{(1)}{=}$$
$$\overset{(1)}{=} (n(\tau_h(n')\tau_h(\tau_{h'}(n''))), h(h'h'')) \overset{(2)}{=} ((n\tau_h(n'))(\tau_h \circ \tau_{h'})(n''), (hh')h'') \overset{(3)}{=}$$
$$\overset{(3)}{=} ((n\tau_h(n'))\tau_{hh'}(n''), (hh')h'') = (n\tau_h(n'), hh') \cdot (n'', h'') = ((n, h) \cdot (n', h')) \cdot (n'', h''),$$

ahol a $\cdot$ művelet értelmezését alkalmaztuk, és

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk azt, hogy a $\tau_h : N \to N$ leképezés csoport-morfizmus, ezért $\tau_h(n'\tau_{h'}(n'')) = \tau_h(n')\tau_h(\tau_{h'}(n''))$;

– a $\overset{(2)}{=}$ egyenlőségnél az N és H csoportok műveletének asszociativitását alkalmaztuk;

– a $\overset{(3)}{=}$ egyenlőségnél arra hivatkozhatunk, hogy $\tau_h \circ \tau_{h'} = \tau_{hh'}$, mert $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus.

Az (e_N, e_H) pár neutrális eleme a $\cdot$ műveletnek, ugyanis $(n,h) \in N \times H$ esetén

$$(e_N, e_H) \cdot (n,h) = (e_N \tau_{e_H}(n), e_H h) = (\tau_{e_H}(n), h) = (n,h),$$

hiszen $\tau_{e_H} = \mathrm{id}_N$, mert $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus, továbbá

$$(n,h) \cdot (e_N, e_H) = (n\tau_h(e_N), he_H) = (ne_N, h) = (n,h),$$

hiszen $\tau_h(e_N) = e_N$, mert $\tau_h : N \to N$ csoport-morfizmus.

Legyen $(n,h) \in N \times H$. Megmutatjuk, hogy az $(\tau_{h^{-1}}(n^{-1}), h^{-1})$ pár inverze (n,h)-nak a $\cdot$ művelet szerint. Valóban,

$$(\tau_{h^{-1}}(n^{-1}), h^{-1}) \cdot (n,h) = (\tau_{h^{-1}}(n^{-1})\tau_{h^{-1}}(n), h^{-1}h) = (e_N, e_H),$$

mert $\tau_{h^{-1}}(n^{-1})\tau_{h^{-1}}(n) = \tau_{h^{-1}}(n^{-1}n) = \tau_{h^{-1}}(e_N) = e_N$, hiszen $\tau_{h^{-1}} : N \to N$ csoport-morfizmus, továbbá

$$\begin{aligned}(n,h) \cdot (\tau_{h^{-1}}(n^{-1}), h^{-1}) &= (n\tau_h(\tau_{h^{-1}}(n^{-1})), hh^{-1}) = \\ &= (n(\tau_h \circ \tau_{h^{-1}})(n^{-1}), e_H) = (nn^{-1}, e_H) = (e_N, e_H),\end{aligned}$$

mert $\tau_h \circ \tau_{h^{-1}} = \tau_{hh^{-1}} = \tau_{e_H} = \mathrm{id}_N$, hiszen $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus. ■

13.6.3. Definíció. *Ha N és H csoportok, valamint $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus, akkor az $N \times H$ halmazt az*

$$(N \times H) \times (N \times H) \to N \times H; \quad ((n,h),(n',h')) \mapsto (n\tau_h(n'), hh')$$

művelettel ellátva az N és H csoportok τ szerinti **féldirekt szorzatának** *nevezzük, és az $N \underset{\tau}{\otimes} H$ szimbólummal jelöljük.*

Nyilvánvaló, hogy ha N és H csoportok, valamint $\tau : H \to \mathbf{Aut}(N)$ a triviális csoport-morfizmus, vagyis minden $h \in H$ esetén $\tau_h = \mathrm{id}_N$, akkor $N \underset{\tau}{\otimes} H = N \otimes H$. Ezért két csoport esetében a féldirekt szorzat a direkt szorzat általánosítása. Az alábbi állítás következménye szerint valódi általánosításról van szó.

13.6.4. Állítás. *Legyenek N és H csoportok, valamint $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus. Az $N \underset{\tau}{\otimes} H$ féldirekt szorzatcsoport pontosan akkor kommutatív, ha N és H kommutatívak és τ a triviális csoport-morfizmus.*

Bizonyítás. A feltétel nyilvánvalóan elégséges, mert kommutatív csoportok szorzata kommutatív. Tegyük fel, hogy az $N \underset{\tau}{\otimes} H$ csoport kommutatív, vagyis minden (n,h), $(n',h') \in N \times H$ esetén

$$(n\tau_h(n'), hh') = (n,h) \cdot (n',h') = (n',h') \cdot (n,h) = (n'\tau_{h'}(n), h'h),$$

ahol $\cdot$ az $N \underset{\tau}{\otimes} H$ csoport műveletét jelöli. Ekkor minden $h,\ h' \in H$ elemre $hh' = h'h$, vagyis H kommutatív és minden $(n,h),\ (n',h') \in N \times H$ párra $n\tau_h(n') = n'\tau_{h'}(n)$. Ebből az $n' := e_N$ választással kapjuk, hogy minden $n \in N$ és $h' \in H$ esetén $n = \tau_{h'}(n)$, vagyis minden $h' \in H$ elemre $\tau_{h'} = \mathrm{id}_N$. Ez azt jelenti, hogy τ a triviális csoport-morfizmus, ugyanakkor minden $(n,h),\ (n',h') \in N \times H$ párra $nn' = n\tau_h(n') = n'\tau_{h'}(n) = n'n$, így N is kommutatív. ■

13.6.5. Következmény. *Legyenek N és H kommutatív csoportok, valamint $\tau : H \to$ $\mathbf{Aut}(N)$ csoport-morfizmus. Az $N \underset{\tau}{\otimes} H$ féldirekt szorzatcsoport pontosan akkor kommutatív, ha τ a triviális csoport-morfizmus, vagyis ha $N \underset{\tau}{\otimes} H = N \otimes H$.*

13.6.6. Állítás. *Legyenek N és H csoportok, valamint $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus. Ekkor a*

$$j_N : N \to N \times H; \quad n \mapsto (n, e_H),$$

leképezés injektív csoport-morfizmus az N és $N \underset{\tau}{\otimes} H$ csoportok között, és a

$$p_H : N \times H \to H; \quad (n,h) \mapsto h$$

leképezés szürjektív szürjektív csoport-morfizmus az $N \underset{\tau}{\otimes} H$ és H csoportok között, valamint $\mathrm{Im}(j_N) = \mathrm{Ker}(p_H) = N \times \{e_H\}$.

Bizonyítás. A $j_N : N \to N \times H$ függvény nyilvánvalóan injektív, és csoport-morfizmus is, mert minden $n, n' \in N$ esetén

$$j_N(n)j_N(n') = (n, e_H)\,(n', e_H) = \left(n\tau_{e_H}(n'), e_H e_H\right) = (nn', e_H) = j_N(nn').$$

A $p_H : N \times H \to H$ függvény nyilvánvalóan szürjektív, és csoport-morfizmus is, mert minden $(n,h), (n',h') \in N \times H$ esetén

$$p_H(n,h)p_H(n',h') = hh' = p_H\left(n\tau_h(n'), hh'\right) = p_H((n,h)(n',h')).$$

Világos, hogy

$$\mathrm{Ker}\,(p_N) = \{(n,h) \in N \times H | h = e_H\} = \{(n, e_H)\,| n \in N\} = \mathrm{Im}(j_N). \ ■$$

13.6.7. Állítás. *Legyenek N és H csoportok, valamint $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus. Ekkor $\tilde{N} := N \times \{e_H\}$ és $\tilde{H} := \{e_N\} \times H$ olyan részcsoportjai az $N \underset{\tau}{\otimes} H$ féldirekt szorzatcsoportnak, hogy $\tilde{N}$ invariáns részcsoport, valamint $\tilde{N} \cap \tilde{H} = \{e_{N \underset{\tau}{\otimes} H}\}$ és $\tilde{N}\tilde{H} = N \times H$.*

Bizonyítás. Ha $n, n' \in N$, akkor $(n, e_H)\,(n', e_H) = \left(n\tau_{e_H}(n'), e_H e_H\right) = (nn', e_H) \in \tilde{N}$, és $(e_N, e_H) \in \tilde{N}$, továbbá minden $n \in \mathbb{N}$ esetén $(n, e_H)^{-1} = (n^{-1}, e_H) \in \tilde{N}$. Ez azt jelenti, hogy $\tilde{N}\tilde{N} \subseteq \tilde{N}$, $\tilde{N} \neq \emptyset$, és $\tilde{N}^{-1} \subseteq \tilde{N}$, tehát $\tilde{N}$ részcsoportja $N \underset{\tau}{\otimes} H$-nak. Ez invariáns részcsoport, mert minden $n, n' \in N$ és $h \in H$ esetén

$$\begin{aligned}(n,h)\,(n', e_H)\,(n,h)^{-1} &= (n\tau_h(n'), h)\left(\tau_{h^{-1}}\left(n^{-1}\right), h^{-1}\right) = \\ = \left(n\tau_h(n')\tau_h\left(\tau_{h^{-1}}\left(n^{-1}\right)\right), hh^{-1}\right) &= \left(n\tau_h(n')n^{-1}, e_H\right) \in N \times \{e_H\} = \tilde{N},\end{aligned}$$

mert nyilvánvalóan $\tau_h\left(\tau_{h^{-1}}\left(n^{-1}\right)\right)=\left(\tau_h\circ\tau_{h^{-1}}\right)\left(n^{-1}\right)=\tau_{hh^{-1}}\left(n^{-1}\right)=\tau_{e_H}\left(n^{-1}\right)=n^{-1}$, hiszen $\tau : H\to\mathbf{Aut}(N)$ csoport-morfizmus.

Ha $h,h'\in H$, akkor $(e_N,h)(e_N,h')=(e_N\tau_h(e_N),hh')=(e_N,hh')\in\tilde H$, és $(e_N,e_H)\in\tilde H$, továbbá minden $h\in H$ esetén $(e_N,h)^{-1}=\left(\tau_{h^{-1}}\left(e_N^{-1}\right),h^{-1}\right)=(e_N,h^{-1})\in\tilde H$. Ez azt jelenti, hogy $\tilde H\tilde H\subseteq\tilde H$, $\tilde H\neq\emptyset$, és $\tilde H^{-1}\subseteq\tilde H$, tehát $\tilde H$ részcsoportja $N\underset{\tau}{\otimes}H$-nak.

Nyilvánvaló, hogy $\tilde N\cap\tilde H=\{e_{N\underset{\tau}{\otimes}H}\}$, és ha $(n,h)\in N\times H$, akkor $(n,e_H)(e_N,h)=\left(n\tau_{e_H}(e_N),e_Hh\right)=(n,h)$, tehát $\tilde N\tilde H=N\times H$. ■

13.6.8. Állítás. *Legyen G csoport, valamint legyenek N és H olyan részcsoportjai G-nek, hogy N invariáns részcsoport, továbbá $N\cap H=\{e_G\}$ és $NH=G$. Ekkor minden $h\in H$ esetén $\mathrm{Int}_G(h)|_N\in\mathbf{Aut}(N)$ és a*

$$\tau : H\to\mathbf{Aut}(N);\quad h\mapsto\tau_h:=\mathrm{Int}_G(h)|_N$$

leképezés csoport-morfizmus, továbbá a

$$\pi : N\times H\to G;\quad (n,h)\mapsto nh$$

leképezés csoport-izomorfizmus az $N\underset{\tau}{\otimes}H$ féldirekt szorzat és G között.

Bizonyítás. Az N halmaz invariáns részcsoportja G-nek, ezért minden $h\in H$ esetén $hNh^{-1}\subseteq N$, tehát minden $h\in H$ esetén, $h^{-1}\in H$ miatt $h^{-1}Nh=h^{-1}N\left(h^{-1}\right)^{-1}\subseteq N$, tehát $N\subseteq hNn^{-1}$. Ez azt jelenti, hogy minden $h\in H$ esetén az $\mathrm{Int}_G(h)|_N : N\to N$ leképezés bijektív csoport-morfizmus, vagyis $\mathrm{Int}_G(h)|_N\in\mathbf{Aut}(N)$. Ha $h,\tilde h\in H$, akkor minden $n\in N$ esetén $\tau_{h\tilde h}(n)=(h\tilde h)n(h\tilde h)^{-1}=h\left(\tilde hn\tilde h^{-1}\right)h^{-1}=\tau_h\left(\tau_{\tilde h}(n)\right)$, tehát $\tau_{h\tilde h}=\tau_h\circ\tau_{\tilde h}$, vagyis a $\tau : H\to\mathbf{Aut}(N)$ leképezés csoport-morfizmus.

Minden $(n,h),(n',h')\in N\times H$ esetén $\pi(n,h)\pi(n',h')=(nh)(n'h')=(nhn'h^{-1})(hh')=\pi\left(nhn'h^{-1},hh'\right)=\pi\left(n\tau_h(n'),hh'\right)=\pi\left((n,h)\cdot(n',h')\right)$, ahol $\cdot$ az $N\underset{\tau}{\otimes}H$ féldirekt szorzat csoportműveletét jelöli. Tehát a $\pi : N\times H\to G$ leképezés csoport-morfizmus az $N\underset{\tau}{\otimes}H$ féldirekt szorzat és G között. A π függvény injektív, mert $(n,h)\in\mathrm{Ker}(\pi)$ esetén $nh=e_G$, ezért $n=h^{-1}\in N\cap H=\{e_G\}$, így $(n,h)=(e_N,e_H)$, és (e_N,e_H) a neutrális eleme az $N\underset{\tau}{\otimes}H$ féldirekt szorzatnak. A $\pi : N\times H\to G$ függvény szürjektivitása az $NH=G$ feltételből következik. Tehát π csoport-izomorfizmus az $N\underset{\tau}{\otimes}H$ féldirekt szorzat és G között. ■

13.6.9. Állítás. *Legyenek N és H csoportok, valamint $\tau : H\to\mathbf{Aut}(N)$ csoport-morfizmus. Vezessük be a*

$$j_N : N\to N\times H;\quad n\mapsto(n,e_H),$$
$$j_H : H\to N\times H;\quad h\mapsto(e_N,h)$$

leképezéseket. Ezek csoport-morfizmusok az N és $N\underset{\tau}{\otimes}H$, valamint a H és $N\underset{\tau}{\otimes}H$ csoportok között.

a) *Ha G csoport és $\pi : N\underset{\tau}{\otimes}H\to G$ csoport-morfizmus, akkor a*

$$\pi_N:=\pi\circ j_N : N\to G,$$
$$\pi_H:=\pi\circ j_H : H\to G$$

leképezések olyan csoport-morfizmusok, hogy minden $(n, h) \in N \times H$ *esetén*

$$\pi_H(h)\pi_N(n)\pi_H(h)^{-1} = \pi_N(\tau_h(n)),$$

valamint

$$\pi(n, h) = \pi_N(n)\pi_H(h).$$

b) *Megfordítva, ha* G *csoport és*

$$\begin{aligned} \pi_N &: N \to G, \\ \pi_H &: H \to G \end{aligned}$$

olyan csoport-morfizmusok, hogy minden $(n, h) \in N \times H$ *esetén*

$$\pi_H(h)\pi_N(n)\pi_H(h)^{-1} = \pi_N(\tau_h(n)), \tag{$*$}$$

akkor a

$$\pi : N \underset{\tau}{\otimes} H \to G; \quad (n, h) \mapsto \pi_N(n)\pi_H(h)$$

leképezés az az egyértelműen meghatározott csoport-morfizmus, amelyre

$$\begin{aligned} \pi_N &= \pi \circ j_N : N \to G, \\ \pi_H &= \pi \circ j_H : H \to G \end{aligned}$$

teljesül.

Bizonyítás. Ha $(n, h), (n', h') \in N \times H$, akkor

$$\begin{aligned} j_N(n)\, j_N(n') &= (n, e_H)(n', e_H) = \left(n\tau_{e_H}(n'), e_H e_H\right) = (nn', e_H)\, j_N(n'), \\ j_H(h) j_H(h') &= (e_N, h)(e_N, h') = (e_N \tau_h((e_N, h)), hh') = (e_N, hh') = j_H(hh'), \end{aligned}$$

hiszen $\tau_{e_H} = \mathrm{id}_N$, mert $\tau : H \to \mathbf{Aut}(N)$ csoport-morfizmus, és $\tau_h(e_N) = e_N$, mert $\tau_h : N \to N$ csoport-morfizmus. Ezért a $j_N : N \to N \underset{\tau}{\otimes} H$ és $j_H : H \to N \underset{\tau}{\otimes} H$ leképezések csoport-morfizmusok.

a) Minden $(n, h) \in N \times H$ esetén

$$\begin{aligned} (e_N, h)(n, e_H)(e_N, h)^{-1} &= (e_N \tau_h(n), he_H)\left(e_N, h^{-1}\right) = (\tau_h(n), h)\left(e_N, h^{-1}\right) = \\ &= \left(\tau_h(n)\tau_{e_H}(e_N), hh^{-1}\right) = (\tau_h(n), e_H), \end{aligned}$$

ezért

$$\pi(e_N, h)\,\pi(n, e_H)\,\pi\left((e_N, h)^{-1}\right) = \pi\left((e_N, h)(n, e_H)(e_N, h)^{-1}\right) = \pi(\tau_h(n), e_H),$$

így $\pi\left((e_N, h)^{-1}\right) = (\pi((e_N, h)))^{-1}$ figyelembe vételével, a definíciók alapján kapjuk, hogy

$$\pi_H(h)\pi_N(n)\pi_H(h)^{-1} = \pi_N(\tau_h(n)).$$

Továbbá, nyilvánvaló, hogy $(n, h) \in N \times H$ esetén $(n, e_H)(e_N, h) = \left(n\tau_{e_H}(e_N), e_H h\right) = (n, h)$, ezért $\pi(n, h) = \pi((n, e_H)(e_N, h)) = \pi(n, e_H)\,\pi(e_N, h) = \pi_N(n)\pi_H(h)$.

b) Minden $(n, h), (n', h') \in N \times H$ esetén a π függvény definíciója szerint

$$\begin{aligned} \pi((n, h)(n', h')) &= \pi(n\tau_h(n'), hh') = \pi_N(n\tau_h(n'))\,\pi_H(hh') = \\ = \pi_N(n)(\pi_N(\tau_h(n'))\,\pi_H(h))\,\pi_H(h') &= \pi_N(n)(\pi_H(h)\pi_N(n'))\,\pi_H(h') = \pi(n, h)\pi(n', h'), \end{aligned}$$

ahol az utoló előtti egyenlőségnél felhasználtuk a (*) összefüggést az (n', h) párra. Tehát a $\pi : N \underset{\tau}{\otimes} H \to G$ leképezés csoport-morfizmus, és nyilvánvaló, hogy $\pi_N = \pi \circ j_N$ és $\pi_H = \pi \circ j_H$.
Ha $\pi' : N \underset{\tau}{\otimes} H \to G$ szintén olyan csoport-morfizmus, hogy $\pi_N = \pi' \circ j_N$ és $\pi_H = \pi' \circ j_H$, akkor minden $(n, h) \in N \times H$ esetén $(n, h) = (n, e_H)\,(e_N, h)$ miatt

$$\pi'(n, h) = \pi'\left((n, e_H)\,(e_N, h)\right) = \pi'\,(n, e_H)\,\pi'\,(e_N, h) = \pi_N(n)\pi_H(h) = \pi(n, h),$$

tehát $\pi' = \pi$. ■

Az előző állításban szereplő (*) egyenlőséget *Weyl-féle felcserélési relációnak* nevezzük.

13.7. Elem rendje és ciklikus csoportok

13.8. Csoportelméleti izomorfiatételek

13.9. Véges Abel-csoportok struktúra-tétele

13.10. Normállánc és feloldható csoportok

14. fejezet

Gyűrűk

14.1. Gyűrűk és gyűrű-morfizmusok

14.1.1. Definíció. *Az* $(A, +, \cdot)$ *hármast* **gyűrűnek** *nevezzük, ha* $+$ *és* $\cdot$ *olyan műveletek az* A *halmaz felett, amelyek rendelkeznek a következő tulajdonságokkal.*

$(\mathrm{A_I})$ *A* $+$ *művelet asszociatív, kommutatív, neutrális-elemes és inverzelemes, tehát az* $(A, +)$ *pár kommutatív csoport. (A* $+$ *művelet szerinti neutrális elemet* 0 *(vagy* 0_A*) jelöli, és minden* $x \in A$ *esetén* $-x$ *jelöli az* x *elem inverzét a* $+$ *művelet szerint.)*

$(\mathrm{A_{II}})$ *A* $\cdot$ *művelet asszociatív és disztributív a* $+$ *műveletre nézve.*

Ha $(A, +, \cdot)$ *gyűrű, akkor az* $(A, +)$ *kommutatív csoportot a* $(A, +, \cdot)$ *gyűrű* **additív csoportjának***, és az* $(A, \cdot)$ *félcsoportot az* $(A, +, \cdot)$ *gyűrű* **multiplikatív félcsoportjának** *nevezzük.*

A gyűrűket gyakran egyetlen szimbólummal, az alaphalmaz jelével jelöljük, és a műveleteit a $+$ és $\cdot$ szimbólumokkal jelöljük, ha ez nem okoz félreértést. Továbbá megállapodunk abban, hogy ha A gyűrű, akkor $x, y \in A$ esetén az $x \cdot y$ jelölés helyett az xy jelölést alkalmazzuk.

14.1.2. Definíció. *Azt mondjuk, hogy az* $(A, +, \cdot)$ *gyűrű*

– **kommutatív***, ha a* $\cdot$ *művelet kommutatív;*

– **egységelemes***, ha a* $\cdot$ *művelet neutrális-elemes, és ekkor a* $\cdot$ *művelet szerinti neutrális elemet* 1 *(vagy* 1_A*) jelöli, és ekkor az* $(A, \cdot)$ *monoid invertálható elemeinek halmazát* $\mathbf{G}(A)$ *jelöli;*

– **zérusosztómentes***, ha minden* $x, y \in A \setminus \{0\}$ *esetén* $x \cdot y \in A \setminus \{0\}$*.*

– **nemelfajult***, ha* A *legalább két elemű halmaz, vagyis* $A \neq \{0\}$*.*

– **ferdetest***, ha egységelemes, nemelfajult és* A *minden* 0*-tól különböző elemének létezik inverze a* $\cdot$ *művelet szerint.*

– **test***, ha kommutatív ferdetest.*

A következő állítás a legfontosabb nem triviális gyűrűről szól.

14.1.3. Állítás. *A* $(\mathbb{Z}, +, \cdot)$ *hármas nemelfajult, egységelemes, kommutatív, zérusosztómentes gyűrű, ahol* $+$ *a* $\mathbb{Z}$ *feletti összeadást és* $\cdot$ *a* $\mathbb{Z}$ *feletti szorzást jelöli.*

Bizonyítás. A 7.12.5. állítás a) pontja szerint $(\mathrm{A_I})$ teljesül, és a 7.12.5. állítás b) pontja szerint $(\mathrm{A_{II}})$ is igaz, tehát a $(\mathbb{Z}, +, \cdot)$ hármas gyűrű. A 7.12.5. állítás b) pontja szerint

$(\mathbb{Z},+,\cdot)$ egységelemes és kommutatív gyűrű. A 7.12.5. állítás d) pontja szerint a $(\mathbb{Z},+,\cdot)$ gyűrű zérusosztómentes. Végül, a 7.12.5. állítás *bizonyításában* láttuk, hogy $\mathbf{0} := 0-0$ a neutrális elem a $+$ művelet szerint, és $\mathbf{1} := 1-0$ a neutrális elem a $\cdot$ művelet szerint (ahol $0,1 \in \mathbb{N}$), ezért $\mathbf{0} \neq \mathbf{1}$, különben $0 = 0+0 = 1+0 = 1$ teljesülne, ami nem igaz. Tehát a $(\mathbb{Z},+,\cdot)$ gyűrű nemelfajult. ■

Megállapodunk abban, hogy a továbbiakban az egész számok $\mathbb{Z}$ halmazát a $\mathbb{Z}$ feletti összeadással és $\mathbb{Z}$ feletti szorzással ellátva gyűrűnek tekintjük.

14.1.4. Állítás. *Legyen A gyűrű.*

a) *Ha $a \in A$, akkor*

$$a0 = 0 = 0a.$$

b) *Ha $a, b \in A$, akkor*

$$a(-b) = -(ab) = (-a)b.$$

c) *Ha $a, b, c \in A$, akkor*

$$a(b-c) = ab - ac,$$
$$(b-c)a = ba - ca.$$

(**A szorzás kivonásra vonatkozó disztributivitása.**)

d) *Ha A egységelemes, akkor minden $a \in A$ esetén*

$$(-1)a = -a = a(-1).$$

Bizonyítás. a) Ha $a \in A$, akkor a szorzás öszeadásra vonatkozó disztributivitása szerint $a0 + a0 = a(0+0) = a0$, amiből az összeadás asszociativitása alapján következik, hogy

$$0 = a0 + (-a0) = (a0 + a0) + (-a0) = a0 + (a0 + (-a0)) = a0 + 0 = a0,$$

és teljesen hasonlóan, a szorzás öszeadásra vonatkozó disztributivitása szerint $0a + 0a = (0+0)a = 0a$, amiből az összeadás asszociativitása alapján következik, hogy

$$0 = 0a + (-0a) = (0a + 0a) + (-0a) = 0a + (0a + (-0a)) = 0a + 0 = 0a.$$

b) Ha $a, b \in A$, akkor a szorzás öszeadásra vonatkozó disztributivitása és a) szerint

$$ab + a(-b) = a(b + (-b)) = a0 = 0,$$
$$ab + (-a)b = (a + (-a))b = 0b = 0,$$

ezért $a(-b) = -(ab)$ és $(-a)b = -(ab)$.

c) Ha $a, b, c \in A$, akkor a kivonás definíciója, a szorzás öszeadásra vonatkozó disztributivitása és b) szerint

$$a(b-c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac,$$
$$(b-c)a = (b + (-c))a = ba + (-c)a = ba + (-(ca)) = ba - ca,$$

ezért $a(b-c) = ab - ac$ és $(b-c)a = ba - ca$.

d) Ha A egységelemes, akkor minden $a \in A$ esetén a szorzás öszeadásra vonatkozó disztributivitása és a) miatt

$$a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = a,$$
$$a + a(-1) = a1 + a(-1) = a(1 + (-1)) = a0 = a,$$

ezért $(-1)a = -a$ és $a(-1) = -a$. ■

14.1.5. Definíció. *Ha A és B gyűrűk, akkor a $\pi : A \to B$ leképezést* **gyűrű-morfizmusnak** *nevezzük, ha minden $x, y \in A$ esetén*

$$\pi(x + y) = \pi(x) + \pi(y); \quad \pi(xy) = \pi(x)\pi(y).$$

Ha A és B egységelemes gyűrűk, akkor a $\pi : A \to B$ gyűrű-morfizmust **egységelem-tartónak** *nevezzük, ha $\pi(1_A) = 1_B$.*

Ha A és B gyűrűk, akkor a $\pi : A \to B$ leképezést **gyűrű-izomorfizmusnak** *nevezzük, ha π bijektív gyűrű-morfizmus. Az A és B gyűrűket* **izomorfaknak** *nevezzük, ha létezik $A \to B$ gyűrű-izomorfizmus.*

Megjegyzés. Nyilvánvaló, hogy ha A és B egységelemes gyűrűk, valamint $\pi : A \to B$ egységelem-tartó gyűrű-morfizmus, akkor $\pi\langle \mathbf{G}(A)\rangle \subseteq \mathbf{G}(B)$ és $\pi|_{\mathbf{G}(A)}$ csoport-morfizmus a $\mathbf{G}(A)$ és $\mathbf{G}(B)$ csoportok között. Speciálisan, ha A és B egységelemes gyűrűk, valamint $\pi : A \to B$ gyűrű-izomorfizmus, akkor π szükségképpen egységelem-tartó, és a $\pi|_{\mathbf{G}(A)} : \mathbf{G}(A) \to \mathbf{G}(B)$ leképezés csoport-izomorfizmus a $\mathbf{G}(A)$ és $\mathbf{G}(B)$ csoportok között.

14.1.6. Állítás. *Legyen A gyűrű és $\mathbf{s} : \mathbb{N} \to A$ függvény. Legfeljebb egy olyan $\mathbb{Z} \to A$ csoport-morfizmus létezik a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amely kiterjesztése $\mathbf{s}$-nek. Akkor és csak akkor létezik olyan $\mathbb{Z} \to A$ gyűrű-morfizmus, amely $\mathbf{s}$-nek kiterjesztése, ha minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}(m + n) = \mathbf{s}(m) + \mathbf{s}(n)$ és $\mathbf{s}(mn) = \mathbf{s}(m)\mathbf{s}(n)$.*

Bizonyítás. (*Unicitás.*) A 13.1.10. állításból következik.

(*Egzisztencia.*) Az $\mathbf{s}$-re vonatkozó feltételek nyilvánvalóan szükségesek ahhoz, hogy $\mathbf{s}$ kiterjeszthető legyen $\mathbb{N}$-ről $\mathbb{Z}$-re egy $\mathbb{Z} \to A$ gyűrű-morfizmussá. Az elégségesség bizonyításához a 13.1.10. állítást alkalmazzuk úgy, hogy G az A gyűrű additív csoportja. Azt kapjuk, hogy létezik olyan $\widetilde{\mathbf{s}} : \mathbb{Z} \to A$ csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amely $\mathbf{s}$-nek kiterjesztése. Ekkor 13.1.4. miatt teljesül az, hogy minden $m, n \in \mathbb{N}$ esetén $\widetilde{\mathbf{s}}(m-n) = \mathbf{s}(m) - \mathbf{s}(n)$. Megmutatjuk, hogy $\widetilde{\mathbf{s}}$ félcsoport-morfizmus a $\mathbb{Z}$ és A gyűrűk multiplikatív félcsoportjai között. Ehhez legyenek $m, n, m', n' \in \mathbb{N}$. Ekkor az $\mathbf{s}$-re vonatkozó hipotézis alapján

$$\widetilde{\mathbf{s}}((m - n)(m' - n')) = \widetilde{\mathbf{s}}((mm' + nn') - (mn' + nm')) = \mathbf{s}(mm' + nn') - \mathbf{s}(mn' + nm') =$$
$$= \mathbf{s}(mm') + \mathbf{s}(nn') - (\mathbf{s}(mn') + \mathbf{s}(nm')) = \mathbf{s}(m)\mathbf{s}(m') + \mathbf{s}(n)\mathbf{s}(n') - \mathbf{s}(m)\mathbf{s}(n') - \mathbf{s}(n)\mathbf{s}(m') =$$
$$= (\mathbf{s}(m) - \mathbf{s}(n))(\mathbf{s}(m') - \mathbf{s}(n')) = \widetilde{\mathbf{s}}(m - n)\widetilde{\mathbf{s}}(m' - n'),$$

ahol kihasználtuk, hogy az A gyűrű additív csoportja kommutatív és A szorzása disztributív az összeadására nézve. Ezért $\widetilde{\mathbf{s}}$ gyűrű-morfimus az egész számok $\mathbb{Z}$ gyűrűje és A között. ■

14.1.7. Tétel. *Legyen A gyűrű és $a \in A$.*

a) *Létezik egyetlen olyan $\mathrm{j}_a : \mathbb{Z} \to A$ csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amelyre $\mathrm{j}_a(1) = a$.*

b) *A $\mathrm{j}_a : \mathbb{Z} \to A$ leképezés pontosan akkor gyűrű-morfizmus, ha $a^2 = a$, vagyis $a \in A$ idempotens elem az A gyűrű multiplikatív félcsoportjában.*

c) *Ha A egységelemes, akkor a $\mathrm{j}_{1_A} : \mathbb{Z} \to A$ leképezés gyűrű-morfizmus.*

Bizonyítás. a) (*Unicitás.*) Legyenek $\mathrm{j}_a, \mathrm{j}'_a : \mathbb{Z} \to A$ olyan csoport-morfizmusok a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amelyekre $\mathrm{j}_a(1) = a = \mathrm{j}'_a(1)$. Ekkor világos, hogy az $N := \{n \in \mathbb{N} | \mathrm{j}_a = \mathrm{j}'_a\}$ halmazra $0 \in N$ teljesül, mert $\mathrm{j}_a(0) = 0_A = \mathrm{j}'_a(0)$ (hiszen csoport-morfizmus neutráliselem-tartó), továbbá, $n \in N$ esetén $\mathrm{j}_a(n+1) = \mathrm{j}_a(n) + a = \mathrm{j}'_a(n) + a = \mathrm{j}'_a(n+1)$, vagyis $n+1 \in N$, ami azt jelenti, hogy N monoton részhalmaza $\mathbb{N}$-nek, így $N = \mathbb{N}$, azaz $\mathrm{j}_a = \mathrm{j}'_a$ az $\mathbb{N}$ halmazon. Ebből következik, hogy ha $m, n \in \mathbb{N}$, akkor $\mathrm{j}_a(m-n) = \mathrm{j}_a(m) - \mathrm{j}_a(n) = \mathrm{j}'_a(m) - \mathrm{j}'_a(n) = \mathrm{j}'_a(m-n)$ (hiszen additívan jelölt csoportok közötti morfizmus 13.1.4. szerint különbség-tartó), tehát $\mathrm{j}_a = \mathrm{j}'_a$.

(*Egzisztencia.*) Jelölje $\mathbf{s}_a$ a 0_A kezdőpont és az $A \to A$; $x \mapsto x + a$ függvény által meghatározott iterációs sorozatot, tehát $\mathbf{s}_a : \mathbb{N} \to A$ az a függvény, amelyre $\mathbf{s}_a(0) = 0_A$ és minden $n \in \mathbb{N}$ esetén $\mathbf{s}_a(n+1) = \mathbf{s}_a(n) + a$. Teljes indukcióval könnyen látható, hogy minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}_a(m+n) = \mathbf{s}_a(m) + \mathbf{s}_a(n)$, hiszen rögzített $m \in \mathbb{N}$ esetén $\mathbf{s}_a(m+0) = \mathbf{s}_a(m) = \mathbf{s}_a(m) + 0_A = \mathbf{s}_a(m) + \mathbf{s}_a(0)$, és ha $n \in \mathbb{N}$ olyan, hogy $\mathbf{s}_a(m+n) = \mathbf{s}_a(m) + \mathbf{s}_a(n)$, akkor az $\mathbf{s}_a$ sorozat iterációs definíciója szerint $\mathbf{s}_a(m + (n+1)) = \mathbf{s}_a((m+n)+1) = \mathbf{s}_a(m+n) + a = (\mathbf{s}_a(m) + \mathbf{s}_a(n)) + a = \mathbf{s}_a(m) + (\mathbf{s}_a(n) + a) = \mathbf{s}_a(m) + \mathbf{s}_a(n+1)$. Ezért a 13.1.10. állításból következik, hogy $\mathbf{s}_a$ egyértelműen kiterjeszthető egy $\mathrm{j}_a : \mathbb{Z} \to A$ csoport-morfizmussá. Ez a j_a csoport-morfizmus olyan, hogy $\mathrm{j}_a(1) = \mathbf{s}_a(1) = \mathbf{s}_a(0+1) = \mathbf{s}_a(0) + a = 0_A + a = a$, tehát j_a az a $\mathbb{Z} \to A$ csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amelynek a létezését állítottuk.

b) Ha a $\mathrm{j}_a : \mathbb{Z} \to A$ leképezés gyűrű-morfizmus, akkor $a^2 = (\mathrm{j}_a(1))^2 = \mathrm{j}_a(1^2) = \mathrm{j}_a(1) = a$, tehát $a^2 = a$. Megfordítva, tegyük fel, hogy $a^2 = a$. Azt kell igazolni, hogy j_a morfizmus a $\mathbb{Z}$ és A gyűrűk multiplikatív félcsoportjai között.

Először teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén $\mathrm{j}_a(n)a = \mathrm{j}_a(n)$. Az állítás teljesül, ha $n = 0$, mert $\mathrm{j}_a(0)a = 0_A a = 0_A = \mathrm{j}_a(0)$. Ha $n \in \mathbb{N}$ olyan, hogy $\mathrm{j}_a(n)a = \mathrm{j}_a(n)$, akkor $\mathrm{j}_a(n+1)a = (\mathrm{j}_a(n) + \mathrm{j}_a(1))a = (\mathrm{j}_a(n) + a)a = \mathrm{j}_a(n)a + a^2 = \mathrm{j}_a(n) + a = \mathrm{j}_a(n) + \mathrm{j}_a(1) = \mathrm{j}_a(n+1)$, ahol felhasználtuk az A gyűrű szorzásának összeadásra vonatkozó disztributivitását, az indukciós hipotézist és az $a^2 = a$ egyenlőséget: tehát az állítás az $n+1$ számra is igaz.

Most rögzített $m \in \mathbb{N}$ esetén n-szerinti teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ számra $\mathrm{j}_a(mn) = \mathrm{j}_a(m)\mathrm{j}_a(n)$. Az állítás teljesül, ha $n = 0$, mert $\mathrm{j}_a(m0) = \mathrm{j}_a(0) = 0_A = \mathrm{j}_a(m)0_A = \mathrm{j}_a(m)\mathrm{j}_a(0)$. Ha $n \in \mathbb{N}$ olyan, hogy $\mathrm{j}_a(mn) = \mathrm{j}_a(m)\mathrm{j}_a(n)$, akkor $\mathrm{j}_a(m(n+1)) = \mathrm{j}_a(mn+m) = \mathrm{j}_a(mn) + \mathrm{j}_a(m) = \mathrm{j}_a(m)\mathrm{j}_a(n) + \mathrm{j}_a(m) = \mathrm{j}_a(m)\mathrm{j}_a(n) + \mathrm{j}_a(m)a = \mathrm{j}_a(m)(\mathrm{j}_a(n) + a) = \mathrm{j}_a(m)(\mathrm{j}_a(n) + \mathrm{j}_a(1)) = \mathrm{j}_a(m)\mathrm{j}_a(n+1)$, ahol felhasználtuk az indukciós hipotézist, a $\mathrm{j}_a(m)a = \mathrm{j}_a(m)$ egyenlőséget, és az A gyűrű szorzásának összeadásra vonatkozó disztributivitását: tehát az állítás az $n+1$ számra is igaz.

Ez azt jelenti, hogy az $\mathbf{s} := \mathrm{j}_a|_{\mathbb{N}} : \mathbb{N} \to A$ sorozatra teljesül az, hogy minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}(m+n) = \mathbf{s}(m) + \mathbf{s}(n)$ (mert j_a csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között), és $\mathbf{s}(mn) = \mathbf{s}(m)\mathbf{s}(n)$. Ebből 14.1.6. alapján kapjuk, hogy $\mathrm{j}_a : \mathbb{Z} \to A$ gyűrű-morfizmus.

c) A b) állításból nyilvánvalóan következik, mert $1_A^2 = 1_A$. ■

14.1.8. Definíció. *Legyen A gyűrű. Minden $a \in A$ esetén j_a jelöli azt a $\mathbb{Z} \to A$ csoport-morfizmust a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amelyre $\mathrm{j}_a(1) = a$, továbbá minden $n \in \mathbb{Z}$ számra*

$$na := \mathrm{j}_a(n).$$

Megjegyezzük, hogy a $\mathbb{Z}$ gyűrűben $n, a \in \mathbb{Z}$ esetén az na szimbólumnak most két jelentést tulajdoníthatunk: 1) az iménti definíció szerint $na = \mathrm{j}_a(n)$; 2) $na := n \cdot a$, ahol $\cdot$ a $\mathbb{Z}$ gyűrű szorzása. Azonban ez a kétértelműség csak látszólagos, mert minden $a \in \mathbb{Z}$

esetén a $\mathbb{Z} \to \mathbb{Z}$; $n \mapsto n \cdot a$ leképezés csoport-morfizmus a $(\mathbb{Z}, +)$ és $(\mathbb{Z}, +)$ csoportok között, hiszen a $\mathbb{Z}$ gyűrű szorzása disztributív az összeadására nézve, továbbá $1 \cdot a = a$, így az előző állítás a) pontjában szereplő egyértelműség miatt minden $n \in \mathbb{Z}$ esetén $\mathrm{j}_a(n) = n \cdot a$, következésképpen $\mathbb{Z}$-ben az na szimbólum akár a $\mathrm{j}_a(n)$-et, akár az $n \cdot a$ objektumot jelölheti.

14.1.9. Állítás. *Ha A gyűrű, akkor a*

$$\mathbb{Z} \times A \to A; \quad (n, a) \mapsto na$$

leképezés a következő tulajdonságokkal rendelkezik: minden $m, n \in \mathbb{Z}$ és $a, b \in A$ esetén

$$(m + n)a = ma + na, \tag{1}$$
$$n(a + b) = na + nb, \tag{2}$$
$$(mn)a = m(na), \tag{3}$$
$$n(ab) = (na)b = a(nb), \tag{4}$$
$$0a = 0_A = n0_A, \tag{5}$$
$$1a = a, \tag{6}$$
$$(-n)a = -(na) = n(-a), \tag{7}$$
$$(mn)(ab) = (ma)(nb). \tag{8}$$

Bizonyítás. Ha $a \in A$, akkor a $\mathrm{j}_a : \mathbb{Z} \to A$ leképezés csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, így minden $m, n \in \mathbb{Z}$ esetén $(m + n)a = \mathrm{j}_a(m + n) = \mathrm{j}_a(m) + \mathrm{j}_a(n) = ma + na$, tehát (1) teljesül.

A $\mathrm{j}_a : \mathbb{Z} \to A$ leképezés csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, így neutráliselem-tartó, vagyis $0a = \mathrm{j}_a(0) = 0_A$. Továbbá, a $\mathbb{Z} \to A$; $n \mapsto 0_A$ leképezés olyan csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amely 1-hez a 0_A értéket rendeli, így az előző tétel a) pontjában szereplő egyértelműségi feltétel alapján ez a csoport-morfizmus egyenlő j_{0_A}-val, ami azt jelenti, hogy minden $n \in \mathbb{Z}$ esetén $n0_A = \mathrm{j}_{0_A}(n) = 0_A$. Ezzel az (5) egyenlőségeket igazoltuk.

A j_a függvény definíciója alapján $1a = \mathrm{j}_a(1) = a$ is teljesül, így fennáll a (6) egyenlőség is.

A (2) egyenlőség bizonyításához legyenek $a, b \in A$ rögzítve. Vezessük be a

$$\mathrm{j} : \mathbb{Z} \to A; \quad n \mapsto na + nb$$

függvényt. Ekkor minden $m, n \in \mathbb{Z}$ esetén (1) és A összeadásának asszociativitása és kommutativitása folytán

$$\mathrm{j}(m+n) = (m+n)a+(m+n)b = (ma+na)+(mb+nb) = (ma+mb)+(na+nb) = \mathrm{j}(m)+\mathrm{j}(n),$$

tehát j csoport-morfizmus a $(\mathbb{Z}, +)$ és $(A, +)$ csoportok között. Továbbá, (6) alapján $\mathrm{j}(1) = 1a + 1b = a + b$, ezért az előző tétel a) pontjában szereplő egyértelműségi feltétel alapján $\mathrm{j}_{a+b} = \mathrm{j}$, ami azt jelenti, hogy minden $n \in \mathbb{Z}$ esetén $n(a + b) = na + nb$, amivel a (2) egyenlőséget igazoltuk.

A (3) egyenlőség bizonyításához legyen $a \in A$ és $n \in \mathbb{Z}$ rögzítve. Vezessük be a

$$\mathrm{j} : \mathbb{Z} \to A; \quad m \mapsto (mn)a$$

függvényt. Ekkor minden $m, m' \in \mathbb{Z}$ esetén (1) és $\mathbb{Z}$ szorzásának összeadásra vonatkozó disztributivitása folytán

$$\mathrm{j}(m+m') = ((m+m')n)a = (mn+m'n)a = (mn)a + (m'n)a = \mathrm{j}(m) + \mathrm{j}(m'),$$

tehát j csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között. Továbbá, világos hogy $\mathrm{j}_*(1) = (1n)a = na$, ezért az előző tétel a) pontjában szereplő egyértelműségi feltétel alapján $\mathrm{j} = \mathrm{j}_{na}$, ami azt jelenti, hogy minden $m \in \mathbb{Z}$ esetén $(mn)a = m(na)$, amivel a (3) egyenlőséget igazoltuk.

A (4) egyenlőségek bizonyításához legyenek $a, b \in A$ rögzítve. Vezessük be a

$$\mathrm{j} : \mathbb{Z} \to A; \quad n \mapsto (na)b$$
$$\mathrm{j}' : \mathbb{Z} \to A; \quad n \mapsto a(nb)$$

függvényeket. Ekkor minden $m, n \in \mathbb{Z}$ esetén (1) és A szorzásának összeadásra vonatkozó disztributivitása folytán

$$\mathrm{j}(m+n) = ((m+n)a)b = (ma+na)b = (ma)b + (na)b = \mathrm{j}(m) + \mathrm{j}(n),$$
$$\mathrm{j}'(m+n) = a((m+n)b) = a(mb+nb) = a(mb) + a(nb) = \mathrm{j}'(m) + \mathrm{j}'(n),$$

tehát j és j′ csoport-morfizmusok a $\mathbb{Z}$ és A gyűrűk additív csoportjai között. Továbbá, (6) alapján $\mathrm{j}(1) = (1a)b = ab$ és $\mathrm{j}'(1) = a(1b) = ab$. Ezért az előző tétel a) pontjában szereplő egyértelműségi feltétel alapján $\mathrm{j}_{ab} = \mathrm{j} = \mathrm{j}'$, ami azt jelenti, hogy minden $n \in \mathbb{Z}$ esetén $n(ab) = (na)b = a(nb)$, amivel a (4) egyenlőségeket igazoltuk.

A (7) egyenlőségek bizonyításához legyen $a \in A$ rögzített. Ha $n \in \mathbb{Z}$, akkor (1) és (5) szerint $(-n)a + na = ((-n)+n)a = 0a = 0_A$, ezért $(-n)a = -(na)$. Tehát elég azt igazolni, hogy minden $n \in \mathbb{Z}$ esetén $-(na) = n(-a)$. Ehhez vezessük be a

$$\mathrm{j} : \mathbb{Z} \to A; \quad n \mapsto -(na)$$

függvényt. Ekkor minden $m, n \in \mathbb{Z}$ esetén (1) alapján

$$\mathrm{j}(m+n) = -((m+n)a) = -(ma+na) = (-(ma)) + (-(na)) = \mathrm{j}(m) + \mathrm{j}(n),$$

tehát j csoport-morfizmus a $\mathbb{Z}$ és A gyűrűk additív csoportjai között. Továbbá, (6) alapján $\mathrm{j}(1) = -(1a) = -a$, ezért az előző tétel a) pontjában szereplő egyértelműségi feltétel alapján $\mathrm{j} = \mathrm{j}_{-a}$, ami azt jelenti, hogy minden $n \in \mathbb{Z}$ esetén $-(na) = n(-a)$, amivel a (7) egyenlőségeket igazoltuk.

Végül, a (8) egyenlőség nyilvánvalóan következik a (3) és (4) egyenlőségekből, amelyek szerint: $(mn)(ab) = m(n(ab)) = m(a(nb)) = (ma)(nb)$. ■

Most a 14.1.8. definíció és a 14.1.9. állítás alkalmazásaként bebizonyítunk egy állítást, amelynek fontos szerepe lesz a gyűrűk "egységelemesítésében".

14.1.10. Állítás. *Legyen A gyűrű, és értelmezzük a $\mathbb{Z} \times A$ halmazon azokat a $+$ és $\cdot$ műveleteket, amelyekre minden $(n, a), (n', a') \in \mathbb{Z} \times A$ esetén*

$$(n, a) + (n', a') := (n + n', a + a'),$$
$$(n, a) \cdot (n', a') := (nn', na' + n'a + aa').$$

Ekkor $(\mathbb{Z} \times A, +, \cdot)$ olyan egységelemes gyűrű, amelynek $(1, 0_A)$ az egységeleme, továbbá az

$$A \to \mathbb{Z} \times A; \quad (0, a)$$

leképezés injektív gyűrű-morfizmus az A és $\mathbb{Z} \times A$ gyűrűk között.

Bizonyítás. A $\mathbb{Z}\times A$ halmazon értelmezett összeadás megegyezik a $\mathbb{Z}$ ás A gyűrűk addítív csoportműveleteinek szorzatával (11.4.1.), következésképpen $(\mathbb{Z}\times A,+)$ kommutatív csoport (11.4.2.).

A $\mathbb{Z}\times A$ halmazon értelmezett szorzás asszociativitásának bizonyításához legyenek $(n,a),(n',a'),(n'',a'')\in\mathbb{Z}\times A$. Ekkor a definíció szerint

$$(n,a)\cdot((n',a')\cdot(n'',a''))=(n,a)\cdot(n'n'',\ n'a''+n''a'+a'a'')=$$
$$=(n(n'n''),\ n(n'a''+n''a'+a'a'')+(n'n'')a+a(n'a''+n''a'+a'a''))\overset{(1)}{=}$$
$$\overset{(1)}{=}(n(n'n'')^{①},n(n'a'')^{②}+n(n''a')^{③}+n(a'a'')^{④}+(n'n'')a^{⑤}+a(n'a'')^{⑥}+a(n''a')^{⑦}+a(a'a'')^{⑧}),$$

ahol az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk a 14.1.9. állításban igazolt (2) összefüggést, és az A gyűrű szorzásának összeadásra vonatkozó (baloldali) disztributivitását. Szintén a definíció szerint

$$((n,a)\cdot(n',a'))\cdot(n'',a'')=(nn',na'+n'a+aa')\cdot(n'',a'')=$$
$$=((nn')n'',\ (nn')a''+n''(na'+n'a+aa')+(na'+n'a+aa')a'')\overset{(2)}{=}$$
$$\overset{(2)}{=}((nn')n''^{①},(nn')a''^{②}+n''(na')^{③}+n''(n'a)^{⑤}+n''(aa')^{⑦}+(na')a''^{④}+(n'a)a''^{⑥}+(aa')a''^{⑧}),$$

ahol a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk a 14.1.9. állításban igazolt (2) összefüggést, és az A gyűrű szorzásának összeadásra vonatkozó (jobboldali) disztributivitását. A két előző egyenlőség-lánc jobb oldalán álló kiejezésekben az azonos bekarikázott számmal megjelölt tagok a 14.1.9. állításban igazolt (3) és (4) összefüggések, valamint $\mathbb{Z}$ szorzásának asszociativitása és kommutativitása, továbbá A szorzásának aszociativitása alapján egyenlőek, ezért

$$(n,a)\cdot((n',a')\cdot(n'',a''))=((n,a)\cdot(n',a'))\cdot(n'',a''),$$

vagyis a $\mathbb{Z}\times A$ halmazon bevezett szorzás asszociatív.

A $\mathbb{Z}\times A$ halmazon értelmezett szorzás összeadásra vonatkozó baloldali disztributivitásnak bizonyításához legyenek $(n,a),(n',a'),(n'',a'')\in\mathbb{Z}\times A$. Ekkor a definíciók szerint

$$(n,a)\cdot((n',a')+(n'',a''))=(n,a)\cdot(n'+n'',a'+a'')=$$
$$=(n(n'+n''),n(a'+a'')+(n'+n'')a+a(a'+a''))\overset{(3)}{=}(n(n'+n''),na'+na''+n'a+n''a+aa'+aa''),$$

ahol a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk a 14.1.9. állításban igazolt (2) és (1) összefüggéseket, valamint az A gyűrű szorzásának összeadásra vonatkozó baloldali disztributivitását. Szintén a definíciók szerint

$$(n,a)\cdot(n',a')+(n,a)\cdot(n'',a'')=(nn',na'+n'a+aa')+(nn'',na''+n''a+aa'')=$$
$$=(nn'+nn'',\ na'+n'a+aa'+na''+n''a+aa'').$$

Mivel a $\mathbb{Z}$ gyűrű szorzása disztributív a szorzásra nézve, és A összeadása associatív és kommutatív, így a két előző egyenlőség-lánc jobb oldalán álló kifejezések egyenlőek, tehát

$$(n,a)\cdot((n',a')+(n'',a''))=(n,a)\cdot(n',a')+(n,a)\cdot(n'',a''),$$

vagyis a $\mathbb{Z}\times A$ halmazon bevezett szorzás balról disztributív a $\mathbb{Z}\times A$ halmazon bevezett összeadásra nézve.

A $\mathbb{Z}\times A$ halmazon értelmezett szorzás összeadásra vonatkozó jobboldali disztributivitásnak bizonyításához legyenek $(n,a),(n',a'),(n'',a'')\in\mathbb{Z}\times A$. Ekkor a definíciók szerint

$$((n',a')+(n'',a''))\cdot(n,a)=(n'+n'',a'+a'')\cdot(n,a)=$$
$$=((n'+n'')n,(n'+n'')a+n(a'+a'')+(a'+a'')a)\overset{(4)}{=}((n'+n'')n,n'a+n''a+na'+na''+a'a+a''a),$$

ahol a $\overset{(4)}{=}$ egyenlőségnél felhasználtuk a 14.1.9. állításban igazolt (1) és (2) összefüggéseket, valamint az A gyűrű szorzásának összeadásra vonatkozó jobboldali disztributivitását. Szintén a definíciók szerint

$$(n,a)\cdot(n',a')+(n,a)\cdot(n'',a'')=(nn',na'+n'a+aa')+(nn'',na''+n''a+aa'')=$$
$$=(nn'+nn'',\ na'+n'a+aa'+na''+n''a+aa'').$$

Mivel a $\mathbb{Z}$ gyűrű szorzása disztributív a szorzásra nézve, és A összeadása kommutatív, így a két előző egyenlőség-lánc jobb oldalán álló kifejezések egyenlőek, így

$$((n',a')+(n'',a''))\cdot(n,a)=(n',a')\cdot(n,a)+(n'',a'')\cdot(n,a),$$

vagyis a $\mathbb{Z}\times A$ halmazon bevezetett szorzás jobbról disztributív a $\mathbb{Z}\times A$ halmazon bevezetett összeadásra nézve.

Ezzel bebizonyítottuk, hogy a $(\mathbb{Z}\times A,+,\cdot)$ hármas gyűrű. Ha $(n,a)\in\mathbb{Z}\times A$, akkor a $\cdot$ művelet definíciója, valamint a 14.1.9. állításban igazolt (5) és (6) összefüggések, és 14.1.4. a) alapján

$$(1,0_A)\cdot(n,a)=(1n,1a+n0_A+0a)=(n,a+0_A+0_A)=(n,a),$$
$$(n,a)\cdot(1,0_A)=(n1,n0_A+1a+0_Aa)=(n,0_A+a+0_A)=(n,a),$$

ami azt jelenti, hogy $(1,0_A)$ a $(\mathbb{Z}\times A,\cdot)$ félcsoportnak neutrális eleme, tehát a $(\mathbb{Z}\times A,+,\cdot)$ gyűrűnek egységeleme.

Végül, a definíciók szerint minden $a,b\in A$ esetén $(0,a+b)=(0,a)+(0,b)$ és $(0,ab)=(0,a)\cdot(0,b)$, ezért az $A\to\mathbb{Z}\times A;\ (0,a)$ injekció gyűrű-morfizmus az A és $\mathbb{Z}\times A$ gyűrűk között. ■

14.2. Gyűrű feletti véges műveletek

Legyen $(A,+,\cdot)$ gyűrű. Ekkor $(A,+)$ kommutatív monoid (valójában kommutatív csoport), amelynek 0-val jelöljük a neutrális elemét. Ezért minden olyan A-ban haladó $(a_i)_{i\in I}$ rendszerre, amelyre $\{i\in I|a_i\neq 0\}$ véges halmaz, értelmes a $\underset{i\in I}{+}a_i\in A$ objektum (12.5.3.), amit a továbbiakban a

$$\sum_{i\in I}a_i$$

szimbólummal fogunk jelölni, és az $(a_i)_{i\in I}$ rendszer véges összegének nevezünk az A gyűrűben. Ha $(a_n)_{n\in\mathbb{N}}$ olyan A-ban haladó sorozat, hogy $\{n\in\mathbb{N}|a_n\neq 0\}$ véges halmaz, akkor gyakran a

$$\sum_{n=0}^{\infty}a_n:=\sum_{n\in\mathbb{N}}a_n$$

jelölést alkalmazzuk.

14.2.1. Állítás. *Ha A gyűrű, akkor minden $n \in \mathbb{N}$ és $a \in A$ esetén*

$$na = \sum_{i \in n} a_i,$$

ahol minden $i \in n$ esetén $a_i := a$.

Bizonyítás. Legyen $a \in A$ rögzítve és jelölje $(a_i)_{i \in \mathbb{N}}$ azt sorozatot, amelyre minden $i \in \mathbb{N}$ esetén $a_i := a$. Vezessük be az

$$\mathbf{s} : \mathbb{N} \to A; \quad n \mapsto \sum_{i \in n} a_i$$

sorozatot. Világos, hogy $\mathbf{s}(0) = 0_A$ és

$$\mathbf{s}(1) = \sum_{i \in 1} a_i = a_0 = a,$$

valamint minden $n \in \mathbb{N}$ esetén

$$\mathbf{s}(n+1) = \sum_{i \in n+1} a_i = \sum_{i \in n \cup \{n\}} a_i = \sum_{i \in n} a_i + a_n = \mathbf{s}(n) + a. \tag{1}$$

Rögzített $m \in \mathbb{N}$ esetén, n-szerinti teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{s}(m+n) = \mathbf{s}(m) + \mathbf{s}(n)$. Az állítás teljesül, ha $n = 0$, mert $\mathbf{s}(m+0) = \mathbf{s}(m) = \mathbf{s}(m) + 0_A = \mathbf{s}(m) + \mathbf{s}(0)$. Ha $n \in \mathbb{N}$ olyan, hogy $\mathbf{s}(m+n) = \mathbf{s}(m) + \mathbf{s}(n)$, akkor (1) miatt $\mathbf{s}(m+(n+1)) = \mathbf{s}((m+n)+1) = \mathbf{s}(m+n) + a = (\mathbf{s}(m) + \mathbf{s}(n)) + a = \mathbf{s}(m) + (\mathbf{s}(n) + a) = \mathbf{s}(m) + \mathbf{s}(n+1)$, tehát az állítás az $n+1$ számra is igaz.

Tehát minden $m, n \in \mathbb{N}$ esetén $\mathbf{s}(m+n) = \mathbf{s}(m) + \mathbf{s}(n)$, amiből 13.1.10. alapján következik egyetlen olyan $\mathrm{j} : \mathbb{Z} \to A$ csoport-morfizmus létezése a $\mathbb{Z}$ és A gyűrűk additív csoportjai között, amely $\mathbf{s}$-nek kiterjesztése. Mivel $\mathrm{j}(1) = \mathbf{s}(1) = a$, így a 14.1.7. tétel a) pontjában szereplő egyértelműségi feltétel alapján $\mathrm{j}_a = \mathrm{j}$, ami ekvivalens a bizonyítandó egyenlőséggel. ■

Tehát ha A gyűrű és $n \in \mathbb{N}$ és $a \in A$, akkor az $na \in A$ elemet úgy kapjuk, hogy az $a \in A$ elemet "n-szer önmagával összeadjuk A-ban", ezért azt is szokták írni, hogy

$$na = \overbrace{a + a + \cdots + a}^{n-\text{szer}}.$$

Ennek a jelölésnek csak mnemotechnikai jelentősége van: az előző állításban szereplő pontos formulára emlékeztet.

14.2.2. Állítás. *Legyen A kommutatív gyűrű, I nem üres véges halmaz, $(J_i)_{i \in I}$ nem üres véges halmazok rendszere, és $(f_i)_{i \in I}$ olyan függvényrendszer, hogy minden $i \in I$ esetén $J_i \subseteq \mathrm{Dom}(f_i)$ és $\mathrm{Im}(f_i) \subseteq A$. Ekkor a $J := \prod_{i \in I} J_i$ halmaz nem üres és véges, továbbá fennáll a*

$$\mathop{\mathrm{P}}_{i \in I} \left(\sum_{j \in J_i} f_i(j) \right) = \sum_{\sigma \in J} \left(\mathop{\mathrm{P}}_{i \in I} f_i(\sigma(i)) \right)$$

egyenlőség.

Bizonyítás. A 8.8.3. tétel nyilvánvaló következménye, az $S := A$, $\top := \cdot$, és $\perp := +$ választással. ■

14.2.3. Állítás. *Legyen I véges halmaz és $j, k \in I$ olyan elemek, hogy $j \neq k$. Jelölje $\tau_{j,k} \in \mathfrak{S}(I)$ azt a permutációt, amelyre $\tau_{j,k}(j) = k$ és $\tau_{j,k}(k) = j$ és minden $i \in I$ esetén, ha $i \neq j$ és $i \neq k$, akkor $\tau_{j,k}(i) = i$. Legyen A gyűrű és $f : \mathfrak{S}(I) \to A$ függvény.*

a) *Ha minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma \circ \tau_{j,k}) = -f(\sigma)$, vagy minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\tau_{j,k} \circ \sigma) = -f(\sigma)$, akkor*

$$\sum_{\sigma \in \mathfrak{S}(I)} f(\sigma) = 0_A.$$

b) *Ha A kommutatív egységelemes gyűrű, valamint minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma)$ invertálható elem A-ban, és minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma \circ \tau_{j,k}) = f(\sigma)^{-1}$, vagy minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\tau_{j,k} \circ \sigma) = f(\sigma)^{-1}$, akkor*

$$\prod_{\sigma \in \mathfrak{S}(I)} f(\sigma) = 1_A.$$

Bizonyítás. a) A 13.2.2. állítást kell alkalmazni az $(A, +)$ kommutatív monoidra.

b) A 13.2.2. állítást kell alkalmazni az $(\mathbf{G}(A), \cdot)$ kommutatív monoidra. ■

14.2.4. Állítás. (**Gyűrű szorzásának összeadásra vonatkozó általános disztributivitása.**) *Legyen A gyűrű és $(a_i)_{i \in I}$ olyan rendszer A-ban, hogy $\{i \in I | a_i \neq 0_A\}$ véges halmaz. Ekkor minden $b \in A$ esetén az $\{i \in I | a_i b \neq 0_A\}$ és $\{i \in I | b a_i \neq 0_A\}$ halmazok végesek, és*

$$\Big(\sum_{i \in I} a_i\Big) b = \sum_{i \in I} (a_i b),$$

$$b\Big(\sum_{i \in I} a_i\Big) = \sum_{i \in I} (b a_i).$$

Bizonyítás. Legyen $I_* := \{i \in I | a_i \neq 0_A\}$. Ha $I_* = \emptyset$, akkor minden $i \in I$ esetén $a_i = 0_A$, következésképpen 14.1.4. a) alapján $a_i b = 0_A = b a_i$ is teljesül, ezért 12.5.1. szerint

$$\Big(\sum_{i \in I} a_i\Big) b = 0_A b = 0_A = \sum_{i \in I} (a_i b),$$

$$b\Big(\sum_{i \in I} a_i\Big) = b 0_A = 0_A = \sum_{i \in I} (b a_i).$$

Ha $I_* \neq \emptyset$, akkor a monoidban bevezetett véges művelet definíciója szerint

$$\sum_{i \in I} a_i = \sum_{i \in I_*} a_i,$$

ugyanakkor 14.1.4. a) alapján $\{i \in I | a_i b \neq 0_A\} \subseteq I_*$ és $\{i \in I | b a_i \neq 0_A\} \subseteq I_*$, így az $\{i \in I | a_i b \neq 0_A\}$ és $\{i \in I | b a_i \neq 0_A\}$ halmazok végesek (8.1.8.), valamint

$$\sum_{i \in I} (a_i b) = \sum_{i \in I_*} (a_i b),$$

$$\sum_{i \in I} (b a_i) = \sum_{i \in I_*} (b a_i),$$

ezért a bizonyítandó egyenlőségek nyilvánvalóan következnek a 8.8.2. állításból, ha abban $\perp$ helyére az A gyűrű összeadását, $\top$ helyére az A gyűrű szorzását, és J helyére az I_* nem üres véges halmazt helyettesítjük. ■

14.2.5. Állítás. *Legyen A gyűrű, $N \in \mathbb{N}$, valamint $(a_i)_{i\in[\![0,N]\!]}$ és $(b_i)_{i\in[\![0,N]\!]}$ tetszőleges A-ban haladó rendszerek. Ekkor*

$$\left(\sum_{i=0}^{N} a_i\right)\left(\sum_{i=0}^{N} b_i\right) = \sum_{(i,j)\in[\![0,N]\!]\times[\![0,N]\!]} a_i b_j = \sum_{n=0}^{2N}\left(\sum_{k=0}^{n} \tilde{a}_k \tilde{b}_{n-k}\right),$$

ahol minden $i \in [\![0,2N]\!]$ esetén

$$\tilde{a}_i := \begin{cases} a_i & \text{, ha } i \le N, \\ 0 & \text{, ha } i > N, \end{cases}$$

és hasonlóan

$$\tilde{b}_i := \begin{cases} b_i & \text{, ha } i \le N, \\ 0 & \text{, ha } i > N. \end{cases}$$

Bizonyítás. Nyilvánvaló, hogy a

$$\sigma : [\![0,N]\!] \times [\![0,N]\!] \to [\![0,2N]\!]; \quad (i,j) \mapsto i+j$$

függvény szürjektív, ezért a $\left(\overset{-1}{\sigma}\langle\{n\}\rangle\right)_{n\in[\![0,2N]\!]}$ halmazrendszer partíciója a $[\![0,N]\!]\times[\![0,N]\!]$ halmaznak, így

$$\sum_{(i,j)\in[\![0,N]\!]\times[\![0,N]\!]} a_i b_j \overset{(1)}{=} \sum_{n\in[\![0,2N]\!]}\Bigg(\sum_{(i,j)\in\overset{-1}{\sigma}\langle\{n\}\rangle} a_i b_j\Bigg) \overset{(2)}{=} \sum_{n=0}^{2N}\Bigg(\sum_{\substack{(i,j)\in[\![0,N]\!]\times[\![0,N]\!]\\ i+j=n}} a_i b_j\Bigg) \overset{(3)}{=}$$

$$\overset{(3)}{=} \sum_{n=0}^{2N}\Bigg(\sum_{k\in[\![\max(0,n-N),\min(n,N)]\!]} a_k b_{n-k}\Bigg) \overset{(4)}{=} \sum_{n=0}^{2N}\Bigg(\sum_{k=\max(0,n-N)}^{\min(n,N)} a_k b_{n-k}\Bigg), \tag{1}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél az A gyűrű $+$ műveletének általános asszociativitását (8.7.1.) alkalmaztuk;

– a $\overset{(2)}{=}$ és $\overset{(4)}{=}$ egyenlőségnél a véges műveletek definíciójára (8.5.3.) hivatkoztunk;

– a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk azt, hogy az

$$[\![\max(0,n-N),\min(n,N)]\!] \to \{(i,j)\in[\![0,N]\!]\times[\![0,N]\!] \mid i+j=n\}; \quad k\mapsto (k,n-k)$$

leképezés bijekció (amelynek inverze az

$$\{(i,j)\in[\![0,N]\!]\times[\![0,N]\!] \mid i+j=n\} \to [\![\max(0,n-N),\min(n,N)]\!]; \quad (i,j)\mapsto i$$

leképezés), így alkalmazhatjuk az A gyűrű $+$ műveletének általános kommutativitását (8.6.1.).

Legyen $n \in [\![0,2N]\!]$ rögzített. Ha $k\in[\![0,n]\!]$ és $k > \min(n,N)$, akkor $k > N$, így $\tilde{a}_k = 0$, következésképpen $\tilde{a}_k\tilde{b}_{n-k} = 0$. Ha $k\in[\![0,n]\!]$ és $k < \min(0,n-N)$, akkor $n-k > N$, így $\tilde{b}_{n-k} = 0$, következésképpen $\tilde{a}_k\tilde{b}_{n-k} = 0$. Ez azt jelenti, hogy ha $k\in[\![0,n]\!]$ és $\tilde{a}_k\tilde{b}_{n-k}\neq 0$, akkor $\tilde{a}_k \neq 0$ vagy $\tilde{b}_{n-k}\neq 0$, következésképpen $k\in[\![\max(0,n-N),\min(n,N)]\!]$, vagyis

$$\{k\in[\![0,n]\!] \mid \tilde{a}_k\tilde{b}_{n-k}\neq 0\} \subseteq [\![\max(0,n-N),\min(n,N)]\!] \subseteq [\![0,n]\!].$$

Ebből 12.5.2. alapján kapjuk, hogy

$$\sum_{k=0}^{n} \tilde{a}_k \tilde{b}_{n-k} = \sum_{k=\max(0,n-N)}^{\min(n,N)} \tilde{a}_k \tilde{b}_{n-k} = \sum_{k=\max(0,n-N)}^{\min(n,N)} a_k b_{n-k}.$$

Ebből (1) alapján kapjuk, hogy

$$\sum_{(i,j)\in[\![0,N]\!]\times[\![0,N]\!]} a_i b_j = \sum_{n=0}^{2N} \left(\sum_{k=0}^{n} \tilde{a}_k \tilde{b}_{n-k} \right).$$

Nyilvánvaló, hogy a

$$\tau : [\![0,N]\!] \times [\![0,N]\!] \to [\![0,N]\!]; \quad (i,j) \mapsto i$$

függvény szürjektív, ezért a $\left(\overset{-1}{\tau}\langle\{n\}\rangle\right)_{n\in[\![0,N]\!]}$ halmazrendszer partíciója a $[\![0,N]\!] \times [\![0,N]\!]$ halmaznak, így

$$\sum_{(i,j)\in[\![0,N]\!]\times[\![0,N]\!]} a_i b_j \overset{(5)}{=} \sum_{i=0}^{N} \Big(\sum_{j\in \overset{-1}{\tau}\langle\{i\}\rangle} a_i b_j \Big) \overset{(6)}{=} \sum_{i=0}^{N} \left(\sum_{j=0}^{N} a_i b_j \right) \overset{(7)}{=}$$
$$\overset{(7)}{=} \sum_{i=0}^{N} \left(a_i \left(\sum_{j=0}^{N} b_j \right) \right) \overset{(8)}{=} \left(\sum_{i=0}^{N} a_i \right) \left(\sum_{j=0}^{N} b_j \right),$$

ahol

– az $\overset{(5)}{=}$ egyenlőségnél az A gyűrű $+$ műveletének általános asszociativitását (8.7.1.) alkalmaztuk;

– a $\overset{(6)}{=}$ egyenlőségnél felhasználtuk azt, hogy minden $i \in [\![0,N]\!]$ esetén a

$$[\![0,N]\!] \to \overset{-1}{\tau}\langle\{i\}\rangle; \quad j \mapsto (i,j)$$

leképezés bijekció, így alkalmazhatjuk az A gyűrű $+$ műveletének általános kommutativitását (8.6.1.);

– a $\overset{(7)}{=}$ és $\overset{(8)}{=}$ egyenlőségnél a 14.2.4. állításra hivatkozunk. ■

14.2.6. Következmény. *Legyen A gyűrű, valamint $(a_n)_{n\in\mathbb{N}}$ és $(b_n)_{n\in\mathbb{N}}$ olyan A-ban haladó sorozatok, amelyekre $\{n \in \mathbb{N} | a_n \neq 0_A\}$ és $\{n \in \mathbb{N} | b_n \neq 0_A\}$ véges halmazok. Ekkor a $\left(\sum_{k=0}^{n} a_k b_{n-k}\right)_{n\in\mathbb{N}}$ sorozatra is teljesül az, hogy a $\left\{ n \in \mathbb{N} \,\middle|\, \sum_{k=0}^{n} a_k b_{n-k} \neq 0_A \right\}$ halmaz véges, valamint az $\{(i,j) \in \mathbb{N}\times\mathbb{N} | a_i b_j \neq 0_A\}$ halmaz is véges, és fennállnak a*

$$\left(\sum_{i=0}^{\infty} a_i \right) \left(\sum_{i=0}^{\infty} b_i \right) = \sum_{(i,j)\in\mathbb{N}\times\mathbb{N}} a_i b_j = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right).$$

egyenlőségek.

Bizonyítás. Legyen $N \in \mathbb{N}$ olyan szám, amely felső korlátja a $\{i \in \mathbb{N} | a_i \neq 0_A\}$ és $\{j \in \mathbb{N} | b_j \neq 0_A\}$ véges halmazoknak. Ekkor $\{i \in \mathbb{N} | a_i \neq 0_A\} \cup \{j \in \mathbb{N} | b_j \neq 0_A\} \subseteq [\![0,N]\!]$, ezért

$$\sum_{i=0}^{\infty} a_i = \sum_{i=0}^{N} a_i, \quad \sum_{i=0}^{\infty} b_i = \sum_{i=0}^{N} b_i. \tag{1}$$

Ha $(i,j) \in \mathbb{N} \times \mathbb{N}$ olyan, hogy $a_i b_j \neq 0_A$, akkor $a_i \neq 0_A$ és $b_j \neq 0_A$, következésképpen $(i,j) \in [\![0,N]\!] \times [\![0,N]\!]$, tehát

$$\sum_{(i,j)\in\mathbb{N}\times\mathbb{N}} a_i b_j = \sum_{(i,j)\in[\![0,N]\!]\times[\![0,N]\!]} a_i b_j. \tag{2}$$

Ha $n \in \mathbb{N}$ olyan, hogy $\sum_{k=0}^{n} a_k b_{n-k} \neq 0_A$, akkor van olyan $k \leq n$ természetes szám, amelyre $a_k b_{n-k} \neq 0_A$, tehát $a_k \neq 0_A$ és $b_{n-k} \neq 0_A$, így $k \leq N$ és $n - k \leq N$, következésképpen $n = k + (n-k) \leq 2N$, ezért az $\left\{ n \in \mathbb{N} \,\middle|\, \sum_{k=0}^{n} a_k b_{n-k} \neq 0_A \right\}$ halmaz véges és

$$\sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) = \sum_{n=0}^{2N} \left(\sum_{k=0}^{n} a_k b_{n-k} \right). \tag{3}$$

Az (1), (2) és (3) egyenlőségekből és 14.2.5.-ból következik az állítás. ■

14.3. Gyűrű egységelemesítése

14.3.1. Állítás. *Legyen A gyűrű.*

a) *Létezik olyan (B, π) pár, hogy teljesülnek a következők:*

– *B egységelemes gyűrű és $\pi : A \to B$ gyűrű-morfizmus;*

– *minden C egységelemes gyűrűhöz és minden $\sigma : A \to C$ gyűrű-morfizmushoz létezik egyetlen olyan $\widetilde{\sigma} : B \to C$ egységelem-tartó gyűrű-morfizmus, hogy $\widetilde{\sigma} \circ \pi = \sigma$, vagyis a*

$$\begin{tikzcd} A \arrow[r, "\pi"] \arrow[dr, "\sigma"'] & B \arrow[d, "\widetilde{\sigma}"] \\ & C \end{tikzcd}$$

diagram kommutatív.

b) *Ha (A', π') és (A'', π'') olyan párok, amelyekre az* a) *állításban megfogalmazott tulajdonságok teljesülnek, ha abban (B, π) helyére (A', π')-t és (A'', π'')-t helyettesítjük, akkor létezik egyetlen olyan $\sigma : A' \to A''$ gyűrű-izomorfizmus, amelyre $\sigma \circ \pi' = \pi''$.*

Bizonyítás. a) Értelmezzük a $\mathbb{Z} \times A$ halmazon azokat a $+$ és $\cdot$ műveleteket, amelyekre minden $(n, a), (n', a') \in \mathbb{Z} \times A$ esetén

$$(n, a) + (n', a') := (n + n', a + a'),$$
$$(n, a) \cdot (n', a') := (nn', na' + n'a + aa').$$

A 14.1.10. állítás szerint $(\mathbb{Z} \times A, +, \cdot)$ olyan egységelemes gyűrű, amelynek $(1, 0_A)$ a multiplikatív neutrális eleme. Könnyen látható, hogy minden $(n, a) \in \mathbb{Z} \times A$ esetén $(n, a) = (n, 0_A) + (0, a) = n(1, 0_A) + (0, a)$.

Vezessük be a

$$\pi : A \to \mathbb{Z} \times A; \quad a \mapsto (0, a)$$

leképezést. Ez gyűrű-morfizmus, mert minden $a, b \in A$ esetén

$$\pi(a + b) = (0, a + b) = (0 + 0, a + b) = (0, a) + (0, b) = \pi(a) + \pi(b),$$
$$\pi(ab) = (0, ab) = (00, 0b + 0a + ab) = (0, a) \cdot (0, b) = \pi(a) \cdot \pi(b).$$

Ha C egységelemes gyűrű és $\sigma : A \to C$ gyűrű-morfizmus, akkor a

$$\widetilde{\sigma} : \mathbb{Z} \times A \to \mathbb{C}; \quad (n,a) \mapsto n1_C + \sigma(a)$$

leképezés egységelem-tartó gyűrű-morfizmus, mert minden $(n,a),(n',a') \in \mathbb{Z} \times A$ esetén

$$\widetilde{\sigma}((n,a)+(n',a)) = \widetilde{\sigma}(n+n', a+a') = (n+n')1_C + \sigma(a+a') = n1_C + n'1_C + \sigma(a) + \sigma(a') =$$
$$= (n1_C + \sigma(a)) + (n'1_C + \sigma(a')) = \widetilde{\sigma}(n,a) + \widetilde{\sigma}(n',a'),$$

továbbá

$$\widetilde{\sigma}((n,a)\cdot(n',a)) = \widetilde{\sigma}(nn', na' + n'a + aa') = (nn')1_C + \sigma(na' + n'a + aa') =$$
$$= (n1_C)(n'1_C) + \sigma(na') + \sigma(n'a) + \sigma(aa') = (n1_C)(n'1_C) + n\sigma(a') + n'\sigma(a) + \sigma(a)\sigma(a') =$$
$$= (n1_C + \sigma(a))(n'1_C + \sigma(a')) = \widetilde{\sigma}(n,a)\widetilde{\sigma}(n',a'),$$

valamint

$$\widetilde{\sigma}(1, 0_A) = 11_C + \sigma(0_A) = 1_C.$$

Nyilvánvaló, hogy $a \in A$ esetén

$$(\widetilde{\sigma} \circ \pi)(a) = \widetilde{\sigma}(0,a) = 01_C + \sigma(a) = \sigma(a),$$

tehát $\widetilde{\sigma} \circ \pi = \sigma$. Ha $\widetilde{\sigma}' : \mathbb{Z} \times A \to \mathbb{C}$ szintén olyan egységelem-tartó gyűrű-morfizmus, amelyre $\widetilde{\sigma}' \circ \pi = \sigma$, akkor minden $(n,a) \in \mathbb{Z} \times A$ esetén $(n,a) = (n, 0_A) + (0,a) = n(1, 0_A) + (0,a)$ miatt:

$$\widetilde{\sigma}'(n,a) = \widetilde{\sigma}'(n(1,0_A) + (0,a)) = n\widetilde{\sigma}'(1,0_A) + \widetilde{\sigma}'(0,a) =$$
$$= n1_C + (\widetilde{\sigma}' \circ \pi)(a) = n1_C + \sigma(a) = \widetilde{\sigma}(n,a),$$

vagyis $\widetilde{\sigma}' = \widetilde{\sigma}$.

b) Az (A', π') párra vonatkozó feltétel alapján a $\pi'' : A \to A''$ gyűrű-morfizmushoz létezik egyetlen olyan $\sigma : A' \to A''$ gyűrű-morfizmus, amelyre $\sigma \circ \pi' = \pi''$, vagyis az

$$\begin{tikzcd} A \arrow[r, "\pi'"] \arrow[dr, "\pi''"'] & A' \arrow[d, "\sigma"] \\ & A'' \end{tikzcd}$$

diagram kommutatív. Az (A'', π'') párra vonatkozó feltétel alapján a $\pi' : A \to A'$ gyűrű-morfizmushoz létezik egyetlen olyan $\sigma' : A'' \to A'$ gyűrű-morfizmus, amelyre $\sigma' \circ \pi'' = \pi'$, vagyis az

$$\begin{tikzcd} A \arrow[r, "\pi''"] \arrow[dr, "\pi'"'] & A'' \arrow[d, "\sigma'"] \\ & A' \end{tikzcd}$$

diagram kommutatív. Ekkor fennállnak a

$$(\sigma' \circ \sigma) \circ \pi' = \sigma' \circ (\sigma \circ \pi') = \sigma' \circ \pi'' = \pi', \tag{1}$$
$$(\sigma \circ \sigma') \circ \pi'' = \sigma \circ (\sigma' \circ \pi'') = \sigma \circ \pi' = \pi''. \tag{2}$$

egyenlőségek.

Az (1) egyenlőség szerint $\sigma' \circ \sigma : A' \to A'$ olyan gyűrű morfizmus, amelyre $(\sigma' \circ \sigma) \circ \pi' = \pi'$, vagyis az

$$\begin{tikzcd} A \arrow[r, "\pi'"] \arrow[dr, "\pi'"'] & A' \arrow[d, "\sigma' \circ \sigma"] \\ & A' \end{tikzcd}$$

diagram kommutatív. De nyilvánvalóan az $\mathrm{id}_{A'} : A' \to A'$ gyűrű-morfizmusra is fennáll az $\mathrm{id}_{A'} \circ \pi' = \pi'$ egyenlőség, így az (A', π') párral kapcsolatos egyértelműségi feltétel alapján $\sigma' \circ \sigma = \mathrm{id}_{A'}$.

A (2) egyenlőség szerint $\sigma \circ \sigma' : A'' \to A''$ olyan gyűrű morfizmus, amelyre $(\sigma \circ \sigma') \circ \pi'' = \pi''$, vagyis az

$$\begin{tikzcd} A \arrow[r, "\pi''"] \arrow[dr, "\pi''"'] & A'' \arrow[d, "\sigma \circ \sigma'"] \\ & A'' \end{tikzcd}$$

diagram kommutatív. De nyilvánvalóan az $\mathrm{id}_{A''} : A'' \to A''$ gyűrű-morfizmusra is fennáll az $\mathrm{id}_{A''} \circ \pi'' = \pi''$ egyenlőség, így az (A'', π'') párral kapcsolatos egyértelműségi feltétel alapján $\sigma \circ \sigma' = \mathrm{id}_{A''}$.

Ez azt jelenti, hogy $\sigma : A' \to A''$ olyan gyűrű-izomorfizmus, amelyre $\sigma \circ \pi' = \pi''$. Az (A', π') párral kapcsolatos egyértelműségi feltétel alapján már azon $\tau : A' \to A''$ *gyűrű-morfizmusok* halmaza is pontosan egy elemű, amelyekre $\tau \circ \pi' = \pi''$. Mivel σ eleme ennek a halmaznak, így a $\sigma : A' \to A''$ gyűrű-izomorfizmus egyértelműen van meghatározva a $\sigma \circ \pi' = \pi''$ feltétel által. ■

Az előző állítás a) pontjának bizonyításából látható, hogy π *injektív* gyűrű-morfizmus, és b)-ből következik, hogy bármely olyan (B, π) párra, amelyre a) feltételei teljesülnek, π injektív lesz, tehát az A gyűrű π által *beágyazódik* a B egységelemes gyűrűbe.

14.3.2. Definíció. *Az A gyűrű* **egységelemesítésének** *nevezünk minden olyan (B, π) párt, amelyre az előző állítás a) feltétele teljesül. Ha A gyűrű, akkor a $\mathbb{Z} \times A$ halmazt a*

$$(\mathbb{Z} \times A) \times (\mathbb{Z} \times A) \to \mathbb{Z} \times A; \quad ((n,a),(n',a')) \mapsto (n,a) + (n',a') := (n+n', a+a'),$$
$$(\mathbb{Z} \times A) \times (\mathbb{Z} \times A) \to \mathbb{Z} \times A; \quad ((n,a),(n',a')) \mapsto (n,a) \cdot (n',a') := (nn', na' + n'a + aa')$$

műveletekkel ellátva az A gyűrű **standard egységelemesítésének** *nevezzük.*

14.4. Félcsoportgyűrűk és polinomgyűrűk

14.4.1. Definíció. *Ha A gyűrű és f olyan függvény, hogy $\mathrm{Im}(f) \subseteq A$, akkor*

$$[f \neq 0] \;:=\; \{\; x \in \mathrm{Dom}(f) \mid f(x) \neq 0_A \;\},$$

ahol 0_A az A gyűrű additív neutrális eleme. Ha X halmaz és A gyűrű, akkor

$$A^{(X)} \;:=\; \{\; f \in A^X \mid [f \neq 0] \text{ véges halmaz} \;\},$$

tehát $A^{(X)}$ azon $f : X \to A$ függvények halmaza, amelyekre az $\{x \in X | f(x) \neq 0_A\}$ halmaz véges, amit úgy fogalmazhatunk meg, hogy f csak véges sok helyen vesz fel nem 0_A értéket.

14.4.2. Definíció. *Legyen S (multiplikatívan jelölt) félcsoport és A gyűrű. Ekkor minden $f, g \in A^{(S)}$ és $a \in A$ esetén*

$$f + g : S \to A; \quad s \mapsto f(s) + g(s),$$
$$a.f : S \to A; \quad s \mapsto af(s),$$

valamint

$$f * g : S \to A; \quad s \mapsto \sum_{\substack{(s',s'') \in S \times S \\ s's''=s}} f(s')g(s'').$$

Ha $f, g \in A^{(S)}$, akkor az $f * g$ függvényt az f és g függvények (S, A) pár szerinti **konvolúciós szorzatának** *nevezzük, és az*

$$* : A^{(S)} \times A^{(S)} \to A^S; \quad (f, g) \mapsto f * g$$

leképezést az (S, A) pár szerinti **konvolúciós szorzásnak** *nevezzük.*

Megjegyezzük, hogy az előző definícióban szereplő $f * g : S \to A$ függvény értelmes, mert minden $s \in S$ esetén a

$$h : \{(s', s'') \in S \times S | s's'' = s\} \to A; \quad (s', s'') \mapsto f(s')g(s'')$$

függvényre 14.1.4. a) szerint $[h \neq 0] \subseteq [f \neq 0] \times [g \neq 0]$, és itt a jobb oldalon véges halmaz áll (8.1.17.), tehát $[h \neq 0]$ véges halmaz (8.1.8.), így a 12.5.3. definíció alapján értelmes a

$$\sum_{\substack{(s',s'') \in S \times S \\ s's''=s}} h(s', s'')$$

összeg az $(A, +)$ kommutatív monoidban, akkor is, ha az $\{(s', s'') \in S \times S | s's'' = s\}$ indexhalmaz üres vagy végtelen.

Bizonyos esetekben a konvolúciós szorzatok kiszámítása jelentősen egyszerűsödik. Ilyen esetekről lesz szó a következő állításban.

14.4.3. Állítás. a) Legyen G csoport és A gyűrű. Ekkor minden $f, g \in A^{(G)}$ és $s \in G$ esetén

$$(f * g)(s) = \sum_{t \in G} f(t)g(t^{-1}s),$$

ahol $*$ a (G, A) pár szerinti konvolúciós szorzás.

b) Jelölje $\mathbb{N}_{\text{add}}$ az $\mathbb{N}$ halmazt a természetes összeadással ellátva (tehát $\mathbb{N}$ additív félcsoportját) és legyen A gyűrű. Ha $P, Q \in A^{(\mathbb{N})}$, akkor minden $n \in \mathbb{N}$ esetén

$$(P * Q)(n) = \sum_{k=0}^{n} P(k)Q(n - k),$$

ahol $*$ az $(\mathbb{N}_{\text{add}}, A)$ pár szerinti konvolúciós szorzás.

Bizonyítás. a) Legyen $f, g \in A^{(G)}$ és $s \in G$. Ekkor a

$$G \to \{(s', s'') \in G \times G | s's'' = s\}; \quad t \mapsto (t, t^{-1}s)$$

leképezés nyilvánvalóan bijekció, így a monoidokra vonatkozó általános kommutativitás tétele (12.5.9.) és a (G, A) pár szerinti konvolúciós szorzás definíciója szerint

$$(f * g)(s) = \sum_{\substack{(s',s'')\in G\times G\\ s's''=s}} f(s')g(s'') = \sum_{t\in G} f(t)g(t^{-1}s).$$

b) Legyen $P, Q \in A^{(\mathbb{N})}$ és $n \in \mathbb{N}$. Ekkor az

$$\{k \in \mathbb{N} | k \leq n\} \to \{(n', n'') \in \mathbb{N} \times \mathbb{N} | n' + n'' = n\}; \quad k \mapsto (k, n-k)$$

leképezés nyilvánvalóan bijekció, így a monoidokra vonatkozó általános kommutativitás tétele (12.5.9.) és az $(\mathbb{N}_{\mathrm{add}}, A)$ pár szerinti konvolúciós szorzás definíciója szerint

$$(P * Q)(n) = \sum_{\substack{(n',n'')\in \mathbb{N}\times\mathbb{N}\\ n'+n''=n}} P(n')Q(n'') = \sum_{k=0}^{n} P(k)Q(n-k). \blacksquare$$

14.4.4. Állítás. *Legyen S (multiplikatívan jelölt) félcsoport és A gyűrű. Tegyük fel, hogy S és A egységelemesek, és jelölje $\mathfrak{n}$ az S félcsoport neutrális elemét, valamint 1_A az A gyűrű egységelemét. Legyen $\mathbf{1} \in A^{(S)}$ az a függvény, amelyre minden $s \in S$ esetén*

$$\mathbf{1}(s) := \begin{cases} 1_A & , \textit{ha } s = \mathfrak{n}, \\ 0_A & , \textit{egyébként.} \end{cases}$$

Ekkor $\mathbf{1}$ neutrális elem a $*$ műveletre nézve.

Bizonyítás. Legyen $f \in A^{(S)}$ tetszőleges. Ekkor minden $s \in S$ esetén

$$(\mathbf{1} * f)(s) = \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} \mathbf{1}(s')f(s'') = \sum_{\substack{(s',s'')\in S\times S\\ s's''=s\\ \mathbf{1}(s')f(s''))\neq 0_A}} \mathbf{1}(s')f(s'') = \mathbf{1}(\mathfrak{n})f(s) = 1_A f(s) = f(s),$$

hiszen $\{(s', s'') \in S \times S | (s's'' = s) \wedge (\mathbf{1}(s')f(s'')) \neq 0_A\} = \{(\mathfrak{n}, s)\}$, továbbá

$$(f * \mathbf{1})(s) = \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} f(s')\mathbf{1}(s'') = \sum_{\substack{(s',s'')\in S\times S\\ s's''=s\\ f(s')\mathbf{1}(s''))\neq 0_A}} f(s')\mathbf{1}(s'') = f(s)\mathbf{1}(\mathfrak{n}) = f(s)1_A = f(s),$$

hiszen $\{(s', s'') \in S \times S | (s's'' = s) \wedge (f(s')\mathbf{1}(s'')) \neq 0_A\} = \{(s, \mathfrak{n})\}$. Ez azt jelenti, hogy $\mathbf{1} * f = f = f * \mathbf{1}$. $\blacksquare$

14.4.5. Tétel. *Legyen S (multiplikatívan jelölt) félcsoport és A gyűrű.*

a) *Minden $f, g \in A^{(S)}$ és $a \in A$ esetén $f + g$, $a.f$, $f * g \in A^{(S)}$ és az $A^{(S)}$ halmaz az*

$$A^{(S)} \times A^{(S)} \to A^{(S)}; \quad (f, g) \mapsto f + g,$$
$$A^{(S)} \times A^{(S)} \to A^{(S)}; \quad (f, g) \mapsto f * g$$

műveletekkel ellátva gyűrű.

b) *Minden $f, g \in A^{(S)}$ és $a, b \in A$ esetén*

$$a.(b.f) = (ab).f,$$
$$(a + b).f = a.f + b.f,$$
$$a.(f + g) = a.f + a.g,$$
$$a.(f * g) = (a.f) * g,$$

és ha A egységelemes, akkor $1_A.f = f$.

c) *Ha A egységelemes, akkor minden $s \in S$ esetén az*

$$\mathrm{e}_s : S \to A; \quad s' \mapsto \begin{cases} 1_A & , \text{ha } s' = s \\ 0_A & , \text{ha } s' \neq s \end{cases}$$

függvény eleme $A^{(S)}$-nek, és minden $s, t \in S$ esetén $\mathrm{e}_s * \mathrm{e}_t = \mathrm{e}_{st}$, továbbá minden $f \in A^{(S)}$ függvényre

$$f = \sum_{s \in S} f(s).\mathrm{e}_s,$$

ahol az összeget az $(A^{(S)}, +)$ kommutatív monoidban kell képezni. Ha A egységelemes és nemelfajult (vagyis $A \neq \{0_A\}$), akkor az

$$S \to A^{(S)}; \quad s \mapsto \mathrm{e}_s$$

leképezés injekció.

Bizonyítás. a) Ha $f, g \in A^{(S)}$, akkor nyilvánvalóan

$$[f + g \neq 0] \subseteq [f \neq 0] \cup [g \neq 0],$$

és itt a jobb oldalon véges halmaz áll (8.1.12.), így $[f + g \neq 0]$ véges halmaz (8.1.8.), vagyis $f + g \in A^{(S)}$.

Ha $f \in A^{(S)}$ és $a \in A$, akkor 14.1.4. a) szerint

$$[a.f \neq 0] \subseteq [f \neq 0],$$

és itt a jobb oldalon véges halmaz áll, így $[a.f \neq 0]$ véges halmaz (8.1.8.), vagyis $a.f \in A^{(S)}$.

Legyen $f, g \in A^{(S)}$ és $s \in [f * g \neq 0]$. Ekkor 12.5.1. alapján van olyan $(s', s'') \in S \times S$, hogy $s's'' = s$ és $f(s')g(s'') \neq 0$, így a 14.1.4. a) állításból következik, hogy $f(s') \neq 0_A$ és $g(s'') \neq 0_A$, vagyis $s = s's'' \in [f \neq 0] \cdot [g \neq 0]$. Ez azt jelenti, hogy

$$[f * g \neq 0] \subseteq [f \neq 0] \cdot [g \neq 0],$$

és itt a jobb oldalon véges halmaz áll, mert az

$$[f \neq 0] \times [g \neq 0] \to [f \neq 0] \cdot [g \neq 0]; \quad (s', s'') \mapsto s's''$$

leképezés szürjekció, és $[f \neq 0] \times [g \neq 0]$ véges halmaz (8.1.17.), így elegendő a 8.1.11. állításra hivatkozni. Tehát $[f * g \neq 0]$ véges halmaz (8.1.8.), vagyis $f * g \in A^{(S)}$.

Most három lépésben igazolni fogjuk, hogy az $A^{(S)}$ halmaz az 14.4.2. definícióban értelmezett $+$ összeadással és $*$ szorzással ellátva gyűrű.

(I) Megmutatjuk, hogy a 14.4.2. definícióban értelmezett $A^{(S)}$ feletti $+$ művelet kommutatív csoportművelet.

Legyenek $f, g, h \in A^{(S)}$ és $s \in [f * g \neq 0]$. Ekkor az $A^{(S)}$ feletti $+$ művelet definíciója és az A feletti összeadás asszociativitása szerint

$$\begin{aligned}((f + g) + h)(s) &= (f + g)(s) + h(s) = (f(s) + g(s)) + h(s) = \\ &= f(s) + (g(s) + h(s)) = f(s) + (g + h)(s) = (f + (g + h))(s),\end{aligned}$$

amiből következik, hogy $(f+g)+h = f+(g+h)$, tehát az $A^{(S)}$ feletti $+$ művelet asszociatív.

Legyenek $f, g \in A^{(S)}$ és $s \in [f*g \neq 0]$. Ekkor az $A^{(S)}$ feletti $+$ művelet definíciója és az A feletti összeadás kommutativitása szerint

$$(f+g)(s) = f(s)+g(s) = g(s)+f(s) = (g+f)(s),$$

amiből következik, hogy $f+g = g+f$, tehát az $A^{(S)}$ feletti $+$ művelet kommutatív.

Jelölje $\mathbf{0}$ a 0_A értékű $S \to A$ konstansfüggvényt. Világos, hogy $\mathbf{0} \in A^{(S)}$, mert $[\mathbf{0} \neq 0] = \emptyset$ véges halmaz, továbbá minden $f \in A^{(S)}$ és $s \in S$ esetén

$$(f+\mathbf{0})(s) = f(s)+\mathbf{0}(s) = f(s)+0_A = f(s),$$

hiszen 0_A az additív neutrális elem az A gyűrűben. Ebből következik, hogy minden $f \in A^{(S)}$ függvényre $f+\mathbf{0} = f$, és mivel az $A^{(S)}$ feletti $+$ művelet kommutatív, így $\mathbf{0}+f = f$ is teljesül, vagyis $\mathbf{0}$ neutrális elem az $A^{(S)}$ feletti $+$ műveletre nézve.

Legyen $f \in A^{(S)}$, és vezessük be a $-f : S \to A;\ s \mapsto -f(s)$ függvényt, ahol minden $s \in S$ esetén $-f(s)$ az $f(s) \in A$ elem inverze az A feletti összeadás szerint. Világos, hogy $[-f \neq 0] = [f \neq 0]$, ezért $-f \in A^{(S)}$, és minden $s \in S$ esetén

$$(f+(-f))(s) := f(s)+(-f)(s) = f(s)+(-f(s)) = 0_A = \mathbf{0}(s),$$

amiből következik, hogy $f+(-f) = \mathbf{0}$, és mivel az $A^{(S)}$ feletti $+$ művelet kommutatív, így $(-f)+f = \mathbf{0}$ is teljesül, vagyis $-f$ az f elem inverze $A^{(S)}$-ben az $A^{(S)}$ feletti $+$ műveletre nézve.

Ezzel igazoltuk, hogy az $(A^{(S)}, +)$ pár kommutatív csoport.

(II) Megmutatjuk, hogy az $A^{(S)} \times A^{(S)} \to A^{(S)};\ (f,g) \mapsto f*g$ művelet *asszociatív*. Ehhez legyenek $f, g, h \in A^{(S)}$ és $s \in S$ rögzítve. A definíció szerint

$$\begin{aligned}((f*g)*h)(s) &= \sum_{\substack{(t,s''')\in S\times S\\ ts'''=s}} (f*g)(t)h(s''') = \sum_{\substack{(t,s''')\in S\times S\\ ts'''=s}} \Big(\sum_{\substack{(s',s'')\in S\times S\\ s's''=t}} f(s')g(s'')\Big) h(s''') = \\ &= \sum_{\substack{(t,s''')\in S\times S\\ ts'''=s}} \Big(\sum_{\substack{(s',s'')\in S\times S\\ s's''=t}} (f(s')g(s''))h(s''')\Big), \qquad (1)\end{aligned}$$

ahol az utolsó egyenlőségnél felhasználtuk a gyűrű szorzásának összeadásra vonatkozó általános disztributivitását (14.2.4.). Megmutatjuk, hogy

$$\sum_{\substack{(s',s'',s''')\in S\times S\times S\\ (s's'')s'''=s}} f(s')g(s'')h(s''') = \sum_{\substack{(t,s''')\in S\times S\\ ts'''=s}} \Big(\sum_{\substack{(s',s'')\in S\times S\\ s's''=t}} (f(s')g(s''))h(s''')\Big), \qquad (1')$$

Ehhez legyenek

$$I := \{(s',s'',s''') \in S\times S\times S \mid (s's'')s''' = s\},$$
$$L := \{(t,s''') \in S\times S \mid ts''' = s\},$$

és minden $(t,s''') \in L$ párra vezessük be az

$$I_L(t,s''') := \{(s',s'',s''') \mid ((s',s'') \in S\times S) \wedge s's'' = t\} \subseteq I$$

halmazt. Az $(I_L(t,s'''))_{(t,s''')\in L}$ halmazrendszer nyilván diszjunkt, mert ha $(t,s'''), (\widetilde{t},\widetilde{s}''') \in L$ olyanok, hogy $(s',s'',r) \in I_L(t,s''') \cap I_L(\widetilde{t},\widetilde{s}''')$, akkor $r = s'''$ és $r = \widetilde{s}'''$, ezért $s''' = \widetilde{s}'''$, valamint $s's'' = t$ és $s's'' = \widetilde{t}$, ezért $t = \widetilde{t}$, tehát $(t,s''') = (\widetilde{t},\widetilde{s}''')$. Továbbá nyilvánvaló, hogy

$$I = \bigcup_{(t,s''')\in L} I_L(t,s'''),$$

ezért a monoidban értelmezett összeadás általános asszociativitása (12.5.10.) miatt

$$\sum_{\substack{(s',s'',s''')\in S\times S\times S\\ (s's'')s'''=s}} f(s')g(s'')h(s''') = \sum_{(s',s'',s''')\in I} f(s')g(s'')h(s''') =$$
$$= \sum_{(t,s''')\in L}\Bigg(\sum_{(s',s'',s''')\in I_L(t,s''')} f(s')g(s'')h(s''')\Bigg) \overset{(1)}{=} \sum_{\substack{(t,s''')\in S\times S\\ ts'''=s}}\Bigg(\sum_{\substack{(s',s'')\in S\times S\\ s's''=t}} (f(s')g(s''))h(s''')\Bigg),$$

ahol az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk a kommutatív monoidban értelmezett összeadás általános kommutativitását (12.5.9.), ugyanis minden $(t,s''') \in L$ esetén az

$$\{(s',s'') \in S\times S | s's'' = t\} \to I_L(t,s'''); \quad (s',s'') \mapsto (s',s'',s''')$$

leképezés bijekció. Ezzel az $(1')$ egyenlőséget igazoltuk.

Ugyanakkor, a definíció szerint

$$(f*(g*h))(s) = \sum_{\substack{(s',r)\in S\times S\\ s'r=s}} f(s')(g*h)(r) = \sum_{\substack{(s',r)\in S\times S\\ s'r=s}} f(s')\Bigg(\sum_{\substack{(s'',s''')\in S\times S\\ s''s'''=r}} g(s'')h(s''')\Bigg) =$$
$$= \sum_{\substack{(s',r)\in S\times S\\ s'r=s}}\Bigg(\sum_{\substack{(s'',s''')\in S\times S\\ s''s'''=r}} f(s')(g(s'')h(s'''))\Bigg), \tag{2}$$

ahol az utolsó egyenlőségnél felhasználtuk a gyűrű szorzásának összeadásra vonatkozó általános disztributivitását (14.2.4.). Megmutatjuk, hogy

$$\sum_{\substack{(s',s'',s''')\in S\times S\times S\\ s'(s''s''')=s}} f(s')g(s'')h(s''') = \sum_{\substack{(s',r)\in S\times S\\ s'r=s}}\Bigg(\sum_{\substack{(s'',s''')\in S\times S\\ s''s'''=r}} f(s')(g(s'')h(s'''))\Bigg). \tag{2'}$$

Ehhez legyenek

$$\check{I} := \{(s',s'',s''') \in S\times S\times S | s'(s''s''') = s\},$$
$$R := \{(s',r) \in S\times S | s'r = s\},$$

és minden $(s',r) \in R$ párra vezessük be az

$$I_R(s',r) := \{(s',s'',s''') | ((s'',s''') \in S\times S) \wedge s''s''' = r\} \subseteq \check{I}$$

halmazt. Az $(I_R(s',r))_{(s',r)\in R}$ halmazrendszer nyilván diszjunkt, mert ha $(s',r), (\widetilde{s}',\widetilde{r}) \in L$ olyanok, hogy $(t,s'',s''') \in I_R(s',r) \cap I_R(\widetilde{s}',\widetilde{r})$, akkor $t = s'$ és $t = \widetilde{s}'$, ezért $s' = \widetilde{s}'$, valamint $s''s''' = r$ és $s''s''' = \widetilde{r}$, ezért $r = \widetilde{r}$, tehát $(s',r) = (\widetilde{s}',\widetilde{r})$. Továbbá nyilvánvaló, hogy

$$\check{I} = \bigcup_{(s',r)\in R} I_R(s',r),$$

ezért a monoidban értelmezett összeadás általános asszociativitása (12.5.10.) miatt

$$\sum_{\substack{(s',s'',s''')\in S\times S\times S\\ s'(s''s''')=s}} f(s')g(s'')h(s''') = \sum_{(s',s'',s''')\in \check{I}} f(s')g(s'')h(s''') =$$

$$= \sum_{(s',r)\in R}\Big(\sum_{(s',s'',s''')\in I_R(s',r)} f(s')g(s'')h(s''')\Big) \overset{(2)}{=} \sum_{\substack{(s',r)\in S\times S\\ s'r=s}}\Big(\sum_{\substack{(s'',s''')\in S\times S\\ s''s'''=r}} f(s')(g(s'')h(s'''))\Big),$$

ahol a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk a kommutatív monoidban értelmezett összeadás általános kommutativitását (12.5.9.), ugyanis minden $(s',r)\in R$ esetén az

$$\{(s'',s''')\in S\times S | s''s'''=r\}\to I_R(s',r);\quad (s'',s''')\mapsto (s',s'',s''')$$

leképezés bijekció. Ezzel a $(2')$ egyenlőséget igazoltuk.

Az S halmazon adott művelet asszociativitása miatt az $(1')$ és $(2')$ egyenlőségek bal oldalán ugyanaz az elem áll, így az (1) és (2) egyenlőségekből következik, hogy $((f*g)*h)(s) = (f*(g*h))(s)$. Ezért az $A^{(S)}\times A^{(S)}\to A^{(S)}$; $(f,g)\mapsto f*g$ művelet asszociatív.

(III) Megmutatjuk, hogy az $A^{(S)}\times A^{(S)}\to A^{(S)}$; $(f,g)\mapsto f*g$ művelet disztributív az $A^{(S)}\times A^{(S)}\to A^{(S)}$; $(f,g)\mapsto f+g$ műveletre nézve.

Legyen $f,g,h\in A^{(S)}$ és $s\in S$ rögzítve. A definíció szerint

$$(f*(g+h))(s) = \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} f(s')(g+h)(s'') \overset{(3)}{=} \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} (f(s')g(s'')+f(s')h(s'')) \overset{(4)}{=}$$

$$\overset{(4)}{=} \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} f(s')g(s'') + \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} f(s')h(s'')=(f*g)(s)+(f*h)(s)=((f*g)+(f*h))(s),$$

ahol

– a $\overset{(3)}{=}$ egyenlőségnél alkalmaztuk $A^{(S)}$ feletti összeadás definícióját és felhasználtuk azt, hogy A szorzása balról disztributív A összeadására nézve;

– a $\overset{(4)}{=}$ egyenlőségnél a 12.5.8. állítást alkalmaztuk.

Ebből következik, hogy minden $f,g,h\in A^{(S)}$ esetén $f*(g+h)=(f*g)+(f*h)$, tehát az $A^{(S)}$ feletti $*$ művelet *balról disztributív* az $A^{(S)}$ feletti $+$ műveletre nézve.

Legyen $f,g,h\in A^{(S)}$ és $s\in S$ rögzítve. A definíció szerint

$$((g+h)*f)(s) = \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} (g+h)(s')f(s'') \overset{(5)}{=} \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} (g(s')f(s'')+h(s')f(s'')) \overset{(6)}{=}$$

$$\overset{(6)}{=} \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} g(s')f(s'') + \sum_{\substack{(s',s'')\in S\times S\\ s's''=s}} h(s')f(s'')=(g*f)(s)+(h*f)(s)=((g*f)+(h*f))(s),$$

ahol

– az $\overset{(5)}{=}$ egyenlőségnél alkalmaztuk $A^{(S)}$ feletti összeadás definícióját és felhasználtuk azt, hogy A szorzása jobbról disztributív A összeadására nézve;

– a $\overset{(6)}{=}$ egyenlőségnél a 12.5.8. állítást alkalmaztuk.

Ebből következik, hogy minden $f, g, h \in A^{(S)}$ esetén $(g+h)*f = (g*f)+(h*f)$, tehát az $A^{(S)}$ feletti $*$ művelet *jobbról disztributív* az $A^{(S)}$ feletti $+$ műveletre nézve.

Tehát az $A^{(S)}$ halmaz az 14.4.2. definícióban értelmezett $+$ összeadással és $*$ szorzással ellátva gyűrű.

b) Legyen $f, g \in A^{(S)}$ és $a, b \in A$. Ekkor minden $s \in S$ esetén

$$(a.(b.f))(s) = a(b.f)(s) = a(bf(s)) = (ab)f(s) = ((ab).f)(s),$$

ahol kihasználtuk A szorzásának asszociativitását, ezért $a.(b.f) = (ab).f$; továbbá

$$((a+b).f)(s) = (a+b)f(s) = af(s) + bf(s) = (a.f)(s) + (b.f)(s) = (a.f + b.f)(s),$$

ahol kihasználtuk, hogy A szorzása jobbról disztributív az összeadásra nézve, ezért $(a+b).f = a.f + b.f$; továbbá

$$(a.(f+g))(s) = a(f+g)(s) = a(f(s)+g(s)) = af(s) + ag(s) = (a.f + a.g)(s),$$

ahol kihasználtuk, hogy A szorzása balról disztributív az összeadásra nézve, ezért $a.(f+g) = a.f + a.g$; továbbá

$$(a.(f*g))(s) = a(f*g)(s) = a \sum_{\substack{(s',s'')\in S\times S \\ s's''=s}} f(s')g(s'') = \sum_{\substack{(s',s'')\in S\times S \\ s's''=s}} a(f(s')g(s'')) =$$
$$= \sum_{\substack{(s',s'')\in S\times S \\ s's''=s}} (af(s'))g(s'') = \sum_{\substack{(s',s'')\in S\times S \\ s's''=s}} (a.f) = f(s')g(s'') = ((a.f)*g)(s),$$

ahol felhasználtuk azt, hogy A szorzása balról disztributív az összeadásra nézve, és hogy A szorzása asszociatív, ezért $a.(f*g) = (a.f)*g$.

c) Legyenek $s, t \in S$ rögzítve, és minden $r \in S$ esetén $\mathrm{I}_r := \{(r', r'') \in S \times S | r'r'' = r\}$. Világos, hogy $(r', r'') \in S \times S$ és $(r', r'') \neq (s, t)$ esetén $\mathrm{e}_s(r') = 0$ vagy $\mathrm{e}_t(r'') = 0$, így 14.1.4. a) alapján $\mathrm{e}_s(r')\mathrm{e}_t(r'') = 0$. Ha $r \in S$ olyan, hogy $st \neq r$, akkor minden $(r', r'') \in \mathrm{I}_r$ esetén $(r', r'') \neq (s, t)$, tehát $\mathrm{e}_s(r')\mathrm{e}_t(r'') = 0$, amiből következik, hogy

$$(\mathrm{e}_s * \mathrm{e}_t)(r) = \sum_{(r',r'')\in \mathrm{I}_r} \mathrm{e}_s(r')\mathrm{e}_t(r'') = 0.$$

Ugyanakkor 12.5.5. alkalmazásával kapjuk, hogy

$$(\mathrm{e}_s * \mathrm{e}_t)(st) = \sum_{(r',r'')\in \mathrm{I}_{st}} \mathrm{e}_s(r')\mathrm{e}_t(r'') = \mathrm{e}_s(s)\mathrm{e}_t(t) + \sum_{(r',r'')\in \mathrm{I}_{st}\setminus\{(s,t)\}} \mathrm{e}_s(r')\mathrm{e}_t(r'') = 1\cdot 1 + 0 = 1,$$

ami a definíció szerint azt jelenti, hogy $\mathrm{e}_s * \mathrm{e}_t = \mathrm{e}_{st}$.

Ha $f \in A^{(S)}$, akkor 11.4.6. szerint minden $t \in S$ esetén

$$\Big(\sum_{s\in S} f(s).\mathrm{e}_s\Big)(t) = \sum_{s\in S} (f(s).\mathrm{e}_s)(t) = \sum_{s\in S} f(s)\mathrm{e}_s(t) =$$
$$= \sum_{s\in S\setminus\{t\}} f(s)\mathrm{e}_s(t) + f(t)\mathrm{e}_t(t) = 0_A + f(t)1_A = f(t),$$

ahol felhasználtuk a 12.5.5. állítást.

Végül, ha $s, t \in S$ és $\mathrm{e}_s = \mathrm{e}_t$, akkor $1_A = \mathrm{e}_s(s) = \mathrm{e}_t(s)$, tehát ha $1_A \neq 0_A$, akkor ebből

$s = t$ következik, vagyis az $S \to A^{(S)}$; $s \mapsto \mathrm{e}_s$ leképezés injektív. ■

Vigyázzunk arra, hogy ha az A gyűrű nem kommutatív, és S félcsoport, akkor $f, g \in A^{(S)}$ és $a \in A$ esetén lehetséges az, hogy

$$a.(f * g) \neq f * (a.g).$$

14.4.6. Definíció. *Ha S félcsoport és A gyűrű, akkor az előző tételben bevezetett gyűrűt az (S, A) pár által meghatározott* **félcsoportgyűrűnek** *nevezzük, és ennek alaphalmazát változatlanul az $A^{(S)}$ szimbólummal jelöljük.*

14.4.7. Állítás. *Legyen S (multiplikatívan jelölt) félcsoport és A gyűrű.*

a) *Ha S és A kommutatív, akkor az (S, A) pár által meghatározott félcsoportgyűrű kommutatív, és minden $f, g \in A^{(S)}$ és $a \in A$ esetén*

$$a.(f * g) = (a.f) * g = f * (a.g).$$

b) *Ha az A gyűrű egységelemes és nemelfajult, és az (S, A) pár által meghatározott félcsoportgyűrű kommutatív, akkor S kommutatív, és ha még $S \neq \emptyset$ is teljesül, akkor A is kommutatív.*

Bizonyítás. a) Legyen $f, g \in A^{(S)}$ és $s \in S$. Vezessük be az

$$I := \{(s', s'') \in S \times S | s's'' = s\}, \quad \check{I} = \{(s', s'') \in S \times S | s''s' = s\}$$

halmazokat. Világos, hogy az $I \to \check{I}$; $(s', s'') \mapsto (s'', s')$ leképezés bijekció, ezért a véges összegek általános kommutativitása miatt

$$(f * g)(s) = \sum_{(s', s'') \in I} f(s')g(s'') = \sum_{(s', s'') \in \check{I}} f(s'')g(s'),$$

tehát ha S és A kommutatív, akkor $I = \check{I}$ és minden $(s', s'') \in \check{I}$ esetén $f(s'')g(s') = g(s')f(s'')$, következésképpen $(f * g)(s) = (g * f)(s)$, így $f * g = g * f$.

Ebből az előző tétel b) pontjának alkalmazásával következik, hogy ha $f, g \in A^{(S)}$ és $a \in A$, akkor

$$(a.f) * g = a.(f * g) = a.(g * f) = (a.g) * f = f * (a.g).$$

b) Tegyük fel, hogy az A gyűrű egységelemes és nemelfajult, valamint az (S, A) pár által meghatározott félcsoportgyűrű kommutatív. Ekkor minden $s, t \in S$ esetén az előző tétel c) része szerint $\mathrm{e}_{ts} = \mathrm{e}_t * \mathrm{e}_s = \mathrm{e}_s * \mathrm{e}_t = \mathrm{e}_{st}$, ezért $ts = st$, hiszen az $S \to A^{(S)}$; $r \mapsto \mathrm{e}_r$ leképezés injektív. Tehát ekkor az S félcsoport kommutatív.

Tegyük fel, hogy $S \neq \emptyset$ is teljesül, és legyen $s \in S$ rögzítve. Ha $a, b \in A$, akkor a $*$ művelet kommutativitása és az előző tétel b) része alapján

$$\begin{aligned}(ab).\mathrm{e}_{s^2} &= (ab).(\mathrm{e}_s * \mathrm{e}_s) = a(b.(\mathrm{e}_s * \mathrm{e}_s)) = a.((b.\mathrm{e}_s) * \mathrm{e}_s) = a.(\mathrm{e}_s * (b.\mathrm{e}_s)) = \\ &= (a.\mathrm{e}_s) * (b.\mathrm{e}_s) = (b.\mathrm{e}_s) * (a.\mathrm{e}_s) = b.(\mathrm{e}_s * (a.\mathrm{e}_s)) = b.((a.\mathrm{e}_s) * \mathrm{e}_s) = b(a.(\mathrm{e}_s * \mathrm{e}_s)) = \\ &= (ba).(\mathrm{e}_s * \mathrm{e}_s) = (ba).\mathrm{e}_{s^2},\end{aligned}$$

amiből következik, hogy

$$ab = (ab)1_A = (ab)\mathrm{e}_{s^2}(s^2) = ((ab).\mathrm{e}_{s^2})(s^2) = ((ba).\mathrm{e}_{s^2})(s^2) = (ba).\mathrm{e}_{s^2}(s^2) = (ba)1_A = ba,$$

tehát az A gyűrű kommutatív. ∎

Nyilvánvaló, hogy ha S félcsoport és A gyűrű, valamint az (S, A) pár által meghatározott félcsoportgyűrű kommutatív, akkor

– $S = \emptyset$ esetén $A^{(S)} = \{0\}$, így az (S, A) pár által meghatározott félcsoportgyűrű kommutatív, függetlenül attól, hogy A kommutatív-e vagy sem.

– $A = \{0\}$ esetén $A^{(S)} = \{0\}$, így az (S, A) pár által meghatározott félcsoportgyűrű kommutatív, függetlenül attól, hogy S kommutatív-e vagy sem.

14.4.8. Állítás. *Legyen S monoid és jelölje $e \in S$ a neutrális elemet S-ben. Ha A egységelemes, akkor e_e jobboldali egységelem az (S, A) pár által meghatározott félcsoportgyűrűben, és ha még A kommutatív is, akkor e_e egységeleme az (S, A) pár által meghatározott félcsoportgyűrűnek.*

Bizonyítás. Ha $f \in A^{(S)}$, akkor 14.4.5. b) és c) szerint minden $s \in S$ esetén $(f(s).\mathrm{e}_s) * \mathrm{e}_e = f(s).\mathrm{e}_s$, tehát gyűrű szorzásának összeadásra vonatkozó általános disztributivitása folytán

$$f * \mathrm{e}_e = \Big(\sum_{s \in S} f(s).\mathrm{e}_s\Big) * \mathrm{e} = \sum_{s \in S} ((f(s).\mathrm{e}_s) * \mathrm{e}_e) = \sum_{s \in S} f(s).\mathrm{e}_e = f,$$

és ha A kommutatív, akkor 14.4.5. b) és c) szerint minden $s \in S$ esetén $\mathrm{e}_e * (f(s).\mathrm{e}_s) = f(s).\mathrm{e}_s$, tehát gyűrű szorzásának összeadásra vonatkozó általános disztributivitása folytán

$$\mathrm{e}_e * f = \mathrm{e}_e * \Big(\sum_{s \in S} f(s).\mathrm{e}_s\Big) = \sum_{s \in S} (\mathrm{e}_e * (f(s).\mathrm{e}_s)) = \sum_{s \in S} f(s).\mathrm{e}_e = f,$$

amit bizonyítani kellett. ∎

14.5. Részgyűrűk, ideálok és faktorgyűrűk

14.5.1. Definíció. *Ha A gyűrű, akkor az $S \subseteq A$ nem üres halmazt* **részgyűrűnek** *nevezzük, ha $S + S \subseteq S$, $-S \subseteq S$, és $S \cdot S \subseteq S$.*

Tehát gyűrű részgyűrűje olyan részcsoportja a gyűrű additív csoportjának, amely *multiplikatív*, vagyis zárt a gyűrű szorzására nézve.

Vigyázzunk arra, hogy gyűrű nem üres részhalmazának *additivitása*, vagyis a gyűrű összeadására vonatkozó zártsága és a multiplikativitása általában nem elegendő ahhoz, hogy a halmaz részgyűrű legyen. Például, $\mathbb{N}$ olyan részhalmaza $\mathbb{Z}$-nek, hogy $\mathbb{N} + \mathbb{N} \subseteq \mathbb{N}$ és $\mathbb{N} \cdot \mathbb{N} \subseteq \mathbb{N}$, de $-\mathbb{N} \subseteq \mathbb{N}$ nem teljesül, tehát $\mathbb{N}$ nem részgyűrűje az egész számok gyűrűjének.

14.5.2. Definíció. *Az A gyűrűben* **baloldali ideálnak** (*illetve* **jobboldali ideálnak**) *nevezünk minden olyan $\mathfrak{m} \subseteq A$ nem üres halmazt, amelyre $\mathfrak{m} + \mathfrak{m} \subseteq \mathfrak{m}$ és $A \cdot \mathfrak{m} \subseteq \mathfrak{m}$ (illetve $\mathfrak{m} \cdot A \subseteq \mathfrak{m}$). Az A gyűrűben* **ideálnak** *vagy* **kétoldali ideálnak** *nevezünk minden olyan $\mathfrak{m} \subseteq A$ halmazt, amely egyszerre baloldali és jobboldali ideál A-ban.*

Nyilvánvaló, hogy gyűrűben minden ideál részgyűrű, de ennek megfordítása általában nem igaz.

14.5.3. Állítás. *Legyen $(S_i)_{i\in I}$ az A gyűrű részgyűrűinek (illetve ideáljainak) nem üres rendszere.*

a) *A* $\bigcap_{i\in I} S_i$ *halmaz részgyűrű (illetve ideál) A-ban.*

b) *Ha teljesül az, hogy minden $i, j \in I$ esetén van olyan $k \in I$, amelyre $S_i \cup S_j \subseteq S_k$ (vagyis az $(S_i)_{i\in I}$ halmazrendszer tartalmazás tekintetében felfelé irányított), akkor a* $\bigcup_{i\in I} S_i$ *halmaz részgyűrű (illetve ideál) A-ban.*

c) *Tegyük fel, hogy A kommutatív. Ekkor a* $\mathrm{P}_{i\in I} S_i :=$

Bizonyítás. a) Legyen $S := \bigcap_{i\in I} S_i$. Ekkor minden $i \in I$ esetén $0 \in S_i$, tehát $S \neq \emptyset$, továbbá $S + S \subseteq S_i + S_i \subseteq S_i$, és $-S \subseteq -S_i \subseteq S_i$, valamint $S \cdot S \subseteq S_i \cdot S_i \subseteq S_i$, tehát $S + S \subseteq S$, és $-S \subseteq S$, valamint $S \cdot S \subseteq S$, ezért S részgyűrű A-ban.

Legyen $S := \sum_{i\in I} S_i$. Mivel $I \neq \emptyset$, így $0 \in S$, vagyis $S \neq \emptyset$. Legyenek $(s_i)_{i\in I} \in \prod_{i\in I} S_i$ $(s'_i)_{i\in I} \in \prod_{i\in I} S_i$ olyan rendszerek, hogy $\{i \in I | s_i \neq 0\}$ és $\{i \in I | s'_i \neq 0\}$ véges részhalmazai I-nek.

■

14.5.4. Állítás. *Legyen A gyűrű és $\mathfrak{m}$ ideál A-ban. Ekkor az*

$$\approx_{\mathfrak{m}} := \{ (a, b) \in A \times A \mid b - a \in \mathfrak{m}\}$$

reláció ekvivalencia az A halmaz felett, és ha $A/\mathfrak{m}$ jelöli az $A/\approx_{\mathfrak{m}}$ faktorhalmazt és $\pi_{A/\mathfrak{m}}$ az $A \to A/\mathfrak{m}$ kanonikus szürjekciót, akkor egyértelműen léteznek A felett olyan $+$ és $\cdot$ műveletek, hogy minden $a, b \in A$ esetén

$$\pi_{A/\mathfrak{m}}(a + b) = \pi_{A/\mathfrak{m}}(a) + \pi_{A/\mathfrak{m}}(b),$$
$$\pi_{A/\mathfrak{m}}(ab) = \pi_{A/\mathfrak{m}}(a) \cdot \pi_{A/\mathfrak{m}}(b).$$

Továbbá, ekkor az $(A/\mathfrak{m}, +, \cdot)$ hármas gyűrű.

Bizonyítás. Ha $a \in A$, akkor $a - a = 0 \in \mathfrak{m}$, ezért a $\approx_{\mathfrak{m}}$ reláció reflexív az A halmazon. Ha $a, b \in A$, akkor $a \approx_{\mathfrak{m}} b$ esetén $b - a \in \mathfrak{m}$, ezért $a - b = -(b - a) \in -\mathfrak{m} \subseteq \mathfrak{m}$, tehát $b \approx_{\mathfrak{m}} a$, vagyis az $\approx_{\mathfrak{m}}$ reláció szimmetrikus. Ha $a, b, c \in A$, akkor $a \approx_{\mathfrak{m}} b$ esetén $b \approx_{\mathfrak{m}} c$ esetén $b - a \in \mathfrak{m}$ és $c - b \in \mathfrak{m}$, tehát $c - a = (c - b) + (b - a) \in \mathfrak{m} + \mathfrak{m} \subseteq \mathfrak{m}$, vagyis $a \approx_{\mathfrak{m}} c$, ami azt jelenti, hogy az $\approx_{\mathfrak{m}}$ reláció tranzitív.

Legyenek $a, a', b, b' \in A$ olyanok, hogy $a \approx_{\mathfrak{m}} a'$ és $b \approx_{\mathfrak{m}} b'$, vagyis $a - a' \in \mathfrak{m}$ és $b - b' \in \mathfrak{m}$. Ekkor

$$(a + b) - (a' + b') = (a - a') + (b - b') \in \mathfrak{m} + \mathfrak{m} \subseteq \mathfrak{m},$$

tehát $a + b \approx_{\mathfrak{m}} a' + b'$, továbbá

$$ab - a'b' = (a - a')b + a'(b - b') \in \mathfrak{m}A + A\mathfrak{m} \subseteq \mathfrak{m} + \mathfrak{m} \subseteq \mathfrak{m},$$

tehát $ab \approx_{\mathfrak{m}} a'b'$. Ezért egyértelműen léteznek olyan $+$ és $\cdot$ műveletek $A/\mathfrak{m}$ felett, amelyekre teljesül az, hogy minden $a, b \in A$ esetén $\pi_{A/\mathfrak{m}}(a) + \pi_{A/\mathfrak{m}}(b) = \pi_{A/\mathfrak{m}}(a + b)$ és $\pi_{A/\mathfrak{m}}(a) \cdot \pi_{A/\mathfrak{m}}(b) = \pi_{A/\mathfrak{m}}(ab)$. ■

14.5.5. Definíció. *Ha A gyűrű és $\mathfrak{m}$ ideál A-ban, akkor az $A/\mathfrak{m}$ faktorhalmazt az előző állításban bevezetett $+$ és $\cdot$ műveletekkel ellátva az A gyűrű $\mathfrak{m}$ ideál szerinti* **faktorgyűrűjének** *nevezzük.*

14.5.6. Definíció. *Az A gyűrűben* **prímideálnak** *nevezünk minden olyan $\mathfrak{p}$ ideált, amelyre $\mathfrak{p} \neq A$ és teljesül az, hogy minden $a, b \in A$ esetén, ha $a \notin \mathfrak{p}$ és $b \notin \mathfrak{p}$, akkor $ab \notin \mathfrak{p}$. Az A gyűrű prímideáljainak halmazát* $\operatorname{Spec}(A)$ *jelöli, és ezt a halmazt az A gyűrű* **egyszerű spektrumának** *nevezzük.*

14.5.7. Állítás. *Az A gyűrű $\mathfrak{p}$ ideálja pontosan akkor prímideál, ha az $A/\mathfrak{p}$ faktorgyűrű nemelfajult és zérusosztómentes.*

Bizonyítás. Legyen $\mathfrak{p}$ prímideál A-ban. Ekkor $\mathfrak{p} \neq A$ miatt $A/\mathfrak{p} \neq \{0\}$, vagyis az $A/\mathfrak{p}$ faktorgyűrű nemelfajult. Ha $a, b \in A$ olyanok, hogy $\pi_{A/\mathfrak{m}}(a) \neq 0$ és $\pi_{A/\mathfrak{m}}(b) \neq 0$, akkor $a \notin \mathfrak{p}$ és $b \notin \mathfrak{p}$, tehát $ab \notin \mathfrak{p}$, hiszen $\mathfrak{p}$ prímideál, következésképpen $\pi_{A/\mathfrak{m}}(a) \cdot \pi_{A/\mathfrak{m}}(b) = \pi_{A/\mathfrak{m}}(ab) \neq 0$, ami azt jelenti, hogy $A/\mathfrak{p}$ zérusosztómentes gyűrű.

Megfordítva, tegyük fel, hogy az $A/\mathfrak{p}$ faktorgyűrű nemelfajult és zérusosztómentes. A nemelfajultság miatt $\mathfrak{p} \neq A$. Ha $a, b \in A \setminus \mathfrak{p}$, akkor $\pi_{A/\mathfrak{m}}(a) \neq 0$ és $\pi_{A/\mathfrak{m}}(b) \neq 0$, tehát $A/\mathfrak{p}$ zérusosztómentessége miatt $\pi_{A/\mathfrak{m}}(ab) = \pi_{A/\mathfrak{m}}(a) \cdot \pi_{A/\mathfrak{m}}(b) \neq 0$, így $ab \in A \setminus \mathfrak{p}$, ami azt jelenti, hogy az $A \setminus \mathfrak{p}$ halmaz multiplikatív, vagyis $\mathfrak{p}$ prímideál. ■

14.5.8. Állítás. *Ha az A gyűrű kommutatív, akkor minden $\mathfrak{m} \subseteq A$ ideálra az $A/\mathfrak{m}$ faktorgyűrű kommutatív. Ha az A gyűrű egységelemes, akkor minden $\mathfrak{m} \subseteq A$ ideálra az $A/\mathfrak{m}$ faktorgyűrű egységelemes és a $\pi_{A/\mathfrak{m}} : A \to A/\mathfrak{m}$ kanonikus leképezés egységelem-tartó gyűrű-morfizmus.*

Bizonyítás. Az első állítás $\pi_{A/\mathfrak{m}}$ multiplikativitásából és szürjektivitásából következik. Ha A egységelemes gyűrű, akkor minden $a \in A$ esetén $\pi_{A/\mathfrak{m}}(1)\pi_{A/\mathfrak{m}}(a) = \pi_{A/\mathfrak{m}}(1a) = \pi_{A/\mathfrak{m}}(a)$ és $\pi_{A/\mathfrak{m}}(a)\pi_{A/\mathfrak{m}}(1) = \pi_{A/\mathfrak{m}}(a1) = \pi_{A/\mathfrak{m}}(a)$, így $\pi_{A/\mathfrak{m}}$ szürjektivitása miatt $\pi_{A/\mathfrak{m}}(1)$ egységeleme az $A/\mathfrak{m}$ faktorgyűrűnek. ■

14.5.9. Állítás. *Legyenek A és B gyűrűk, valamint $\pi : A \to B$ gyűrű-morfizmus.*

a) *Ha S részgyűrű A-ban és T részgyűrű B-ben, akkor $\pi\langle S\rangle$ részgyűrű B-ben és $\overset{-1}{\pi}\langle T\rangle$ részgyűrű A-ban. Az* $\operatorname{Im}(\pi)$ *halmaz részgyűrű B-ben és a* $\operatorname{Ker}(\pi)$ *halmaz részgyűrű A-ban.*

b) *Ha $\mathfrak{m}$ ideál A-ban és $\mathfrak{n}$ ideál B-ben, akkor $\pi\langle\mathfrak{m}\rangle$ ideál az* $\operatorname{Im}(\pi)$ *gyűrűben és $\overset{-1}{\pi}\langle\mathfrak{n}\rangle$ ideál A-ban. A* $\operatorname{Ker}(\pi)$ *halmaz ideál A-ban. Ha π szürjektív és $\mathfrak{m}$ ideál A-ban, akkor $\pi\langle\mathfrak{m}\rangle$ ideál B-ben.*

Bizonyítás. a) Ha S részgyűrű A-ban, akkor $S \neq \emptyset$ miatt $\pi\langle S\rangle \neq \emptyset$, továbbá π additivitása és $S + S \subseteq S$ miatt $\pi\langle S\rangle + \pi\langle S\rangle \subseteq \pi\langle S + S\rangle \subseteq \pi\langle S\rangle$, valamint π additív inverzelem-tartása és $-S \subseteq S$ miatt $-\pi\langle S\rangle = \pi\langle -S\rangle \subseteq \pi\langle S\rangle$, valamint π multiplikativitása és $SS \subseteq S$ miatt $\pi\langle S\rangle\pi\langle S\rangle \subseteq \pi\langle SS\rangle \subseteq \pi\langle S\rangle$, ezért $\pi\langle S\rangle$ részgyűrű B-ben. Speciálisan, $\operatorname{Im}(\pi)$ is részgyűrű B-ben, mert A részgyűrű A-ban és $\operatorname{Im}(\pi) = \pi\langle A\rangle$.

Legyen T részgyűrű B-ben. Ekkor $0 \in T$, ezért $\pi(0) = 0$ miatt $0 \in \overset{-1}{\pi}\langle T\rangle$, tehát $\overset{-1}{\pi}\langle T\rangle \neq \emptyset$. Továbbá, ha $a, a' \in \overset{-1}{\pi}\langle T\rangle$, akkor π additivitása és $T + T \subseteq T$ miatt $\pi(a + a') = \pi(a) + \pi(a') \in T + T \subseteq T$, vagyis $a + a' \in \overset{-1}{\pi}\langle T\rangle$, ami azt jelenti, hogy $\overset{-1}{\pi}\langle T\rangle + \overset{-1}{\pi}\langle T\rangle \subseteq \overset{-1}{\pi}\langle T\rangle$. Ha $a \in \overset{-1}{\pi}\langle T\rangle$, akkor π additív inverzelem-tartása és $-T \subseteq T$ miatt $\pi(-a) = -\pi(a) \in -T \subseteq T$, tehát $-a \in \overset{-1}{\pi}\langle T\rangle$, ami azt jelenti, hogy $-\overset{-1}{\pi}\langle T\rangle \subseteq \overset{-1}{\pi}\langle T\rangle$. Ha $a, a' \in \overset{-1}{\pi}\langle T\rangle$, akkor π multiplikativitása és $TT \subseteq T$ miatt $\pi(aa') = \pi(a)\pi(a') \in TT \subseteq T$, vagyis $aa' \in \overset{-1}{\pi}\langle T\rangle$, ami azt jelenti, hogy $\overset{-1}{\pi}\langle T\rangle\overset{-1}{\pi}\langle T\rangle \subseteq \overset{-1}{\pi}\langle T\rangle$. Tehát $\overset{-1}{\pi}\langle T\rangle$ részgyűrű A-ban. Speciálisan, $\mathrm{Ker}(\pi)$ részgyűrű A-ban, mert $\{0\}$ részgyűrű B-ben és $\mathrm{Ker}(\pi) = \overset{-1}{\pi}\langle\{0\}\rangle$.

Legyen $\mathfrak{m}$ ideál A-ban. Ekkor $\mathfrak{m}$ részgyűrű A-ban, így a) alapján $\pi\langle\mathfrak{m}\rangle$ részgyűrű B-ben. Ha $b \in \mathrm{Im}(\pi)$, akkor van olyan $a \in A$, hogy $b = \pi(a)$, tehát minden $a' \in \mathfrak{m}$ esetén π multiplikativitása és $\mathfrak{m}A \subseteq \mathfrak{m}$ és $A\mathfrak{m} \subseteq \mathfrak{m}$ miatt $\pi(a')b = \pi(a')\pi(a) = \pi(a'a) \in \pi\langle\mathfrak{m}A\rangle \subseteq \pi\langle\mathfrak{m}\rangle$, valamint $b\pi(a') = \pi(a)\pi(a') = \pi(aa') \in \pi\langle A\mathfrak{m}\rangle \subseteq \pi\langle\mathfrak{m}\rangle$. Ez azt jelenti, hogy $\pi\langle\mathfrak{m}\rangle$ ideál az $\mathrm{Im}(\pi)$ gyűrűben. Ezért szürjektív π esetén $\pi\langle\mathfrak{m}\rangle$ ideál B-ben.

Legyen $\mathfrak{n}$ ideál B-ben. Ekkor $\mathfrak{n}$ részgyűrű B-ben, tehát a) alapján $\overset{-1}{\pi}\langle\mathfrak{n}\rangle$ részgyűrű A-ban. Legyen $a \in \overset{-1}{\pi}\langle\mathfrak{n}\rangle$ és $a' \in A$ tetszőleges. Ekkor π multiplikativitása és $\mathfrak{n}B \subseteq B$ valamint $B\mathfrak{n} \subseteq B$ miatt $\pi(a'a) = \pi(a')\pi(a) \in B\mathfrak{n} \subseteq B$ és $\pi(aa') = \pi(a)\pi(a') \in \mathfrak{n}B \subseteq \mathfrak{n}$, vagyis $a'a \in \overset{-1}{\pi}\langle\mathfrak{n}\rangle$ és $aa' \in \overset{-1}{\pi}\langle\mathfrak{n}\rangle$, ami azt jelenti, hogy $\overset{-1}{\pi}\langle\mathfrak{n}\rangle$ ideál A-ban. Speciálisan, $\{0\}$ ideál B-ben, ezért $\mathrm{Ker}(\pi)$ ideál A-ben, hiszen $\mathrm{Ker}(\pi) = \overset{-1}{\pi}\langle\{0\}\rangle$. ■

Vigyázzunk arra, hogy ha A és B gyűrűk, valamint $\pi : A \to B$ gyűrű-morfizmus, és $\mathfrak{m}$ ideál A-ban, akkor $\pi\langle\mathfrak{m}\rangle$ ideál az $\mathrm{Im}(\pi)$ gyűrűben, de nem feltétlenül ideál B-ben, bár részgyűrűje B-nek.

14.5.10. Következmény. *Legyen A gyűrű és $\mathfrak{m}$ ideál A-ban. Ekkor minden $\mathfrak{n}' \subseteq A/\mathfrak{m}$ ideálhoz van olyan $\mathfrak{n} \subseteq A$ ideál, amelyre $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = \mathfrak{n}'$.*

Bizonyítás. Ha $\mathfrak{n}'$ ideál $A/\mathfrak{m}$-ben, akkor π szürjektivitása miatt $\mathfrak{n}' = \pi_{A/\mathfrak{m}}\langle\overset{-1}{\pi}_{A/\mathfrak{m}}\langle\mathfrak{n}'\rangle\rangle$, ezért az előző állítás b) része alapján $\mathfrak{n} := \overset{-1}{\pi}_{A/\mathfrak{m}}\langle\mathfrak{n}'\rangle$ olyan ideál A-ban, amelyre $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = \mathfrak{n}'$. ■

14.5.11. Definíció. *Az A gyűrű $\mathfrak{m}$ ideálját* **maximális ideálnak** *nevezzük, ha $\mathfrak{m} \neq A$ és minden $\mathfrak{n} \subseteq A$ ideálra, ha $\mathfrak{n} \neq A$ és $\mathfrak{m} \subseteq \mathfrak{n}$, akkor $\mathfrak{m} = \mathfrak{n}$.*

Tehát az $\mathfrak{m}$ halmaz pontosan akkor maximális ideálja az A gyűrűnek, ha $\mathfrak{m}$ tartalmazás tekintetében maximális eleme az A gyűrű valódi ideáljai halmazának.

14.5.12. Tétel. (**Krull-tétel**) *Ha A egységelemes gyűrű, akkor minden $\mathfrak{n} \subseteq A$ valódi ideálhoz létezik A-nak olyan $\mathfrak{m}$ maximális ideálja, hogy $\mathfrak{n} \subseteq \mathfrak{m}$.*

Bizonyítás. Legyen $\mathfrak{n}$ valódi ideál A-ban és jelölje $\mathfrak{S}_\mathfrak{n}$ az A gyűrű $\mathfrak{n}$-t tartalmazó valódi ideáljainak halmazát. Az $\mathfrak{S}_\mathfrak{n}$ halmazt a tartalmazás relációval rendezzük. Ekkor az $\mathfrak{S}_\mathfrak{n}$ rendezett halmaz *induktívan rendezett.* Valóban, legyen $(\mathfrak{m}_i)_{i\in I}$ olyan $\mathfrak{S}_\mathfrak{n}$-ben haladó nem üres rendszer, amelyre minden $i, j \in I$ esetén $\mathfrak{m}_i \subseteq \mathfrak{m}_j$ vagy $\mathfrak{m}_j \subseteq \mathfrak{m}_i$. Ekkor $\mathfrak{m} := \bigcup_{i\in I}\mathfrak{m}_i$ ideál A-ban, és minden $i \in I$ esetén $1 \notin \mathfrak{m}_i$, hiszen $\mathfrak{m}_i$ valódi ideál A-ban, ezért $1 \notin \mathfrak{m}$, következésképpen $\mathfrak{m} \in \mathfrak{S}_\mathfrak{n}$ és minden $i \in I$ esetén $\mathfrak{m}_i \subseteq \mathfrak{m}$. Ezért a Zorn-lemma szerint az $\mathfrak{S}_\mathfrak{n}$ rendezett halmaznak létezik maximális eleme: legyen $\mathfrak{m}$ ilyen elem. Ekkor $\mathfrak{m}$ olyan valódi ideál A-ban, amelyre $\mathfrak{n} \subseteq \mathfrak{m}$. Ha $\mathfrak{m}'$ olyan valódi ideál A-ban, amelyre $\mathfrak{m} \subseteq \mathfrak{m}'$, akkor $\mathfrak{m}' \in \mathfrak{S}_\mathfrak{n}$, így az $\mathfrak{m}$ elem $\mathfrak{S}_\mathfrak{n}$-beli maximalitása miatt $\mathfrak{m} = \mathfrak{m}'$. Ez azt jelenti, hogy $\mathfrak{m}$ olyan maximális ideál A-ban, amelyre $\mathfrak{n} \subseteq \mathfrak{m}$. ■

14.5.13. Definíció. *Azt mondjuk, hogy az A gyűrű* **egyszerű***, ha A-nak $\{0\}$-n és A-n kívül nincs más ideálja.*

Később látni fogjuk, hogy minden test egyszerű gyűrű, és minden K testre és $n > 1$ természetes számra az $\mathrm{M}_n(K)$ mátrixgyűrű olyan egyszerű gyűrű, amely nem test.

14.5.14. Állítás. *Az A egységelemes gyűrű $\mathfrak{m}$ ideálja pontosan akkor maximális, ha az $A/\mathfrak{m}$ faktorgyűrű nemelfajult és egyszerű.*

Bizonyítás. Tegyük fel, hogy $\mathfrak{m} \subsetneq A$ maximális ideál, és legyen $\mathfrak{n}' \subseteq A/\mathfrak{m}$ ideál. Ekkor van olyan $\mathfrak{n} \subseteq A$ ideál, hogy $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = \mathfrak{n}'$. Az $\mathfrak{m}+\mathfrak{n}$ halmaz $\mathfrak{m}$-t tartalmazó ideál A-ban, ezért $\mathfrak{m}$ maximalitása miatt $\mathfrak{m}+\mathfrak{n} = \mathfrak{m}$ vagy $\mathfrak{m}+\mathfrak{n} = A$. Ha $\mathfrak{m}+\mathfrak{n} = \mathfrak{m}$, akkor $\mathfrak{m} = \mathrm{Ker}(\pi_{A/\mathfrak{m}})$ miatt $\mathfrak{n}' = \pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = \pi_{A/\mathfrak{m}}\langle\mathfrak{m}+\mathfrak{n}\rangle = \pi_{A/\mathfrak{m}}\langle\mathfrak{m}\rangle = \{0\}$. Ha $\mathfrak{m}+\mathfrak{n} = A$, akkor $\mathfrak{m} = \mathrm{Ker}(\pi_{A/\mathfrak{m}})$ és $\pi_{A/\mathfrak{m}}$ szürjektivitása miatt $\mathfrak{n}' = \pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = \pi_{A/\mathfrak{m}}\langle\mathfrak{m}+\mathfrak{n}\rangle = \pi_{A/\mathfrak{m}}\langle A\rangle = A/\mathfrak{m}$. Ez azt jelenti, hogy az $A/\mathfrak{m}$ faktorgyűrű egyszerű. Továbbá, $\mathfrak{m} \neq A$ miatt $A/\mathfrak{m} \neq \{0\}$, tehát az $A/\mathfrak{m}$ faktorgyűrű nemelfajult.

Megfordítva, tegyük fel, hogy $\mathfrak{m} \subseteq A$ olyan ideál, hogy az $A/\mathfrak{m}$ faktorgyűrű nemlfajult és egyszerű. Ekkor a nemelfajultságból $\mathfrak{m} \neq A$ következik. Legyen $\mathfrak{n} \subseteq A$ olyan ideál, hogy $\mathfrak{m} \subseteq \mathfrak{n}$. Ekkor $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle$ ideál $A/\mathfrak{m}$-ben, ezért a hipotézis alapján $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = \{0\}$ vagy $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = A/\mathfrak{m}$. Ha $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = \{0\}$, akkor $\mathfrak{n} \subseteq \mathfrak{m}$, tehát $\mathfrak{n} = \mathfrak{m}$. Tegyük fel, hogy $\pi_{A/\mathfrak{m}}\langle\mathfrak{n}\rangle = A/\mathfrak{m}$. Ekkor a $\pi_{A/\mathfrak{m}}(1) \in A/\mathfrak{m}$ elemhez van olyan $e \in \mathfrak{n}$, hogy $\pi_{A/\mathfrak{m}}(1) = \pi_{A/\mathfrak{m}}(e)$, vagyis $1-e \in \mathfrak{m} \subseteq \mathfrak{n}$. Mivel pedig $e \in \mathfrak{n}$, így $1 = (1-e)+e \in \mathfrak{n}+\mathfrak{n} \subseteq \mathfrak{n}$, tehát $\mathfrak{n} = A$. Ezért $\mathfrak{m}$ maximális ideál A-ban. ■

14.5.15. Állítás. *Egyszerű egységelemes kommutatív gyűrűben minden nem* 0 *elemnek létezik multiplikatív inverze.*

Bizonyítás. Legyen A egyszerű egységelemes kommutatív gyűrű és $a \in A$ olyan elem, hogy $a \neq 0$. Az A gyűrű kommutativitása miatt aA ideál A-ban, tehát $aA = \{0\}$ vagy $aA = A$. De $aA = \{0\}$ lehetetlen, különben $a = a1 \in aA = \{0\}$, azaz $a = 0$ teljesülne. Tehát $aA = A$, így $1 \in aA$, vagyis létezik olyan $b \in A$, hogy $1 = ab$. Ismét az A gyűrű kommutativitása miatt ekkor b multiplikatív inverze a-nak. ■

14.5.16. Következmény. *Ha A egységelemes kommutatív gyűrű és $\mathfrak{m}$ maximális ideál A-ban, akkor az $A/\mathfrak{m}$ faktorgyűrű test.*

Bizonyítás. Láttuk, hogy $A/\mathfrak{m}$ egyszerű gyűrű, továbbá ez nyilvánvalóan kommutatív és egységelemes, tehát az előző állítás szerint $A/\mathfrak{m}$ minden nem nulla elemének létezik multiplikatív inverze. Továbbá, $\mathfrak{m}$ valódi ideál A-ban, így $A/\mathfrak{m} \neq \{0\}$, tehát az $A/\mathfrak{m}$ faktorgyűrű test. ■

14.5.17. Következmény. *Egységelemes kommutatív gyűrűben minden maximális ideál prímideál.*

Bizonyítás. Ha A egységelemes kommutatív gyűrű és $\mathfrak{m}$ maximális ideál A-ban, akkor az előző állítás szerint az $A/\mathfrak{m}$ faktorgyűrű test, tehát zérusosztómentes, tehát 14.5.7. alapján $\mathfrak{m}$ prímideál. ■

14.5.18. Következmény. *Egységelemes kommutatív gyűrűben pontosan akkor létezik prímideál, ha létezik benne valódi ideál.*

Bizonyítás. Ha A egységelemes kommutatív gyűrű és $\mathfrak{n}$ valódi ideálja A-nak, akkor a Krull-tétel (14.5.12.) szerint van olyan $\mathfrak{m}$ maximális ideál A-ban, amelyre $\mathfrak{n} \subseteq \mathfrak{m}$, tehát az előző állításból következik, hogy $\mathfrak{m}$ prímideál A-ban. ■

14.6. Integritástartományok és főideálgyűrűk

14.6.1. Definíció. *A nemelfajult, kommutatív, egységelemes, zérusosztómentes gyűrűket* **integritástartományoknak** *nevezzük.*

14.6.2. Állítás. *Az egész számok gyűrűje integritástartomány.*

Bizonyítás. A 7.12.5. d) állítás szerint a $\mathbb{Z}$ nemelfajult kommutatív, egységelemes gyűrű zérusosztómentes. ■

°Később látni fogjuk, hogy test minden részgyűrűje integritástartomány, továbbá minden integritástartomány valamely testnek a részgyűrűje, vagyis az integritástartományok éppen a testek egységelemes részgyűrűi.°

14.6.3. Definíció. *Az A gyűrűt* **főideálgyűrűnek** *nevezzük, ha A integritástartomány, és minden $\mathfrak{m} \subseteq A$ ideálhoz létezik olyan $a \in A$, hogy $\mathfrak{m} = aA$.*

14.6.4. Állítás. *Az egész számok gyűrűje főideálgyűrű.*

Bizonyítás. Legyen $\mathfrak{m}$ ideál $\mathbb{Z}$-ben. Ha $\mathfrak{m} = \{0\}$, akkor $\mathfrak{m} = 0\mathbb{Z}$, tehát $\mathfrak{m}$ főideál.

Tegyük fel, hogy $\mathfrak{m} \neq \{0\}$. Ha $x \in \mathfrak{m}$ és $x \neq 0$, akkor $x > 0$ esetén $x \in \mathfrak{m} \cap \mathbb{N}^*$, és $x < 0$ esetén $-x \in \mathfrak{m} \cap \mathbb{N}^*$, tehát $\mathfrak{m} \cap \mathbb{N}^* \neq \emptyset$. Legyen $a := \min(\mathfrak{m} \cap \mathbb{N}^*)$. Ekkor $a \in \mathfrak{m}$ miatt $a\mathbb{Z} \subseteq \mathfrak{m}\mathbb{Z} \subseteq \mathfrak{m}$. Megmutatjuk, hogy $\mathfrak{m} \subseteq a\mathbb{Z}$ is teljesül.

Legyen $x \in \mathfrak{m}$ olyan, hogy $x \neq 0$. Ha $x \geq 0$, akkor egyértelműen léteznek olyan $q, r \in \mathbb{N}$, hogy $x = aq + r$ és $0 \leq r < a$ (7.11.8.); ekkor $r > 0$ lehetetlen, különben $r = x - aq$ az $\mathfrak{m} \cap \mathbb{N}^*$ halmaznak a-nál kisebb eleme lenne, ezért $r = 0$, tehát $x = aq \in a\mathbb{Z}$. Ha $x < 0$, akkor $-x \in \mathfrak{m}$ olyan, hogy $-x > 0$, így az előzőek szerint $-x \in a\mathbb{Z}$, tehát $x \in a\mathbb{Z}$. Ez azt jelenti, hogy $\mathfrak{m} \subseteq a\mathbb{Z}$, tehát $\mathfrak{m}$ egyenlő az $a \in \mathfrak{m} \cap \mathbb{N}^*$ elem által generált főideállal. ■

14.6.5. Definíció. *Legyen A kommutatív gyűrű. Ha $a, b \in A$, akkor azt mondjuk, hogy a* **osztója** *b-nek, vagy b* **többszöröse** *a-nak, vagy b* **osztható** *a-val, ha létezik olyan $c \in A$, hogy $ac = b$, és ezt a kijelentést az $a \mid b$ szimbólummal jelöljük. Ha $a, b \in A$, akkor az $a \mid b$ kijelentés tagadását az $a \nmid b$ szimbólummal jelöljük. Továbbá, az*

$$\{\ (a, b) \in A \times A \mid a \mid b\ \}$$

halmazt A feletti **oszthatóság-relációnak** *nevezzük.*

14.6.6. Definíció. *Legyen A egységelemes kommutatív gyűrű. Az A gyűrű multiplikatív neutrális elemének osztóit* **egységosztóknak** *vagy* **egységeknek** *nevezzük. Azt mondjuk, hogy az $a, b \in A$ elemek* **asszociáltak**, *ha léteznek olyan $c, d \in A$ egységek, hogy $ac = b$ és $bd = a$.*

Az oszthatóság-relációval kapcsolatban a következő megjegyzéseket tesszük.

– Ha A *egységelemes* kommutatív gyűrű, akkor az A feletti oszthatóság-reláció nyilvánvalóan *reflexív*, mert minden $a \in A$ esetén $a1 = a$. Azonban nem egységelemes kommutatív gyűrű felett az oszthatóság-reláció nem feltétlenül reflexív. Például, ha $A \neq \{0\}$ nulla szorzású gyűrű, akkor $a \in A$ és $a \neq 0$ esetén $a \mid a$ nem teljesül, hiszen minden $b \in A$ esetén $ab = 0 \neq a$.

– Ha A egységelemes kommutatív gyűrű és $a, b \in A$, akkor nyilvánvaló, hogy

$$a \mid b \quad \Leftrightarrow \quad b \in aA \quad \Leftrightarrow \quad bA \subseteq aA,$$

következésképpen

$$(a \mid b) \wedge (b \mid a) \quad \Leftrightarrow \quad aA = bA.$$

Ebből látható, hogy az oszthatóság-reláció általában nem antiszimmetrikus. Ha A integritástartomány, akkor $a, b \in A$ esetén $aA = bA$ maga után vonja, hogy a és b *asszociált* elemek. Valóban, ha $a = 0$, akkor világos, hogy $b = 0$, így $a = b$. Ha $a \neq 0$ és $c, d \in A$ olyan elemek, hogy $ac = b$ és $bd = a$, akkor $a(cd) = a$, vagyis $a(cd - 1) = 0$, így $cd = 1$, tehát c és d egységosztók. Az nyilvánvaló, hogy egységelemes kommutatív gyűrűben asszociált elemek kölcsönösen osztói egymásnak.

– Az oszthatóság-reláció minden esetben tranzitív, mert ha A kommutatív gyűrű és $a, b, c \in A$ olyan elemek, hogy $a \mid b$ és $b \mid c$, akkor léteznek olyan $r, s \in A$, hogy $ar = b$ és $bs = c$, így az A szorzásának asszociativitása miatt $a(rs) = (ar)s = bs = c$, következésképpen $a \mid c$.

– Ha A kommutatív gyűrű, és $a, b \in A$ olyanok, hogy $a \mid b$ és $a \neq 0$, akkor létezhetnek olyan $c, c' \in A$, hogy $ac = b = ac'$, de $c \neq c'$, hiszen az $ac = ac'$ egyenlőség azzal ekvivalens, hogy $a(c - c') = 0$, tehát ha $a \in A$ zérusosztó, akkor ebből nem szükségképpen következik, hogy $c - c' = 0$. Ezért kommutatív gyűrű esetén általában nem beszélhetünk a *b/a hányadosról.* De ha A zérusosztómentes kommutatív gyűrű, akkor $a, b \in A$, $a \mid b$ és $a \neq 0$ esetén egyetlen olyan $c \in A$ létezik, amelyre $ac = b$, ezért ilyenkor van értelme a b/a hányadosnak, amely tehát az az egyértelműen meghatározott elem A-ban, amelyre $a(b/a) = b$.

14.6.7. Állítás. *Ha A egységelemes kommutatív gyűrű, akkor minden $e \in A$ esetén a következő állítások ekvivalensek.*

(i) *Minden $a \in A$ esetén $e \mid a$.*

(ii) *$e \mid 1$, vagyis az $e \in A$ elem egységosztó.*

(iii) *$eA = A$, vagyis az $e \in A$ elem által generált főideál egyenlő A-val.*

(iv) *$e \in \mathbf{G}(A)$, vagyis az $e \in A$ elem invertálható az A szorzása szerint.*

Bizonyítás. (i)⇒(ii) Nyilvánvaló.

(ii)⇒(iii) Ha $e' \in A$ olyan, hogy $ee' = 1$, akkor minden $a \in A$ esetén A szorzásának asszociativitása miatt $a = 1a = (ee')a = e(e'a) \in eA$, tehát $A \subseteq eA$.

(iii)⇒(iv) Ha $eA = A$, akkor $1 \in eA$, tehát van olyan $e' \in A$, amelyre $1 = ee'$, ezért az A szorzásának kommutativitása miatt $e \in \mathbf{G}(A)$.

(iv)⇒(i) Ha $e \in \mathbf{G}(A)$, akkor minden $a \in A$ esetén $a = 1a = (ee^{-1})a = e(e^{-1}a)$, tehát $e \mid a$. ■

14.6.8. Következmény. *Ha A egységelemes kommutatív gyűrű, akkor az $a, b \in A$ elemek pontosan akkor asszociáltak, ha létezik olyan $c \in A$ egységosztó, hogy $ac = b$.*

Bizonyítás. Ha $a, b \in A$ és $c \in A$ olyan egységosztó, hogy $ac = b$, akkor az előző állítás szerint $c \in \mathbf{G}(A)$, ezért $bc^{-1} = (ac)c^{-1} = a(cc^{-1}) = a1 = a$, és $c^{-1} \in \mathbf{G}(A)$, így az előző állítás szerint c^{-1} is egységosztó, tehát az a és b elemek asszociáltak. ■

A 7.12.5. e) állításból látszik, hogy a $\mathbb{Z}$ gyűrűben 1 és -1 az egyedüli egységosztók.

14.6.9. Állítás. *$\mathbb{Z}$-ben a nem nulla prímideálok azonosak a $p\mathbb{Z}$ alakú főideálokkal, ahol $p \in \mathbb{N}$ prímszám.*

Bizonyítás. Legyen $\mathfrak{p}$ nem nulla prímideál $\mathbb{Z}$-ben, és vegyünk olyan $p \in \mathbb{Z}$ elemet, hogy $\mathfrak{p} = p\mathbb{Z}$. Ha $p \leq 0$, akkor $-p \geq 0$ és $(-p)\mathbb{Z} = p\mathbb{Z} = \mathfrak{p}$, ezért feltehető, hogy $p \geq 0$, vagyis $p \in \mathbb{N}$. Ha $p = 0$, akkor $\mathfrak{p} = \{0\}$, holott $\mathfrak{p}$ nem nulla ideál. Ezért $p \geq 1$, és $p = 1$ lehetetlen, mert $\mathfrak{p} \neq \mathbb{Z}$ (a prímideálok definíciója szerint). Ezért $p \geq 2$ természetes szám. Tegyük fel, hogy p nem prímszám, tehát léteznek olyan $a, b \in \mathbb{N}$, hogy $a > 1$ és $b > 1$ és $p = ab$. Ekkor $a \mid p$, és $a \notin p\mathbb{Z} = \mathfrak{p}$, különben $p \mid a$ is teljesülne, így létezne olyan $e \in \mathbb{Z}$ egységosztó, hogy $a = pe$, tehát $e \in \{-1, 1\}$ és $a > 0$, $p > 0$ miatt $a = p$ lenne, ami lehetetlen, mert ebből $p = ab$ és az $\mathbb{N}$ feletti szorzás kancellativitása miatt $b = 1$ következne, holott $b > 1$. Hasonló meggondolással kapjuk, hogy $b \mid p$ és $b \notin p\mathbb{Z} = \mathfrak{p}$. Mivel $\mathfrak{p}$ prímideál, így $p = ab \notin \mathfrak{p} = p\mathbb{Z}$, holott $p \in p\mathbb{Z}$. Ez azt jelenti, hogy p prímszám.

Megfordítva, legyen $p \in \mathbb{N}$ prímszám. Ha $a, b \in \mathbb{Z}$ olyanok, hogy $a \notin p\mathbb{Z}$ és $b \notin p\mathbb{Z}$, akkor p sem a-nak, sem b-nek nem osztója. Ezért az Euklidész-lemma (7.11.11.) alapján p az ab szorzatnak sem osztója, vagyis $ab \notin p\mathbb{Z}$. Ugyanakkor $p\mathbb{Z} \neq \mathbb{Z}$, hiszen $1 \notin p\mathbb{Z}$, mert p nem osztója 1-nek. Ez azt jelenti, hogy $p\mathbb{Z}$ nem nulla prímideál $\mathbb{Z}$-ben. ■

Ha A egységelemes kommutatív gyűrű és $e \in A$ egységosztó, akkor minden A-ban haladó $(a_i)_{i \in I}$ rendszerre, minden $i \in I$ esetén $e \mid a_i$, amit úgy fejezünk ki, hogy az $e \in A$ elem *közös osztója* az $(a_i)_{i \in I}$ rendszernek. Külön nevet adunk azoknak a rendszereknek, amelyeknek minden közös osztója egységosztó.

14.6.10. Definíció. *Az A egységelemes kommutatív gyűrűben haladó $(a_i)_{i \in I}$ rendszert* **relatív prímnek** *nevezzük, ha az $(a_i)_{i \in I}$ rendszer minden közös osztója egységosztó. Ha A egységelemes kommutatív gyűrű, akkor az $a \in A$ és $b \in A$ elemeket relatív prímeknek nevezzük, ha az a $(c_i)_{i \in \{0,1\}}$ rendszer relatív prím, amelyre $c_0 := a$ és $c_1 := b$.*

14.6.11. Tétel. (**Bézout-tétel**.) *Legyen A főideálgyűrű és $(a_i)_{i \in I}$ nem üres rendszer A-ban. Tegyük fel, hogy $d \in A$ rendelkezik a következő tulajdonsággal:*

(lnko) *Minden $i \in I$ esetén $d \mid a_i$, és ha $d' \in A$ olyan elem, hogy minden $i \in I$ esetén $d' \mid a_i$, akkor $d' \mid d$.*

Ekkor létezik olyan $(x_i)_{i \in I} \in A^{(I)}$, hogy $d = \sum_{i \in I} a_i x_i$.

Bizonyítás. Képezzük az

$$\mathfrak{m} := \left\{ \sum_{i \in I} a_i x_i \;\middle|\; (x_i)_{i \in I} \in A^{(I)} \right\}$$

halmazt. Világos, hogy $\mathfrak{m}$ ideál A-ban, mert

– $I \neq \emptyset$ miatt $\mathfrak{m} \neq \emptyset$;

– ha $(x_i)_{i \in I} \in A^{(I)}$ és $(y_i)_{i \in I} \in A^{(I)}$, akkor $(x_i + y_i)_{i \in I} \in A^{(I)}$ olyan rendszer, hogy

$$\Big(\sum_{i \in I} a_i x_i\Big) + \Big(\sum_{i \in I} a_i y_i\Big) = \sum_{i \in I} (a_i x_i + a_i y_i) = \sum_{i \in I} a_i (x_i + y_i) \in \mathfrak{m},$$

vagyis $\mathfrak{m} + \mathfrak{m} \subseteq \mathfrak{m}$;

– ha $(x_i)_{i \in I} \in A^{(I)}$ és $a \in A$, akkor $(x_i a)_{i \in I} \in A^{(I)}$ olyan rendszer, hogy

$$\Big(\sum_{i \in I} a_i x_i\Big) a = \sum_{i \in I} (a_i x_i) a = \sum_{i \in I} a_i (x_i a) \in \mathfrak{m},$$

vagyis $\mathfrak{m}A \subseteq \mathfrak{m}$.

Világos továbbá, hogy minden $j \in I$ esetén $a_j \in \mathfrak{m}$, mert ha $(x_i)_{i\in I} \in A^{(I)}$ az a rendszer, melyre $x_j := 1$ és minden $i \in I \setminus \{j\}$ esetén $x_i := 0$, akkor $a_j = \sum_{i\in I} a_i x_i$.

Az A gyűrű főideálgyűrű, ezért vehetünk olyan $d' \in A$ elemet, amelyre $d'A = \mathfrak{m}$. Ha $i \in I$, akkor $a_i \in \mathfrak{m} = d'A$, tehát $d' \mid a_i$. Ezért az (lnko) hipotézis alapján $d' \mid d$, tehát $d \in d'A = \mathfrak{m}$, vagyis létezik olyan $(x_i)_{i\in I} \in A^{(I)}$, hogy $d = \sum_{i\in I} a_i x_i$. ■

14.6.12. Következmény. (**Bézout-tétel relatív prímekre**.) *Ha A főideálgyűrű, akkor az A-ban haladó $(a_i)_{i\in I}$ nem üres rendszer pontosan akkor relatív prím, ha létezik olyan $(x_i)_{i\in I} \in A^{(I)}$, hogy $\sum_{i\in I} a_i x_i = 1$.*

Bizonyítás. Tegyük fel, hogy az $(a_i)_{i\in I}$ rendszer relatív prím. Ekkor a Bézout-tételben felírt (lnko) feltétel teljesül a $d := 1 \in A$ elemre, ezért létezik olyan $(x_i)_{i\in I} \in A^{(I)}$, hogy $\sum_{i\in I} a_i x_i = 1$.

Megfordítva, legyen $(x_i)_{i\in I} \in A^{(I)}$ olyan rendszer, hogy $\sum_{i\in I} a_i x_i = 1$. Tegyük fel, hogy a $d \in A$ elemre teljesül az, hogy minden $i \in I$ esetén $d \mid a_i$. Ekkor a kiválasztási axióma alkalmazásával kiválaszthatunk olyan A-ban haladó $(a'_i)_{i\in I}$ rendszert, hogy minden $i \in I$ esetén $da'_i = a_i$. Ekkor az $a' := \sum_{i\in I} a'_i x_i \in A$ elemre

$$da' = d\Big(\sum_{i\in I} a'_i x_i\Big) = \sum_{i\in I} d(a'_i x_i) = \sum_{i\in I} (da'_i) x_i = \sum_{i\in I} a_i x_i = 1$$

teljesül, tehát d egységosztó, így az $(a_i)_{i\in I}$ rendszer relatív prím. ■

14.6.13. Következmény. *Ha A főideálgyűrű, akkor az A-ban haladó $(a_i)_{i\in I}$ nem üres rendszer pontosan akkor relatív prím, ha létezik olyan $J \subseteq I$ nem üres véges halmaz, hogy az $(a_i)_{i\in J}$ rendszer relatív prím.*

Bizonyítás. A definícióból azonnal következik, hogy ha létezik olyan $J \subseteq I$ nem üres halmaz (akár véges, akár végtelen), hogy az $(a_i)_{i\in J}$ rendszer relatív prím, akkor az $(a_i)_{i\in I}$ rendszer is relatív prím (még akkor is ha A nem főideálgyűrű).

Megfordítva, ha A főideálgyűrű és az A-ban haladó $(a_i)_{i\in I}$ nem üres rendszer relatív prím, akkor a Bézout-tétel szerint van olyan $(x_i)_{i\in I} \in A^{(I)}$, hogy $\sum_{i\in I} a_i x_i = 1$. Ekkor $1 \neq 0$ miatt $J := \{i \in I | x_i \neq 0\}$ nem üres véges halmaz, és $\sum_{i\in J} a_i x_i = 1$. Ismét a Bézout-tételt alkalmazva, de ezúttal az $(a_i)_{i\in J}$ véges rendszerre azt kapjuk, hogy $(a_i)_{i\in J}$ relatív prím. ■

14.6.14. Következmény. (**Bézout-tétel $\mathbb{Z}$-re**.) *Az $a, b \in \mathbb{Z}$ számok pontosan akkor relatív prímek, ha léteznek olyan $x, y \in \mathbb{Z}$, hogy $ax + by = 1$.*

14.6.15. Definíció. *Legyen A egységelemes kommutatív gyűrű.*

– *Azt mondjuk, hogy $a \in A$ elem* **prím**, *ha $a \neq 0$ és nem egységosztó, valamint minden*

$b, c \in A$ esetén, az $a \mid bc$ relációból következik, hogy $a \mid b$ vagy $a \mid c$.

– *Azt mondjuk, hogy $a \in A$ elem* **irreducibilis**, *ha $a \neq 0$ és nem egységosztó, valamint minden $b, c \in A$ esetén, az $a = bc$ egyenlőségből következik, hogy a b és c elemek egységosztók, vagy a-val asszociáltak.*

14.6.16. Állítás. *Legyen A egységelemes kommutatív gyűrű. A $p \in A$ elem pontosan akkor prím, ha pA nem nulla prímideál.*

Bizonyítás. Legyen $p \in A$ prím. Az A gyűrű egységelemessége és $p \neq 0$ miatt pA nem nulla ideál A-ban. Továbbá, pA valódi ideál, mert A egységelemes és p nem egységosztó. Ha $b, c \in A$ olyan elemek, hogy $bc \in pA$, akkor $p \mid bc$, és p prím, ezért $p \mid b$ vagy $p \mid c$, azaz $b \in pA$ vagy $c \in pA$. Ez azt jelenti, hogy pA nem nulla prímideál A-ban.

Megfordítva, tegyük fel, hogy pA nem nulla prímideál A-ban. Világos, hogy $pA \neq \{0\}$ miatt $p \neq 0$. Továbbá, ha p egységosztó volna, akkor $pA = A$ teljesülne, holott pA valódi ideál. Tehát $p \neq 0$ és p nem egységosztó. Ha $b, c \in A$ olyanok, hogy $p \mid bc$, akkor $bc \in\in pA$, és pA prímideál, ezért $b \in pA$ vagy $c \in pA$, vagyis $p \mid b$ vagy $p \mid c$. Ez azt jelenti, hogy a p elem prím. ■

14.6.17. Állítás. *Integritástartományban minden prím elem irreducibilis.*

Bizonyítás. Legyen A integritástartomány és $a \in A$ prím elem. Legyenek $b, c \in A$ olyan elemek, amelyekre $a = bc$. Ekkor A egységelemessége miatt $a \mid bc$, ezért $a \mid b$ *vagy* $a \mid c$. Ugyanakkor $b \mid a$ *és* $c \mid a$.

Ha $a \mid b$, akkor $b \mid a$ miatt a és b asszociáltak, vagyis vehetünk olyan $e \in A$ egységosztót, amelyre $ae = b$. Ekkor $a = bc = aec$, tehát $a(1 - ec) = 0$ és $a \neq 0$, így A zérusosztómentessége miatt $ec = 1$, vagyis c is egységosztó. Ez azt jelenti, hogy $a \mid b$ esetén b asszociált a-val és c egységosztó.

Ha $a \mid c$, akkor $c \mid a$ miatt a és c asszociáltak, vagyis vehetünk olyan $f \in A$ egységosztót, amelyre $fa = c$. Ekkor $a = bc = bfa$, tehát $(1 - bf)a = 0$ és $a \neq 0$, így A zérusosztómentessége miatt $bf = 1$, vagyis b is egységosztó. Ez azt jelenti, hogy $a \mid c$ esetén c asszociált a-val és b egységosztó. ■

Létezik olyan integritástartomány, amelyben nem minden irreducibilis elem prím. °Például legyen $A := \{a + b\sqrt{5}\mathbf{i} \mid (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$, ami egységelemes részgyűrűje a komplex számok $\mathbb{C}$ testének, tehát integritástartomány, és $2 + \sqrt{5}\mathbf{i},\ 2 - \sqrt{5}\mathbf{i} \in A$ olyan elemek, amelyekre $3 \mid 9 = (2 + \sqrt{5}\mathbf{i})(2 - \sqrt{5}\mathbf{i})$, de $3 \nmid 2 + \sqrt{5}\mathbf{i}$ és $3 \nmid 2 - \sqrt{5}\mathbf{i}$, tehát 3 nem prím, ugyanakkor könnyen ellenőrizhető, hogy 3 irreducibilis A-ban.°

14.6.18. Állítás. *Főideálgyűrűben minden irreducibilis elem prím.*

Bizonyítás. Legyen A főideálgyűrű és $a \in A$ irreducibilis elem. Vegyünk olyan $b, c \in A$ elemeket, amelyekre $a \mid bc$. Elegendő azt igazolni, hogy ha $a \nmid b$, akkor $a \mid c$.

Tekintsük az $aA + bA \subseteq A$ halmazt, amely ideál A-ban, tehát létezik olyan $d \in A$, amelyre $aA + bA = dA$. Ekkor $a = a \cdot 1 + b \cdot 0 \in aA + bA = dA$, tehát $d \mid a$, és hasonlóan, $b = a \cdot 0 + b \cdot 1 \in aA + bA = dA$, tehát $d \mid b$. Mivel $d \mid a$ és a hipotézis szerint $a \in A$ irreducibilis elem, így d egységosztó vagy asszociált a-val.

Ha d asszociált a-val, akkor $a \mid d$, és mivel $d \mid b$, így az oszthatóság-reláció tranzitivitása miatt $a|b$, holott az a feltevés, hogy $a \nmid b$. Ezért d egységosztó, következésképpen $A = dA = aA + bA$, tehát vehetünk olyan $x, y \in A$ elemeket, amelyekre $1 = ax + by$.

Ekkor $c = c \cdot 1 = cax + cby$, és $a \mid cax$, valamint $a \mid bc$ miatt $a \mid cby$. Ezért $a \mid c$, amit bizonyítani kellett. ■

°Az előző állítás előtt álló megjegyzés szerint az $\{a + b\sqrt{5}\mathbf{i} \mid (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$ részgyűrű a $\mathbb{C}$ testben olyan integritástartomány, amely nem főideálgyűrű.°

14.6.19. Tétel. *Ha A főideálgyűrű és $a \in A$, akkor az alábbi állítások ekvivalensek.*

(i) *Az $a \in A$ elem prím.*

(ii) *Az $a \in A$ elem irreducibilis.*

(iii) *Az aA ideál maximális.*

(iv) *Az A/aA faktorgyűrű test.*

Bizonyítás. (i)⇒(ii) A 14.6.17. állítás szerint ez még integritástartományban is igaz.

(ii)⇒(iii) Legyen az $a \in A$ elem irreducibilis, és $\mathfrak{m}$ olyan ideál A-ban, amelyre $aA \subseteq \mathfrak{m}$ és $\mathfrak{m} \neq A$. Az A gyűrű főideálgyűrű, ezért vehetünk olyan $b \in A$ elemet, amelyre $\mathfrak{m} = bA$. Ekkor $a \in bA$, tehát van olyan $c \in A$, amelyre $a = bc$. Az $a \in A$ elem irreducibilitása miatt ebből következik, hogy a b és c elemek egységosztók, vagy a-val asszociáltak. A b elem nem egységosztó, különben $\mathfrak{m} = bA = A$ teljesülne. Ezért b asszociált a-val, így $aA = bA = \mathfrak{m}$.

(iii)⇒(iv) A 14.5.16. állításból következik.

(iv)⇒(i) Ha $b, c \in A$ olyanok, hogy $a \mid bc$, akkor $bc \in aA$, így $\pi_{A/aA}(b) \cdot \pi_{A/aA}(c) = \pi_{A/aA}(bc) = 0$, tehát (iv) miatt $\pi_{A/aA}(b) = 0$ vagy $\pi_{A/aA}(c) = 0$, vagyis $b \in aA$ vagy $c \in aA$, azaz $a \mid b$ vagy $a \mid c$. ■

14.7. Euklidészi gyűrűk

14.7.1. Definíció. *Ha A kommutatív gyűrű, akkor A feletti* **euklidészi normának** *nevezünk minden olyan $\omega : A \setminus \{0\} \to \mathbb{N}$ függvényt, amelyre teljesül a következő.*

(DE) *Minden $a, b \in A$ esetén, ha $b \neq 0$, akkor léteznek olyan $q, r \in A$ elemek, hogy $a = bq + r$ és $r = 0$ vagy $r \neq 0$ és $\omega(r) < \omega(b)$.*

Azt mondjuk, hogy A **euklidészi gyűrű***, ha A integritástartomány és létezik A felett euklidészi norma.*

14.7.2. Állítás. *Az egész számok $\mathbb{Z}$ gyűrűje felett euklidészi norma a*

$$\mathbb{Z} \setminus \{0\} \to \mathbb{N}; \quad x \mapsto |x| := \max(-x, x)$$

leképezés.

Bizonyítás. Elegendő az ekildészi maradékos osztás tételét (7.11.8.) alkalmazni megfelelő esetszétválasztással. ■

14.7.3. Állítás. *Minden euklidészi gyűrű főideálgyűrű.*

Bizonyítás. Legyen A euklidészi gyűrű és ω euklidészi norma A felett. Legyen $\mathfrak{m} \subseteq A$ nem nulla ideál. Ekkor $\omega\langle \mathfrak{m} \setminus \{0\}\rangle$ nem üres részhalmaza $\mathbb{N}$-nek, tehát képezhető az $n := \min(\omega\langle \mathfrak{m} \setminus \{0\}\rangle)$ szám. Legyen $b \in \mathfrak{m}\setminus\{0\}$ olyan elem, amelyre $\omega(b) = n$. Igazoljuk, hogy $bA = \mathfrak{m}$.

Mivel $b \in \mathfrak{m}$ és $\mathfrak{m}$ ideál, így $bA \subseteq \mathfrak{m}$. Legyen $a \in \mathfrak{m}$. Az ω függvény euklidészi norma

A felett és $b \neq 0$, így léteznek olyan $q, r \in A$ elemek, hogy $a = bq + r$ és $r = 0$ vagy $r \neq 0$ és $\omega(r) < \omega(b)$. Ha $r \neq 0$ teljesülne, akkor $\omega(r) < \omega(b) = n$, ami lehetetlen, mert n az $\omega\langle \mathfrak{m} \setminus \{0\}\rangle$ halmaz legkisebb eleme, és $\omega(r)$ is eleme ennek a halmaznak, mert $r = a - bq \in \mathfrak{m} - bA \subseteq \mathfrak{m} - \mathfrak{m} \subseteq \mathfrak{m}$. Ezért $r = 0$, tehát $a = bq \in bA$. Ez azt jelenti, hogy $\mathfrak{m} \subseteq bA$, következésképpen $bA = \mathfrak{m}$. ■

14.7.4. Definíció. *Legyen K test. Minden $P \in K[X]$ esetén*

$$\deg(P) := \begin{cases} \max(\{k \in \mathbb{N} | P(k) \neq 0\}) & , \textit{ha } P \neq 0, \\ 0 & , \textit{ha } P = 0, \end{cases}$$

és a $\deg(P)$ *természetes számot a P polinom* **fokszámának** *nevezzük. Ha $P \in K[X]$ és $n := \deg(P)$, akkor azt mondjuk, hogy a P polinom n*-**ed fokú**.

A definícióból azonnal következik, hogy ha K test és $P \in K[X]$, akkor a $\deg(P) = 0$ egyenlőség azzal ekvivalens, hogy minden $k > 0$ természetes számra $P(k) = 0$, és az is nyilvánvaló, hogy $P \in K[X]$ és $n \in \mathbb{N}$ esetén

$$\deg(P) \leq n \iff \{k \in \mathbb{N} | P(k) \neq 0\} \subseteq \{k \in \mathbb{N} | k \leq n\}.$$

Ha K test és $n \in \mathbb{N}$, akkor $\{k \in \mathbb{N} | X^n(k) \neq 0\} = \{n\}$, ezért $\deg(X^n) = n$.

14.7.5. Állítás. *Ha K test, akkor minden $P, Q \in K[X]$ esetén, ha $P \neq 0$ és $Q \neq 0$, akkor $P * Q \neq 0$ és*

$$\deg(P * Q) = \deg(P) + \deg(Q).$$

Bizonyítás. Legyenek $P, Q \in K[X]$ olyanok, hogy $P \neq 0$ és $Q \neq 0$.

Legyen $n \in \mathbb{N}$ olyan, hogy $n > \deg(P) + \deg(Q)$. Ekkor

$$(P * Q)(n) = \sum_{k=0}^{\deg(P)} P(k)Q(n-k) + \sum_{k=\deg(P)+1}^{n} P(k)Q(n-k).$$

Ha a $k \in \mathbb{N}$ számra $k \leq \deg(P)$ teljesül, akkor $n - k \geq n - \deg(P) > \deg(Q)$, tehát $Q(n-k) = 0$, így $\sum_{k=0}^{\deg(P)} P(k)Q(n-k) = 0$. Ha a $k \in \mathbb{N}$ számra $\deg(P) + 1 \leq k$ teljesül, akkor $\deg(P) < k$, tehát $P(k) = 0$, így $\sum_{k=\deg(P)+1}^{n} P(k)Q(n-k) = 0$. Ez azt jelenti, hogy $n \in \mathbb{N}$ és $n > \deg(P) + \deg(Q)$ esetén $(P * Q)(n) = 0$.

Ha $\deg(P) = 0$ *és* $\deg(Q) = 0$, de $P \neq 0$ és $Q \neq 0$, akkor $P(0) \neq 0$ és $Q(0) \neq 0$, tehát $(P * Q)(0) = P(0)Q(0) \neq 0$, így $P * Q \neq 0$. Ugyanakkor $k \in \mathbb{N}$ és $k > 0$ esetén $P(k) = 0$ és $Q(k) = 0$, ezért minden $n \in \mathbb{N}^*$ számra

$$(P * Q)(n) = \sum_{k=0}^{n} P(k)Q(n-k) = P(0)Q(n) = 0,$$

hiszen $n > 0$ miatt $Q(n) = 0$. Tehát $\deg(P) = 0$ és $\deg(Q) = 0$, valamint $P \neq 0$ és $Q \neq 0$ esetén $P * Q \neq 0$ és $\deg(P * Q) = 0 = \deg(P) + \deg(Q)$.

Tegyük fel, hogy $\deg(P) > 0$ *vagy* $\deg(Q) > 0$. Ekkor

$$(P * Q)(\deg(P) + \deg(Q)) =$$

$$= \sum_{\substack{0 \le k \le \deg(P)+\deg(Q) \\ k \neq \deg(P)}} P(k)Q(\deg(P) + \deg(Q) - k) + P(\deg(P))Q(\deg(Q)) =$$

$$= P(\deg(P))Q(\deg(Q)) \neq 0,$$

mert ha $k \in \mathbb{N}$ olyan, hogy $k < \deg(P)$, akkor $\deg(P) + \deg(Q) - k > \deg(Q)$, tehát $Q(\deg(P) + \deg(Q) - k) = 0$, míg $k > \deg(P)$ esetén $P(k) = 0$, így minden $0 \le k \le \deg(P) + \deg(Q)$ és $k \neq \deg(P)$ esetén $P(k)Q(\deg(P) + \deg(Q) - k) = 0$. Ez azt jelenti $P * Q \neq 0$ és $\deg(P * Q) = \deg(P) + \deg(Q)$. ■

14.7.6. Állítás. *Ha K test, akkor minden $P, Q \in K[X]$ esetén*

$$\deg(P + Q) \le \max(\deg(P), \deg(Q)),$$

és ha $\deg(P) \neq \deg(Q)$, akkor

$$\deg(P + Q) = \max(\deg(P), \deg(Q)).$$

Bizonyítás. Nyilvánvaló, hogy

$$\{k \in \mathbb{N} | (P + Q)(k) \neq 0\} \subseteq \{k \in \mathbb{N} | P(k) \neq 0\} \cup \{k \in \mathbb{N} | Q(k) \neq 0\} \subseteq$$

$$\subseteq \{k \in \mathbb{N} | k \le \deg(P)\} \cup \{k \in \mathbb{N} | k \le \deg(Q)\} = \{k \in \mathbb{N} | k \le \max(\deg(P), \deg(Q)\},$$

ezért $\deg(P + Q) \le \max(\deg(P), \deg(Q))$.
Tegyük fel, hogy $\deg(P) \neq \deg(Q)$. A feltételben és az egyenlőségben P és Q szerepe szimmetrikus, ezért feltehető, hogy $\deg(Q) < \deg(P)$. Ha $n \in \mathbb{N}$ olyan, hogy $n > \deg(P)$, akkor $P(n) = 0$ és $n > \deg(Q)$, ezért $Q(n) = 0$ is teljesül, így $(P+Q)(n) = P(n)+Q(n) = 0$. Ugyanakkor $(P + Q)(\deg(P)) = P(\deg(P)) + Q(\deg(P)) = P(\deg(P)) \neq 0$, mert $\deg(Q) < \deg(P)$ miatt $Q(\deg(P)) = 0$. Ez azt jelenti, hogy $\deg(P + Q) = \deg(P) = \max(\deg(P), \deg(Q))$. ■

14.7.7. Lemma. *Ha K test és $P, Q \in K[X]$ olyanok, hogy $\deg(P) = \deg(Q) > 0$ és $P(\deg(P)) = Q(\deg(Q))$, akkor $\deg(P - Q) < \deg(P)$.*

Bizonyítás. Legyen $n := \deg(P) = \deg(Q) > 0$ és tegyük fel, hogy $P(n) = Q(n)$. Ekkor $k \in \mathbb{N}$ és $k > n$ esetén $P(k) = 0 = Q(k)$, vagyis $(P - Q)(k) = 0$, továbbá $(P - Q)(n) = 0$ is teljesül, ezért $\{k \in \mathbb{N} | (P - Q)(k) \neq 0\} \subseteq \{k \in \mathbb{N} | k \le n - 1\}$, így $\deg(P - Q) \le n - 1 < n = \deg(P)$. ■

14.7.8. Tétel. (**Polinomok osztása.**) *Ha K test, $S, P \in K[X]$ és $\deg(P) > 0$, akkor egyértelműen léteznek olyan $Q, R \in K[X]$, hogy*

$$S = P * Q + R$$

és $\deg(R) < \deg(P)$.

Bizonyítás. (Unicitás) Legyenek $Q, R, Q', R' \in K[X]$ olyanok, hogy $P * Q + R = P * Q' + R'$, és $\deg(R) < \deg(P)$, valamint $\deg(R') < \deg(P)$. Ekkor $P*(Q - Q') = R' - R$, tehát ha $Q \neq Q'$ teljesülne, akkor

$$\begin{aligned}\deg(P) > \max(\deg(R'), \deg(-R))) \geq \deg(R' - R) = \deg(P*(Q - Q')) = \\ = \deg(P) + \deg(Q - Q') \geq \deg(P),\end{aligned}$$

ami lehetetlen. Ezért $Q = Q'$, amiből következik, hogy $R = R'$.

(Egzisztencia) Legyen $P \in K[X]$ rögzített nem nulladfokú polinom, és $m := \deg(P)$. Teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén, minden $S \in K[X]$ polinomhoz, ha $\deg(S) = n$, akkor léteznek olyan $Q, R \in K[X]$, hogy $S = P * Q + R$ és $\deg(R) < \deg(P)$. Vagyis az egzisztenciát rögzített P esetén az S polinom fokszáma szerinti teljes indukcióval bizonyítjuk.

Ha $n = 0$ és $S \in K[X]$ olyan polinom, hogy $\deg(S) = n$, akkor $Q := 0$ és $R := S$ nyilvánvalóan olyan polinomok, amelyek létezését állítjuk.

Legyen $n \in \mathbb{N}^*$ olyan, hogy minden $n' < n$ természetes számra, minden $S' \in K[X]$ polinomhoz, ha $\deg(S') = n'$, akkor léteznek olyan $Q', R' \in K[X]$, hogy $S' = P * Q' + R'$ és $\deg(R') < \deg(P)$. Legyen $S \in K[X]$ olyan polinom, hogy $\deg(S) = n$.

Ha $n < m$, akkor $Q := 0$ és $R := S$ nyilvánvalóan olyan polinomok, amelyek létezését állítjuk.

Tegyük fel, hogy $n = m$. Jelölje Q azt a K feletti nulladfokú polinomot, amelyre $Q(0) := P(m)^{-1}S(m)$. Ekkor $(P * Q)(m) = \sum_{k=0}^{m} P(k)Q(m - k) = P(m)P(m)^{-1}S(m) = S(m)$ és $\deg(P * Q) = \deg(P) + \deg(Q) = m$. Ezért az előző lemma szerint $\deg(S - P * Q) < m$, ami azt jelenti, hogy az $R := S - P*Q \in K[X]$ polinomra $S = P*Q + R$ és $\deg(R) < \deg(P)$ teljesül.

Tegyük fel, hogy $n > m$. Ekkor

$$\deg(P * X^{n-m}) = \deg(P) + \deg(X^{n-m}) = m + (n - m) = n = \deg(S),$$

továbbá

$$(P * X^{n-m})(n) = \sum_{k=0}^{n} P(k)X^{n-m}(n - k) = P(m),$$

tehát

$$\frac{S(n)}{P(m)}.(P * X^{n-m})(n) = S(n).$$

Ebből az előző lemma alapján következik, hogy

$$\deg\left(S - \frac{S(n)}{P(m)}.(P * X^{n-m})\right) < n = \deg(S).$$

Legyen $S' := S - \frac{S(n)}{P(m)}.(P * X^{n-m})$. Ha $\deg(S') < m$, akkor a $Q := \frac{S(n)}{P(m)}.X^{n-m}$ és $R := S'$ polinomokra $S = P * Q + R$ és $\deg(R) < m = \deg(P)$ teljesül. Tegyük fel, hogy $\deg(S') \geq m$. Ekkor az indukciós hipotézis alapján léteznek olyan $Q', R' \in K[X]$, hogy $S' = P * Q' + R'$ és $\deg(R') < \deg(P)$. Ekkor

$$\begin{aligned}S = S' + \frac{S(n)}{P(m)}.(P * X^{n-m}) = P * Q' + \frac{S(n)}{P(m)}.(P * X^{n-m}) + R' = \\ = P * \left(Q' + \frac{S(n)}{P(m)}.X^{n-m}\right) + R',\end{aligned}$$

tehát $Q := Q' + \dfrac{S(n)}{P(m)}.X^{n-m}$ és $R := R'$ olyan K feletti polinomok, hogy $S = P * Q + R$ és $\deg(R) < \deg(P)$. ■

14.7.9. Tétel. *Ha K test, akkor a $K[X] \setminus \{0\} \to \mathbb{N}$; $P \mapsto \deg(P)$ leképezés euklidészi norma a $K[X]$ polinomgyűrű felett, tehát $K[X]$ euklidészi gyűrű.*

Bizonyítás. Legyenek $S, P \in K[X]$ és $P \neq 0$. Ha $\deg(P) = 0$, akkor $Q := P(0)^{-1}.S \in K[X]$ olyan, hogy $S = P * Q$. Ha $\deg(P) > 0$, akkor a polinomok euklidészi osztásának tétele szerint léteznek olyan $Q, R \in K[X]$, hogy $S = P * Q + R$ és $\deg(R) < \deg(P)$. ■

14.8. Hányadosgyűrűk

14.8.1. Definíció. *Ha A kommutatív egységelemes gyűrű, akkor az $S \subseteq A$ halmazt* **multiplikatívnak** *nevezzük, ha minden S-ben haladó $(s_i)_{i\in I}$ véges rendszerre $\prod_{i\in I} s_i \in S$.*

Ha A kommutatív egységelemes gyűrű és $\cdot$ jelöli A szorzását, akkor a 12.5.4. állítást alkalmazva az $(A, \cdot)$ kommutatív monoidra kapjuk, hogy az $S \subseteq A$ halmaz multiplikativitása azzal ekvivalens, hogy $S \cdot S \subseteq S$ (vagyis minden $s, t \in S$ esetén $s \cdot t \in S$), és $1_A \in S$.

14.8.2. Tétel. *Legyen A kommutatív egységelemes gyűrű és $S \subseteq A$ multiplikatív halmaz.*

a) *Létezik olyan (B, π) pár, hogy teljesülnek a következők:*

– *B kommutatív egységelemes gyűrű és $\pi : A \to B$ olyan egységelem-tartó gyűrű-morfizmus, hogy $\pi\langle S\rangle \subseteq \mathbf{G}(B)$, vagyis minden $s \in S$ esetén $\pi(s)$ invertálható elem B-ben;*

– *minden C kommutatív egységelemes gyűrűhöz és minden $\sigma : A \to C$ egységelem-tartó gyűrű-morfizmushoz, ha $\sigma\langle S\rangle \subseteq \mathbf{G}(C)$, akkor létezik egyetlen olyan $\widetilde{\sigma} : B \to C$ egységelem-tartó gyűrű-morfizmus, hogy $\widetilde{\sigma} \circ \pi = \sigma$, vagyis a*

$$\begin{tikzcd} A \arrow[r, "\pi"] \arrow[dr, "\sigma"'] & B \arrow[d, "\widetilde{\sigma}"] \\ & C \end{tikzcd}$$

diagram kommutatív.

b) *Ha (A', π') és (A'', π'') olyan párok, amelyekre az a) állításban megfogalmazott tulajdonságok teljesülnek, ha abban (B, π) helyére (A', π')-t és (A'', π'')-t helyettesítjük, akkor létezik egyetlen olyan $\sigma : A' \to A''$ gyűrű-izomorfizmus, amelyre $\sigma \circ \pi' = \pi''$.*

Bizonyítás. a) Tekintsük az $A \times S$ szorzathalmaz felett azt a $\approx$ relációt, amelyre $(a, s), (a', s') \in A \times S$ esetén

$$(a, s) \approx (a', s') \quad \overset{\mathrm{df}}{\Leftrightarrow} \quad (\exists t \in S) \ \ (as' - a's)t = 0.$$

Először megmutatjuk, hogy $\approx$ ekvivalencia $A \times S$ felett.

Ha $(a, s) \in A \times S$, akkor $as - as = 0$, ezért *minden* $t \in S$ esetén $(as - as)t = 0$, és mivel $S \neq \emptyset$, így *létezik* olyan $t \in S$, amelyre $(as - as)t = 0$, vagyis $(a, s) \approx (a, s)$. Ezért az $\approx$ reláció reflexív az $A \times S$ halmaz felett.

Ha $(a, s), (a', s') \in A \times S$ és $(a, s) \approx (a', s')$, akkor létezik olyan $t \in S$, amelyre

$(as' - a's)t = 0$, ezért $0 = -(as' - a's)t = (a's - as')t$, így $(a', s') \approx (a, s)$. Ezért az $\approx$ reláció szimmetrikus.

Legyenek $(a, s), (a', s'), (a'', s'') \in A \times S$ és tegyük fel, hogy $(a, s) \approx (a', s')$ és $(a', s') \approx (a'', s'')$. Vegyünk olyan $t, t' \in S$ elemeket, amelyekre $(as' - a's)t = 0$ és $(a's'' - a''s')t' = 0$. Az első egyenlőséget jobbról $s''t'$-vel szorozva és a második egyenlőséget jobbról st-vel szorozva, valamint kihasználva az A szorzásának asszociativitását és kommutativitását, valamint a szorzás kivonásra vonatkozó disztributivitását kapjuk, hogy

$$\begin{aligned} 0 &= ((as' - a's)t)(s''t') = (as'')(ts't') - (a'sts''t'), \\ 0 &= ((a's'' - a''s')t')(st) = (a's''t'st) - (a''s)(s't't). \end{aligned}$$

Ezt a két egyenlőséget összeadva, és felhasználva azt, hogy $a'sts''t' = a's''t'st$ adódik a

$$0 = (as'')(ts't') - (a''s)(s't't) = (as'' - a''s)(ts't)$$

összefüggés, hiszen $ts't' = s't't$, és ismét alkalmazhatjuk az A szorzásának kivonásra vonatkozó disztributivitását. Az S halmaz multiplikativitása miatt $t'' := ts't' \in S$ és az előzőek szerint $(as'' - a''s)t'' = 0$, így $(a, s) \approx (a'', s'')$. Ezért az $\approx$ reláció tranzitív.

Most bevezetjük az

$$S^{-1}A := (A \times S)/ \approx$$

faktorhalmazt és megállapodunk abban, hogy minden $(a, s) \in A \times S$ esetén az (a, s) pár $\approx$ ekvivalencia szerinti ekvivalencia-osztályát a/s fogja jelölni, vagyis

$$a/s \;:=\; \{\, (a', s') \in A \times S \mid (\exists t \in S) \;\; (as' - a's)t = 0 \,\}.$$

Továbbá, vezessük be a

$$\pi_S : A \to S^{-1}A; \quad a \mapsto a/1$$

leképezést, ami $1 \in S$ miatt értelmes.

Megmutatjuk, hogy létezik egyetlen olyan

$$+ : (S^{-1}A) \times (S^{-1}A) \to S^{-1}A$$

művelet, amelyre teljesül az, hogy minden $(a, s), (b, t) \in A \times S$ esetén

$$(a/s) + (b/t) = (at + bs)/(st).$$

Ehhez azt szükséges és elégséges igazolni, hogy $(a, s), (a', s'), (b, t), (b', t') \in A \times S$ esetén, ha $a/s = a'/s'$ és $b/t = b'/t'$, akkor $(at + bs)/(st) = (a't' + b's')/(s't')$. A hipotézis alapján vehetünk olyan $u, v \in S$ elemeket, amelyekre $(as' - a's)u = 0$ és $(bt' - b't)v = 0$. Szorozva az első egyenlőséget vtt'-vel és szorozva a második egyenlőséget uss'-vel, továbbá kihasználva az A gyűrű szorzásának asszociativitását kapjuk, hogy

$$\begin{aligned} 0 &= ((as' - a's)u)(vtt') = (as' - a's)(uvtt'), \\ 0 &= ((bt' - b't)v)(uss') = (bt' - b't)(vuss'), \end{aligned}$$

amiből az A gyűrű szorzásának asszciativitása és kommutativitása, valamint a gyűrűkre vonatkozó disztributivitás-formulák alapján következik, hogy

$$\begin{aligned} &((at + bs)(s't') - (a't' + b's')(st))(uv) = \\ &= ((as')(uvtt') + (bt')(ss'uv)) - ((a's)(t'tuv)) + (b't)(s'suv)) = \\ &= ((as')(uvtt') - (a's)(t'tuv)) + ((bt')(ss'uv) - (b't)(s'suv)) = \\ &= (as' - a's)(uvtt') + (bt' - bt')(vuss') = 0. \end{aligned}$$

Az S halmaz multiplikativitása miatt $uv \in S$, tehát $(at+bs, st) \approx (a't'+b's', s't')$, ezért $(at+bs)/(st) = (a't'+b's')/(s't')$.

Megmutatjuk, hogy létezik egyetlen olyan

$$\cdot : (S^{-1}A) \times (S^{-1}A) \to S^{-1}A$$

művelet, amelyre teljesül az, hogy minden $(a,s),(b,t) \in A \times S$ esetén

$$(a/s) \cdot (b/t) = (ab)/(st).$$

Ehhez azt szükséges és elégséges igazolni, hogy $(a,s),(a',s'),(b,t),(b',t') \in A \times S$ esetén, ha $a/s = a'/s'$ és $b/t = b'/t'$, akkor $(ab)/(st) = (a'b')/(s't')$. A hipotézis alapján vehetünk olyan $u, v \in S$ elemeket, amelyekre $(as'-a's)u = 0$ és $(bt'-b't)v = 0$. Kihasználva az A gyűrű szorzásának asszociativitását és kommutativitását, valamint az A szorzásának kivonásra vonatkozó disztributivitását kapjuk, hogy

$$\begin{aligned}((ab)(s't') - (a'b')(st))(vu) = (as')(bt'vu) - (a's)(b'tvu) \overset{(*)}{=} (as')(b'tvu) - (a's)(b'tvu) = \\ = (as'-a's)(b'tvu) = ((as'-a's)u)(b'tv) = 0(b'tv) = 0,\end{aligned}$$

ahol a $\overset{(*)}{=}$ egyenlőségnél felhasználtuk azt, hogy $(bt'-b't)v = 0$ következtében $bt'v = b'tv$. Az S halmaz multiplikativitása miatt $vu \in S$, tehát $(ab, st) \approx (a'b', s't')$, ezért $(ab)/(st) = (a'b')/(s't')$.

Bebizonyítjuk, hogy az $(S^{-1}A, +, \cdot)$ hármas kommutatív egységelemes gyűrű.

Az $S^{-1}A$ halmaz feletti $+$ és $\cdot$ műveletek asszociatívak, mert $(a,s),(b,t),(c,u) \in A \times S$ esetén a definíciók és az A gyűrű műveleteinek asszociativitása, kommutativitása és az A gyűrű szorzásának összeadásra vonakozó disztributivitása szerint

$$\begin{aligned}((a/s) + (b/t)) + (c/u) = ((at+bs)/(st)) + (c/u) = ((at+bs)u + c(st))/((st)u) = \\ = (a(tu) + (bu+ct)s)/(s(tu)) = (a/s) + ((bu+ct)/(tu)) = (a/s) + ((b/t) + (c/u)),\end{aligned}$$

valamint

$$\begin{aligned}((a/s) \cdot (b/t)) \cdot (c/u) = ((ab)/(st)) \cdot (c/u) = ((ab)c))/((st)u) = \\ = (a(bc))/(s(tu)) = (a/s) \cdot ((bc)/(tu)) = (a/s) \cdot ((b/t) \cdot (c/u)).\end{aligned}$$

Az $S^{-1}A$ halmaz feletti $+$ és $\cdot$ műveletek kommutatívak, mert $(a,s),(b,t) \in A \times S$ esetén a definíciók és az A gyűrű műveleteinek kommutativitása szerint

$$(a/s) + (b/t) = (at+bs)/(st) = (bs+at)/(ts) = (b/t) + (a/s),$$

valamint

$$(a/s) \cdot (b/t) = (ab)/(st) = (ba)/(ts) = (b/t) + (a/s).$$

A $\mathbf{0} := 0/1 \in S^{-1}A$ elem neutrális az $S^{-1}A$ halmaz feletti $+$ műveletre nézve, mert $(a,s) \in A \times S$ esetén $(a/s) + (0/1) = (a1 + 0s)/(s1) = a/s$. Nyilvánvaló, hogy minden $s \in S$ esetén $0/1 = 0/s$, hiszen $0s - 01 = 0$, ezért bármely $t \in S$ esetén $(0s - 01)t = 0$, és $S \neq \emptyset$. Ebből következik, hogy ha $(a,s) \in A \times S$, akkor $(-a)s = -(as)$ miatt

$$(a/s) + ((-a)/s) = (as + (-a)s)/s = 0/s = 0/1 = \mathbf{0},$$

tehát $(-a)/s$ az a/s elem inverze az $S^{-1}A$ halmaz feletti $+$ műveletre nézve. Ezzel megmutatttuk, hogy az $(S^{-1}A, +)$ pár kommutatív csoport. Az $S^{-1}A$ halmaz feletti $\cdot$

művelet disztributív az $S^{-1}A$ halmaz feletti $+$ műveletre nézve. Ennek bizonyításához először megjegyezzük, hogy ha $a \in A$ és $s, t \in S$, akkor $(at)/(st) = a/s$, hiszen $(at)s - a(st) = 0$, így bármely $u \in S$ esetén $((at)s - a(st))u = 0$, és $S \neq \emptyset$. Ha most $(a, s), (b, t), (c, u) \in A \times S$, akkor

$$\begin{gathered}(a/s) \cdot (b/t) + (a/s) \cdot (c/u) = ((ab)/(st)) + ((ac)/(su)) = \\ = ((ab)(su) + (ac)(st))/((st)(su)) = (a(bu + ct)s)/(s(tu)s) = (a(bu + ct))/(s(tu)) = \\ = (a/s) \cdot ((bu + ct)/(tu)) = (a/s) \cdot ((b/t) + (c/u)).\end{gathered}$$

Világos, hogy az $\mathbf{1} := 1/1 \in S^{-1}A$ elem neutrális az $S^{-1}A$ halmaz feletti $\cdot$ műveletre nézve, mert $(a, s) \in A \times S$ esetén $(a/s) \cdot (1/1) = (a1)/(s1) = a/s$. Tehát az $(S^{-1}A, +\cdot)$ hármas egységelemes kommutatív gyűrű.

A $\pi_S : A \to S^{-1}A;\ a \mapsto a/1$ leképezés egységelem-tartó gyűrű-morfizmus, mert $a, b \in A$ esetén

$$\begin{gathered}\pi_S(a) + \pi_S(b) = (a/1) + (b/1) = (a1 + b1)/(11) = (a + b)/1 = \pi_S(a + b), \\ \pi_S(a) \cdot \pi_S(b) = (a/1) \cdot (b/1) = (ab)/(11) = (ab)/1 = \pi_S(ab),\end{gathered}$$

valamint $\pi_S(1) = 1/1 = \mathbf{1}$.

Ha $s \in S$, akkor $s/s = 1/1 = \mathbf{1}$, mert $s1 - 1s = 0$, így bármely $t \in S$ esetén $(s1 - 1s)t = 0$, és $S \neq \emptyset$. Ebből következik, hogy minden $s \in S$ esetén $(s/1) \cdot (1/s) = (s1)/(1s) = s/s = \mathbf{1}$, tehát a $\pi_S(s) \in S^{-1}A$ elem invertálható a $S^{-1}A$ halmaz feletti $\cdot$ műveletre nézve, vagyis $\pi_S\langle S\rangle \subseteq \mathbf{G}(S^{-1}A)$.

Legyen C kommutatív egységelemes gyűrű és $\pi : A \to C$ olyan egységelem-tartó gyűrű-morfizmus, amelyre $\pi\langle S\rangle \subseteq \mathbf{G}(C)$. Meg fogjuk mutatni, hogy egyértelműen létezik olyan $\widetilde{\pi} : S^{-1}A \to C$ egységelem-tartó gyűrű-morfizmus, amelyre $\widetilde{\pi} \circ \pi_S = \pi$, vagyis $\widetilde{\pi}$ kommutatívvá teszi a következő diagramot:

$$\begin{tikzcd} A \arrow[r, "\pi_S"] \arrow[dr, "\pi"'] & S^{-1}A \arrow[d, "\widetilde{\pi}"] \\ & C \end{tikzcd}$$

Először igazoljuk azt, hogy minden $(a, s), (a', s') \in A \times S$ esetén, ha $a/s = a'/s'$, akkor $\pi(a)\pi(s)^{-1} = \pi(a')\pi(s')^{-1}$, ahol $\pi(s)^{-1}$ (illetve $\pi(s')^{-1}$) a $\pi(s) \in \mathbf{G}(C)$ (illetve $\pi(s') \in \mathbf{G}(C)$) elem inverze C-ben. Valóban, a hipotézis szerint van olyan $t \in S$, hogy $(as' - a's)t = 0$, ezért $(\pi(a)\pi(s') - \pi(a')\pi(s))\pi(t) = 0$, amiből jobbról szorozva a $\pi(t)^{-1}$ elemmel adódik a $\pi(a)\pi(s') - \pi(a')\pi(s) = 0$ egyenlőség, és ezt jobbról szorozva a $\pi(s')^{-1}\pi(s)^{-1}$ elemmel és kihasználva C kommutativitását kapjuk a bizonyítandó egyenlőséget. Ebből következik, hogy létezik egyetlen olyan $\widetilde{\pi} : S^{-1}A \to C$ leképezés, amelyre teljesül az, hogy minden $(a, s) \in A \times S$ esetén

$$\widetilde{\pi}(a/s) = \pi(a)\pi(s)^{-1}.$$

Ez a $\widetilde{\pi}$ függvény egységelem-tartó gyűrű-morfizmus, mert minden $(a, s), (b, t) \in A \times S$ esetén a C gyűrű szorzásának asszociativitása és kommutativitása, valamint a C szorzásának összeadásra vonatkozó disztributivitása miatt

$$\begin{gathered}\widetilde{\pi}(a/s) + \widetilde{\pi}(b/t) = \pi(a)\pi(s)^{-1} + \pi(b)\pi(t)^{-1} = (\pi(a)\pi(t) + \pi(b)\pi(s))\pi(t)^{-1}\pi(s)^{-1} = \\ = \pi(at + bs)\pi(st)^{-1} = \widetilde{\pi}((at + bs)/(st)) = \widetilde{\pi}((a/s) + (b/t)),\end{gathered}$$

továbbá a C gyűrű szorzásának asszociativitása és kommutativitása miatt

$$\begin{aligned}\widetilde{\pi}(a/s)\cdot\widetilde{\pi}(b/t) &= \pi(a)\pi(s)^{-1}\pi(b)\pi(t)^{-1} = \pi(a)\pi(b)\pi(t)^{-1}\pi(s)^{-1} = \\ &= \pi(ab)\pi(st)^{-1} = \widetilde{\pi}((ab)/(st)) = \widetilde{\pi}((a/s)\cdot(b/t)),\end{aligned}$$

valamint $\widetilde{\pi}(1/1) = \pi(1)\pi(1)^{-1} = 1$.

Nyilvánvaló, hogy $a \in A$ esetén

$$(\widetilde{\pi}\circ\pi_S)(a) = \widetilde{\pi}(a/1) = \pi(a)\pi(1)^{-1} = \pi(a),$$

tehát $\widetilde{\pi}\circ\pi_S = \pi$.

Végül, tegyük fel, hogy $\widetilde{\pi}' : S^{-1}A \to C$ szintén olyan egységelem-tartó gyűrű-morfizmus, amelyre $\widetilde{\pi}'\circ\pi_S = \pi$, vagyis $\widetilde{\pi}$ kommutatívvá teszi a következő diagramot:

$$\begin{tikzcd} A \arrow[r, "\pi_S"] \arrow[dr, "\pi"'] & S^{-1}A \arrow[d, "\widetilde{\pi}'"] \\ & C \end{tikzcd}$$

Megmutatjuk, hogy ekkor $\widetilde{\pi} = \widetilde{\pi}'$. Valóban, ha $(a,s) \in A\times S$, akkor az $S^{-1}A$ gyűrű szorzásának definíciója szerint $(a/1)\cdot(1/s) = (a1)/(1s) = a/s$, valamint láttuk, hogy $1/s = \pi_S(s)^{-1}$ ezért

$$\begin{aligned}\widetilde{\pi}'(a/s) &= \widetilde{\pi}'((a/1)\cdot(1/s)) = \widetilde{\pi}'(a/1)\widetilde{\pi}'(1/s) = \\ &= \widetilde{\pi}'(\pi_S(a))\widetilde{\pi}'(\pi_S(s)^{-1}) = \pi(a)\pi(s)^{-1} = \widetilde{\pi}(a/s).\end{aligned}$$

b) Legyenek (A',π') és (A'',π'') olyan párok, amelyekre az a) állításban megfogalmazott tulajdonságok teljesülnek, ha abban (B,π) helyére az (A',π') és (A'',π'') párokat helyettesítjük.

Mivel a $\pi'' : A \to A''$ leképezés egységelem-tartó gyűrű-morfizmus, így az (A',π') párra előírt tulajdonság szerint létezik egyetlen olyan $\sigma : A' \to A''$ egységelem-tartó gyűrű-morfizmus, hogy az

$$\begin{tikzcd} A \arrow[r, "\pi'"] \arrow[dr, "\pi''"'] & A' \arrow[d, "\sigma"] \\ & A'' \end{tikzcd}$$

diagram kommutatív. Mivel a $\pi' : A \to A'$ leképezés egységelem-tartó gyűrű-morfizmus, így az (A'',π'') párra előírt tulajdonság szerint létezik egyetlen olyan $\sigma' : A'' \to A'$ egységelem-tartó gyűrű-morfizmus, hogy az

$$\begin{tikzcd} A \arrow[r, "\pi''"] \arrow[dr, "\pi'"'] & A'' \arrow[d, "\sigma'"] \\ & A' \end{tikzcd}$$

diagram kommutatív. Ekkor $\sigma'\circ\sigma : A' \to A'$ olyan egységelem-tartó gyűrű-morfizmus, hogy

$$(\sigma'\circ\sigma)\circ\pi' = \sigma'\circ(\sigma\circ\pi') = \sigma'\circ\pi'' = \pi',$$

vagyis $\sigma'\circ\sigma$ kommutatívvá teszi a következő diagramot:

$$\begin{tikzcd} A \arrow[r, "\pi'"] \arrow[dr, "\pi'"'] & A' \arrow[d, "\sigma'\circ\sigma"] \\ & A' \end{tikzcd}$$

Mivel a $\pi' : A \to A'$ leképezés egységelem-tartó gyűrű-morfizmus, így az (A', π') párra előírt tulajdonság szerint létezik egyetlen olyan $\tau : A' \to A'$ egységelem-tartó gyűrű-morfizmus, hogy $\tau \circ \pi' = \pi'$. De $\tau := \mathrm{id}_{A'}$ triviálisan ilyen tulajdonságú egységelem-tartó gyűrű-morfizmus, és az imént igazoltuk, hogy $\tau := \sigma' \circ \sigma$ is ilyen tulajdonságú egységelem-tartó gyűrű-morfizmus, ezért az egyértelműségi követelmény alapján $\sigma' \circ \sigma = \mathrm{id}_{A'}$.

Továbbá, $\sigma \circ \sigma' : A'' \to A''$ olyan egységelem-tartó gyűrű-morfizmus, hogy

$$(\sigma \circ \sigma') \circ \pi'' = \sigma \circ (\sigma' \circ \pi'') = \sigma \circ \pi' = \pi'',$$

vagyis $\sigma \circ \sigma'$ kommutatívvá teszi a következő diagramot:

$$\begin{tikzcd} A \arrow[r, "\pi''"] \arrow[dr, "\pi''"'] & A'' \arrow[d, "\sigma\circ\sigma'"] \\ & A'' \end{tikzcd}$$

Mivel a $\pi'' : A \to A''$ leképezés egységelem-tartó gyűrű-morfizmus, így az (A'', π'') párra előírt tulajdonság szerint létezik egyetlen olyan $\tau : A'' \to A''$ egységelem-tartó gyűrű-morfizmus, hogy $\tau \circ \pi'' = \pi''$. De $\tau := \mathrm{id}_{A''}$ triviálisan ilyen tulajdonságú egységelem-tartó gyűrű-morfizmus, és az imént igazoltuk, hogy $\tau := \sigma \circ \sigma'$ is ilyen tulajdonságú egységelem-tartó gyűrű-morfizmus, ezért az egyértelműségi követelmény alapján $\sigma \circ \sigma' = \mathrm{id}_{A''}$.

Ez azt jelenti, hogy $\sigma : A' \to A''$ bijektív egységelem-tartó gyűrű-morfizmus (és még azt is látjuk, hogy $\sigma^{-1} = \sigma'$), tehát σ olyan izomorfizmus az A' és A'' gyűrűk között, amelyre $\sigma \circ \pi' = \pi''$. Ha $\widetilde{\sigma} : A' \to A''$ szintén olyan izomorfizmus az A' és A'' gyűrűk között, amelyre $\widetilde{\sigma} \circ \pi' = \pi''$, akkor szükségképpen $\widetilde{\sigma} = \sigma$, hiszen ekkor $\widetilde{\sigma} : A' \to A''$ olyan egységelem-tartó gyűrű-morfizmus, hogy $\widetilde{\sigma} \circ \pi' = \pi''$, és az (A', π') párra vonatkozó feltétel szerint csak egyetlen ilyen létezhet, és a definíció szerint σ is ilyen tulajdonságú leképezés. ■

14.8.3. Definíció. *Az A kommutatív egységelemes gyűrű $S \subseteq A$ multiplikatív halmaz szerinti* **hányadosgyűrűjének** *nevezünk minden olyan (B, π) párt, amelyre a* 14.8.2. *tétel* a) *pontjában megfogalmazott tulajdonságok teljesülnek. A* 14.8.2. *tétel bizonyításában előállított $(S^{-1}A, \pi_S)$ párt az A gyűrű S szerinti* **standard hányadosgyűrűjének** *nevezzük.*

Tehát a 14.8.2. tétel a) pontja szerint *létezik* hányadosgyűrű, és a b) pontja szerint az *lényegében egyértelmű.*

Ha A kommutatív egységelemes gyűrű és $S \subseteq A$ multiplikatív halmaz, akkor a $\pi_S : A \to S^{-1}A$ egységelem-tartó gyűrű-morfizmus általában se nem injektív, se nem szürjektív. Pontosan a következő állítható.

14.8.4. Állítás. *Ha A kommutatív egységelemes gyűrű és $S \subseteq A$ multiplikatív halmaz, akkor a $\pi_S : A \to S^{-1}A$ egységelem-tartó gyűrű-morfizmusra*

$$\mathrm{Ker}(\pi_S) = \{ \ a \in A \mid (\exists s \in S) \ as = 0 \ \},$$
$$\mathrm{Im}(\pi_S) = \{ \ a/s \mid (\exists t \in S) \ st \mid at \ \}.$$

Bizonyítás. Ha $a \in A$, akkor

$$\pi_S(a) = \mathbf{0} \Leftrightarrow a/1 = 0/1 \Leftrightarrow (\exists s \in S) \ (a1 - 01)s = 0 \Leftrightarrow (\exists s \in S) \ as = 0.$$

Továbbá, $(a, s) \in A \times S$ esetén

$$a/s \in \mathrm{Im}(\pi_S) \Leftrightarrow (\exists a' \in A)\ a/s = a'/1 \Leftrightarrow (\exists a' \in A)(\exists t \in S)\ (a1 - a's)t = 0 \Leftrightarrow$$
$$\Leftrightarrow (\exists t \in S)(\exists a' \in A)\ a'(st) = at \Leftrightarrow (\exists t \in S)\ st \mid at. \blacksquare$$

Példák hányadosgyűrűkre.

1) Legyen A kommutatív egységelemes gyűrű és $S := \{1\}$. Ekkor S multiplikatív halmaz és a $\pi_S : A \to S^{-1}A$ leképezés *izomorfizmus* A és az $S^{-1}A$ hányadosgyűrű között. Valóban, az előző állítás szerint $\mathrm{Ker}(\pi_S) = \{a \in A | (\exists s \in S)\ as = 0\} = \{0\}$, ezért π_S injektív. Továbbá, minden $x \in S^{-1}A$ esetén van olyan $(a, s) \in A \times S$, hogy $x = a/s$, így $S := \{1\}$ miatt $x = a/1 = \pi_S(a)$, vagyis π_S szürjektív.

2) Legyen A kommutatív egységelemes gyűrű és $S \subseteq A$ multiplikatív halmaz. Ekkor

$$S^{-1}A = \{0\} \ \Leftrightarrow\ 0/1 = \mathbf{0} = \mathbf{1} = 1/1 \ \Leftrightarrow\ (\exists t \in S)\ (01 - 11)t = 0 \ \Leftrightarrow\ 0 \in S.$$

Tehát a $0 \notin S$ kijelentés ekvivalens azzal, hogy $S^{-1}A$ nemelfajult gyűrű.

3) Legyen A kommutatív egységelemes gyűrű és $\mathfrak{p} \subseteq A$ *prímideál.* Világos, hogy ekkor $S_\mathfrak{p} := A \setminus \mathfrak{p}$ multiplikatív halmaz. Az $S_\mathfrak{p}^{-1}A$ egységelemes kommutatív gyűrűt az $A_\mathfrak{p}$ szimbólummal jelöljük, és a $\mathfrak{p}$ prímideál által meghatározott **lokális gyűrűnek** nevezzük. Világos, hogy $0 \in \mathfrak{p}$ miatt $0 \notin S_\mathfrak{p}$, tehát 1) alapján $A_\mathfrak{p}$ nemelfajult gyűrű.

4) Legyen A *integritástartomány.* Ekkor A zérusosztómentessége miatt $S := A \setminus \{0\}$ multiplikatív halmaz, ezért elkészíthető az $S^{-1}A$ standard hányadosgyűrű.

14.8.5. Definíció. Lokális gyűrűnek *nevezünk minden olyan kommutatív egységelemes gyűrűt, amelyben létezik tartalmazás tekintetében legnagyobb valódi ideál.*

14.8.6. Állítás. *Ha A kommutatív egységelemes gyűrű, $\mathfrak{p} \subseteq A$ prímideál és $S_\mathfrak{p} := A \setminus \mathfrak{p}$, akkor a $\{p/s | (p, s) \in \mathfrak{p} \times S_\mathfrak{p}\}$ halmaz az $A_\mathfrak{p}$ gyűrűben tartalmazás tekintetében legnagyobb valódi ideál, tehát $A_\mathfrak{p}$ lokális gyűrű.*

Bizonyítás. Legyen $\widetilde{\mathfrak{p}} := \{p/s | (p, s) \in \mathfrak{p} \times S_\mathfrak{p}\}$. Először megmutatjuk, hogy $\widetilde{\mathfrak{p}}$ ideál az $A_\mathfrak{p}$ gyűrűben.

Világos, hogy $\mathfrak{p} \neq \emptyset$ és $\mathfrak{p} \neq A$ miatt $\widetilde{\mathfrak{p}} \neq \emptyset$. Ha $(p, s), (p', s') \in \mathfrak{p} \times S_\mathfrak{p}$, akkor $(p/s) + (p'/s') = (ps' + p's)/(ss') \in \widetilde{\mathfrak{p}}$, mert $ps' + p's \in \mathfrak{p}A + \mathfrak{p}A \subseteq \mathfrak{p} + \mathfrak{p} \subseteq \mathfrak{p}$, hiszen $\mathfrak{p}$ ideál A-ban, és $ss' \in S_\mathfrak{p}$, hiszen $\mathfrak{p}$ prímideál A-ban. Ez azt jelenti, hogy $\widetilde{\mathfrak{p}} + \widetilde{\mathfrak{p}} \subseteq \widetilde{\mathfrak{p}}$. Ha $(p, s) \in \mathfrak{p} \times S_\mathfrak{p}$ és $(a, t) \in A \times S_\mathfrak{p}$, akkor $(p/s)(a/t) = (pa)/(st) \in \widetilde{\mathfrak{p}}$, mert $pa \in \mathfrak{p}A \subseteq \mathfrak{p}$ és $st \in S_\mathfrak{p}$. Ez azt jelenti, hogy $\widetilde{\mathfrak{p}}A_\mathfrak{p} \subseteq \widetilde{\mathfrak{p}}$. Tehát $\widetilde{\mathfrak{p}}$ ideál az $A_\mathfrak{p}$ gyűrűben.

A $\widetilde{\mathfrak{p}}$ ideál valódi, mert ha $1/1 \in \widetilde{\mathfrak{p}}$ teljesülne, akkor létezne olyan $p \in \mathfrak{p}$ és $s \in S_\mathfrak{p}$, hogy $1/1 = p/s$, és ekkor létezne olyan $t \in S_\mathfrak{p}$, amelyre $(1s - p1)t = 0$, azaz $st = pt$ teljesülne, ami lehetetlen, mert $st \in S_\mathfrak{p} = A \setminus \mathfrak{p}$ és $pt \in \mathfrak{p}A \subseteq \mathfrak{p}$.

Megmutatjuk, hogy ha $\mathfrak{m} \subseteq A$ tetszőleges valódi ideál, akkor $\mathfrak{m} \subseteq \widetilde{\mathfrak{p}}$. Legyen ugyanis $(a, s) \in A \times S_\mathfrak{p}$ olyan pár, amelyre $a/s \in \mathfrak{m}$. Ekkor $a/s = (a/1)(1/s) = (a/1)(s/1)^{-1}$ miatt $a/1 = (a/s)(s/1) \in \mathfrak{m}A \subseteq \mathfrak{m}$, tehát $a/1 \in \mathfrak{m}$. Ha $a \notin \mathfrak{p}$, akkor $a \in S_\mathfrak{p}$, következésképpen $a/1 \in \mathbf{G}(A_\mathfrak{p}) \cap \mathfrak{m}$, ezért $\mathfrak{m} = A$, vagyis $\mathfrak{m}$ nem valódi ideál. Ezért $a \in \mathfrak{p}$, vagyis $a/1 \in \widetilde{\mathfrak{p}}$, amiből következik, hogy $a/s = (a/1)(1/s) \in \widetilde{\mathfrak{p}}A_\mathfrak{p} \subseteq \widetilde{\mathfrak{p}}$. Tehát $\mathfrak{m} \subseteq \widetilde{\mathfrak{p}}$, ami azt jelenti, hogy $\widetilde{\mathfrak{p}}$ az $A_\mathfrak{p}$ gyűrűben tartalmazás tekintetében legnagyobb valódi ideál. $\blacksquare$

14.8.7. Állítás. *Ha A integritástartomány és $S := A \setminus \{0\}$, akkor az $S^{-1}A$ hányadosgyűrű test, és a $\pi_S : A \to S^{-1}A$ leképezés injektív gyűrű-morfizmus.*

Bizonyítás. Azt kell igazolni, hogy ha $a \in A$ és $s \in A \setminus \{0\}$ és $a/s \neq \mathbf{0}$, akkor a/s invertálható $S^{-1}A$-ben. Mivel $\mathbf{0} = 0/1$, így az $a/s \neq \mathbf{0}$ feltétel azzal ekvivalens, hogy $a/s \neq 0/1$, vagyis nem létezik olyan $t \in A \setminus \{0\}$, amelyre $(a1 - 0s)t = 0$, vagyis $at = 0$ teljesülne. Ezért (a $t = 1$ választással) $a \neq 0$, így képezhető az $s/a \in S^{-1}A$ elem. Az $S^{-1}A$ gyűrű szorzásának értelmezése szerint $(a/s) \cdot (s/a) = (as)/(sa) = 1/1 = \mathbf{1}$, tehát a/s invertálható az $S^{-1}A$ hányadosgyűrűben.

Ha $a \in \mathrm{Ker}(\pi_S)$, akkor a 14.8.4. állítás szerint van olyan $s \in S$, hogy $as = 0$, tehát A zérusosztómentessége folytán $a = 0$ vagy $s = 0$, és mivel $s \in S = A \setminus \{0\}$, így szükségképpen $a = 0$, vagyis π_S injektív leképezés. ■

14.8.8. Definíció. *Ha A integritástartomány és $S := A \setminus \{0\}$, akkor az $S^{-1}A$ testet az A integritástartomány* **standard hányadostestének** *nevezzük.*

°Később látni fogjuk, hogy a $\mathbb{Z}$ integritástartomány standard hányadosteste *egyenlő* a racionális számok $\mathbb{Q}$ testével.$_\circ$

15. fejezet

Gyűrű feletti mátrixok

15.1. Mátrixok és műveletek gyűrű feletti mátrixokkal

15.1.1. Definíció. *Legyenek I, J, F halmazok.*

– $\mathrm{M}_{I,J}(F)$ *jelöli az $I \times J \to F$ függvények halmazát, és $\mathrm{M}_{I,J}(F)$ elemeit F* **feletti $I \times J$-es mátrixoknak** *nevezzük.*

– *Ha $\mathbf{a} \in \mathrm{M}_{I,J}(F)$, akkor $(i,j) \in I \times J$ esetén $\mathbf{a}(i,j)$ helyett az $\mathbf{a}_{i,j}$ jelölést is alkalmazzuk, és az $\mathbf{a}_{i,j} \in F$ elemet az $\mathbf{a}$ mátrix* **(i,j)-edik komponensének** *nevezzük.*

– *Ha $\mathbf{a} \in \mathrm{M}_{I,J}(F)$, akkor minden $i \in I$ esetén az $(\mathbf{a}_{i,j})_{j \in J}$ rendszert az $\mathbf{a}$ mátrix* **i-edik sorának** *és minden $j \in J$ esetén az $(\mathbf{a}_{i,j})_{i \in I}$ rendszert az $\mathbf{a}$ mátrix* **j-edik oszlopának** *nevezzük.*

Megállapodunk abban, hogy ha F és I halmazok, akkor az $\mathrm{M}_{I,I}(F)$ halmazt az $\mathrm{M}_I(F)$ szimbólummal jelöljük, és $\mathrm{M}_I(F)$ elemeit F feletti $I \times I$-es **négyzetes mátrixoknak** nevezzük.

15.1.2. Definíció. *Legyen A gyűrű és legyenek I és J halmazok.*

– *Ha $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ és $\lambda \in A$, akkor $\lambda.\mathbf{a}$ jelöli azt az $I \times J \to A$ függvényt, amelyre minden $(i,j) \in I \times J$ esetén*

$$(\lambda.\mathbf{a})_{i,j} := \lambda \mathbf{a}_{i,j},$$

és az $\lambda.\mathbf{a} \in \mathrm{M}_{I,J}(A)$ mátrixot a λ elem és az $\mathbf{a}$ mátrix **szorzatának** *nevezzük.*

– *Ha $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ és $\mathbf{b} \in \mathrm{M}_{I,J}(A)$, akkor $\mathbf{a}+\mathbf{b}$ jelöli azt az $I \times J \to A$ függvényt, amelyre minden $(i,j) \in I \times J$ esetén*

$$(\mathbf{a}+\mathbf{b})_{i,j} := \mathbf{a}_{i,j} + \mathbf{b}_{i,j},$$

és az $\mathbf{a}+\mathbf{b} \in \mathrm{M}_{I,J}(A)$ mátrixot az $\mathbf{a}$ és $\mathbf{b}$ mátrixok **összegének** *nevezzük.*

15.1.3. Állítás. *Ha A gyűrű és I, J halmazok, akkor az*

$$\mathrm{M}_{I,J}(A) \times \mathrm{M}_{I,J}(A) \to \mathrm{M}_{I,J}(A); \quad (\mathbf{a},\mathbf{b}) \mapsto \mathbf{a}+\mathbf{b}$$

leképezés kommutatív csoportművelet az $\mathrm{M}_{I,J}(A)$ halmaz felett.

Bizonyítás. Ha $\mathbf{a},\mathbf{b},\mathbf{c} \in \mathrm{M}_{I,J}(A)$, akkor minden $(i,j) \in I \times J$ esetén az A gyűrű összeadásának asszociativitása miatt:

$$((\mathbf{a}+\mathbf{b})+\mathbf{c})_{i,j} = (\mathbf{a}+\mathbf{b})_{i,j} + \mathbf{c}_{i,j} = (\mathbf{a}_{i,j} + \mathbf{b}_{i,j}) + \mathbf{c}_{i,j} =$$
$$= \mathbf{a}_{i,j} + (\mathbf{b}_{i,j} + \mathbf{c}_{i,j}) = \mathbf{a}_{i,j} + (\mathbf{b}+\mathbf{c})_{i,j} = (\mathbf{a}+(\mathbf{b}+\mathbf{c}))_{i,j},$$

tehát $(\mathbf{a}+\mathbf{b})+\mathbf{c}=\mathbf{a}+(\mathbf{b}+\mathbf{c})$, vagyis az $\mathrm{M}_{I,J}(A)$ halmazon értelmezett összeadás asszociatív.

Ha $\mathbf{a},\mathbf{b}\in\mathrm{M}_{I,J}(A)$, akkor minden $(i,j)\in I\times J$ esetén $(\mathbf{a}+\mathbf{b})_{i,j}=\mathbf{a}_{i,j}+\mathbf{b}_{i,j}=\mathbf{b}_{i,j}+\mathbf{a}_{i,j}=(\mathbf{b}+\mathbf{a})_{i,j}$, tehát $\mathbf{a}+\mathbf{b}=\mathbf{b}+\mathbf{a}$, vagyis az $\mathrm{M}_{I,J}(A)$ halmazon értelmezett összeadás kommutatív.

Jelölje $\mathbf{0}$ azt az elemet $\mathrm{M}_{I,J}(A)$-ben, amelyre minden $(i,j)\in I\times J$ esetén $\mathbf{0}_{i,j}:=0$. Ekkor minden $\mathbf{a}\in\mathrm{M}_{I,J}(A)$ mátrixra, minden $(i,j)\in I\times J$ esetén

$$(\mathbf{a}+\mathbf{0})_{i,j}=\mathbf{a}_{i,j}+\mathbf{0}_{i,j}=\mathbf{a}_{i,j}+0=\mathbf{a}_{i,j},$$

tehát $\mathbf{a}+\mathbf{0}=\mathbf{a}$, így az $\mathrm{M}_{I,J}(A)$ halmazon értelmezett összeadás kommutativitása miatt $\mathbf{0}$ neutrális eleme az $\mathrm{M}_{I,J}(A)$ halmazon értelmezett összeadás.

Legyen $\mathbf{a}\in\mathrm{M}_{I,J}(A)$ és értelmezzük azt a $-\mathbf{a}\in\mathrm{M}_{I,J}(A)$ mátrixot, amelyre minden $(i,j)\in I\times J$ esetén $(-\mathbf{a})_{i,j}:=-(\mathbf{a}_{i,j})$. Ekkor minden $(i,j)\in I\times J$ esetén $(\mathbf{a}+(-\mathbf{a}))_{i,j}=\mathbf{a}_{i,j}+(-\mathbf{a})_{i,j}=\mathbf{a}_{i,j}+(-\mathbf{a}_{i,j})=\mathbf{0}$, tehát $\mathbf{a}+(-\mathbf{a})=\mathbf{0}$, így az $\mathrm{M}_{I,J}(A)$ halmazon értelmezett összeadás kommutativitása miatt $-\mathbf{a}$ az $\mathbf{a}$ elem inverze az $\mathrm{M}_{I,J}(A)$ halmazon értelmezett összeadás szerint. ■

15.1.4. Állítás. *Ha A gyűrű és I, J halmazok, akkor minden $\lambda,\sigma\in A$ és $\mathbf{a},\mathbf{b}\in\mathrm{M}_{I,J}(A)$ esetén*

$$(\lambda\sigma).\mathbf{a}=\lambda.(\sigma.\mathbf{a}),$$
$$(\lambda+\sigma).\mathbf{a}=\lambda.\mathbf{a}+\sigma.\mathbf{a},$$
$$\lambda.(\mathbf{a}+\mathbf{b})=\lambda.\mathbf{a}+\lambda.\mathbf{b},$$

és ha A egységelemes, akkor minden $\mathbf{a}\in\mathrm{M}_{I,J}(A)$ esetén

$$1_A.\mathbf{a}=\mathbf{a}.$$

Bizonyítás. Legyenek $\lambda,\sigma\in A$ és $\mathbf{a},\mathbf{b}\in\mathrm{M}_{I,J}(A)$.

Ha $(i,j)\in I\times J$, akkor a definíció és A szorzásának asszociativitása szerint

$$((\lambda\sigma).\mathbf{a})_{i,j}=(\lambda\sigma)\mathbf{a}_{i,j}=\lambda(\sigma\mathbf{a}_{i,j})=\lambda(\sigma.\mathbf{a})_{i,j}=(\lambda.(\sigma.\mathbf{a}))_{i,j},$$

ezért $(\lambda\sigma).\mathbf{a}=\lambda.(\sigma.\mathbf{a})$.

Ha $(i,j)\in I\times J$, akkor a definíciók és A szorzásának az összeadásra vonatkozó disztributivitása szerint

$$((\lambda+\sigma).\mathbf{a})_{i,j}=(\lambda+\sigma)\mathbf{a}_{i,j}=\lambda\mathbf{a}_{i,j}+\sigma\mathbf{a}_{i,j}=(\lambda.\mathbf{a})_{i,j}+(\sigma.\mathbf{a})_{i,j}=(\lambda.\mathbf{a}+\sigma.\mathbf{a})_{i,j},$$

ezért $(\lambda+\sigma).\mathbf{a}=\lambda.\mathbf{a}+\sigma.\mathbf{a}$.

Ha $(i,j)\in I\times J$, akkor a definíciók és A szorzásának az összeadásra vonatkozó disztributivitása szerint

$$(\lambda.(\mathbf{a}+\mathbf{b}))_{i,j}=\lambda(\mathbf{a}+\mathbf{b})_{i,j}=\lambda(\mathbf{a}_{i,j}+\mathbf{b}_{i,j})=\lambda\mathbf{a}_{i,j}+\lambda\mathbf{b}_{i,j}=(\lambda.\mathbf{a})_{i,j}+(\lambda.\mathbf{b})_{i,j}=(\lambda.\mathbf{a}+\lambda.\mathbf{b})_{i,j},$$

ezért $\lambda.(\mathbf{a}+\mathbf{b})=\lambda.\mathbf{a}+\lambda.\mathbf{b}$.

Ha A egységelemes és $\mathbf{a}\in\mathrm{M}_{I,J}(A)$, akkor minden $(i,j)\in I\times J$ esetén a definíció szerint

$$(1_A.\mathbf{a})_{i,j}=1_A\mathbf{a}_{i,j}=\mathbf{a}_{i,j},$$

ezért $1_A.\mathbf{a}=\mathbf{a}$. ■

15.1.5. Definíció. *Legyen A gyűrű és legyenek I, J halmazok. Ekkor*

$$\dot{\mathrm{M}}_{I,J}(A) \;:=\; \{\ \mathbf{a} \in \mathrm{M}_{I,J}(A) \mid (\forall j \in J) : (\mathbf{a}_{i,j})_{i\in I} \in A^{(I)}\ \},$$

vagyis $\dot{\mathrm{M}}_{I,J}(A)$ azon $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ mátrixok halmaza, amelyekre minden $j \in J$ esetén az $\{i \in I | \mathbf{a}_{i,j} \neq 0_A\}$ halmaz véges. Az $\dot{\mathrm{M}}_{I,I}(A)$ szimbólum helyett az $\dot{\mathrm{M}}_I(A)$ rövidítést alkalmazzuk.

Nyilvánvaló, hogy ha A gyűrű és I *véges* halmaz, akkor minden J halmazra $\dot{\mathrm{M}}_{I,J}(A) = \mathrm{M}_{I,J}(A)$.

15.1.6. Állítás. *Legyen A gyűrű és legyenek I, J halmazok. Ekkor $\dot{\mathrm{M}}_{I,J}(A)$ olyan részcsoportja az $(\mathrm{M}_{I,J}(A), +)$ additív csoportnak, amelyre minden $\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$ és $\lambda \in A$ esetén $\lambda.\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$.*

Bizonyítás. Ha $\mathbf{a}, \mathbf{b} \in \dot{\mathrm{M}}_{I,J}(A)$, akkor minden $j \in J$ esetén $I_j(\mathbf{a}) := \{i \in I | \mathbf{a}_{i,j} \neq 0_A\}$ és $I_j(\mathbf{b}) := \{i \in I | \mathbf{b}_{i,j} \neq 0_A\}$ véges halmazok, ezért $I_j(\mathbf{a}) \cup I_j(\mathbf{b})$ is véges, és nyilvánvalóan $\{i \in I | (\mathbf{a}+\mathbf{b})_{i,j} \neq 0_A\} = \{i \in I | \mathbf{a}_{i,j} + \mathbf{b}_{i,j} \neq 0_A\} \subseteq I_j(\mathbf{a}) \cup I_j(\mathbf{b})$, így $\mathbf{a}+\mathbf{b} \in \dot{\mathrm{M}}_{I,J}(A)$.

Ha $\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$, akkor minden $j \in J$ esetén $\{i \in I | (-\mathbf{a})_{i,j} \neq 0_A\} = \{i \in I | -\mathbf{a}_{i,j} \neq 0_A\} = \{i \in I | \mathbf{a}_{i,j} \neq 0_A\}$, tehát $-\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$. Világos, hogy $\dot{\mathrm{M}}_{I,J}(A) \neq \emptyset$, ezért az előzőek szerint $\dot{\mathrm{M}}_{I,J}(A)$ részcsoportja az $(\mathrm{M}_{I,J}(A), +)$ additív csoportnak.

Ha $\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$ és $\lambda \in A$, akkor minden $j \in J$ esetén $\{i \in I | (\lambda.\mathbf{a})_{i,j} \neq 0_A\} = \{i \in I | \lambda.\mathbf{a}_{i,j} \neq 0_A\} \subseteq \{i \in I | \mathbf{a}_{i,j} \neq 0_A\}$, és $\{i \in I | \mathbf{a}_{i,j} \neq 0_A\}$ véges halmaz, ezért $\lambda.\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$. ■

15.1.7. Lemma. *Legyen A gyűrű és legyenek I, J, K halmazok. Ha $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ és $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$, akkor minden $(i,k) \in I \times K$ esetén $\{j \in J | \mathbf{a}_{i,j}\mathbf{b}_{j,k} \neq 0_A\}$ véges halmaz, tehát jól értelmezett a*

$$\left(\sum_{j\in J} \mathbf{a}_{i,j}\mathbf{b}_{j,k}\right)_{(i,k)\in I\times K} \in \mathrm{M}_{I,K}(A)$$

mátrix, és ha $\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$ is teljesül, akkor

$$\left(\sum_{j\in J} \mathbf{a}_{i,j}\mathbf{b}_{j,k}\right)_{(i,k)\in I\times K} \in \dot{\mathrm{M}}_{I,K}(A).$$

Bizonyítás. Ha $(i,k) \in I \times K$, akkor $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$ miatt $\{j \in J | \mathbf{b}_{j,k} \neq 0_A\}$ véges halmaz, és nyilvánvalóan $\{j \in J | \mathbf{a}_{i,j}\mathbf{b}_{j,k} \neq 0_A\} \subseteq \{j \in J | \mathbf{b}_{j,k} \neq 0_A\}$, ezért jól értelmezett a $\sum_{j\in J} \mathbf{a}_{i,j}\mathbf{b}_{j,k}$ összeg az $(A, +)$ monoidban (12.5.3.).

Tegyük fel, hogy $\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$. Rögzítsünk egy $k \in K$ indexet. Ekkor a $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$ feltételből következik, hogy $J_k := \{j \in J | \mathbf{b}_{j,k} \neq 0_A\}$ véges részhalmaza J-nek, és $\mathbf{a} \in \dot{\mathrm{M}}_{I,J}(A)$ miatt minden $j \in J$ esetén $I_j := \{i \in I | \mathbf{a}_{i,j} \neq 0_A\}$ véges részhalmaza I-nek. Ekkor $I_* := \bigcup_{j\in J_k} I_j$ véges halmaz, hiszen egyenlő véges sok véges halmaz uniójával, és nyilvánvaló, hogy $\left\{i \in I \;\middle|\; \sum_{j\in J} \mathbf{a}_{i,j}\mathbf{b}_{j,k} \neq 0_A\right\} \subseteq I_*$, tehát a tartalmazás bal oldalán álló halmaz is véges. ■

15.1.8. Definíció. *Legyen A gyűrű és legyenek I, J, K halmazok. Ha $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ és $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$, akkor $\mathbf{a}\cdot\mathbf{b}$ jelöli azt az $I\times K \to A$ függvényt, amelyre minden $(i,k) \in I\times K$ esetén*

$$(\mathbf{a}\cdot\mathbf{b})_{i,k} := \sum_{j\in J} \mathbf{a}_{i,j}\mathbf{b}_{j,k},$$

és az $\mathbf{a}\cdot\mathbf{b} \in \mathrm{M}_{I,K}(A)$ mátrixot az $\mathbf{a}$ és $\mathbf{b}$ **mátrixok szorzatának** *nevezzük. Továbbá, az*

$$\mathrm{M}_{I,J}(A) \times \dot{\mathrm{M}}_{J,K}(A) \to \mathrm{M}_{I,K}(A); \quad (\mathbf{a},\mathbf{b}) \mapsto \mathbf{a}\cdot\mathbf{b}$$

leképezést **mátrixszorzásnak** *nevezzük.*

15.1.9. Állítás. *Legyen A gyűrű és legyenek I, J, K, L halmazok. Ha $\mathbf{a} \in \mathrm{M}_{I,J}(A)$, $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$ és $\mathbf{c} \in \dot{\mathrm{M}}_{K,L}(A)$, akkor*

$$\mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c}) = (\mathbf{a}\cdot\mathbf{b})\cdot\mathbf{c}.$$

Bizonyítás. Legyen $(i,l) \in I \times L$ rögzítve. Ekkor

$$(\mathbf{a}\cdot(\mathbf{b}\cdot\mathbf{c}))_{i,l} = \sum_{j\in J}\mathbf{a}_{i,j}(\mathbf{b}\cdot\mathbf{c})_{j,l} = \sum_{j\in J}\mathbf{a}_{i,j}\Big(\sum_{k\in K}\mathbf{b}_{j,k}\mathbf{c}_{k,l}\Big) \overset{(1)}{=}$$
$$\overset{(1)}{=} \sum_{j\in J}\Big(\sum_{k\in K}\mathbf{a}_{i,j}(\mathbf{b}_{j,k}\mathbf{c}_{k,l})\Big) \overset{(2)}{=} \sum_{j\in J}\Big(\sum_{k\in K}(\mathbf{a}_{i,j}\mathbf{b}_{j,k})\mathbf{c}_{k,l}\Big) \overset{(3)}{=} \sum_{k\in K}\Big(\sum_{j\in J}(\mathbf{a}_{i,j}\mathbf{b}_{j,k})\mathbf{c}_{k,l}\Big) \overset{(4)}{=}$$
$$\overset{(4)}{=} \sum_{k\in K}\Big(\Big(\sum_{j\in J}\mathbf{a}_{i,j}\mathbf{b}_{j,k}\Big)\mathbf{c}_{k,l}\Big) = \sum_{k\in K}(\mathbf{a}\cdot\mathbf{b})_{i,k}\mathbf{c}_{k,l} = ((\mathbf{a}\cdot\mathbf{b})\cdot\mathbf{c})_{i,l},$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk azt, hogy az A gyűrű szorzása balról disztributív az összeadásra nézve, és alkalmaztuk a 12.5.15. állítást, ahol $\perp$ az A gyűrű összeadása és $\top$ az A gyűrű szorzása;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk A szorzásának asszociativitását;

– a $\overset{(3)}{=}$ egyenlőségnél a 12.5.11. állításra hivatkozva felcseréltük a J és K halmazon való összegzések sorrendjét, ami azért lehetséges, mert $\mathbf{c} \in \dot{\mathrm{M}}_{K,L}(A)$ miatt $K_l := \{k \in K | \mathbf{c}_{k,l} \neq 0_A\}$ véges halmaz, és $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$ miatt minden $k \in K$ esetén $J_k := \{j \in J | \mathbf{b}_{j,k} \neq 0_A\}$ is véges halmaz, következésképpen $\Big(\bigcup_{k\in K_l} J_k\Big) \times K_l$ véges halmaz és ez nyilvánvalóan tartalmazza a $\{(j,k) \in J \times K | (\mathbf{a}_{i,j}\mathbf{b}_{j,k})\mathbf{c}_{k,l} \neq 0_A\}$ halmazt, tehát ez utóbbi halmaz is véges;

– a $\overset{(4)}{=}$ egyenlőségnél felhasználtuk azt, hogy az A gyűrű szorzása jobbról disztributív az összeadásra nézve, és ismét alkalmaztuk a 12.5.15. állítást, ahol $\perp$ az A gyűrű összeadása és $\top$ az A gyűrű szorzása;

továbbá, a jelöletlen egyenlőségeknél a mátrixszorzás definícióját alkalmaztuk. ∎

15.1.10. Lemma. *Legyen A gyűrű és legyenek I, J, K halmazok.*

a) *Ha $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ és $\mathbf{b}, \mathbf{c} \in \dot{\mathrm{M}}_{J,K}(A)$, akkor*

$$\mathbf{a}\cdot(\mathbf{b}+\mathbf{c}) = (\mathbf{a}\cdot\mathbf{b}) + (\mathbf{a}\cdot\mathbf{c}).$$

b) *Ha $\mathbf{a}, \mathbf{b} \in \mathrm{M}_{I,J}(A)$ és $\mathbf{c} \in \dot{\mathrm{M}}_{J,K}(A)$, akkor*

$$(\mathbf{a}+\mathbf{b})\cdot\mathbf{c} = (\mathbf{a}\cdot\mathbf{c}) + (\mathbf{b}\cdot\mathbf{c}).$$

Bizonyítás. a) Legyen $(i,k) \in I \times K$ rözítve. Ekkor

$$(\mathbf{a}\cdot(\mathbf{b}+\mathbf{c}))_{i,k}=\sum_{j\in J}\mathbf{a}_{i,j}(\mathbf{b}+\mathbf{c})_{j,k}=\sum_{j\in J}\mathbf{a}_{i,j}(\mathbf{b}_{j,k}+\mathbf{c}_{j,k})\overset{(1)}{=}\sum_{j\in J}((\mathbf{a}_{i,j}\mathbf{b}_{j,k})+(\mathbf{a}_{i,j}\mathbf{c}_{j,k}))\overset{(2)}{=}$$
$$\overset{(2)}{=}\Big(\sum_{j\in J}\mathbf{a}_{i,j}\mathbf{b}_{j,k}\Big)+\Big(\sum_{j\in J}\mathbf{a}_{i,j}\mathbf{c}_{j,k}\Big)=(\mathbf{a}\cdot\mathbf{b})_{i,k}+(\mathbf{a}\cdot\mathbf{c})_{i,k}=((\mathbf{a}\cdot\mathbf{b})+(\mathbf{a}\cdot\mathbf{c}))_{i,k},$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk azt, hogy az A gyűrű szorzása balról disztributív az összeadásra nézve;

– a $\overset{(2)}{=}$ egyenlőségnél alkalmaztuk a 12.5.8. állítást, ahol $\top$ az A gyűrű összeadása;

továbbá, a jelöletlen egyenlőségeknél a mátrixszorzás definícióját alkalmaztuk.

b) Legyen $(i,k) \in I \times K$ rözítve. Ekkor

$$((\mathbf{a}+\mathbf{b})\cdot\mathbf{c})_{i,k}=\sum_{j\in J}(\mathbf{a}+\mathbf{b})_{i,j}\mathbf{c}_{j,k}=\sum_{j\in J}(\mathbf{a}_{i,j}+\mathbf{b}_{i,j})\mathbf{c}_{j,k}\overset{(3)}{=}\sum_{j\in J}((\mathbf{a}_{i,j}\mathbf{c}_{j,l})+(\mathbf{b}_{i,j}\mathbf{c}_{j,k}))\overset{(4)}{=}$$
$$\overset{(4)}{=}\Big(\sum_{j\in J}\mathbf{a}_{i,j}\mathbf{c}_{j,k}\Big)+\Big(\sum_{j\in J}\mathbf{b}_{i,j}\mathbf{c}_{j,k}\Big)=(\mathbf{a}\cdot\mathbf{c})_{i,k}+(\mathbf{b}\cdot\mathbf{c})_{i,k}=((\mathbf{a}\cdot\mathbf{c})+(\mathbf{b}\cdot\mathbf{c}))_{i,k},$$

ahol

– az $\overset{(3)}{=}$ egyenlőségnél felhasználtuk azt, hogy az A gyűrű szorzása jobbról disztributív az összeadásra nézve;

– a $\overset{(4)}{=}$ egyenlőségnél alkalmaztuk a 12.5.8. állítást, ahol $\top$ az A gyűrű összeadása;

továbbá, a jelöletlen egyenlőségeknél a mátrixszorzás definícióját alkalmaztuk. ■

15.1.11. Tétel. *Ha A gyűrű és I halmaz, akkor az $\dot{\mathrm{M}}_I(A)$ halmaz a mátrixösszeadással és mátrixszorzással ellátva gyűrű, és ha A egységelemes, akkor ez a gyűrű is egyégelemes, és egységeleme az az* $\mathbf{1}$ *mátrix, amelyre minden $i,j \in I$ esetén*

$$\mathbf{1}_{i,j} := \begin{cases} 1_A & , \text{ ha } i=j, \\ 0_A & , \text{ ha } i\neq j. \end{cases}$$

Bizonyítás. A 15.1.6. állítás szerint az $\dot{\mathrm{M}}_I(A)$ halmazon a mátrixösszeadás kommutatív csoportművelet. A 15.1.7. állítás szerint $\dot{\mathrm{M}}_I(A)$ zárt a mátrixszorzásra nézve, és 15.1.9. alapján az $\dot{\mathrm{M}}_I(A)$ feletti mátrixszorzás asszociatív, és 15.1.10. alapján disztributív az $\dot{\mathrm{M}}_I(A)$ feletti mátrixösszeadásra nézve. Tehát $\dot{\mathrm{M}}_I(A)$ a mátrixösszeadással és mátrixszorzással ellátva gyűrű.

Tegyük fel, hogy A egységelemes gyűrű. Világos, hogy ekkor $\mathbf{1} \in \dot{\mathrm{M}}_I(A)$.

Minden $\mathbf{a} \in \dot{\mathrm{M}}_I(A)$ mátrixra, minden $(i,j) \in I \times I$ esetén

$$(\mathbf{a}\cdot\mathbf{1})_{i,j}=\sum_{k\in I}\mathbf{a}_{i,k}\mathbf{1}_{k,j}=\Big(\sum_{k\in I\setminus\{j\}}\mathbf{a}_{i,k}\mathbf{1}_{k,j}\Big)+\mathbf{a}_{i,j}\mathbf{1}_{j,j}=\mathbf{a}_{i,j},$$

ahol a 8.5.4. és 12.5.2. állításokat alkalmaztuk, ami indokolt, mert minden $k \in I \setminus \{j\}$ indexre $\mathbf{a}_{i,k}\mathbf{1}_{k,j} = \mathbf{a}_{i,k}0_A = 0_A$. Továbbá, minden $\mathbf{a} \in \dot{\mathrm{M}}_I(A)$ mátrixra, és minden $(i,j) \in I \times I$ párra

$$(\mathbf{1}\cdot\mathbf{a})_{i,j}=\sum_{k\in I}\mathbf{1}_{i,k}\mathbf{a}_{k,j}=\Big(\sum_{k\in I\setminus\{i\}}\mathbf{1}_{i,k}\mathbf{a}_{k,j}\Big)+\mathbf{1}_{i,i}\mathbf{a}_{i,j}=\mathbf{a}_{i,j},$$

ahol a 8.5.4. és 12.5.2. állításokat alkalmaztuk, ami indokolt, mert minden $k \in I \setminus \{j\}$ indexre $\mathbf{1}_{i,k}\mathbf{a}_{k,j} = 0_A\mathbf{a}_{i,k} = 0_A$. Ez azt jelenti, hogy minden $\mathbf{a} \in \dot{\mathrm{M}}_I(A)$ mátrixra $\mathbf{a} \cdot \mathbf{1} = \mathbf{a} = \mathbf{1} \cdot \mathbf{a}$, tehát $\mathbf{1}$ az $\dot{\mathrm{M}}_I(A)$ halmaz feletti szorzás neutrális eleme. ■

15.1.12. Definíció. *Ha A gyűrű és I halmaz, akkor a* 15.1.11. *tételben értelmezett* $(\dot{\mathrm{M}}_I(A), +, \cdot)$ *gyűrűt* **mátrixgyűrűnek** *nevezzük.*

Vigyázzunk arra, hogy ha A gyűrű, és I legalább két elemű véges halmaz, akkor $\mathrm{M}_I(A)$ felett a mátrixszorzás még akkor sem szükségképpen kommutatív, ha A kommutatív gyűrű.

Továbbá, ha A tetszőleges nemelfajult gyűrű, és I legalább két elemű halmaz, akkor az $\dot{\mathrm{M}}_I(A)$ mátrixgyűrű biztosan nem zérusosztómentes, mert ha $\lambda \in A$ és $\lambda \neq 0_A$, és $i_*, j_* \in I$ olyan indexek, hogy $i_* \neq j_*$, valamint $\mathbf{a}, \mathbf{b} \in \dot{\mathrm{M}}_I(A)$ azok a mátrixok, amelyre minden $(i,j) \in I \times I$ esetén

$$\mathbf{a}_{i,j} := \begin{cases} \lambda & \text{, ha } i = j = i_*, \\ 0_A & \text{, egyébként,} \end{cases}$$

$$\mathbf{b}_{i,j} := \begin{cases} \lambda & \text{, ha } i = j = j_*, \\ 0_A & \text{, egyébként,} \end{cases}$$

akkor könnyen látható, hogy $\mathbf{a} \cdot \mathbf{b} = \mathbf{0}$, de $\mathbf{a} \neq \mathbf{0} \neq \mathbf{b}$.

15.1.13. Állítás. *Legyen A gyűrű, és legyenek I, J, K halmazok. Ha $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ és $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$, akkor minden $\lambda \in A$ esetén*

$$(\lambda.\mathbf{a}) \cdot \mathbf{b} = \lambda.(\mathbf{a} \cdot \mathbf{b}),$$

és ha A kommutatív, akkor

$$\mathbf{a} \cdot (\lambda.\mathbf{b}) = \lambda.(\mathbf{a} \cdot \mathbf{b})$$

is teljesül.

Bizonyítás. Ha $(i,k) \in I \times K$, akkor a definíciók és A szorzásának asszociativitása és az összeadásra vonatkozó disztributivitása, valamint 12.5.15. szerint

$$((\lambda.\mathbf{a}) \cdot \mathbf{b})_{i,k} = \sum_{j \in J} (\lambda.\mathbf{a})_{i,j}\mathbf{b}_{j,k} = \sum_{j \in J} (\lambda \mathbf{a}_{i,j})\, \mathbf{b}_{j,k} = \sum_{j \in J} \lambda\, (\mathbf{a}_{i,j}\mathbf{b}_{j,k}) =$$

$$= \lambda \sum_{j \in J} \mathbf{a}_{i,j}\mathbf{b}_{j,k} = \lambda(\mathbf{a} \cdot \mathbf{b})_{i,k} = (\lambda.(\mathbf{a} \cdot \mathbf{b}))_{i,k},$$

ezért $(\lambda.\mathbf{a}) \cdot \mathbf{b} = \lambda.(\mathbf{a} \cdot \mathbf{b})$.

Ha A kommutatív, akkor $(i,k) \in I \times K$ esetén a definíciók és A szorzásának asszociativitása és az összeadásra vonatkozó disztributivitása, valamint 12.5.15. szerint

$$(\mathbf{a} \cdot (\lambda.\mathbf{b}))_{i,k} = \sum_{j \in J} \mathbf{a}_{i,j}(\lambda.\mathbf{b})_{j,k} = \sum_{j \in J} \mathbf{a}_{i,j}(\lambda \mathbf{b}_{j,k}) = \sum_{j \in J} \lambda\, (\mathbf{a}_{i,j}\mathbf{b}_{j,k}) =$$

$$= \lambda \sum_{j \in J} \mathbf{a}_{i,j}\mathbf{b}_{j,k} = \lambda(\mathbf{a} \cdot \mathbf{b})_{i,k} = (\lambda.(\mathbf{a} \cdot \mathbf{b}))_{i,k},$$

ezért $\mathbf{a} \cdot (\lambda.\mathbf{b}) = \lambda.(\mathbf{a} \cdot \mathbf{b})$. ■

15.1.14. Definíció. *Ha I, J, F halmazok és $\mathbf{a} \in \mathrm{M}_{I,J}(F)$, akkor ${}^{\mathrm{t}}\mathbf{a} \in \mathrm{M}_{J,I}(F)$ az a mátrix, amelyre minden $(i,j) \in I \times J$ esetén $\left({}^{\mathrm{t}}\mathbf{a}\right)_{j,i} := \mathbf{a}_{i,j}$, és az ${}^{\mathrm{t}}\mathbf{a}$ mátrixot az $\mathbf{a}$ mátrix* **transzponáltjának** *nevezzük.*

15.1.15. Állítás. *Legyen A gyűrű.*

a) *Ha I, J halmazok és $\mathbf{a} \in \mathrm{M}_{I,J}(A)$, akkor*

$${}^{\mathrm{t}}({}^{\mathrm{t}}\mathbf{a}) = \mathbf{a}.$$

b) *Ha I, J halmazok és $\mathbf{a}, \mathbf{b} \in \mathrm{M}_{I,J}(A)$, akkor*

$${}^{\mathrm{t}}(\mathbf{a}+\mathbf{b}) = {}^{\mathrm{t}}\mathbf{a} + {}^{\mathrm{t}}\mathbf{b}.$$

c) *Ha I, J halmazok és $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ és $\lambda \in A$, akkor*

$${}^{\mathrm{t}}(\lambda.\mathbf{a}) = \lambda.{}^{\mathrm{t}}\mathbf{a}.$$

d) *Ha az A gyűrű kommutatív, és I, J, K halmazok, és $\mathbf{a} \in \mathrm{M}_{I,J}(A)$ olyan, hogy ${}^{\mathrm{t}}\mathbf{a} \in \dot{\mathrm{M}}_{J,I}(A)$, valamint $\mathbf{b} \in \dot{\mathrm{M}}_{J,K}(A)$, akkor*

$${}^{\mathrm{t}}(\mathbf{a}\cdot\mathbf{b}) = {}^{\mathrm{t}}\mathbf{b} \cdot {}^{\mathrm{t}}\mathbf{a}.$$

Bizonyítás. a) Ha $i \in I$ és $j \in J$, akkor

$$\left({}^{\mathrm{t}}({}^{\mathrm{t}}\mathbf{a})\right)_{i,j} = ({}^{\mathrm{t}}\mathbf{a})_{j,i} = \mathbf{a}_{i,j},$$

ezért ${}^{\mathrm{t}}({}^{\mathrm{t}}\mathbf{a}) = \mathbf{a}$.

b) Ha $i \in I$ és $j \in J$, akkor

$$\left({}^{\mathrm{t}}(\mathbf{a}+\mathbf{b})\right)_{j,i} = (\mathbf{a}+\mathbf{b})_{i,j} = \mathbf{a}_{i,j} + \mathbf{b}_{i,j} = \left({}^{\mathrm{t}}\mathbf{a}\right)_{j,i} + \left({}^{\mathrm{t}}\mathbf{b}\right)_{j,i} = \left({}^{\mathrm{t}}\mathbf{a} + {}^{\mathrm{t}}\mathbf{b}\right)_{j,i},$$

ezért ${}^{\mathrm{t}}(\mathbf{a}+\mathbf{b}) = {}^{\mathrm{t}}\mathbf{a} + {}^{\mathrm{t}}\mathbf{b}$.

c) Ha $i \in I$ és $j \in J$, akkor

$$\left({}^{\mathrm{t}}(\lambda.\mathbf{a})\right)_{j,i} = (\lambda.\mathbf{a})_{i,j} = \lambda\mathbf{a}_{i,j} = \lambda({}^{\mathrm{t}}\mathbf{a})_{j,i} = \left(\lambda.{}^{\mathrm{t}}\mathbf{a}\right)_{j,i}.$$

d) Tegyük fel, hogy A kommutatív gyűrű. Ha $i \in I$ és $k \in K$, akkor

$$\left({}^{\mathrm{t}}(\mathbf{a}\cdot\mathbf{b})\right)_{k,i} = (\mathbf{a}\cdot\mathbf{b})_{i,k} = \sum_{j\in J}\mathbf{a}_{i,j}\mathbf{b}_{j,k} = \sum_{j\in J}\left({}^{\mathrm{t}}\mathbf{a}\right)_{j,i}\left({}^{\mathrm{t}}\mathbf{b}\right)_{k,j} = \sum_{j\in J}\left({}^{\mathrm{t}}\mathbf{b}\right)_{k,j}\left({}^{\mathrm{t}}\mathbf{a}\right)_{j,i} = \left({}^{\mathrm{t}}\mathbf{b}\cdot{}^{\mathrm{t}}\mathbf{a}\right)_{k,i},$$

ahol az utolsó előtti egyenlőségnél felhasználtuk A szorzásának kommutativitását. Tehát minden $(i,k) \in I \times K$ esetén $({}^{\mathrm{t}}(\mathbf{a}\cdot\mathbf{b}))_{k,i} = ({}^{\mathrm{t}}\mathbf{b}\cdot{}^{\mathrm{t}}\mathbf{a})_{k,i}$, vagyis ${}^{\mathrm{t}}(\mathbf{a}\cdot\mathbf{b}) = {}^{\mathrm{t}}\mathbf{b}\cdot{}^{\mathrm{t}}\mathbf{a}$. ■

15.1.16. Következmény. *Legyen A egységelemes kommutatív gyűrű, I véges halmaz, és $\mathbf{a} \in \mathrm{M}_I(A)$ invertálható elem az $\mathrm{M}_I(A)$ mátrixgyűrűben. Ekkor az ${}^{\mathrm{t}}\mathbf{a}$ transzponált mátrix is invertálható, és $\left({}^{\mathrm{t}}\mathbf{a}\right)^{-1} = {}^{\mathrm{t}}\left(\mathbf{a}^{-1}\right)$.*

Bizonyítás. Jelölje $\mathbf{1}$ azt az elemet $\mathrm{M}_I(A)$-ban, amelyre minden $i,j \in I$ esetén.

$$\mathbf{1}_{i,j} := \begin{cases} 1_A & \text{, ha } i = j, \\ 0_A & \text{, ha } i \neq j. \end{cases}$$

A 15.1.11. tétel szerint $\mathbf{1}$ a multiplikatív neutrális elem az $\mathrm{M}_I(A)$ mátrixgyűrűben, és látható, hogy ${}^{\mathrm{t}}\mathbf{1} = \mathbf{1}$, így az előző állítás d) pontjának alkalmazásával kapjuk, hogy az $\mathbf{a}\cdot\mathbf{a}^{-1} = \mathbf{1} = \mathbf{a}^{-1}\cdot\mathbf{a}$ egyenlőségekből ${}^{\mathrm{t}}\left(\mathbf{a}^{-1}\right)\cdot{}^{\mathrm{t}}\mathbf{a} = \mathbf{1} = {}^{\mathrm{t}}\mathbf{a}\cdot{}^{\mathrm{t}}\left(\mathbf{a}^{-1}\right)$ következik, tehát ${}^{\mathrm{t}}\mathbf{a}$ invertálható elem az $\mathrm{M}_I(A)$ mátrixgyűrűben, és $\left({}^{\mathrm{t}}\mathbf{a}\right)^{-1} = {}^{\mathrm{t}}\left(\mathbf{a}^{-1}\right)$. ■

15.2. Kommutatív gyűrű feletti mátrix determinánsa

Emlékeztetünk arra, hogy minden I halmazra $\mathfrak{S}(I)$ jelöli az $I \to I$ bijekcióknak (vagyis I *permutációinak*) halmazát a függvénykompozíció művelettel ellátva (tehát $\mathfrak{S}(I)$ az I halmaz *teljes permutációcsoportja*). Továbbá, véges I halmaz esetén ε_I jelöli az $\mathfrak{S}(I)$ csoport *előjel-függvényét*, tehát $\varepsilon_I : \mathfrak{S}(I) \to \{-1, 1\}$ az a csoport-morfizmus az $\mathfrak{S}(I)$ csoport és a $\{-1, 1\}$ multiplikatív csoport között, amelyre teljesül az, hogy I minden τ transzpozíciójára (13.3.1.) $\varepsilon_I(\tau) = -1$ (13.3.4.).

15.2.1. Definíció. *Legyen A kommutatív gyűrű és I nem üres véges halmaz. Ekkor minden $\mathbf{a} \in \mathrm{M}_I(A)$ esetén*

$$\det(\mathbf{a}) := \sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i \in I} \mathbf{a}_{i,\sigma(i)}\Big),$$

és a $\det(\mathbf{a}) \in A$ elemet az $\mathbf{a}$ mátrix **determinánsának** *nevezzük.*

15.2.2. Állítás. *Ha A kommutatív gyűrű és I nem üres véges halmaz, akkor minden $\mathbf{a} \in \mathrm{M}_I(A)$ és $\lambda \in A$ esetén*

$$\det(\lambda.\mathbf{a}) = \lambda^{\mathrm{Card}(I)} \det(\mathbf{a}).$$

Bizonyítás. A definíció szerint

$$\det(\lambda.\mathbf{a}) = \sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i \in I} (\lambda.\mathbf{a})_{i,\sigma(i)}\Big) = \sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i \in I} \left(\lambda \left(\mathbf{a}_{i,\sigma(i)}\right)\right)\Big) \overset{(1)}{=}$$

$$\overset{(1)}{=} \sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i \in I} \lambda\Big)\Big(\prod_{i \in I} \mathbf{a}_{i,\sigma(i)}\Big) = \Big(\prod_{i \in I} \lambda\Big) \sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i \in I} \mathbf{a}_{i,\sigma(i)}\Big) \overset{(2)}{=} \lambda^{\mathrm{Card}(I)} \det(\mathbf{a}),$$

ahol az $\overset{(1)}{=}$ egyenlőségnél a 8.5.9. állítást alkalmaztuk az $(A, \cdot)$ kommutatív félcsoportra, és a $\overset{(2)}{=}$ egyenlőségnél a 12.4.3. állítást és a determináns definícióját alkalmaztuk. ■

15.2.3. Lemma. *Ha A kommutatív gyűrű és I nem üres véges halmaz, akkor minden $\mathbf{b} \in \mathrm{M}_I(A)$ mátrixra és minden $\sigma' : I \to I$ függvényre:*

$$\sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i \in I} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = \begin{cases} \varepsilon_I(\sigma')\det(\mathbf{b}) & , \text{ ha } \sigma' \in \mathfrak{S}(I), \\ 0_A & , \text{ ha } \sigma' \notin \mathfrak{S}(I). \end{cases}$$

Bizonyítás. (I) Tegyük fel, hogy $\sigma' \in \mathfrak{S}(I)$. Ekkor az

$$\mathfrak{S}(I) \to \mathfrak{S}(I); \quad \sigma \mapsto \sigma \circ \sigma'$$

függvény bijekció, így A összeadásának általános kommutativitása (8.6.1.) szerint

$$\sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i \in I} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = \sum_{\sigma \in \mathfrak{S}(I)} \varepsilon_I(\sigma \circ \sigma')\Big(\prod_{i \in I} \mathbf{b}_{\sigma'(i),(\sigma \circ \sigma')(i)}\Big).$$

Ha $\sigma \in \mathfrak{S}(I)$, akkor A szorzásának általános kommutativitása (8.6.1.) szerint

$$\prod_{i \in I} \mathbf{b}_{\sigma'(i),(\sigma \circ \sigma')(i)} = \prod_{i \in I} \mathbf{b}_{i,\sigma(i)},$$

hiszen a $\sigma' : I \to I$ függvény bijekció. Ezért az $\varepsilon_I : \mathfrak{S}(I) \to \{-1, 1\}$ függvény multiplikativitását alkalmazva

$$\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = \varepsilon_I(\sigma') \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{b}_{i,\sigma(i)}\Big) = \varepsilon_I(\sigma')\det(\mathbf{b}).$$

(II) Tegyük fel, hogy $\sigma' \notin \mathfrak{S}(I)$, vagyis σ' *nem injektív* (8.1.11.). Legyenek $j, k \in I$ olyanok, hogy $j \neq k$ és $\sigma'(j) = \sigma'(k)$. Jelölje $\tau_{j,k} \in \mathfrak{S}(I)$ azt a transzpozíciót, amelyre $\tau_{j,k}(j) = k$ és $\tau_{j,k}(k) = j$ és minden $i \in I$ esetén, ha $i \neq j$ és $i \neq k$, akkor $\tau_{j,k}(i) = i$. Ekkor A szorzásának kommutativitása miatt

$$\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{b}_{\sigma'(j),\sigma(j)}\mathbf{b}_{\sigma'(k),\sigma(k)}\Big(\prod_{i\in I\setminus\{j,k\}} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big).$$

Vezessük be a következő függvényt:

$$f : \mathfrak{S}(I) \to A; \quad \sigma \mapsto \varepsilon_I(\sigma)\mathbf{b}_{\sigma'(j),\sigma(j)}\mathbf{b}_{\sigma'(k),\sigma(k)}\Big(\prod_{i\in I\setminus\{j,k\}} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big).$$

Ekkor minden $\sigma \in \mathfrak{S}(I)$ permutációra, A szorzásának kommutativitását alkalmazva kapjuk, hogy

$$\begin{aligned}
f(\sigma\circ\tau_{j,k}) &= \varepsilon_I(\sigma\circ\tau_{j,k})\mathbf{b}_{\sigma'(j),\sigma(\tau_{j,k}(j))}\mathbf{b}_{\sigma'(k),\sigma(\tau_{j,k}(k))}\Big(\prod_{i\in I\setminus\{j,k\}} \mathbf{b}_{\sigma'(i),\sigma(\tau_{j,k}(i))}\Big) = \\
&= \varepsilon_I(\sigma)\varepsilon_I(\tau_{j,k})\,\mathbf{b}_{\sigma'(j),\sigma(k)}\mathbf{b}_{\sigma'(k),\sigma(j)}\Big(\prod_{i\in I\setminus\{j,k\}} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big) \overset{(*)}{=} \\
&\overset{(*)}{=} -\varepsilon_I(\sigma)\mathbf{b}_{\sigma'(k),\sigma(k)}\mathbf{b}_{\sigma'(j),\sigma(j)}\Big(\prod_{i\in I\setminus\{j,k\}} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = -f(\sigma),
\end{aligned}$$

ahol az $\overset{(*)}{=}$ egyenlőségnél használtuk ki, hogy $\sigma'(j) = \sigma'(k)$. Ezért a 13.2.2. állítást alkalmazva az $(S, \top) := (A, +)$ kommutatív csoportra kapjuk, hogy

$$\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} f(\sigma) = 0. \ \blacksquare$$

15.2.4. Állítás. *Ha A kommutatív gyűrű és I nem üres véges halmaz, akkor minden $\mathbf{a}, \mathbf{b} \in \mathrm{M}_I(A)$ esetén*

$$\det(\mathbf{a}\cdot\mathbf{b}) = \det(\mathbf{a})\det(\mathbf{b}).$$

Bizonyítás. A determináns és a mátrixszorzás definícióját alkalmazva

$$\det(\mathbf{a}\cdot\mathbf{b}) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} (\mathbf{a}\cdot\mathbf{b})_{i,\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\Big(\sum_{k\in I} \mathbf{a}_{i,k}\mathbf{b}_{k,\sigma(i)}\Big)\Big).$$

Minden $\sigma \in \mathfrak{S}(I)$ esetén felhasználva A szorzásának A összeadására vonatkozó általános disztributivitását (8.8.3.) kapjuk, hogy

$$\prod_{i\in I}\Big(\sum_{k\in I} \mathbf{a}_{i,k}\mathbf{b}_{k,\sigma(i)}\Big) = \sum_{\sigma'\in I^I}\Big(\prod_{i\in I} \mathbf{a}_{i,\sigma'(i)}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big).$$

Ebből következik, hogy

$$\begin{aligned}
\det(\mathbf{a}\cdot\mathbf{b}) &= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\sum_{\sigma'\in I^I}\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big)\Big) = \\
&= \sum_{\sigma'\in I^I}\Big(\sum_{\sigma\in\mathfrak{S}(I)}\varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big)\Big) = \\
&= \sum_{\sigma'\in I^I}\Big(\sum_{\sigma\in\mathfrak{S}(I)}\varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\Big)\Big(\prod_{i\in I}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big)\Big) = \\
&= \sum_{\sigma'\in I^I}\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\Big)\Big(\sum_{\sigma\in\mathfrak{S}(I)}\varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big)\Big).
\end{aligned}$$

Az előző lemma szerint, ha $\sigma'\in I^I$ és $\sigma'\notin\mathfrak{S}(I)$, akkor

$$\sum_{\sigma\in\mathfrak{S}(I)}\varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = 0,$$

és ha $\sigma'\in\mathfrak{S}(I)$, akkor

$$\sum_{\sigma\in\mathfrak{S}(I)}\varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big) = \varepsilon_I(\sigma')\det(\mathbf{b}),$$

ezért

$$\begin{aligned}
\det(\mathbf{a}\cdot\mathbf{b}) &= \sum_{\sigma'\in I^I}\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\Big)\Big(\sum_{\sigma\in\mathfrak{S}(I)}\varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big)\Big) = \\
&= \sum_{\sigma'\in\mathfrak{S}(I)}\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\Big)\Big(\sum_{\sigma\in\mathfrak{S}(I)}\varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{b}_{\sigma'(i),\sigma(i)}\Big)\Big) = \\
&= \sum_{\sigma'\in\mathfrak{S}(I)}\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\Big)\Big(\varepsilon_I(\sigma')\det(\mathbf{b})\Big) = \det(\mathbf{a})\det(\mathbf{b}). \blacksquare
\end{aligned}$$

15.2.5. Következmény. *Legyen A egységelemes kommutatív gyűrű és I nem üres véges halmaz. Ha $\mathbf{a}\in\mathrm{M}_I(A)$ invertálható elem az $\mathrm{M}_I(A)$ mátrixgyűrűben, akkor a $\det(\mathbf{a})\in A$ elem invertálható az A gyűrűben és*

$$\det\left(\mathbf{a}^{-1}\right) = (\det(\mathbf{a}))^{-1}.$$

Bizonyítás. Az előző állításból következik, hogy

$$\det(\mathbf{1}) = \det\left(\mathbf{a}\cdot\mathbf{a}^{-1}\right) = \det(\mathbf{a})\det\left(\mathbf{a}^{-1}\right),$$

ahol $\mathbf{1}$ az $\mathrm{M}_I(A)$ mátrixgyűrű egységeleme, vagyis az a mátrix, amelyre minden $i,j\in I$ esetén

$$\mathbf{1}_{i,j} = \begin{cases} 1_A & \text{, ha } i=j, \\ 0_A & \text{, ha } i\neq j \end{cases}$$

(15.1.11.). Világos, hogy a definíció alapján minden $\sigma\in\mathfrak{S}(I)$ esetén

$$\prod_{i\in I}\mathbf{1}_{i,\sigma(i)} = \begin{cases} 1_A & \text{, ha } \sigma=\mathrm{id}_I, \\ 0_A & \text{, ha } \sigma\neq\mathrm{id}_I \end{cases},$$

így a determináns definíciója szerint

$$\det(\mathbf{1}) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{1}_{i,\sigma(i)}\Big) = \varepsilon_I\left(\mathrm{id}_I\right)1_A = 1_A.$$

Tehát $1_A = \det(\mathbf{a})\det\left(\mathbf{a}^{-1}\right)$, és mivel az A gyűrű kommutatív, így a $\det(\mathbf{a}) \in A$ elem invertálható az A gyűrűben és $\det\left(\mathbf{a}^{-1}\right) = (\det(\mathbf{a}))^{-1}$. ■

Később megmutatjuk, hogy a mátrix-invertálhatóság előző állításban megfogalmazott szükséges feltétele elégséges is (15.4.9.).

15.2.6. Állítás. *Ha A kommutatív gyűrű és I nem üres véges halmaz, akkor minden $\mathbf{a} \in \mathrm{M}_I(A)$ esetén*

$$\det({}^{\mathrm{t}}\mathbf{a}) = \det(\mathbf{a}).$$

Bizonyítás. Legyen $\mathbf{a} \in \mathrm{M}_I(A)$. Az $\mathfrak{S}(I) \to \mathfrak{S}(I);\ \sigma \mapsto \sigma^{-1}$ leképezés (vagyis az $\mathfrak{S}(I)$ teljes permutációcsoport inverzió-függvénye) bijekció, ezért A összeadásának általános kommutativitása (8.6.1.) és a transzponálás értelmezése alapján

$$\det({}^{\mathrm{t}}\mathbf{a}) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma^{-1})\Big(\prod_{i\in I} ({}^{\mathrm{t}}\mathbf{a})_{i,\sigma^{-1}(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{a}_{\sigma^{-1}(i),i}\Big),$$

ahol felhasználtuk azt, hogy minden $\sigma \in \mathfrak{S}(I)$ esetén $\varepsilon_I(\sigma^{-1}) = \varepsilon_I(\sigma)$. Ha $\sigma \in \mathfrak{S}(I)$, akkor $\sigma : I \to I$ bijekció, így A szorzásának általános kommutativitása (8.6.1.) miatt

$$\prod_{i\in I} \mathbf{a}_{\sigma^{-1}(i),i} = \prod_{i\in I} \mathbf{a}_{\sigma^{-1}(\sigma(i)),\sigma(i)} = \prod_{i\in I} \mathbf{a}_{i,\sigma(i)},$$

amiből következik, hogy

$$\det({}^{\mathrm{t}}\mathbf{a}) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{a}_{\sigma^{-1}(i),i}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{a}_{i,\sigma(i)}\Big) = \det(\mathbf{a}).\ ■$$

15.2.7. Állítás. *Legyen A kommutatív gyűrű és I nem üres véges halmaz. Ha $(a_{i,j})_{(i,j)\in I\times I} \in \mathrm{M}_I(A)$ és $(\lambda_i)_{i\in I} \in A^I$, akkor*

$$\det\left((\lambda_j a_{i,j})_{(i,j)\in I\times I}\right) = \Big(\prod_{i\in I}\lambda_i\Big)\det\left((a_{i,j})_{(i,j)\in I\times I}\right).$$

Bizonyítás. A definíció szerint

$$\begin{aligned}\det\left((\lambda_j a_{i,j})_{(i,j)\in I\times I}\right) &= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\left(\lambda_{\sigma(i)}a_{i,\sigma(i)}\right)\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\lambda_{\sigma(i)}\Big)\Big(\prod_{i\in I}a_{i,\sigma(i)}\Big) \overset{(*)}{=} \\ &\overset{(*)}{=} \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\lambda_i\Big)\Big(\prod_{i\in I}a_{i,\sigma(i)}\Big) = \Big(\prod_{i\in I}\lambda_i\Big)\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\prod_{i\in I}a_{i,\sigma(i)} = \\ &= \Big(\prod_{i\in I}\lambda_i\Big)\det\left((a_{i,j})_{(i,j)\in I\times I}\right),\end{aligned}$$

ahol az $\overset{(*)}{=}$ egyenlőségnél azt használtuk ki, hogy A szorzásának általános kommutativitása folytán minden $\sigma \in \mathfrak{S}(I)$ permutációra $\prod_{i\in I}\lambda_{\sigma(i)} = \prod_{i\in I}\lambda_i$, így ez az elem kiemelhető a szummából. ■

15.2.8. Állítás. *Legyen A kommutatív gyűrű és I nem üres véges halmaz. Ha $(a_{i,j})_{(i,j)\in I\times I} \in \mathrm{M}_I(A)$ olyan, hogy minden $i, j \in I$, $i \neq j$ esetén $a_{i,j} = 0$, akkor*

$$\det\left((a_{i,j})_{(i,j)\in I\times I}\right) = \prod_{i\in I} a_{i,i}.$$

Bizonyítás. Ha $\sigma \in \mathfrak{S}(I)$ és $\sigma \neq \mathrm{id}_I$, akkor van olyan $i \in I$, hogy $i \neq \sigma(i)$, ezért a hipotézis szerint $a_{i,\sigma(i)} = 0$. Ezért minden $\sigma \in \mathfrak{S}(I)$ permutációra, ha $\sigma \neq \mathrm{id}_I$, akkor $\prod_{i\in I} a_{i,\sigma(i)} = 0$, így a definíció szerint

$$\det\left((a_{i,j})_{(i,j)\in I\times I}\right) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} a_{i,\sigma(i)}\Big) =$$

$$= \varepsilon_I\left(\mathrm{id}_I\right)\Big(\prod_{i\in I} a_{i,\mathrm{id}_\mathrm{I}(i)}\Big) + \sum_{\substack{\sigma\in\mathfrak{S}(I)\\ \sigma\neq\mathrm{id}_\mathrm{I}}} \varepsilon_I(\sigma)\Big(\prod_{i\in I} a_{i,\sigma(i)}\Big) = \prod_{i\in I} a_{i,i}. \ \blacksquare$$

15.2.9. Állítás. *Legyen A kommutatív gyűrű, I véges halmaz, és $\mathbf{a} \in \mathrm{M}_I(A)$. Minden $i \in I$ esetén legyen $\mathbf{a}_i := (\mathbf{a}_{i,j})_{j\in I} \in A^I$ és minden $j \in I$ esetén legyen $\tilde{\mathbf{a}}_j := (\mathbf{a}_{i,j})_{i\in I} \in A^I$. Ha létezik olyan $k \in I$ index, és létezik olyan $(\lambda_i)_{i\in I\setminus\{k\}} \in A^{I\setminus\{k\}}$ rendszer, amelyre $\mathbf{a}_k = \sum_{i\in I\setminus\{k\}} \lambda_i \mathbf{a}_i$ vagy $\tilde{\mathbf{a}}_k = \sum_{i\in I\setminus\{k\}} \lambda_i \tilde{\mathbf{a}}_i$, akkor* $\det(\mathbf{a}) = 0$.

Bizonyítás. (I) Tegyük fel, hogy $k \in I$ olyan index, és $(\lambda_i)_{i\in I\setminus\{k\}} \in A^{I\setminus\{k\}}$ olyan rendszer, amelyre $\mathbf{a}_k = \sum_{i\in I\setminus\{k\}} \lambda_i \mathbf{a}_i$, vagyis minden $l \in I$ esetén

$$\mathbf{a}_{k,l} = \sum_{i\in I\setminus\{k\}} \lambda_i \mathbf{a}_{i,l}.$$

Ekkor a determináns definíciója szerint

$$\det(\mathbf{a}) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I} \mathbf{a}_{i,\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{k,\sigma(k)}\Big(\prod_{j\in I\setminus\{k\}} \mathbf{a}_{j,\sigma(j)}\Big) =$$

$$= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\sum_{i\in I\setminus\{k\}} \lambda_i \mathbf{a}_{i,\sigma(k)}\Big)\Big(\prod_{j\in I\setminus\{k\}} \mathbf{a}_{j,\sigma(j)}\Big) =$$

$$= \sum_{i\in I\setminus\{k\}} \lambda_i\Big(\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{i,\sigma(k)}\Big(\prod_{j\in I\setminus\{k\}} \mathbf{a}_{j,\sigma(j)}\Big)\Big) =$$

$$= \sum_{i\in I\setminus\{k\}} \lambda_i\Big(\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{i,\sigma(k)}\mathbf{a}_{i,\sigma(i)}\Big(\prod_{j\in I\setminus\{i,k\}} \mathbf{a}_{j,\sigma(j)}\Big)\Big).$$

Minden $i \in I \setminus \{k\}$ esetén jelölje $\tau_{i,k} \in \mathfrak{S}(I)$ azt a transzpozíciót, amelyre $\tau_{i,k}(i) = k$ és $\tau_{i,k}(k) = i$, továbbá vezessük be az

$$f_i : \mathfrak{S}(I) \to A; \quad \sigma \mapsto \varepsilon_I(\sigma)\mathbf{a}_{i,\sigma(k)}\mathbf{a}_{i,\sigma(i)}\Big(\prod_{j\in I\setminus\{i,k\}} \mathbf{a}_{j,\sigma(j)}\Big)$$

függvényt. Ekkor minden $i \in I \setminus \{k\}$ indexre és $\sigma \in \mathfrak{S}(I)$ permutációra

$$f_i\left(\sigma\circ\tau_{i,k}\right) = \varepsilon_I\left(\sigma\circ\tau_{i,k}\right)\mathbf{a}_{i,\sigma\left(\tau_{i,k}(k)\right)}\mathbf{a}_{i,\sigma\left(\tau_{i,k}(i)\right)}\Big(\prod_{j\in I\setminus\{i,k\}} \mathbf{a}_{j,\sigma\left(\tau_{i,k}(j)\right)}\Big) =$$

$$= \varepsilon_I(\sigma)\varepsilon_I\left(\tau_{i,k}\right)\mathbf{a}_{i,\sigma(i)}\mathbf{a}_{i,\sigma(k)}\Big(\prod_{j\in I\setminus\{i,k\}} \mathbf{a}_{j,\sigma(j)}\Big) = -f_i(\sigma),$$

ezért 13.2.2. alapján

$$\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{i,\sigma(k)}\mathbf{a}_{i,\sigma(i)}\Big(\prod_{j\in I\setminus\{i,k\}} \mathbf{a}_{j,\sigma(j)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} f_i(\sigma) = 0.$$

Ez minden $i \in I \setminus \{k\}$ esetén teljesül, így

$$\det(\mathbf{a}) = \sum_{i\in I\setminus\{k\}} \lambda_i\Big(\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{i,\sigma(k)}\mathbf{a}_{i,\sigma(i)}\Big(\prod_{j\in I\setminus\{i,k\}} \mathbf{a}_{j,\sigma(j)}\Big)\Big) = 0.$$

(II) Világos, hogy minden $j \in I$ esetén $\tilde{\mathbf{a}}_j = ({}^{\mathrm{t}}\mathbf{a}_{j,i})_{i\in I} = {}^{\mathrm{t}}\mathbf{a}_j$, ezért (I) szerint $\det({}^{\mathrm{t}}\mathbf{a}) = 0$, és tudjuk, hogy $\det({}^{\mathrm{t}}\mathbf{a}) = \det(\mathbf{a})$. ■

15.2.10. Következmény. *Legyen A kommutatív gyűrű és I nem üres véges halmaz.*

a) *Ha az $\mathbf{a} \in \mathrm{M}_I(A)$ mátrix valamelyik sorának vagy oszlopának minden tagja nulla, akkor* $\det(\mathbf{a}) = 0$.

b) *Ha A egységelemes gyűrű és az $\mathbf{a} \in \mathrm{M}_I(A)$ mátrixnak létezik két megegyező sora vagy két megegyező oszlopa, akkor* $\det(\mathbf{a}) = 0$.

Bizonyítás. a) Ha az $\mathbf{a} \in \mathrm{M}_I(A)$ mátrix k-adik sorának (illetve oszlopának) minden eleme egyenlő 0_A-val, akkor $\mathbf{a}_k = \sum_{i\in I\setminus\{k\}} 0_A\mathbf{a}_i$ (illetve $\tilde{\mathbf{a}}_k = \sum_{i\in I\setminus\{k\}} 0_A\tilde{\mathbf{a}}_i$), ezért az előző állítás szerint $\det(\mathbf{a}) = 0$.

b) Ha $k, l \in I$, $k \neq l$ és $\mathbf{a}_k = \mathbf{a}_l$ (illetve $\tilde{\mathbf{a}}_k = \tilde{\mathbf{a}}_l$), akkor $\mathbf{a}_k = 1_A\mathbf{a}_l + \sum_{i\in I\setminus\{k,l\}} 0_A\tilde{\mathbf{a}}_i$ (illetve $\tilde{\mathbf{a}}_k = 1_A\tilde{\mathbf{a}}_l + \sum_{i\in I\setminus\{k,l\}} 0_A\tilde{\mathbf{a}}_i$), ezért az előző állítás szerint $\det(\mathbf{a}) = 0$. ■

15.2.11. Állítás. *Legyen A kommutatív gyűrű, I véges halmaz, $\mathbf{a} \in \mathrm{M}_I(A)$, és $k, l \in I$ olyanok, hogy $k \neq l$. Vezessük be az $\mathbf{a}', \mathbf{a}'' \in \mathrm{M}_I(A)$ mátrixokat úgy, hogy minden $i, j \in I$ esetén*

$$\mathbf{a}'_{i,j} := \begin{cases} \mathbf{a}_{i,j} & \text{, ha } i \neq k \text{ és } j \neq l, \\ \mathbf{a}_{l,j} & \text{, ha } i = k, \\ \mathbf{a}_{k,j} & \text{, ha } i = l, \end{cases}$$

tehát $\mathbf{a}'$ úgy keletkezik $\mathbf{a}$-ból, hogy annak k-adik és l-edik sorát felcseréljük, és

$$\mathbf{a}''_{i,j} := \begin{cases} \mathbf{a}_{i,j} & \text{, ha } i \neq k \text{ és } j \neq l, \\ \mathbf{a}_{i,l} & \text{, ha } j = k, \\ \mathbf{a}_{k,j} & \text{, ha } k = l, \end{cases}$$

tehát $\mathbf{a}''$ úgy keletkezik $\mathbf{a}$-ból, hogy annak k-adik és l-edik oszlopát felcseréljük. Ekkor

$$\det(\mathbf{a}') = -\det(\mathbf{a}) = \det(\mathbf{a}'').$$

Bizonyítás. Jelölje $\tau_{k,l} \in \mathfrak{S}(I)$ azt a transzpozíciót, amelyre $\tau_{k,l}(k) = l$ és $\tau_{k,l}(l) = k$.

Ekkor

$$\det(\mathbf{a}') = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}'_{i,\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}'_{k,\sigma(k)}\mathbf{a}'_{l,\sigma(l)}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}'_{i,\sigma(i)}\Big) =$$
$$= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{l,\sigma(k)}\mathbf{a}_{k,\sigma(l)}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{i,\sigma(i)}\Big) =$$
$$= \sum_{\sigma'\in\mathfrak{S}(I)} \varepsilon_I\left(\sigma'\circ\tau_{k,l}\right)\mathbf{a}_{l,\sigma'(\tau_{k,l}(k))}\mathbf{a}_{k,\sigma'(\tau_{k,l}(l))}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{i,\sigma'(\tau_{k,l}(i))}\Big) =$$
$$= -\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma')\mathbf{a}_{l,\sigma'(l)}\mathbf{a}_{k,\sigma'(k)}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{i,\sigma'(i)}\Big) = -\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma')\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma'(i)}\Big) = -\det(\mathbf{a}).$$

Hasonlóan kapjuk, hogy

$$\det(\mathbf{a}'') = \det\left({}^{\mathrm{t}}(\mathbf{a}'')\right) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}{}^{\mathrm{t}}(\mathbf{a}'')_{i,\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}''_{\sigma(i),i}\Big) =$$
$$= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}''_{\sigma(k),k}\mathbf{a}''_{\sigma(l),l}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}''_{\sigma(i),i}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{\sigma(k),l}\mathbf{a}_{\sigma(l),k}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{\sigma(i),i}\Big) =$$
$$= \sum_{\sigma'\in\mathfrak{S}(I)} \varepsilon_I\left(\sigma'\circ\tau_{k,l}\right)\mathbf{a}_{\sigma'(\tau_{k,l}(k)),l}\mathbf{a}_{\sigma'(\tau_{k,l}(l)),k}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{\sigma'(\tau_{k,l}(i)),i}\Big) =$$
$$= -\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma')\mathbf{a}_{\sigma'(l),l}\mathbf{a}_{\sigma'(k),k}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{\sigma'(i),i}\Big) =$$
$$= -\sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma')\Big(\prod_{i\in I}\mathbf{a}_{\sigma'(i),i}\Big) = -\det({}^{\mathrm{t}}\mathbf{a}) = -\det(\mathbf{a}). \ \blacksquare$$

15.2.12. Állítás. *Legyen A kommutatív gyűrű, I véges halmaz, $\mathbf{a}\in \mathrm{M}_I(A)$, és $k,l\in I$ olyanok, hogy $k\neq l$. Legyen $\lambda\in A$, és vezessük be az $\mathbf{a}',\mathbf{a}''\in\mathrm{M}_I(A)$ mátrixokat úgy, hogy minden $i,j\in I$ esetén*

$$\mathbf{a}'_{i,j} := \begin{cases} \mathbf{a}_{i,j} & ,\ ha\ i\neq k, \\ \mathbf{a}_{k,j}+\lambda\mathbf{a}_{l,j} & ,\ ha\ i=k, \end{cases}$$

tehát $\mathbf{a}'$ úgy keletkezik $\mathbf{a}$-ból, hogy annak l-edik sorának λ-szorosát hozzáadjuk a k-adik sorához, továbbá legyen

$$\mathbf{a}''_{i,j} := \begin{cases} \mathbf{a}_{i,j} & ,\ ha\ j\neq k, \\ \mathbf{a}_{i,k}+\lambda\mathbf{a}_{i,l} & ,\ ha\ j=k, \end{cases}$$

tehát $\mathbf{a}''$ úgy keletkezik $\mathbf{a}$-ból, hogy annak l-edik oszlopának λ-szorosát hozzáadjuk a k-adik oszlopához. Ekkor

$$\det(\mathbf{a}') = \det(\mathbf{a}) = \det(\mathbf{a}'').$$

Bizonyítás. Jelölje $\tau_{k,l}\in\mathfrak{S}(I)$ azt a transzpozíciót, amelyre $\tau_{k,l}(k)=l$ és $\tau_{k,l}(l)=k$.

Ekkor

$$\begin{aligned}
\det(\mathbf{a}') = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}'_{i,\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}'_{k,\sigma(k)}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}'_{i,\sigma(i)}\Big) = \\
= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\left(\mathbf{a}_{k,\sigma(k)} + \lambda\mathbf{a}_{l,\sigma(k)}\right)\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{i,\sigma(i)}\Big) = \\
= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{k,\sigma(k)}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{i,\sigma(i)}\Big) + \lambda \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{l,\sigma(k)}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{i,\sigma(i)}\Big) = \\
= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}_{i,\sigma(i)}\Big) + \lambda \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{l,\sigma(k)}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{i,\sigma(i)}\Big) = \det(\mathbf{a}) + \lambda\sum_{\sigma\in\mathfrak{S}(I)} f(\sigma),
\end{aligned}$$

ahol bevezettük az $f : \mathfrak{S}(I) \to A$ függvényt úgy, hogy $I \neq \{k,l\}$ esetén minden $\sigma \in \mathfrak{S}(I)$ permutációra

$$f(\sigma) := \varepsilon_I(\sigma)\mathbf{a}_{l,\sigma(k)}\mathbf{a}_{l,\sigma(l)}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{i,\sigma(i)}\Big),$$

és $I = \{k,l\}$ esetén minden $\sigma \in \mathfrak{S}(I)$ permutációra

$$f(\sigma) := \varepsilon_I(\sigma)\mathbf{a}_{l,\sigma(k)}\mathbf{a}_{l,\sigma(l)}.$$

Nyilvánvaló, hogy ha $I \neq \{k,l\}$, akkor minden $\sigma \in \mathfrak{S}(I)$ esetén

$$\begin{aligned}
f(\sigma\circ\tau_{k,l}) = \varepsilon_I(\sigma\circ\tau_{k,l})\mathbf{a}_{l,\sigma(\tau_{k,l}(k))}\mathbf{a}_{l,\sigma(\tau_{k,l}(l))}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{i,\sigma(\tau_{k,l}(i))}\Big) = \\
= \varepsilon_I(\sigma)\varepsilon_I(\tau_{k,l})\mathbf{a}_{l,\sigma(l)}\mathbf{a}_{l,\sigma(k)}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{i,\sigma(i)}\Big) = -f(\sigma),
\end{aligned}$$

és ha $I = \{k,l\}$, akkor minden $\sigma \in \mathfrak{S}(I)$ esetén

$$f(\sigma\circ\tau_{k,l}) = \varepsilon_I(\sigma\circ\tau_{k,l})\mathbf{a}_{l,\sigma(\tau_{k,l}(k))}\mathbf{a}_{l,\sigma(\tau_{k,l}(l))} = \varepsilon_I(\sigma)\varepsilon_I(\tau_{k,l})\mathbf{a}_{l,\sigma(l)}\mathbf{a}_{l,\sigma(k)} = -f(\sigma).$$

Ezért 13.2.2. alapján $\sum\limits_{\sigma\in\mathfrak{S}(I)} f(\sigma) = 0_A$, tehát $\det(\mathbf{a}') = \det(\mathbf{a})$.

Hasonlóan kapjuk, hogy

$$\begin{aligned}
\det(\mathbf{a}'') = \det({}^{t}(\mathbf{a}'')) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}''_{\sigma(i),i}\Big) = \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}''_{\sigma(k),k}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}''_{\sigma(i),i}\Big) = \\
= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\left(\mathbf{a}_{\sigma(k),k} + \lambda\mathbf{a}_{\sigma(k),l}\right)\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{\sigma(i),i}\Big) = \\
= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{\sigma(k),k}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{\sigma(i),i}\Big) + \lambda \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{\sigma(k),l}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{\sigma(i),i}\Big) = \\
= \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\Big(\prod_{i\in I}\mathbf{a}_{\sigma(i),i}\Big) + \lambda \sum_{\sigma\in\mathfrak{S}(I)} \varepsilon_I(\sigma)\mathbf{a}_{\sigma(k),l}\Big(\prod_{i\in I\setminus\{k\}}\mathbf{a}_{\sigma(i),i}\Big) = \det({}^{t}\mathbf{a}) + \lambda\sum_{\sigma\in\mathfrak{S}(I)} f(\sigma),
\end{aligned}$$

ahol bevezettük az $f : \mathfrak{S}(I) \to A$ függvényt úgy, hogy $I \neq \{k,l\}$ esetén minden $\sigma \in \mathfrak{S}(I)$ permutációra

$$f(\sigma) := \varepsilon_I(\sigma)\mathbf{a}_{\sigma(k),l}\mathbf{a}_{\sigma(l),l}\Big(\prod_{i\in I\setminus\{k,l\}}\mathbf{a}_{\sigma(i),i}\Big),$$

és $I = \{k, l\}$ esetén minden $\sigma \in \mathfrak{S}(I)$ permutációra

$$f(\sigma) := \varepsilon_I(\sigma)\mathbf{a}_{\sigma(k),l}\mathbf{a}_{\sigma(l),l}.$$

Nyilvánvaló, hogy ha $I \neq \{k, l\}$, akkor minden $\sigma \in \mathfrak{S}(I)$ esetén

$$f(\sigma \circ \tau_{k,l}) = \varepsilon_I(\sigma \circ \tau_{k,l})\mathbf{a}_{\sigma(\tau_{k,l}(k)),l}\mathbf{a}_{\sigma(\tau_{k,l}(l)),l}\Big(\prod_{i\in I\setminus\{k,l\}} \mathbf{a}_{\sigma(\tau_{k,l}(i)),i}\Big) =$$
$$= \varepsilon_I(\sigma)\varepsilon_I(\tau_{k,l})\mathbf{a}_{\sigma(l),l}\mathbf{a}_{\sigma(k),l}\Big(\prod_{i\in I\setminus\{k,l\}} \mathbf{a}_{\sigma(i),i}\Big) = -f(\sigma),$$

és ha $I = \{k, l\}$, akkor minden $\sigma \in \mathfrak{S}(I)$ esetén

$$f(\sigma \circ \tau_{k,l}) = \varepsilon_I(\sigma \circ \tau_{k,l})\mathbf{a}_{\sigma(\tau_{k,l}(k)),l}\mathbf{a}_{\sigma(\tau_{k,l}(l)),l} = \varepsilon_I(\sigma)\varepsilon_I(\tau_{k,l})\mathbf{a}_{\sigma(l),l}\mathbf{a}_{\sigma(k),l} = -f(\sigma).$$

Ezért 13.2.2. alapján $\sum_{\sigma\in\mathfrak{S}(I)} f(\sigma) = 0_A$, tehát $\det(\mathbf{a}'') = \det(\mathbf{a})$. ■

15.2.13. Állítás. *Legyen A kommutatív gyűrű, $n \in \mathbb{N}$, valamint $(a_{i,j})_{(i,j)\in(n+1)\times(n+1)} \in \mathrm{M}_{n+1}(A)$. Tegyük fel, hogy minden $j \in n+1$ esetén*

$$a_{0,j} = \begin{cases} 0 & , \text{ ha } j \in n \\ 1 & , \text{ ha } j = n \end{cases}.$$

Ekkor

$$\det\left((a_{i,j})_{(i,j)\in(n+1)\times(n+1)}\right) = (-1)^n \det\left((a_{i+1,j})_{(i,j)\in n\times n}\right),$$

tehát

$$\det\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ a_{1,0} & a_{1,1} & \dots & a_{1,n-1} & a_{1,n} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{n,0} & a_{n,1} & \dots & a_{n,n-1} & a_{n,n} \end{pmatrix} = (-1)^n \det\begin{pmatrix} a_{1,0} & a_{1,1} & \dots & a_{1,n-1} \\ \vdots & \vdots & & \vdots \\ a_{n,0} & a_{n,1} & \dots & a_{n,n-1} \end{pmatrix}.$$

Bizonyítás. A determináns definíciója szerint

$$\det\left((a_{i,j})_{(i,j)\in(n+1)\times(n+1)}\right) = \sum_{\sigma\in\mathfrak{S}_{n+1}} \varepsilon_{n+1}(\sigma)\Big(\prod_{i\in n+1} a_{i,\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_{n+1}} \varepsilon_{n+1}(\sigma)a_{0,\sigma(0)}\Big(\prod_{\substack{i\in n+1\\0<i}} a_{i,\sigma(i)}\Big).$$

Világos, hogy az $n \to \{i \in n+1 | 0 < i\}$; $i \mapsto i+1$ leképezés bijekció, így A szorzásának általános kommutativitása folytán minden $\sigma \in \mathfrak{S}_{n+1}$ esetén

$$\prod_{\substack{i\in n+1\\0<i}} a_{i,\sigma(i)} = \prod_{i\in n} a_{i+1,\sigma(i+1)}.$$

Ebből és az $\mathfrak{S}_{n+1} = \{\sigma \in \mathfrak{S}_{n+1} | \sigma(0) = n\} \cup \{\sigma \in \mathfrak{S}_{n+1} | \sigma(0) \neq n\}$ diszjunkt felbontásból következik, hogy

$$\det\left((a_{i,j})_{(i,j)\in(n+1)\times(n+1)}\right) =$$
$$= \sum_{\substack{\sigma\in\mathfrak{S}_{n+1}\\\sigma(0)=n}} \varepsilon_{n+1}(\sigma)a_{0,n}\Big(\prod_{i\in n} a_{i+1,\sigma(i+1)}\Big) + \sum_{\substack{\sigma\in\mathfrak{S}_{n+1}\\\sigma(0)\neq n}} \varepsilon_{n+1}(\sigma)a_{0,\sigma(0)}\Big(\prod_{i\in n} a_{i+1,\sigma(i+1)}\Big).$$

Az egyenlőség jobb oldalán álló második összeg egyenlő 0-val, mert ha $\sigma \in \mathfrak{S}_{n+1}$ olyan, hogy $\sigma(0) \neq n$, akkor $\sigma(0) \in n$, így a hipotézis szerint $a_{0,\sigma(0)} = 0$. Mivel pedig $a_{0,n} = 1$, így írható, hogy

$$\det\Big((a_{i,j})_{(i,j)\in(n+1)\times(n+1)}\Big) = \sum_{\substack{\sigma\in\mathfrak{S}_{n+1}\\ \sigma(0)=n}} \varepsilon_{n+1}(\sigma)\Big(\prod_{i\in n} a_{i+1,\sigma(i+1)}\Big)$$

Most minden $\tau \in \mathfrak{S}_n$ permutációhoz vezessük be a

$$\sigma_\tau : n+1 \to n+1; \quad i \mapsto \begin{cases} n & \text{, ha } i = 0 \\ \tau(i-1) & \text{, ha } 0 < i \in n+1 \end{cases}$$

leképezést. Nyilvánvaló, hogy minden $\tau \in \mathfrak{S}_n$ esetén $\sigma_\tau \in \mathfrak{S}_{n+1}$ és $\sigma_\tau(0) = n$, továbbá az

$$\mathfrak{S}_n \to \{\sigma \in \mathfrak{S}_{n+1} | \sigma(0) = n\}; \quad \tau \mapsto \sigma_\tau$$

leképezés bijekció, mert $\sigma \in \mathfrak{S}_{n+1}$ és $\sigma(0) = n$ esetén a $\tau : n \to n;\ i \mapsto \sigma(i+1)$ függvényre $\tau \in \mathfrak{S}_n$ és $\sigma_\tau = \sigma$ teljesül. Ezért A összeadásának általános kommutativitása miatt

$$\sum_{\substack{\sigma\in\mathfrak{S}_{n+1}\\ \sigma(0)=n}} \varepsilon_{n+1}(\sigma)\Big(\prod_{i\in n} a_{i+1,\sigma(i+1)}\Big) = \sum_{\tau\in\mathfrak{S}_n} \varepsilon_{n+1}(\sigma_\tau)\Big(\prod_{i\in n} a_{i+1,\sigma_\tau(i+1)}\Big) = \sum_{\tau\in\mathfrak{S}_n} \varepsilon_{n+1}(\sigma_\tau)\Big(\prod_{i\in n} a_{i+1,\tau(i)}\Big),$$

ahol az utolsó egyenlőségnél felhasználtuk azt, hogy $i \in n$ esetén minden $\tau \in \mathfrak{S}_n$ permutációra definíció szerint $\sigma_\tau(i+1) = \tau(i)$. Tehát azt kaptuk, hogy

$$\det\Big((a_{i,j})_{(i,j)\in(n+1)\times(n+1)}\Big) = \sum_{\tau\in\mathfrak{S}_n} \varepsilon_{n+1}(\sigma_\tau)\Big(\prod_{i\in n} a_{i+1,\tau(i)}\Big). \tag{$*$}$$

A bizonyítást azzal fejezzük be, hogy igazoljuk az

$$\varepsilon_{n+1}(\sigma_\tau) = (-1)^n \varepsilon_n(\tau)$$

egyenlőséget minden $\tau \in \mathfrak{S}_n$ esetén. Ha ez az egyenlőség igaz, akkor ezt $(*)$-ba helyettesítve kapjuk a bizonyítandó formulát.

Legyen $\tau \in \mathfrak{S}_n$ rögzítve, és vezessük be a

$$\mathrm{T}(\sigma_\tau) := \{(i,j) \in (n+1)\times(n+1) \mid (i<j) \wedge (\sigma_\tau(i) > \sigma_\tau(j)\},$$
$$\mathrm{T}(\tau) := \{(i,j) \in n \times n \mid (i<j) \wedge (\tau(i) > \tau(j))\}$$

halmazokat. Ekkor a permutációcsoportok előjelfüggvényének alaptulajdonsága szerint

$$\varepsilon_{n+1}(\sigma_\tau) = (-1)^{\mathrm{Card}(\mathrm{T}(\sigma_\tau))},$$
$$\varepsilon_n(\tau) = (-1)^{\mathrm{Card}(\mathrm{T}(\tau))}.$$

Nyilvánvaló, hogy $\mathrm{T}(\sigma_\tau) = \mathrm{T}'(\sigma_\tau) \cup \mathrm{T}''(\sigma_\tau)$, ahol

$$\mathrm{T}'(\sigma_\tau) := \{(0,j) \in (n+1)\times(n+1) \mid (0<j) \wedge (\sigma_\tau(0) > \sigma_\tau(j))\},$$
$$\mathrm{T}''(\sigma_\tau) := \{(i,j) \in (n+1)\times(n+1) \mid (0<i<j) \wedge (\sigma_\tau(i) > \sigma_\tau(j))\},$$

és természetesen $\mathrm{T}'(\sigma_\tau) \cap \mathrm{T}''(\sigma_\tau) = \emptyset$, ezért $\mathrm{Card}(\mathrm{T}(\sigma_\tau)) = \mathrm{Card}(\mathrm{T}'(\sigma_\tau)) + \mathrm{Card}(\mathrm{T}''(\sigma_\tau))$.

Ha $(i,j) \in \mathrm{T}''(\sigma_\tau)$, akkor $(i-1,j-1) \in n \times n$ és $i-1 < j-1$ és $\tau(i-1) = \sigma_\tau(i) > \sigma_\tau(j) = \tau(j-1)$, tehát $(i-1,j-1) \in \mathrm{T}(\tau)$. Megfordítva, ha $(i',j') \in \mathrm{T}(\tau)$, akkor $(i'+1,j'+1) \in (n+1)\times(n+1)$ és $0 < i'+1 < j'+1$ és $\sigma_\tau(i'+1) = \tau(i') < \tau(j') = \sigma_\tau(j'+1)$, tehát $(i'+1,j'+1) \in \mathrm{T}''(\sigma_\tau)$. Ez azt jelenti, hogy a

$$\mathrm{T}''(\sigma_\tau) \to \mathrm{T}(\tau); \quad (i,j) \mapsto (i-1,j-1)$$

leképezés bijekció, ezért $\mathrm{Card}(\mathrm{T}''(\sigma_\tau)) = \mathrm{Card}(\mathrm{T}(\tau))$. Ugyanakkor, $\sigma_\tau(0) = n$, ezért $\mathrm{T}'(\sigma_\tau) = \{(0,j) \in (n+1)\times(n+1) \mid (0 < j) \wedge (n > \sigma_\tau(j))\}$ és $0 < j \in n+1$ esetén $\sigma_\tau(j) = \tau(j-1) < n$ automatikusan teljesül, vagyis $\mathrm{T}'(\sigma_\tau) = \{(0,j) | 0 < j \in n+1\}$. Ebből látható, hogy $\mathrm{Card}(\mathrm{T}'(\sigma_\tau)) = n$, következésképpen

$$\begin{aligned}\varepsilon_{n+1}(\sigma_\tau) = (-1)^{\mathrm{Card}(\mathrm{T}(\sigma_\tau))} &= (-1)^{\mathrm{Card}(\mathrm{T}'(\sigma_\tau))} \cdot (-1)^{\mathrm{Card}(\mathrm{T}''(\sigma_\tau))} = \\ &= (-1)^n \cdot (-1)^{\mathrm{Card}(\mathrm{T}(\tau))} = (-1)^n \varepsilon_n(\tau),\end{aligned}$$

amit bizonyítani kellett. ■

Most a 15.2.11., 15.2.12. és 15.2.13. állítások alkalmazásaként kiszámítjuk a Vandermonde-mátrixok determinánsát.

15.2.14. Definíció. *Ha A egységelemes kommutatív gyűrű, $m \in \mathbb{N}^*$ és $(a_k)_{k\in m} \in A^m$, akkor az $((a_j)^i)_{(i,j)\in m\times m} \in \mathrm{M}_m(A)$ mátrixot az $(a_k)_{k\in m}$ rendszer által meghatározott* **Vandermonde-mátrixnak** *nevezzük, és a $\mathrm{V}((a_k)_{k\in m})$ szimbólummal jelöljük, tehát*

$$\mathrm{V}((a_k)_{k\in m}) := \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_0 & a_1 & \dots & a_{m-1} \\ a_0^2 & a_1^2 & \dots & a_{m-1}^2 \\ \vdots & & & \vdots \\ a_0^{m-1} & a_1^{m-1} & \dots & a_{m-1}^{m-1} \end{pmatrix}.$$

Megjegyezzük, hogy a szakirodalomban néhol a fenti mátrix transzponáltját nevezik Vandermonde-mátrixnak.

15.2.15. Állítás. *Ha A egységelemes kommutatív gyűrű, $m \in \mathbb{N}^*$ és $(a_k)_{k\in m} \in A^m$, akkor*

$$\det(\mathrm{V}((a_k)_{k\in m})) = \mathop{\mathrm{P}}_{\substack{(i,j)\in m\times m \\ i<j}} (a_j - a_i).$$

Bizonyítás. Az állítást 1-től indított m-szerinti teljes indukcióval bizonyítjuk. Ha $m = 1$, akkor az $\{(i,j) \in m\times m | i < j\}$ halmaz *üres*, és az üres rendszer szorzata 1 az A egységelemes kommutatív monoidban, és természetesen ekkor $\det(\mathrm{V}((a_0)_{k\in m})) = 1$ is teljesül.

Tegyük fel, hogy $m \in \mathbb{N}^*$ olyan, hogy minden $(a_k)_{k\in m} \in A^m$ rendszerre fennáll a szóban forgó egyenlőség. Legyen $(a_k)_{k\in m+1} \in A^{m+1}$ rögzített rendszer, és tekintsük a

$$\mathrm{V}((a_k)_{k\in m+1}) := \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ a_0 & a_1 & \dots & a_{m-1} & a_m \\ a_0^2 & a_1^2 & \dots & a_{m-1}^2 & a_m^2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_0^m & a_1^m & \dots & a_{m-1}^m & a_m^m \end{pmatrix}$$

Vandermonde-mátrixot. Ennek utolsó oszlopát kivonjuk az előtte álló oszlopok mindegyikéből: így a következő mátrixot kapjuk:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ a_0 - a_m & a_1 - a_m & \dots & a_{m-1} - a_m & a_m \\ a_0^2 - a_m^2 & a_1^2 - a_m^2 & \dots & a_{m-1}^2 - a_m^2 & a_m^2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_0^m - a_m^m & a_1^m - a_m^m & \dots & a_{m-1}^m - a_m^m & a_m^m \end{pmatrix},$$

és 15.2.12. szerint ennek a mátrixnak a determinánsa ugyanaz, mint a $\mathrm{V}\left((a_k)_{k\in m+1}\right)$ mátrix determinánsa. A 15.2.13. állításból következik, hogy

$$\det\left(\mathrm{V}\left((a_k)_{k\in m+1}\right)\right) = \det \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ a_0 - a_m & a_1 - a_m & \dots & a_{m-1} - a_m & a_m \\ a_0^2 - a_m^2 & a_1^2 - a_m^2 & \dots & a_{m-1}^2 - a_m^2 & a_m^2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_0^m - a_m^m & a_1^m - a_m^m & \dots & a_{m-1}^m - a_m^m & a_m^m \end{pmatrix} =$$

$$= (-1)^m \cdot \det \begin{pmatrix} a_0 - a_m & a_1 - a_m & \dots & a_{m-1} - a_m \\ a_0^2 - a_m^2 & a_1^2 - a_m^2 & \dots & a_{m-1}^2 - a_m^2 \\ \vdots & \vdots & & \vdots \\ a_0^m - a_m^m & a_1^m - a_m^m & \dots & a_{m-1}^m - a_m^m \end{pmatrix}.$$

Az utolsóként felírt $m \times m$-es mátrix (i,j)-edik komponense $a_j^{i+1} - a_m^{i+1}$, és nyilvánvaló, hogy

$$a_j^{i+1} - a_m^{i+1} = (a_j - a_m) \sum_{k=0}^{i} a_j^{i-k} a_m^k.$$

Ezért 15.2.7. alapján

$$\begin{aligned} \det\left(\mathrm{V}\left((a_k)_{k\in m+1}\right)\right) &= (-1)^m \det \begin{pmatrix} a_0 - a_m & a_1 - a_m & \dots & a_{m-1} - a_m \\ a_0^2 - a_m^2 & a_1^2 - a_m^2 & \dots & a_{m-1}^2 - a_m^2 \\ \vdots & \vdots & & \vdots \\ a_0^m - a_m^m & a_1^m - a_m^m & \dots & a_{m-1}^m - a_m^m \end{pmatrix} = \\ &= (-1)^m \left(\prod_{i=0}^{m-1} (a_i - a_m) \right) \det\left(\left(\sum_{k=0}^{i} a_j^{i-k} a_m^k \right)_{(i,j)\in m\times m} \right) = \\ &= \left(\prod_{i=0}^{m-1} (a_m - a_i) \right) \det\left(\left(\sum_{k=0}^{i} a_j^{i-k} a_m^k \right)_{(i,j)\in m\times m} \right). \end{aligned} \tag{1}$$

Most közvetlenül kiszámoljuk a $\left(\sum_{k=0}^{i} a_j^{i-k} a_m^k \right)_{(i,j)\in m\times m} \in \mathrm{M}_m(A)$ mátrix determinánsát.

A definíció szerint

$$\det\Big(\Big(\sum_{k=0}^{i} a_j^{i-k}a_m^k\Big)_{(i,j)\in m\times m}\Big) = \sum_{\sigma\in\mathfrak{S}_m}\varepsilon_m(\sigma)\Big(\prod_{i=0}^{m-1}\Big(\sum_{k=0}^{i} a_{\sigma(i)}^{i-k}a_m^k\Big)\Big) =$$

$$= \sum_{\sigma\in\mathfrak{S}_m}\varepsilon_m(\sigma)\sum_{\tau\in\prod\limits_{i\in m}(i+1)}\Big(\prod_{i=0}^{m-1} a_{\sigma(i)}^{i-\tau(i)}a_m^{\tau(i)}\Big) = \sum_{\tau\in\prod\limits_{i\in m}(i+1)} a_m^{\sum\limits_{k\in m}\tau(k)}\sum_{\sigma\in\mathfrak{S}_m}\varepsilon_m(\sigma)\Big(\prod_{i=0}^{m-1} a_{\sigma(i)}^{i-\tau(i)}\Big) =$$

$$= \sum_{\sigma\in\mathfrak{S}_m}\varepsilon_m(\sigma)\Big(\prod_{i=0}^{m-1} a_{\sigma(i)}^{i}\Big) + \sum_{\substack{\tau\in\prod\limits_{i\in m}(i+1)\\ \tau\neq 0}} a_m^{\sum\limits_{k\in m}\tau(k)}\sum_{\sigma\in\mathfrak{S}_m}\varepsilon_m(\sigma)\Big(\prod_{i=0}^{m-1} a_{\sigma(i)}^{i-\tau(i)}\Big) =$$

$$= \det\left(\mathrm{V}\left((a_k)_{k\in m}\right)\right) + \sum_{\substack{\tau\in\prod\limits_{i\in m}(i+1)\\ \tau\neq 0}} a_m^{\sum\limits_{k\in m}\tau(k)}\det\Big(\Big(a_j^{i-\tau(i)}\Big)_{(i,j)\in m\times m}\Big). \qquad (2)$$

Megmutatjuk, hogy minden $\tau\in\prod\limits_{i\in m}(i+1)$ esetén, ha $\tau\neq 0$, akkor

$$\det\Big(\Big(a_j^{i-\tau(i)}\Big)_{(i,j)\in m\times m}\Big) = 0.$$

Valóban, ha $\tau\in\prod\limits_{i\in m}(i+1)$ és az $m\to m;\ i\mapsto i-\tau(i)$ függvény injektív, akkor 8.1.16. szerint ez a függvény szürjektív is, ezért 8.2.7. alapján ez a függvény egyenlő m identikus függvényével, vagyis minden $i\in m$ esetén $i-\tau(i)=i$, azaz $\tau=0$. Tehát, ha $\tau\in\prod\limits_{i\in m}(i+1)$, akkor $\tau\neq 0$ esetén az $m\to m;\ i\mapsto i-\tau(i)$ függvény *nem injektív*, ami azt jelenti, hogy a $\Big(a_j^{i-\tau(i)}\Big)_{(i,j)\in m\times m}$ mátrixnak van két egyenlő sora, így 15.2.10. b) szerint $\det\Big(\Big(a_j^{i-\tau(i)}\Big)_{(i,j)\in m\times m}\Big)=0$.

Ebből és az (1) és (2) egyenlőségekből következik, hogy

$$\det\left(\mathrm{V}\left((a_k)_{k\in m+1}\right)\right) = \Big(\prod_{i=0}^{m-1}(a_m-a_i)\Big)\det\left(\mathrm{V}\left((a_k)_{k\in m}\right)\right),$$

és az indukciós hipotézis szerint

$$\det\left(\mathrm{V}\left((a_k)_{k\in m}\right)\right) = \prod_{\substack{(i,j)\in m\times m\\ i<j}}(a_j-a_i),$$

amiből kapjuk, hogy

$$\det\left(\mathrm{V}\left((a_k)_{k\in m+1}\right)\right) = \Big(\prod_{i=0}^{m-1}(a_m-a_i)\Big)\prod_{\substack{(i,j)\in m\times m\\ i<j}}(a_j-a_i) = \prod_{\substack{(i,j)\in (m+1)\times(m+1)\\ i<j}}(a_j-a_i),$$

amivel az indukciót végrehajtottuk. ■

15.3. Gyűrű feletti mátrix nyoma

15.3.1. Definíció. *Legyen A gyűrű és I véges halmaz. Ekkor minden $\mathbf{a} \in \mathrm{M}_I(A)$ esetén*

$$\mathrm{tr}(\mathbf{a}) := \sum_{i \in I} \mathbf{a}_{i,i},$$

és a $\mathrm{tr}(\mathbf{a}) \in A$ elemet az $\mathbf{a}$ mátrix **nyomának** *nevezzük, továbbá az*

$$\mathrm{M}_I(A) \to A; \quad \mathbf{a} \mapsto \mathrm{tr}(\mathbf{a})$$

leképezést az $\mathrm{M}_I(A)$ mátrixgyűrű feletti **nyom-formának** *nevezzük.*

15.3.2. Állítás. *Legyen A gyűrű és I véges halmaz. Ekkor minden $\mathbf{a}, \mathbf{b} \in \mathrm{M}_I(A)$ és $\lambda \in A$ esetén*

$$\mathrm{tr}({}^{\mathrm{t}}\mathbf{a}) = \mathrm{tr}(\mathbf{a}),$$
$$\mathrm{tr}(\lambda.\mathbf{a}) = \lambda \mathrm{tr}(\mathbf{a}),$$
$$\mathrm{tr}(\mathbf{a} + \mathbf{b}) = \mathrm{tr}(\mathbf{a}) + \mathrm{tr}(\mathbf{b}).$$

Ha az A gyűrű kommutatív, akkor minden $\mathbf{a}, \mathbf{b} \in \mathrm{M}_I(A)$ esetén

$$\mathrm{tr}(\mathbf{a} \cdot \mathbf{b}) = \mathrm{tr}(\mathbf{b} \cdot \mathbf{a}).$$

Bizonyítás. Ha $\mathbf{a}, \mathbf{b} \in \mathrm{M}_I(A)$ és $\lambda \in A$, akkor a definíciók szerint

$$\mathrm{tr}({}^{\mathrm{t}}\mathbf{a}) = \sum_{i \in I} ({}^{\mathrm{t}}\mathbf{a})_{i,i} = \sum_{i \in I} \mathbf{a}_{i,i} = \mathrm{tr}(\mathbf{a});$$
$$\mathrm{tr}(\lambda.\mathbf{a}) = \sum_{i \in I} (\lambda \mathbf{a})_{i,i} = \sum_{i \in I} \lambda \mathbf{a}_{i,i} = \lambda \sum_{i \in I} \mathbf{a}_{i,i} = \lambda \mathrm{tr}(\mathbf{a});$$
$$\mathrm{tr}(\mathbf{a} + \mathbf{b}) = \sum_{i \in I} (\mathbf{a} + \mathbf{b})_{i,i} = \sum_{i \in I} (\mathbf{a}_{i,i} + \mathbf{b}_{i,i}) = \sum_{i \in I} \mathbf{a}_{i,i} + \sum_{i \in I} \mathbf{b}_{i,i} = \mathrm{tr}(\mathbf{a}) + \mathrm{tr}(\mathbf{b}).$$

Tegyük fel, hogy A kommutatív gyűrű és $\mathbf{a}, \mathbf{b} \in \mathrm{M}_I(A)$. Ekkor

$$\mathrm{tr}(\mathbf{a} \cdot \mathbf{b}) = \sum_{i \in I} (\mathbf{a} \cdot \mathbf{b})_{i,i} = \sum_{i \in I} \Big(\sum_{j \in I} \mathbf{a}_{i,j} \mathbf{b}_{j,i} \Big) = \sum_{j \in I} \Big(\sum_{i \in I} \mathbf{a}_{i,j} \mathbf{b}_{j,i} \Big) =$$
$$= \sum_{j \in I} \Big(\sum_{i \in I} \mathbf{b}_{j,i} \mathbf{a}_{i,j} \Big) = \sum_{j \in I} (\mathbf{b} \cdot \mathbf{a})_{j,j} = \mathrm{tr}(\mathbf{b} \cdot \mathbf{a}). \blacksquare$$

15.3.3. Következmény. *Legyen A kommutatív egységelemes gyűrű és I véges halmaz. Ha $\mathbf{a} \in \mathrm{M}_I(A)$, valamint $\mathbf{b} \in \mathrm{M}_I(A)$ invertálható mátrix, akkor*

$$\mathrm{tr}(\mathbf{b}^{-1} \cdot \mathbf{a} \cdot \mathbf{b}) = \mathrm{tr}(\mathbf{a}).$$

Bizonyítás. Ha $\mathbf{a} \in \mathrm{M}_I(A)$ tetszőleges és $\mathbf{b} \in \mathrm{M}_I(A)$ invertálható mátrix, akkor a mátrixszorzás asszociativitása és az előző állítás szerint

$$\mathrm{tr}\left(\mathbf{b}^{-1} \cdot \mathbf{a} \cdot \mathbf{b}\right) = \mathrm{tr}\left(\mathbf{b}^{-1} \cdot (\mathbf{a} \cdot \mathbf{b})\right) = \mathrm{tr}\left((\mathbf{a} \cdot \mathbf{b}) \cdot \mathbf{b}^{-1}\right) = \mathrm{tr}\left(\mathbf{a} \cdot \left(\mathbf{b} \cdot \mathbf{b}^{-1}\right)\right) = \mathrm{tr}(\mathbf{a}). \blacksquare$$

15.4. Kifejtési tétel

Ha $p \in \mathbb{N}$ és $k \in p+1$, akkor $\mathrm{Card}((p+1) \setminus \{k\}) = p$, ezért létezik bijekció p és $(p+1) \setminus \{k\}$ között, és mivel mindkét halmaz lineárisan rendezett a természetes számok rendezése által, így 8.2.5. szerint létezik egyetlen olyan $p \to (p+1) \setminus \{k\}$ bijekció, amely *szigorúan monoton növő.* Mivel ez a függvény gyakran előfordul a determinánsok elméletében, így külön jelölést vezetünk be rá.

15.4.1. Definíció. *Ha $p \in \mathbb{N}$ és $k \in p+1$, akkor $\mathrm{m}_{p,k} : p \to (p+1) \setminus \{k\}$ jelöli az (egyértelműen meghatározott) szigorúan monoton növő bijekciót, vagyis minden $i \in p$ esetén*

$$\mathrm{m}_{p,k}(i) := \begin{cases} i & , \text{ha } i < k, \\ i+1 & , \text{ha } k \le i < p. \end{cases}$$

15.4.2. Definíció. *Legyen A kommutatív gyűrű, $n \in \mathbb{N}$, $n \geq 2$, és $\mathbf{a} \in \mathrm{M}_n(A)$. Minden $(k,l) \in n \times n$ esetén $\hat{\mathbf{a}}_{k,l} \in \mathrm{M}_{n-1}(A)$ az a mátrix, amelyre minden $(i,j) \in (n-1) \times (n-1)$ esetén*

$$\left(\hat{\mathbf{a}}_{k,l}\right)_{i,j} := \mathbf{a}_{\mathrm{m}_{n-1,k}(i),\mathrm{m}_{n-1,l}(j)},$$

és a $\det(\hat{\mathbf{a}}_{k,l}) \in A$ elemet az $\mathbf{a}$ mátrix (k,l)-edik **aldeterminánsának** *nevezzük. Továbbá, $\mathrm{adj}(\mathbf{a})$ jelöli azt az $n \times n$-es mátrixot, amelyre minden $(k,l) \in n \times n$ esetén*

$$(\mathrm{adj}(\mathbf{a}))_{k,l} := (-1)^{k+l} \det(\hat{\mathbf{a}}_{l,k}),$$

és az $\mathrm{adj}(\mathbf{a}) \in \mathrm{M}_n(A)$ mátrixot az $\mathbf{a}$ mátrix **adjungáltjának** *nevezzük.*

Megjegyezzük, hogy a szakirodalomban néhol a $(-1)^{k+l}\det(\hat{\mathbf{a}}_{k,l}) \in A$ elemet nevezik az $\mathbf{a}$ mátrix (k,l)-edik aldeterminánsának. Mi a fenti definícióhoz tartjuk magunkat.

Vigyázzunk arra, hogy az adjungált mátrix (k,l)-edik komponensének definíciójában a mátrix (l,k)-adik aldeterminánsa szerepel, nem pedig a (k,l)-edik!

A definíciók alapján nyilvánvaló, hogy ha A kommutatív gyűrű, $n \in \mathbb{N}$, $n \geq 2$, és $\mathbf{a} \in \mathrm{M}_n(A)$, akkor minden $(k,l) \in n \times n$ és $(i,j) \in (n-1) \times (n-1)$ esetén

$$\left(\hat{\mathbf{a}}_{k,l}\right)_{i,j} := \begin{cases} \mathbf{a}_{i,j} & , \text{ha } i < k \text{ és } j < l, \\ \mathbf{a}_{i,j+1} & , \text{ha } i < k \text{ és } j \geq l, \\ \mathbf{a}_{i+1,j} & , \text{ha } i \geq k \text{ és } j < l, \\ \mathbf{a}_{i+1,j+1} & , \text{ha } i \geq k \text{ és } j \geq l, \end{cases}$$

tehát az $(n-1) \times (n-1)$-szeres $\hat{\mathbf{a}}_{k,l}$ mátrixot úgy kaphatjuk $\mathbf{a}$-ból, hogy annak k-adik sorát és l-edik oszlopát töröljük.

15.4.3. Lemma. *Legyen A kommutatív gyűrű, és $n \in \mathbb{N}$, $n \geq 2$. Ha $\mathbf{a}, \mathbf{b} \in \mathrm{M}_n(A)$ és $\lambda \in A$, akkor minden $(k,l) \in n \times n$ esetén*

$$\widehat{(\mathbf{a}+\mathbf{b})}_{k,l} = \hat{\mathbf{a}}_{k,l} + \hat{\mathbf{b}}_{k,l},$$
$$\widehat{(\lambda\mathbf{a})}_{k,l} = \lambda\hat{\mathbf{a}}_{k,l}.$$

Bizonyítás. A definíciók alapján minden $(i,j) \in (n-1) \times (n-1)$ párra

$$\left(\widehat{(\mathbf{a}+\mathbf{b})}_{k,l}\right)_{i,j} = (\mathbf{a}+\mathbf{b})_{\mathrm{m}_{n-1,k}(i),\mathrm{m}_{n-1,l}(j)} = \mathbf{a}_{\mathrm{m}_{n-1,k}(i),\mathrm{m}_{n-1,l}(j)} + \mathbf{b}_{n-1,k(i),\mathrm{m}_{n-1,l}(j)} =$$
$$= \left(\hat{\mathbf{a}}_{k,l}\right)_{i,j} + \left(\hat{\mathbf{b}}_{k,l}\right)_{i,j} = \left(\hat{\mathbf{a}}_{k,l} + \hat{\mathbf{b}}_{k,l}\right)_{i,j},$$

valamint

$$\left(\widehat{(\lambda\mathbf{a})}_{k,l}\right)_{i,j} = (\lambda\mathbf{a})_{\mathrm{m}_{n-1,k}(i),\mathrm{m}_{n-1,l}(j)} = \lambda\mathbf{a}_{\mathrm{m}_{n-1,k}(i),\mathrm{m}_{n-1,l}(j)} = \lambda\left(\hat{\mathbf{a}}_{k,l}\right)_{i,j} = \left(\lambda\hat{\mathbf{a}}_{k,l}\right)_{i,j}. \blacksquare$$

15.4.4. Lemma. *Legyen A kommutatív gyűrű, $n \in \mathbb{N}$, $n \geq 2$, és $\mathbf{a} \in \mathrm{M}_n(A)$. Minden $(k,l) \in n \times n$ esetén*

$$^{\mathrm{t}}\left(\hat{\mathbf{a}}_{l,k}\right) = \widehat{(^{\mathrm{t}}\mathbf{a})}_{k,l}.$$

Bizonyítás. Ha $(i,j) \in (n-1) \times (n-1)$, akkor a definíció szerint

$$\left(^{\mathrm{t}}\left(\hat{\mathbf{a}}_{l,k}\right)\right)_{i,j} = \left(\hat{\mathbf{a}}_{l,k}\right)_{j,i} = \mathbf{a}_{\mathrm{m}_{n-1,l}(j),\mathrm{m}_{n-1,k}(i)} = (^{\mathrm{t}}\mathbf{a})_{\mathrm{m}_{n-1,k}(i),\mathrm{m}_{n-1,l}(j)} = \left(\widehat{(^{\mathrm{t}}\mathbf{a})}_{k,l}\right)_{i,j},$$

ezért $^{\mathrm{t}}\left(\hat{\mathbf{a}}_{l,k}\right) = \widehat{(^{\mathrm{t}}\mathbf{a})}_{k,l}$. $\blacksquare$

15.4.5. Lemma. *Legyen A kommutatív gyűrű, $n \in \mathbb{N}$, $n \geq 2$, és $\mathbf{a} \in \mathrm{M}_n(A)$. Legyen $(k,l) \in n \times n$ olyan pár, amelyre a következő feltételek valamelyike teljesül:*

a) *minden $j \in n \setminus \{l\}$ indexre $\mathbf{a}_{k,j} = 0_A$ (vagyis az $\mathbf{a}$ mátrix k-adik sorában, az l-edik tagot kivéve minden komponens 0_A);*

b) *minden $i \in n \setminus \{k\}$ indexre $\mathbf{a}_{i,l} = 0_A$ (vagyis az $\mathbf{a}$ mátrix l-edik oszlopában, a k-adik tagot kivéve minden komponens 0_A).*

Ekkor

$$\det(\mathbf{a}) = (-1)^{k+l}\mathbf{a}_{k,l}\det\left(\hat{\mathbf{a}}_{k,l}\right).$$

Bizonyítás. (I) Tegyük fel, hogy az a) feltétel teljesül, tehát ha $\sigma \in \mathfrak{S}_n$, akkor

$$\mathbf{a}_{k,\sigma(k)} = \begin{cases} \mathbf{a}_{k,l} & \text{, ha } \sigma(k) = l, \\ 0 & \text{, ha } \sigma(k) \neq l, \end{cases}$$

következésképpen

$$\det(\mathbf{a}) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma)\Big(\prod_{i \in n} \mathbf{a}_{i,\sigma(i)}\Big) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma)\mathbf{a}_{k,\sigma(k)}\Big(\prod_{i \in n\setminus\{k\}} \mathbf{a}_{i,\sigma(i)}\Big) =$$
$$= \mathbf{a}_{k,l} \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(k)=l}} \varepsilon_n(\sigma)\Big(\prod_{i \in n\setminus\{k\}} \mathbf{a}_{i,\sigma(i)}\Big).$$

Ha $\sigma \in \mathfrak{S}_n$ olyan, hogy $\sigma(k) = l$, akkor $\sigma|_{n\setminus\{k\}} : n \setminus \{k\} \to n \setminus \{l\}$ bijekció, így $\mathrm{m}_{n-1,l}^{-1} \circ \left(\sigma|_{n\setminus\{k\}}\right) \circ \mathrm{m}_{n-1,k} \in \mathfrak{S}_{n-1}$. Ez azt jelenti, hogy ha bevezetjük az

$$f : \mathfrak{S}_{n-1} \to \{\sigma \in \mathfrak{S}_n | \sigma(k) = l\}$$

leképezést, amelyre minden $\sigma' \in \mathfrak{S}_{n-1}$ esetén $f(\sigma')|_{n\setminus\{k\}} = \mathrm{m}_{n-1,l} \circ \sigma' \circ \mathrm{m}_{n-1,k}^{-1}$ és $f(\sigma')(k) = l$, akkor f *bijekció*. Mivel pedig a $\mathrm{m}_{n-1,k} : n-1 \to n \setminus \{k\}$ leképezés bijekció, így

$$\sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(k)=l}} \varepsilon_n(\sigma)\Big(\prod_{i \in n\setminus\{k\}} \mathbf{a}_{i,\sigma(i)}\Big) = \sum_{\sigma' \in \mathfrak{S}_{n-1}} \varepsilon_n(f(\sigma'))\Big(\prod_{i \in n\setminus\{k\}} \mathbf{a}_{i,f(\sigma')(i)}\Big) =$$
$$= \sum_{\sigma' \in \mathfrak{S}_{n-1}} \varepsilon_n(f(\sigma'))\Big(\prod_{j \in n-1} \mathbf{a}_{\mathrm{m}_{n-1,k}(j),f(\sigma')\left(\mathrm{m}_{n-1,k}(j)\right)}\Big) \overset{(*)}{=}$$
$$\overset{(*)}{=} \sum_{\sigma' \in \mathfrak{S}_{n-1}} \varepsilon_n(f(\sigma'))\Big(\prod_{j \in n-1} \mathbf{a}_{\mathrm{m}_{n-1,k}(j),\mathrm{m}_{n-1,l}(\sigma'(j))}\Big) = \sum_{\sigma' \in \mathfrak{S}_{n-1}} \varepsilon_n(f(\sigma'))\Big(\prod_{j \in n-1} \hat{\mathbf{a}}_{j,\sigma'(j)}\Big), \tag{1}$$

ahol az $\overset{(*)}{=}$ egyenlőségnél azt használtuk fel, hogy minden $\sigma' \in \mathfrak{S}_{n-1}$ és $j \in n-1$ esetén f definíciója szerint

$$f(\sigma')\left(\mathrm{m}_{n-1,k}(j)\right) = \left(\mathrm{m}_{n-1,l} \circ \sigma' \circ \mathrm{m}_{n-1,k}^{-1}\right)\left(\mathrm{m}_{n-1,k}(j)\right) = \mathrm{m}_{n-1,l}(\sigma'(j)).$$

Ebből látható, hogy a kívánt egyenlőség igazolásához tisztázni kell az $\varepsilon_n(f(\sigma'))$ és $\varepsilon_{n-1}(\sigma')$ előjelek kapcsolatát, ahol $\sigma' \in \mathfrak{S}_{n-1}$ tetszőleges.

Legyen tehát $\sigma' \in \mathfrak{S}_{n-1}$ rögzített, és vezessük be a

$$\mathrm{T}(f(\sigma')) := \{(i,j) \in n \times n | (i < j) \wedge (f(\sigma')(i) > f(\sigma')(j))\},$$
$$\mathrm{T}(\sigma') := \{((i,j) \in (n-1) \times (n-1) | (i < j) \wedge (\sigma'(i) > \sigma'(j))\}$$

halmazokat. A 13.3.4. állításból tudjuk, hogy

$$\varepsilon_n(f(\sigma')) = (-1)^{\mathrm{Card}(\mathrm{T}(f(\sigma')))}, \quad \varepsilon_{n-1}(\sigma') = (-1)^{\mathrm{Card}(\mathrm{T}(\sigma'))},$$

tehát csak a $\mathrm{T}(f(\sigma'))$ és $\mathrm{T}(\sigma')$ halmazok számosságának kapcsolata érdekes.

Ha $(i,j) \in \mathrm{T}(\sigma')$, akkor $i < j$, így a $\mathrm{m}_{n-1,k}$ függvény szigorú monoton növése miatt $\mathrm{m}_{n-1,k}(i) < \mathrm{m}_{n-1,k}(j)$, ugyanakkor $\sigma'(i) > \sigma'(j)$, így a $\mathrm{m}_{n-1,l}$ függvény szigorú monoton növése miatt $\mathrm{m}_{n-1,l}(\sigma'(i)) > \mathrm{m}_{n-1,l}(\sigma'(j))$, tehát az f függvény definíciója szerint

$$f(\sigma')\left(\mathrm{m}_{n-1,k}(i)\right) = \left(\mathrm{m}_{n-1,l} \circ \sigma' \circ \mathrm{m}_{n-1,k}^{-1}\right)\left(\mathrm{m}_{n-1,k}(i)\right) = \mathrm{m}_{n-1,l}\left(\sigma'(i)\right) >$$
$$> \mathrm{m}_{n-1,l}\left(\sigma'(j)\right) = \left(\mathrm{m}_{n-1,l} \circ \sigma' \circ \mathrm{m}_{n-1,k}^{-1}\right)\left(\mathrm{m}_{n-1,k}(j)\right) = f(\sigma')\left(\mathrm{m}_{n-1,k}(j)\right),$$

következésképpen $(\mathrm{m}_{n-1,k}(i), \mathrm{m}_{n-1,k}(j)) \in \mathrm{T}(f(\sigma'))$. Ezért jól értelmezett a

$$\varphi : \mathrm{T}(\sigma') \to \mathrm{T}(f(\sigma')); \quad (i,j) \mapsto (\mathrm{m}_{n-1,k}(i), \mathrm{m}_{n-1,k}(j))$$

függvény, amely $\mathrm{m}_{n-1,k}$ injektivitása folytán nyilvánvalóan injektív.

Az $\mathrm{Im}\,(\mathrm{m}_{n-1,k}) = n \setminus \{k\}$ egyenlőség miatt világos, hogy

$$\mathrm{Im}(\varphi) \subseteq \{(\tilde{i},\tilde{j}) \in \mathrm{T}(f(\sigma')) | (\tilde{i} \neq k) \wedge (\tilde{j} \neq k\}.$$

Megmutatjuk, hogy itt egyenlőség áll. Ehhez legyen $(\tilde{i},\tilde{j}) \in \mathrm{T}(f(\sigma'))$ olyan pár, hogy $\tilde{i} \neq k \neq \tilde{j}$. Legyenek $i := \mathrm{m}_{n-1,k}^{-1}(\tilde{i})$ és $j := \mathrm{m}_{n-1,k}^{-1}(\tilde{j})$. Mivel $\tilde{i} < \tilde{j}$ és a $\mathrm{m}_{n-1,k}$ függvény szigorú monoton növő, így $i < j$. Továbbá, $f(\sigma')(\tilde{i}) > f(\sigma')(\tilde{j})$, ezért f definíciója szerint

$$\mathrm{m}_{n-1,l}(\sigma'(i)) = \mathrm{m}_{n-1,l}\left(\sigma'\left(\mathrm{m}_{n-1,k}^{-1}(\tilde{i})\right)\right) = f(\sigma')(\tilde{i}) >$$
$$> f(\sigma')(\tilde{j}) = \mathrm{m}_{n-1,l}\left(\sigma'\left(\mathrm{m}_{n-1,k}^{-1}(\tilde{j})\right)\right) = \mathrm{m}_{n-1,l}(\sigma'(j)),$$

így a $\mathrm{m}_{n-1,l}$ függvény szigorú monoton növése miatt $\sigma'(i) > \sigma'(j)$, következésképpen $(i,j) \in \mathrm{T}(\sigma')$ és $\varphi(i,j) = (\tilde{i},\tilde{j})$. Ezért

$$\varphi\langle\mathrm{T}(\sigma')\rangle = \{(\tilde{i},\tilde{j}) \in \mathrm{T}(f(\sigma')) | (\tilde{i} \neq k) \wedge (\tilde{j} \neq k\}.$$

Vezessük be a következő halmazokat:

$$A(\sigma') := \{(\tilde{i},\tilde{j}) \in \mathrm{T}(f(\sigma')) | \tilde{i} = k\}, \quad B(\sigma') := \{(\tilde{i},\tilde{j}) \in \mathrm{T}(f(\sigma')) | \tilde{j} = k\}.$$

Nyilvánvaló, hogy

$$\mathrm{T}(f(\sigma')) = \varphi\langle\mathrm{T}(\sigma')\rangle \cup A(\sigma') \cup B(\sigma'),$$

és a jobb oldalon álló halmazok páronként disztjunktak, tehát

$$\mathrm{Card}\,(\mathrm{T}(f(\sigma'))) = \mathrm{Card}\,(\mathrm{T}(\sigma')) + \mathrm{Card}(A(\sigma')) + \mathrm{Card}(B(\sigma')),$$

amiből következik, hogy

$$\varepsilon_n(f(\sigma')) = \varepsilon_{n-1}(\sigma') \cdot (-1)^{\mathrm{Card}(A(\sigma'))+\mathrm{Card}(B(\sigma'))}. \tag{2}$$

Ha $j \in \llbracket k, n-1\llbracket$ és $\sigma'(j) \in \llbracket 0, l\llbracket$, akkor f és $\mathrm{m}_{n-1,l}$ definíciója szerint $f(\sigma')(k) = l > \sigma'(j) = \mathrm{m}_{n-1,l}\,(\sigma'(j)) = f(\sigma')\,(\mathrm{m}_{n-1,k}(j))$, valamint $\mathrm{m}_{n-1,k}$ definíciója szerint $k < j+1 = \mathrm{m}_{n-1,k}(j)$, tehát $(k, \mathrm{m}_{n-1,k}(j)) \in A(\sigma')$. Megfordítva, ha $(k, \tilde{j}) \in A(\sigma')$, akkor $k < \tilde{j}$, így $\tilde{j} \in n \setminus \{k\}$, tehát jól értelmezett a $j := \mathrm{m}_{n-1,k}^{-1}(\tilde{j}) \in n-1$ elem, és ekkor $k < \tilde{j} = \mathrm{m}_{n-1,k}(j)$, továbbá f és $\mathrm{m}_{n-1,l}$ definíciója szerint $l = f(\sigma')(k) > f(\sigma')(\tilde{j}) = f(\sigma')\,(\mathrm{m}_{n-1,k}(j)) = \mathrm{m}_{n-1,l}(\sigma'(j))$, így $\sigma'(j) \in \overset{-1}{\mathrm{m}}_{n-1,l}\langle\llbracket 0, l\rrbracket\rangle = \llbracket 0, l\llbracket$, vagyis $j \in \llbracket k, n-1\llbracket$ és $\sigma'(j) \in \llbracket 0, l\llbracket$ és $(k, \mathrm{m}_{n-1,k}(j)) = (k, \tilde{j})$. Ez azt jelenti, hogy a

$$\llbracket k, n-1\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle \to A(\sigma'); \quad j \mapsto (k, \mathrm{m}_{n-1,k}(j))$$

leképezés bijekció, hiszen a $\mathrm{m}_{n-1,k}$ függvény injektív. Ezért

$$\mathrm{Card}(A(\sigma')) = \mathrm{Card}\left(\llbracket k, n-1\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle\right).$$

Ha $i \in \llbracket 0, k\llbracket$ és $\sigma'(i) \in \llbracket l, n-1\llbracket$, akkor $\mathrm{m}_{n-1,k}$ definíciója szerint $\mathrm{m}_{n-1,k}(i) = i < k$, ugyanakkor f és $\mathrm{m}_{n-1,l}$ definíciója szerint $f\,(\mathrm{m}_{n-1,k}(i)) = \mathrm{m}_{n-1,l}(\sigma'(i)) = \sigma'(i) + 1 > l = f(\sigma')(k)$, tehát $(\mathrm{m}_{n-1,k}(i), k) \in B(\sigma')$. Megfordítva, ha $(\tilde{i}, k) \in B(\sigma')$, akkor $\tilde{i} < k$, így $\tilde{i} \in n \setminus \{k\}$, tehát jól értelmezett a $i := \mathrm{m}_{n-1,k}^{-1}(\tilde{i}) \in n-1$ elem, és ekkor $\mathrm{m}_{n-1,k}(i) = \tilde{i} < k$, így $\mathrm{m}_{n-1,k}$ definíciója szerint $i < k$, továbbá f szerint $\mathrm{m}_{n-1,l}(\sigma'(i)) = f(\sigma')\,(\mathrm{m}_{n-1,k}(i)) = f(\sigma')(\tilde{i}) > f(\sigma')(k) = l$, így és $\mathrm{m}_{n-1,l}$ definíciója alapján $\sigma'(i) \geq l$. Tehát $i \in \llbracket 0, k\llbracket$ és $\sigma'(i) \in \llbracket l, n-1\llbracket$, és $(\mathrm{m}_{n-1,k}(i), k) = (\tilde{i}, k)$. Ez azt jelenti, hogy a

$$\llbracket 0, k\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket l, n-1\rrbracket\rangle \to B(\sigma'); \quad i \mapsto (\mathrm{m}_{n-1,k}(i), k)$$

leképezés bijekció, hiszen a $\mathrm{m}_{n-1,k}$ függvény injektív. Ezért

$$\mathrm{Card}(B(\sigma')) = \mathrm{Card}\left(\llbracket 0, k\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket l, n-1\rrbracket\rangle\right).$$

Nyilvánvaló, hogy $\overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle \subseteq \llbracket 0, n-1\llbracket$ miatt

$$\overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle = \left(\llbracket 0, k\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle\right) \;\cup\; \left(\llbracket k, n-1\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle\right),$$

és a jobb oldalon diszjunkt halmazok állnak, így

$$l = \mathrm{Card}\left(\overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle\right) = \mathrm{Card}\left(\llbracket 0, k\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle\right) + \mathrm{Card}\left(\llbracket k, n-1\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle\right). \tag{3}$$

Az is nyilvánvaló, hogy

$$\llbracket 0, k\llbracket = \left(\llbracket 0, k\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket 0, l\rrbracket\rangle\right) \;\cup\; \left(\llbracket 0, k\llbracket \;\cap\; \overset{-1}{\sigma'}\langle\llbracket l, n-1\rrbracket\rangle\right),$$

és a jobb oldalon diszjunkt halmazok állnak, így

$$k = \mathrm{Card}\,([\![0,k[\![) = \mathrm{Card}\left([\![0,k[\![\ \cap\ \overset{-1}{\sigma'}\langle[\![0,l[\![\rangle\right) + \mathrm{Card}\left([\![0,k[\![\ \cap\ \overset{-1}{\sigma'}\langle[\![l,n-1[\![\rangle\right). \quad (4)$$

Összeadva a (4) és (3) egyenlőségeket kapjuk, hogy

$$k+l = 2\cdot\mathrm{Card}\left([\![0,k[\![\ \cap\ \overset{-1}{\sigma'}\langle[\![0,l[\![\rangle\right) + \mathrm{Card}\left([\![0,k[\![\ \cap\ \overset{-1}{\sigma'}\langle[\![l,n-1[\![\rangle\right) +$$
$$+\mathrm{Card}\left([\![k,n-1[\![\ \cap\ \overset{-1}{\sigma'}\langle[\![0,l[\![\rangle\right) =$$
$$= 2\cdot\mathrm{Card}\left([\![0,k[\![\ \cap\ \overset{-1}{\sigma'}\langle[\![0,l[\![\rangle\right) + \mathrm{Card}(A(\sigma')) + \mathrm{Card}(B(\sigma')),$$

Ebből (2) alapján következik, hogy

$$\varepsilon_n(f(\sigma')) = \varepsilon_{n-1}(\sigma')\cdot(-1)^{\mathrm{Card}(A(\sigma'))+\mathrm{Card}(B(\sigma'))} = \varepsilon_{n-1}(\sigma')\cdot(-1)^{k+l},$$

amit (1)-be helyettesítve kapjuk, hogy

$$\det(\mathbf{a}) = (-1)^{k+l}\mathbf{a}_{k,l}\det\left(\hat{\mathbf{a}}_{k,l}\right).$$

(II) Tegyük fel, hogy a b) feltétel teljesül. Ekkor ${}^{\mathrm{t}}\mathbf{a} \in \mathrm{M}_n(A)$ olyan mátrix és $(l,k) \in n\times n$ olyan pár, hogy minden $i \in n\setminus\{k\}$ indexre ${}^{\mathrm{t}}\mathbf{a}_{l,i} = \mathbf{a}_{i,l} = 0$, tehát $\mathbf{a}$ helyett ${}^{\mathrm{t}}\mathbf{a}$-ra és (k,l) helyett az (l,k) párra teljesül az a) feltétel. Ezért 15.2.6., (I) és az előző lemma szerint

$$\det(\mathbf{a}) = \det({}^{\mathrm{t}}\mathbf{a}) = (-1)^{l+k}\left({}^{\mathrm{t}}\mathbf{a}\right)_{l,k}\det\left(\widehat{({}^{\mathrm{t}}\mathbf{a})}_{l,k}\right) =$$
$$= (-1)^{k+l}\mathbf{a}_{k,l}\det\left({}^{\mathrm{t}}\left(\hat{\mathbf{a}}_{k,l}\right)\right) = (-1)^{k+l}\mathbf{a}_{k,l}\det\left(\hat{\mathbf{a}}_{k,l}\right). \ \blacksquare$$

15.4.6. Állítás. *Legyen A kommutatív gyűrű, $n\in\mathbb{N}^*$, $n\geq 2$, és $\mathbf{a}\in\mathrm{M}_n(A)$. Ekkor*

a) *minden $i\in n$ esetén*

$$\det(\mathbf{a}) = (-1)^i\sum_{j=0}^{n-1}(-1)^j\mathbf{a}_{i,j}\det(\hat{\mathbf{a}}_{i,j}),$$

b) *minden $j\in n$ esetén*

$$\det(\mathbf{a}) = (-1)^j\sum_{i=0}^{n-1}(-1)^i\mathbf{a}_{i,j}\det(\hat{\mathbf{a}}_{i,j}).$$

Bizonyítás. a) Legyen $i\in n$ rögzített, és minden $j\in n$ indexre vezessük be azt az $\mathbf{a}_j\in\mathrm{M}_n(A)$ mátrixot, amelyre minden $k,l\in n$ esetén

$$(\mathbf{a}_j)_{l,k} = \begin{cases} \mathbf{a}_{l,k} & \text{, ha } l\neq i,\\ \delta_{k,j}\mathbf{a}_{i,j} & \text{, ha } l = i \end{cases}$$

tehát minden $j\in n$ esetén az $\mathbf{a}_j$ mátrix i-edik sorában a j-edik komponens $\mathbf{a}_{i,j}$, és a többi komponens 0_A, valamint az $\mathbf{a}_j$ mátrix l-edik sora $l\neq i$ esetén egyenlő az $\mathbf{a}$ mátrix l-edik sorával. Világos, hogy a definíció szerint minden $k\in n$ esetén

$$\sum_{j=0}^{n-1}(\mathbf{a}_j)_{i,k} = \sum_{j=0}^{n-1}\delta_{k,j}\mathbf{a}_{i,j} = \mathbf{a}_{i,k},$$

ezért a determináns definíciója alapján

$$\det(\mathbf{a}) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon_n(\sigma)\Big(\prod_{k\in n} \mathbf{a}_{k,\sigma(k)}\Big) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon_n(\sigma)\mathbf{a}_{i,\sigma(i)}\Big(\prod_{k\in n\setminus\{i\}} \mathbf{a}_{k,\sigma(k)}\Big) =$$

$$= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon_n(\sigma)\left(\sum_{j=0}^{n-1}(\mathbf{a}_j)_{i,\sigma(i)}\right)\Big(\prod_{k\in n\setminus\{i\}} \mathbf{a}_{k,\sigma(k)}\Big) = \sum_{j=0}^{n-1}\sum_{\sigma\in\mathfrak{S}_n} \varepsilon_n(\sigma)(\mathbf{a}_j)_{i,\sigma(i)}\Big(\prod_{k\in n\setminus\{i\}} \mathbf{a}_{k,\sigma(k)}\Big) =$$

$$= \sum_{j=0}^{n-1}\sum_{\sigma\in\mathfrak{S}_n} \varepsilon_n(\sigma)(\mathbf{a}_j)_{i,\sigma(i)}\Big(\prod_{k\in n\setminus\{i\}} (\mathbf{a}_j)_{k,\sigma(k)}\Big) = \sum_{j=0}^{n-1}\sum_{\sigma\in\mathfrak{S}_n} \varepsilon_n(\sigma)\Big(\prod_{k\in n} (\mathbf{a}_j)_{k,\sigma(k)}\Big) = \sum_{j=0}^{n-1}\det(\mathbf{a}_j).$$

Ugyanakkor minden $j\in n$ esetén az $\mathbf{a}_j$ mátrix i-edik sorában a j-edik komponens $\mathbf{a}_{i,j}$, és a többi komponens 0_A, így az előző lemmát alkalmazva $\mathbf{b}_j$-re kapjuk, hogy

$$\det(\mathbf{a}_j) = (-1)^{i+j}\mathbf{a}_{i,j}\det\left(\hat{\mathbf{a}}_{i,j}\right),$$

következésképpen

$$\det(\mathbf{a}) = (-1)^i\sum_{j=0}^{n-1}(-1)^j\mathbf{a}_{i,j}\det\left(\hat{\mathbf{a}}_{i,j}\right).$$

b) Legyen $i\in n$ rögzített. Ekkor minden $i\in n$ esetén 15.4.4. szerint ${}^{\mathrm{t}}\left(\hat{\mathbf{a}}_{i,j}\right) = \widehat{{}^{\mathrm{t}}\mathbf{a}}_{j,i}$, ezért 15.2.6. alapján

$$(-1)^j\sum_{i=0}^{n-1}(-1)^i\mathbf{a}_{i,j}\det(\hat{\mathbf{a}}_{i,j}) = (-1)^j\sum_{i=0}^{n-1}(-1)^i\left({}^{\mathrm{t}}\mathbf{a}\right)_{j,i}\det({}^{\mathrm{t}}(\hat{\mathbf{a}}_{i,j})) =$$

$$= (-1)^j\sum_{i=0}^{n-1}(-1)^i\left({}^{\mathrm{t}}\mathbf{a}\right)_{j,i}\det(\widehat{{}^{\mathrm{t}}\mathbf{a}}_{j,i}) = \det({}^{\mathrm{t}}\mathbf{a}) = \det(\mathbf{a}),$$

ahol az utolsó előtti egyenlőségnél az a) állítást alkalmaztuk $\mathbf{a}$ helyett a ${}^{\mathrm{t}}\mathbf{a}$ mátrixra és i helyett a j indexre. ■

15.4.7. Tétel. (**Kifejtési tétel.**) *Legyen A kommutatív egységelemes gyűrű, $n\in\mathbb{N}$, $n\geq 2$, és $\mathbf{a}\in \mathrm{M}_n(A)$. Ha $i,j\in n$, akkor*

$$\delta_{i,j}\det(\mathbf{a}) = (-1)^j\sum_{k=0}^{n-1}(-1)^k\mathbf{a}_{i,k}\det(\hat{\mathbf{a}}_{j,k}) = (-1)^j\sum_{k=0}^{n-1}(-1)^k\mathbf{a}_{k,i}\det(\hat{\mathbf{a}}_{k,j}).$$

Bizonyítás. Ha $i=j$, akkor a formula nyilvánvalóan következik az előző állításból. Tegyük fel, hogy $i\neq j$, és vezessük be azt a $\mathbf{b}\in\mathrm{M}_n(A)$ mátrixot, amelyre minden $(l,k)\in n\times n$ esetén

$$\mathbf{b}_{l,k} := \begin{cases} \mathbf{a}_{l,k} & \text{, ha } l\neq j,\\ \mathbf{a}_{i,k} & \text{, ha } l=j.\end{cases}$$

Ekkor minden $k\in n$ esetén $i\neq j$ miatt $\mathbf{b}_{i,k}=\mathbf{a}_{i,k}=\mathbf{b}_{j,k}$, vagyis a $\mathbf{b}$ mátrix i-edik és j-edik sora egyenlő, így 15.2.10. szerint $\det(\mathbf{b})=0_A$. Ugyanakkor, minden $k\in n$ esetén $\hat{\mathbf{b}}_{j,k}=\hat{\mathbf{a}}_{j,k}$, mert minden $(\alpha,\beta)\in(n-1)\times(n-1)$ indexpárra $\mathrm{Im}\left(\mathrm{m}_{n-1,j}\right)=n\setminus\{j\}$ miatt $\mathrm{m}_{n-1,j}(\alpha)\neq j$, ezért

$$\left(\hat{\mathbf{b}}_{j,k}\right)_{\alpha,\beta} = \mathbf{b}_{\mathrm{m}_{n-1,j}(\alpha),\mathrm{m}_{n-1,k}(\beta)} = \mathbf{a}_{\mathrm{m}_{n-1,j}(\alpha),\mathrm{m}_{n-1,k}(\beta)} = \left(\hat{\mathbf{a}}_{j,k}\right)_{\alpha,\beta}.$$

Tehát az előző állítást alkalmazva a $\mathbf{b}$ mátrixra kapjuk, hogy

$$0_A = \det(\mathbf{b}) = (-1)^j \sum_{k=0}^{n-1} (-1)^k \mathbf{b}_{j,k} \det\left(\hat{\mathbf{b}}_{j,k}\right) = (-1)^j \sum_{k=0}^{n-1} (-1)^k \mathbf{a}_{i,k} \det\left(\hat{\mathbf{a}}_{j,k}\right),$$

valamint

$$0_A = \det(\mathbf{b}) = (-1)^j \sum_{k=n}^{n-1} (-1)^k \mathbf{b}_{k,i} \det\left(\hat{\mathbf{b}}_{k,j}\right) = (-1)^j \sum_{l=0}^{n-1} (-1)^k \mathbf{a}_{i,k} \det\left(\hat{\mathbf{a}}_{j,k}\right). \blacksquare$$

15.4.8. Következmény. *Ha A kommutatív egységelemes gyűrű, $n \in \mathbb{N}$, $n \geq 2$, és $\mathbf{a} \in \mathrm{M}_n(A)$, akkor*

$$\mathbf{a} \cdot \mathrm{adj}(\mathbf{a}) = \det(\mathbf{a}).\mathbf{1} = \mathrm{adj}(\mathbf{a}) \cdot \mathbf{a}.$$

Bizonyítás. Minden $i, j \in n$ esetén

$$(\mathbf{a} \cdot \mathrm{adj}(\mathbf{a}))_{i,j} = \sum_{k=0}^{n-1} \mathbf{a}_{i,k} \left(\mathrm{adj}(\mathbf{a})\right)_{k,j} = \sum_{k=0}^{n-1} \mathbf{a}_{i,k} (-1)^{k+j} \det\left(\hat{\mathbf{a}}_{j,k}\right) =$$

$$= (-1)^j \sum_{k=0}^{n-1} (-1)^k \mathbf{a}_{i,k} \det\left(\hat{\mathbf{a}}_{j,k}\right) \overset{(*)}{=} \delta_{i,j} \det(\mathbf{a}),$$

ahol a $\overset{(*)}{=}$ egyenlőségnél a kifejtési tételt alkalmaztuk. Ezért

$$\mathbf{a} \cdot \mathrm{adj}(\mathbf{a}) = \det(\mathbf{a}).\mathbf{1},$$

ahol $\mathbf{1}$ az $\mathrm{M}_n(A)$ mátrixgyűrű egységeleme. Továbbá, minden $i, j \in n$ esetén

$$(\mathrm{adj}(\mathbf{a}) \cdot \mathbf{a})_{i,j} = \sum_{k=0}^{n-1} \left(\mathrm{adj}(\mathbf{a})\right)_{i,k} \mathbf{a}_{k,j} = \sum_{k=0}^{n-1} (-1)^{i+k} \det\left(\hat{\mathbf{a}}_{k,i}\right) \mathbf{a}_{k,j} =$$

$$= (-1)^i \sum_{k=0}^{n-1} (-1)^k \mathbf{a}_{k,j} \det\left(\hat{\mathbf{a}}_{k,i}\right) \overset{(**)}{=} \delta_{i,j} \det(\mathbf{a}),$$

ahol a $\overset{(**)}{=}$ egyenlőségnél a kifejtési tételt alkalmaztuk. Ezért

$$\mathrm{adj}(\mathbf{a}) \cdot \mathbf{a} = \det(\mathbf{a}).\mathbf{1}. \blacksquare$$

15.4.9. Állítás. *Legyen A kommutatív egységelemes gyűrű és $n \in \mathbb{N}$, $n \geq 2$. Az $\mathbf{a} \in \mathrm{M}_n(A)$ mátrix pontosan akkor invertálható az $\mathrm{M}_n(A)$ mátrixgyűrűben, ha $\det(\mathbf{a}) \in A$ invertálható A-ban, és ha $\mathbf{a}$ invertálható, akkor*

$$\mathbf{a}^{-1} = \left(\det(\mathbf{a})\right)^{-1}.\mathrm{adj}(\mathbf{a}),$$

valamint

$$\det\left(\mathbf{a}^{-1}\right) = \left(\det(\mathbf{a})\right)^{-1}.$$

Bizonyítás. A 15.4.8. állításból 15.1.13. alapján látható, hogy ha $\det(\mathbf{a})$ invertálható az A gyűrűben, akkor $\mathbf{a}$ invertálható az $\mathrm{M}_n(A)$ mátrixgyűrűben és $\mathbf{a}^{-1} = (\det(\mathbf{a}))^{-1}.\mathrm{adj}(\mathbf{a})$. Ha $\mathbf{a}$ invertálható az $\mathrm{M}_n(A)$ gyűrűben, akkor 15.2.4. szerint

$$1 = \det\left(\mathbf{1}_n\right) = \det\left(\mathbf{a} \cdot \mathbf{a}^{-1}\right) = \det(\mathbf{a}) \det\left(\mathbf{a}^{-1}\right),$$

ezért a $\det(\mathbf{a}) \in A$ elem invertálható az A gyűrűben, és $(\det(\mathbf{a}))^{-1} = \det\left(\mathbf{a}^{-1}\right)$. $\blacksquare$

15.5. Cayley–Hamilton-tétel mátrixokra

15.5.1. Lemma. *Legyen A kommutatív egységelemes gyűrű, $n \in \mathbb{N}^*$, és $\mathbf{x}, \mathbf{y} \in \mathrm{M}_n(A)$. Ekkor*

$$\det(\mathbf{x}+\mathbf{y}) = \sum_{j=0}^{n} \Big(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=j}} \Big(\mathrm{P}_{i \in H} \mathbf{x}_{i,\sigma(i)} \Big) \Big(\mathrm{P}_{i \in n \setminus H} \mathbf{y}_{i,\sigma(i)} \Big) \Big).$$

Bizonyítás. Minden $i \in n$, $k \in \{0,1\}$ és $\sigma \in \mathfrak{S}_n$ esetén vezessük be a

$$\mathrm{c}_{i,k}(\sigma) := \begin{cases} \mathbf{y}_{i,\sigma(i)} & , \text{ha } k=0, \\ \mathbf{x}_{i,\sigma(i)} & , \text{ha } k=1 \end{cases}$$

A-beli elemeket. Ekkor teljesülnek a következő egyenlőségek.

$$\det(\mathbf{x}+\mathbf{y}) \overset{(1)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \Big(\mathrm{P}_{i \in n} (\mathbf{x}+\mathbf{y})_{i,\sigma(i)} \Big) \overset{(2)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \Big(\mathrm{P}_{i \in n} (\mathbf{x}_{i,\sigma(i)} + \mathbf{y}_{i,\sigma(i)}) \Big) \overset{(3)}{=}$$

$$\overset{(3)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \Big(\mathrm{P}_{i \in n} \Big(\sum_{k \in \{0,1\}} \mathrm{c}_{i,k}(\sigma) \Big) \Big) \overset{(4)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\tau \in \{0,1\}^n} \Big(\mathrm{P}_{i \in n} \mathrm{c}_{i,\tau(i)}(\sigma) \Big) \overset{(5)}{=}$$

$$\overset{(5)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{H \subseteq n} \Big(\mathrm{P}_{i \in n} \mathrm{c}_{i,\chi_H(i)}(\sigma) \Big) \overset{(6)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{H \subseteq n} \Big(\mathrm{P}_{i \in H} \mathrm{c}_{i,1}(\sigma) \Big) \Big(\mathrm{P}_{i \in n \setminus H} \mathrm{c}_{i,0}(\sigma) \Big) \overset{(7)}{=}$$

$$\overset{(7)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{H \subseteq n} \Big(\mathrm{P}_{i \in H} \mathbf{x}_{i,\sigma(i)} \Big) \Big(\mathrm{P}_{i \in n \setminus H} \mathbf{y}_{i,\sigma(i)} \Big) \overset{(8)}{=}$$

$$\overset{(8)}{=} \sum_{H \subseteq n} \Big(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \Big(\mathrm{P}_{i \in H} \mathbf{x}_{i,\sigma(i)} \Big) \Big(\mathrm{P}_{i \in n \setminus H} \mathbf{y}_{i,\sigma(i)} \Big) \Big) \overset{(9)}{=}$$

$$\overset{(9)}{=} \sum_{j=0}^{n} \Big(\sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=j}} \Big(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \Big(\mathrm{P}_{i \in H} \mathbf{x}_{i,\sigma(i)} \Big) \Big(\mathrm{P}_{i \in n \setminus H} \mathbf{y}_{i,\sigma(i)} \Big) \Big) \Big) \overset{(10)}{=}$$

$$\overset{(10)}{=} \sum_{j=0}^{n} \Big(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=j}} \Big(\mathrm{P}_{i \in H} \mathbf{x}_{i,\sigma(i)} \Big) \Big(\mathrm{P}_{i \in n \setminus H} \mathbf{y}_{i,\sigma(i)} \Big) \Big),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a determináns definícióját alkalmaztuk;

– a $\overset{(2)}{=}$ egyenlőségnél a mátrixok összeadásának definícióját alkalmaztuk;

– a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk azt, hogy minden $i \in n$ és $\sigma \in \mathfrak{S}_n$ esetén a definíció alapján: $\mathbf{x}_{i,\sigma(i)} + \mathbf{y}_{i,\sigma(i)} = \sum_{k \in \{0,1\}} \mathrm{c}_{i,k}(\sigma)$;

– a $\overset{(4)}{=}$ egyenlőségnél alkalmaztuk az A gyűrű szorzásának összeadásra vonatkozó általános disztributivitását (8.8.3.);

– az $\overset{(5)}{=}$ egyenlőségnél felhasználtuk azt, hogy a $\mathscr{P}(n) \to \{0,1\}^n$; $H \mapsto \chi_H$ leképezés bijekció, így alkalmazható a véges műveletek általános kommutativitásának tétele az $(A,+)$ monoidban (12.5.9.);

– a $\overset{(6)}{=}$ egyenlőségnél minden $\sigma \in \mathfrak{S}_n$ permutációra és $H \subseteq n$ halmazra alkalmaztuk a

$\prod_{i\in n} c_{i,\chi_H(i)}(\sigma) = \Big(\prod_{i\in H} c_{i,1}(\sigma)\Big)\Big(\prod_{i\in n\setminus H} c_{i,0}(\sigma)\Big)$ egyenlőséget (12.5.6.);

– a $\overset{(7)}{=}$ egyenlőségnél a $c_{i,k}(\sigma) \in A$ elemek definícióját alkalmaztuk;

– a $\overset{(8)}{=}$ egyenlőségnél felcseréltük az összegzések sorrendjét (12.5.11.);

– a $\overset{(9)}{=}$ egyenlőségnél felhasználtuk azt, hogy $\mathscr{P}(n) = \bigcup_{j=0}^{n}\{H \subseteq n | \mathrm{Card}(H) = j\}$, és a $(\{H \subseteq n | \mathrm{Card}(H) = j\})_{j\in n+1}$ halmazrendszer diszjunkt, tehát alkalmazható a véges műveletek általános asszociativitásának első tétele az $(A, +)$ monoidra (12.5.10.);

– a $\overset{(10)}{=}$ egyenlőségnél felcseréltük a $\sum\limits_{\substack{H\subseteq n\\ \mathrm{Card}(H)=j}}$ és $\sum\limits_{\sigma\in\mathfrak{S}_n}$ összegzések sorrendjét (12.5.11.).■

15.5.2. Állítás. *Legyen A kommutatív egységelemes gyűrű és $n \in \mathbb{N}^*$. Ha $\mathbf{a} \in \mathrm{M}_n(A)$, akkor létezik olyan $\mathrm{M}_n(A)$-ban haladó $(\mathbf{b}_j)_{j\in n}$ rendszer, amelyre minden $\lambda \in A$ esetén*

$$\mathrm{adj}(\lambda.\mathbf{1} - \mathbf{a}) = \sum_{j=0}^{n-1} \lambda^j.\mathbf{b}_j.$$

Bizonyítás. Legyenek $k, l \in n$ és $\lambda \in A$ rögzítve. Ekkor az adjungált mátrix definíciója (15.4.2.) és 15.4.3. szerint

$$(\mathrm{adj}(\lambda.\mathbf{1} - \mathbf{a}))_{k,l} = (-1)^{k+l}\det\Big(\big(\widehat{\lambda.\mathbf{1} - \mathbf{a}}\big)_{l,k}\Big) = (-1)^{k+l}\det\left(\lambda.\hat{\mathbf{1}}_{l,k} - \hat{\mathbf{a}}_{l,k}\right),$$

így alkalmazhatjuk a 15.5.1. lemmát az $\mathbf{x} := \lambda.\hat{\mathbf{1}}_{l,k}$ és $\mathbf{y} := -\hat{\mathbf{a}}_{l,k}$ választással. Azt kapjuk, hogy

$$(\mathrm{adj}(\lambda.\mathbf{1} - \mathbf{a}))_{k,l} =$$

$$= (-1)^{k+l}\sum_{j=0}^{n-1}\Bigg(\sum_{\sigma\in\mathfrak{S}_{n-1}}\varepsilon_{n-1}(\sigma)\sum_{\substack{H\subseteq n-1\\ \mathrm{Card}(H)=j}}\Big(\prod_{i\in H}\lambda\left(\hat{\mathbf{1}}_{l,k}\right)_{i,\sigma(i)}\Big)\Big(\prod_{i\in(n-1)\setminus H}(-\hat{\mathbf{a}}_{l,k})_{i,\sigma(i)}\Big)\Bigg) \overset{(*)}{=}$$

$$\overset{(*)}{=} (-1)^{k+l}\sum_{j=0}^{n-1}\Bigg(\sum_{\sigma\in\mathfrak{S}_{n-1}}\varepsilon_{n-1}(\sigma)\sum_{\substack{H\subseteq n-1\\ \mathrm{Card}(H)=j}}\lambda^j\Big(\prod_{i\in H}\left(\hat{\mathbf{1}}_{l,k}\right)_{i,\sigma(i)}\Big)\Big(\prod_{i\in n\setminus H}(-\hat{\mathbf{a}}_{l,k})_{i,\sigma(i)}\Big)\Bigg),$$

ahol a $\overset{(*)}{=}$ egyenlőségnél 12.5.8. alapján felhasználtuk, hogy $H \subseteq n-1$, $\mathrm{Card}(H) = j$ és $\sigma \in \mathfrak{S}_{n-1}$ esetén

$$\prod_{i\in H}\lambda\left(\hat{\mathbf{1}}_{l,k}\right)_{i,\sigma(i)} = \Big(\prod_{i\in H}\lambda\Big)\Big(\prod_{i\in H}\left(\hat{\mathbf{1}}_{l,k}\right)_{i,\sigma(i)}\Big) = \lambda^j\Big(\prod_{i\in H}\left(\hat{\mathbf{1}}_{l,k}\right)_{i,\sigma(i)}\Big).$$

Ebből látható, hogy ha minden $j \leq n$ természetes számra $\mathbf{b}_j \in \mathrm{M}_n(A)$ az a mátrix, amelyre minden $(k, l) \in n \times n$ esetén

$$(\mathbf{b}_j)_{k,l} := (-1)^{k+l}\sum_{\sigma\in\mathfrak{S}_{n-1}}\varepsilon_{n-1}(\sigma)\sum_{\substack{H\subseteq n-1\\ \mathrm{Card}(H)=j}}\Big(\prod_{i\in H}\left(\hat{\mathbf{1}}_{l,k}\right)_{i,\sigma(i)}\Big)\Big(\prod_{i\in n\setminus H}(-\hat{\mathbf{a}}_{l,k})_{i,\sigma(i)}\Big),$$

akkor minden $\lambda \in A$ elemre $\mathrm{adj}(\lambda.\mathbf{1} - \mathbf{a}) = \sum\limits_{j=0}^{n-1}\lambda^j.\mathbf{b}_j$. ■

15.5.3. Állítás. *Legyen A kommutatív egységelemes gyűrű és $n \in \mathbb{N}^*$. Ekkor minden $\mathbf{a} \in \mathrm{M}_n(A)$ mátrixhoz létezik olyan $(c_j)_{j \in n+1} \in A^{n+1}$ rendszer, hogy minden $\lambda \in A$ elemre*

$$\det(\lambda.\mathbf{1} - \mathbf{a}) = \sum_{j=0}^{n} \lambda^j c_j.$$

Bizonyítás. A 15.5.1. lemmát alkalmazzuk az $\mathbf{x} := \lambda.\mathbf{1}$ és $\mathbf{y} := -\mathbf{a}$ választással. Azt kapjuk, hogy

$$\det(\lambda.\mathbf{1} - \mathbf{a}) = \sum_{j=0}^{n} \Bigg(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=j}} \Big(\prod_{i \in H} \lambda \delta_{i,\sigma(i)} \Big) \Big(\prod_{i \in n \setminus H} (-\mathbf{a}_{i,\sigma(i)}) \Big) \Bigg) \overset{(*)}{=}$$

$$\overset{(*)}{=} \sum_{j=0}^{n} \Bigg(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=j}} \lambda^j \Big(\prod_{i \in H} \delta_{i,\sigma(i)} \Big) \Big(\prod_{i \in n \setminus H} (-\mathbf{a}_{i,\sigma(i)}) \Big) \Bigg),$$

ahol a $\overset{(*)}{=}$ egyenlőségnél 12.5.8. alapján felhasználtuk, hogy $H \subseteq n$, $\mathrm{Card}(H) = j$ és $\sigma \in \mathfrak{S}_n$ esetén

$$\prod_{i \in H} (\lambda \delta_{i,\sigma(i)}) = \Big(\prod_{i \in H} \lambda \Big) \Big(\prod_{i \in H} \delta_{i,\sigma(i)} \Big) = \lambda^j \Big(\prod_{i \in H} \delta_{i,\sigma(i)} \Big).$$

Ebből látható, hogy ha minden $j \leq n$ természetes számra

$$c_j := \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq n \\ \mathrm{Card}(H)=j}} \Big(\prod_{i \in H} \delta_{i,\sigma(i)} \Big) \Big(\prod_{i \in n \setminus H} (-\mathbf{a}_{i,\sigma(i)}) \Big),$$

akkor minden $\lambda \in A$ elemre $\det(\lambda.\mathbf{1} - \mathbf{a}) = \sum_{j=0}^{n} \lambda^j c_j$. ■

Megjegyzés. Ha $n \in \mathbb{N}^*$, $\sigma \in \mathfrak{S}_n$ és $H \subseteq n$, akkor

$$\prod_{i \in H} \delta_{i,\sigma(i)} = \begin{cases} 1 & \text{, ha } H \subseteq [\sigma = \mathrm{id}_n], \\ 0 & \text{, ha } H \nsubseteq [\sigma = \mathrm{id}_n], \end{cases}$$

ezért az előző állításban előállított konkrét $(c_j)_{j \in n+1} \in A^{n+1}$ rendszerre teljesül az, hogy minden $j \leq n$ természetes számra

$$c_j = (-1)^{n-j} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq [\sigma = \mathrm{id}_n] \\ \mathrm{Card}(H)=j}} \Big(\prod_{i \in n \setminus H} \mathbf{a}_{i,\sigma(i)} \Big).$$

Ebből azonnal látható, hogy

$$c_0 = (-1)^{n-0} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq [\sigma = \mathrm{id}_n] \\ \mathrm{Card}(H)=0}} \Big(\prod_{i \in n \setminus H} \mathbf{a}_{i,\sigma(i)} \Big) = (-1)^n \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \Big(\prod_{i \in n} \mathbf{a}_{i,\sigma(i)} \Big) = (-1)^n \det(\mathbf{a}),$$

továbbá

$$c_{n-1} = (-1)^{n-(n-1)} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq [\sigma = \mathrm{id}_n] \\ \mathrm{Card}(H)=n-1}} \Big(\prod_{i \in n \setminus H} \mathbf{a}_{i,\sigma(i)} \Big) = - \sum_{(\sigma,H) \in \mathscr{J}} \varepsilon_n(\sigma) \Big(\prod_{i \in n \setminus H} \mathbf{a}_{i,\sigma(i)} \Big),$$

ahol $\mathscr{J} := \{(\sigma, H) | (\sigma \in \mathfrak{S}_n) \wedge (H \subseteq [\sigma = \mathrm{id}_n]) \wedge \mathrm{Card}(H) = n-1\}$, és nyilvánvaló, hogy az

$$n \to \mathscr{J}; \quad k \mapsto (\mathrm{id}_n, n \setminus \{k\})$$

leképezés *bijekció*, így A összeadásának általános kommutativitása folytán

$$c_{n-1} = -\sum_{k \in n} \varepsilon_n(\mathrm{id}_n) \Big(\prod_{i \in n \setminus (n \setminus \{k\})} \mathbf{a}_{i, \mathrm{id}_n(i)} \Big) = -\sum_{k \in n} \mathbf{a}_{k,k} = -\mathrm{tr}(\mathbf{a}).$$

Továbbá, triviális, hogy

$$c_n = (-1)^{n-n} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \sum_{\substack{H \subseteq [\sigma = \mathrm{id}_n] \\ \mathrm{Card}(H) = n}} \Big(\prod_{i \in n \setminus H} \mathbf{a}_{i, \sigma(i)} \Big) = 1,$$

hiszen $\sigma \in \mathfrak{S}_n$, $H \subseteq [\sigma = \mathrm{id}_n]$ és $\mathrm{Card}(H) = n$ esetén $H = n$ és $\sigma = \mathrm{id}_n$.

15.5.4. Tétel. (**Cayley–Hamilton-tétel mátrixokra.**) *Legyen A kommutatív egységelemes gyűrű és $n \in \mathbb{N}^*$. Tegyük fel, hogy A és n rendelkezik a következő tulajdonsággal.*

$(*)$ Minden $(c_j)_{j \in n+1} \in A^{n+1}$ rendszerre: ha minden $\lambda \in A$ elemre $\sum_{j=0}^{n} \lambda^j c_j = 0_A$, akkor minden $j \leq n$ természetes számra $c_j = 0_A$.

Ekkor minden $\mathbf{a} \in \mathrm{M}_n(A)$ mátrixhoz egyértelműen létezik olyan $(c_j)_{j \in n+1} \in A^{n+1}$ rendszer, hogy minden $\lambda \in A$ elemre

$$\det(\lambda.\mathbf{1} - \mathbf{a}) = \sum_{j=0}^{n} \lambda^j c_j,$$

és erre a $(c_j)_{j \in n+1}$ rendszerre fennáll a

$$\sum_{j=0}^{n} c_j.\mathbf{a}^j = \mathbf{0}$$

egyenlőség.

Bizonyítás. Legyen $\mathbf{a} \in \mathrm{M}_n(A)$ rögzítve. A 15.5.3. állítás szerint van olyan $(c_j)_{j \in n+1} \in A^{n+1}$ rendszer, hogy minden $\lambda \in A$ elemre

$$\det(\lambda.\mathbf{1} - \mathbf{a}) = \sum_{j=0}^{n} \lambda^j c_j.$$

Ha $(c'_j)_{j \in n+1} \in A^{n+1}$ szintén olyan rendszer, hogy minden $\lambda \in A$ elemre

$$\det(\lambda.\mathbf{1} - \mathbf{a}) = \sum_{j=0}^{n} \lambda^j c'_j,$$

akkor minden $\lambda \in A$ esetén

$$\sum_{j=0}^{n} \lambda^j (c'_j - c_j) = 0,$$

így $(*)$ alapján minden $j \leq n$ természetes számra $c'_j - c_j = 0_A$, tehát a $(c_j)_{j \in n+1} \in A^{n+1}$ rendszer egyértelműen van meghatározva.

A 15.5.2. állítást alkalmazva vegyünk olyan $\mathrm{M}_n(A)$-ban haladó $(\mathbf{b}_j)_{j\in n}$ rendszert, amelyre minden $\lambda \in A$ esetén

$$\mathrm{adj}(\lambda.\mathbf{1}-\mathbf{a}) = \sum_{j=0}^{n-1} \lambda^j.\mathbf{b}_j.$$

Ekkor 15.4.8. szerint minden $\lambda \in A$ esetén

$$\det(\lambda.\mathbf{1}-\mathbf{a}).\mathbf{1}{=}\mathrm{adj}(\lambda.\mathbf{1}-\mathbf{a})\cdot(\lambda.\mathbf{1}-\mathbf{a}){=}\Big(\sum_{j=0}^{n-1}\lambda^j.\mathbf{b}_j\Big)\cdot(\lambda.\mathbf{1}-\mathbf{a}){=}\sum_{j=0}^{n-1}\lambda^j.\mathbf{b}_j\cdot(\lambda.\mathbf{1}-\mathbf{a}){=}$$

$$=\sum_{j=0}^{n-1}\lambda^j.(\lambda.\mathbf{b}_j-\mathbf{b}_j\cdot\mathbf{a})=\sum_{j=0}^{n-1}\lambda^{j+1}.\mathbf{b}_j-\sum_{j=0}^{n-1}\lambda^j.\mathbf{b}_j\cdot\mathbf{a}=\sum_{j=1}^{n}\lambda^j.\mathbf{b}_{j-1}-\sum_{j=0}^{n-1}\lambda^j.\mathbf{b}_j\cdot\mathbf{a}=$$

$$=\lambda^n.\mathbf{b}_{n-1}+\sum_{j=1}^{n-1}\lambda^j.\mathbf{b}_{j-1}-\sum_{j=1}^{n-1}\lambda^j.\mathbf{b}_j\cdot\mathbf{a}-\mathbf{b}_0\cdot\mathbf{a}=\sum_{j=0}^{n}\lambda^j.\mathbf{d}_j,$$

ahol minden $j \leq n$ természetes számra

$$\mathbf{d}_j := \begin{cases} -\mathbf{b}_0\cdot\mathbf{a} & \text{, ha } j=0,\\ \mathbf{b}_{j-1}-\mathbf{b}_j\cdot\mathbf{a} & \text{, ha } 1\leq j\leq n-1,\\ \mathbf{b}_{n-1} & \text{, ha } j=n. \end{cases}$$

Ez azt jelenti, hogy minden $\lambda \in A$ esetén

$$\sum_{j=0}^{n}\lambda^j c_j.\mathbf{1} = \sum_{j=0}^{n}\lambda^j.\mathbf{d}_j,$$

vagyis minden $(k,l) \in n\times n$ párra minden $\lambda \in A$ esetén

$$\sum_{j=0}^{n}\lambda^j c_j.\mathbf{1}_{k,l} = \sum_{j=0}^{n}\lambda^j.(\mathbf{d}_j)_{k,l}.$$

Ebből $(*)$ alapján következik, hogy minden $(k,l) \in n\times n$ párra és minden $j \leq n$ természetes számra $c_j.\mathbf{1}_{k,l} = (\mathbf{d}_j)_{k,l}$. Tehát minden $j \leq n$ természetes számra teljesül a $c_j.\mathbf{1} = \mathbf{d}_j$ mátrix-egyenlőség. Speciálisan, minden $1 \leq j \leq n-1$ természetes számra $c_j.\mathbf{1} = \mathbf{d}_j = \mathbf{b}_{j-1}-\mathbf{b}_j\cdot\mathbf{a}$, amit jobbról $\mathbf{a}^j$-vel szorozva $c_j.\mathbf{a}^j = (\mathbf{b}_{j-1}-\mathbf{b}_j\cdot\mathbf{a})\cdot\mathbf{a}^j = \mathbf{b}_{j-1}\cdot\mathbf{a}^j-\mathbf{b}_j\cdot\mathbf{a}^{j+1}$ adódik. Ebből kapjuk, hogy

$$\sum_{j=0}^{n}c_j.\mathbf{a}^j = c_0.\mathbf{1}+\Big(\sum_{j=1}^{n-1}c_j.\mathbf{a}^j\Big)+c_n.\mathbf{a}^n = \mathbf{d}_0+\Big(\sum_{j=1}^{n-1}\big(\mathbf{b}_{j-1}\cdot\mathbf{a}^j-\mathbf{b}_j\cdot\mathbf{a}^{j+1}\big)\Big)+\mathbf{d}_n\cdot\mathbf{a}^n=$$

$$=-\mathbf{b}_0\cdot\mathbf{a}{+}\sum_{j=1}^{n-1}\mathbf{b}_{j-1}\cdot\mathbf{a}^j-\sum_{j=1}^{n-1}\mathbf{b}_j\cdot\mathbf{a}^{j+1}{+}\mathbf{b}_{n-1}\cdot\mathbf{a}^n{=}$$

$$=-\mathbf{b}_0\cdot\mathbf{a}{+}\sum_{j=1}^{n-1}\mathbf{b}_{j-1}\cdot\mathbf{a}^j-\sum_{j=2}^{n}\mathbf{b}_{j-1}\cdot\mathbf{a}^{j}{+}\mathbf{b}_{n-1}\cdot\mathbf{a}^n{=}$$

$$=-\mathbf{b}_0\cdot\mathbf{a}+\Big(\mathbf{b}_0\cdot\mathbf{a}+\sum_{j=2}^{n-1}\mathbf{b}_{j-1}\cdot\mathbf{a}^j\Big)-\Big(\sum_{j=2}^{n-1}\mathbf{b}_{j-1}\cdot\mathbf{a}^j+\mathbf{b}_{n-1}\cdot\mathbf{a}^n\Big)+\mathbf{b}_{n-1}\cdot\mathbf{a}^n=\mathbf{0}.\ \blacksquare$$

Később megmutatjuk, hogy ha A végtelen test, akkor minden $n \in \mathbb{N}^*$ esetén teljesül az előző tételben megfogalmazott $(*)$ állítás (16.7.5.).

16. fejezet

Testek

16.1. A racionális számok teste

Emlékeztetünk arra, hogy $\mathbb{Z}^*$ jelöli a nem nulla egész számok halmazát, tehát $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$.

16.1.1. Állítás. *A $\mathbb{Z} \times \mathbb{Z}^*$ halmazon bevezetjük a következő relációt:*

$$R := \{((a, b), (a', b')) \in (\mathbb{Z} \times \mathbb{Z}^*) \times (\mathbb{Z} \times \mathbb{Z}^*) \mid a \cdot b' = a' \cdot b\}.$$

Ekkor R ekvivalencia az $\mathbb{Z} \times \mathbb{Z}^*$ halmaz felett.

Bizonyítás. Az R reláció nyilvánvalóan reflexív $\mathbb{Z} \times \mathbb{Z}^*$ felett, és szimmetrikus is, mert ha $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ és $(a', b') \in \mathbb{Z} \times \mathbb{Z}^*$, akkor $((a, b), (a', b')) \in R$ esetén $a \cdot b' = a' \cdot b$ tehát az egyenlőség szimmetrikussága miatt $a' \cdot b = a \cdot b'$, vagyis $((a', b'), (a, b)) \in R$.

Az R reláció tranzitivitásának bizonyításához legyenek $(a, b), (a', b'), (a'', b'') \in \mathbb{Z} \times \mathbb{Z}^*$ olyanok, hogy $((a, b), (a', b')) \in R$ és $((a', b'), (a'', b'')) \in R$. Ekkor $a \cdot b' = a' \cdot b$ és $a' \cdot b'' = a'' \cdot b'$. Az első egyenlőséget b''-vel szorozva, a $\mathbb{Z}$ feletti szorzás asszociativitása és kommutativitása alapján $(a \cdot b'') \cdot b' = (a' \cdot b'') \cdot b$ adódik. Itt a jobb oldalra behelyettesítve $a' \cdot b''$ helyére az $a'' \cdot b'$ számot, és ismét felhasználva a $\mathbb{Z}$ feletti szorzás asszociativitását és kommutativitását kapjuk, hogy $(a \cdot b'') \cdot b' = (a'' \cdot b) \cdot b'$. Ebből a $\mathbb{Z}$ feletti szorzás kancellativitása (7.12.6.) és $b' \neq 0$ miatt kapjuk, hogy $a \cdot b'' = a'' \cdot b$, tehát $((a, b), (a'', b'')) \in R$. Ez azt jelenti, hogy az R reláció tranzitív. ■

16.1.2. Definíció. *Ha R jelöli az $\{((a, b), (a', b')) \in (\mathbb{Z} \times \mathbb{Z}^*) \times (\mathbb{Z} \times \mathbb{Z}^*) \mid a \cdot b' = a' \cdot b\}$ ekvivalenciát $\mathbb{Z} \times \mathbb{Z}^*$ felett, akkor*

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/R$$

és a $\mathbb{Q}$ faktorhalmazt a **racionális számok halmazának** *nevezzük, és $\mathbb{Q}$ elemei a* **racionális számok**. *Minden $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ esetén az (a, b) pár R szerinti ekvivalencia-osztályát a/b jelöli, vagyis*

$$a/b \;:=\; \{(a', b') \in \mathbb{Z} \times \mathbb{Z}^* \mid a \cdot b' = a' \cdot b\}.$$

Továbbá, a

$$\mathrm{J}_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}; \quad a \mapsto a/1$$

leképezést a $\mathbb{Z}$ és $\mathbb{Q}$ halmazok közötti **kanonikus leképezésnek** *nevezzük.*

Nyilvánvaló, hogy ha $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ és $(a', b') \in \mathbb{Z} \times \mathbb{Z}^*$, akkor a definíció szerint

$$a/b = a'/b' \quad \Leftrightarrow \quad a \cdot b' = a' \cdot b,$$

továbbá, a $\mathrm{J}_\mathbb{Z} : \mathbb{Z} \to \mathbb{Q}$ kanonikus leképezés injekció, mert $a, b \in \mathbb{Z}$ és $a/1 = b/1$ esetén $a = a \cdot 1 = b \cdot 1 = b$.

Megjegyezzük még, hogy a 16.1.1. definícióban bevezetett R ekvivalencia *egyenlő* a következő relációval:

$$R' := \{((a, b), (a', b')) \in (\mathbb{Z} \times \mathbb{Z}^*) \times (\mathbb{Z} \times \mathbb{Z}^*) \mid (\exists c \in \mathbb{Z}^*)\ (a \cdot b' - a' \cdot b)c = 0\}.$$

Valóban, $((a, b), (a', b')) \in R$ esetén $c := 1 \in \mathbb{Z}$ olyan, hogy $(a \cdot b' - a' \cdot b)c = 0$, tehát $((a, b), (a', b')) \in R'$, vagyis $R \subseteq R'$. Megfordítva, ha $((a, b), (a', b')) \in R'$ és $c \in \mathbb{Z}^*$ olyan, hogy $(a \cdot b' - a' \cdot b)c = 0$, akkor a $\mathbb{Z}$ gyűrű zérusosztómentessége (7.12.5. d) pont) folytán $a \cdot b' - a' \cdot b = 0$, tehát $((a, b), (a', b')) \in R$, vagyis $R' \subseteq R$.

16.1.3. Állítás. a) *Létezik egyetlen olyan $\perp : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ művelet, amelyre teljesül az, hogy minden $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ és $(c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ esetén*

$$(a/b) \perp (c/d) = (a \cdot d + b \cdot c)/(b \cdot d).$$

b) *Létezik egyetlen olyan $\top : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ művelet, amelyre teljesül az, hogy minden $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ és $(c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ esetén*

$$(a/b) \top (c/d) = (a \cdot c)/(b \cdot d).$$

c) *A $\mathrm{J}_\mathbb{Z} : \mathbb{Z} \to \mathbb{Q}$ kanonikus leképezésre teljesül az, hogy minden $a, b \in \mathbb{Z}$ esetén*

$$\mathrm{J}_\mathbb{Z}(a + b) = \mathrm{J}_\mathbb{Z}(a) \perp \mathrm{J}_\mathbb{Z}(b), \quad \mathrm{J}_\mathbb{Z}(a \cdot b) = \mathrm{J}_\mathbb{Z}(a) \top \mathrm{J}_\mathbb{Z}(b).$$

Bizonyítás. Megállapodunk, hogy a racionális számok halmazának definíciójában bevezetett R ekvivalenciát az $\approx$ szimbólummal jelöljük és az infix jelölést alkalmazzuk.

a) Az előírt tulajdonságú $\perp : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ függvény egyértelmű létezésének bizonyításához azt szükséges és elégséges igazolni, hogy $(a, b), (a', b'), (c, d), (c', d') \in \mathbb{Z} \times \mathbb{Z}^*$ esetén teljesül az, hogy ha $(a, b) \approx (a', b')$ és $(c, d) \approx (c', d')$, akkor $(a \cdot d + b \cdot c, b \cdot d) \approx (a' \cdot d' + b' \cdot c', b' \cdot d')$. Ez azért igaz, mert a hipotézis szerint $a \cdot b' = a' \cdot b$ és $c \cdot d' = c' \cdot d$, így a $\mathbb{Z}$ feletti összeadás asszociativitása és kommutativitása, valamint a $\mathbb{Z}$ feletti szorzás összeadásra vonatkozó disztributivitása alapján

$$\begin{aligned}(a \cdot d + b \cdot c) \cdot (b' \cdot d') &= (a \cdot b') \cdot (d \cdot d') + (c \cdot d') \cdot (b \cdot b') = \\ &= (a' \cdot b) \cdot (d \cdot d') + (c' \cdot d) \cdot (b \cdot b') = (a' \cdot d' + b' \cdot c') \cdot (b \cdot d),\end{aligned}$$

ami azt jelenti, hogy $(a \cdot d + b \cdot c, b \cdot d) \approx (a' \cdot d' + b' \cdot c', b' \cdot d')$.

b) Az előírt tulajdonságú $\top : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ függvény egyértelmű létezésének bizonyításához azt szükséges és elégséges igazolni, hogy $(a, b), (a', b'), (c, d), (c', d') \in \mathbb{Z} \times \mathbb{Z}^*$ esetén teljesül az, hogy ha $(a, b) \approx (a', b')$ és $(c, d) \approx (c', d')$, akkor $(a \cdot c, b \cdot d) \approx (a' \cdot c', b' \cdot d')$. Ez viszont nyilvánvalóan igaz, mert a hipotézis szerint $a \cdot b' = a' \cdot b$ és $c \cdot d' = c' \cdot d$, így a $\mathbb{Z}$ feletti szorzás asszociativitása és kommutativitása miatt

$$(a \cdot c) \cdot (b' \cdot d') = (a \cdot b') \cdot (c \cdot d') = (a' \cdot b) \cdot (c' \cdot d) = (a' \cdot c') \cdot (b \cdot d),$$

ami azt jelenti, hogy $(a \cdot c, b \cdot d) \approx (a' \cdot c', b' \cdot d')$.

c) Legyenek $a, b \in \mathbb{Z}$. Ekkor

$$\mathrm{J}_{\mathbb{Z}}(a) \perp \mathrm{J}_{\mathbb{Z}}(b) \stackrel{\text{df}}{=} (a/1) \perp (b/1) = (a \cdot 1 + b \cdot 1)/(1 \cdot 1) = (a+b)/1 \stackrel{\text{df}}{=} \mathrm{J}_{\mathbb{Z}}(a+b),$$
$$\mathrm{J}_{\mathbb{Z}}(a) \top \mathrm{J}_{\mathbb{Z}}(b) \stackrel{\text{df}}{=} (a/1) \top (b/1) = (a \cdot b)/(1 \cdot 1) = (a \cdot b)/1 \stackrel{\text{df}}{=} \mathrm{J}_{\mathbb{Z}}(a \cdot b)$$

teljesül. ■

16.1.4. Definíció. *A* 16.1.3. *állítás* a) *pontjában értelmezett* $\mathbb{Q}$ *feletti* $\perp$ *műveletet a* $+$ *szimbólummal, és a* 16.1.3. *állítás* b) *pontjában értelmezett* $\mathbb{Q}$ *feletti* $\top$ *műveletet a* $\cdot$ *szimbólummal jelöljük, továbbá a* $+$ *műveletet* $\mathbb{Q}$ *feletti* **összszeadásnak** *és a* $\cdot$ *műveletet* $\mathbb{Q}$ *feletti* **szorzásnak** *nevezzük.*

Tehát a $\mathbb{Q}$ feletti $+$ és $\cdot$ műveletekre teljesül az, hogy minden $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ esetén

$$(a/b) + (c/d) = (a \cdot d + b \cdot c)/(b \cdot d),$$
$$(a/b) \cdot (c/d) = (a \cdot c)/(b \cdot d).$$

Megjegyezzük még, hogy azért nem vezetnek félreértésre a $\mathbb{Q}$ feletti műveletek jelölésére alkalmazott $+$ és $\cdot$ szimbólumok, mert a műveletek operandusainak típusából mindig kiderül, hogy egész számok, vagy racionális számok közötti összszeadásról, vagy szorzásról van szó.

16.1.5. Állítás. (**A $\mathbb{Q}$ feletti műveletek tulajdonságai**)

a) *A* $\mathbb{Q}$ *feletti összeadás asszociatív, neutrális-elemes, iverzelemes és kommutatív* (*tehát kommutatív csoportművelet*).

b) *A* $\mathbb{Q}$ *feletti szorzás asszociatív, neutrális-elemes, kommutatív, és* $\mathbb{Q}$ *minden olyan elemének létezik inverze a szorzás szerint, amely különbözik az összedás neutrális elemétől.*

c) *A* $\mathbb{Q}$ *feletti szorzás disztributív a* $\mathbb{Q}$ *feletti összeadásra nézve.*

Bizonyítás. a) Ha $r, s, t \in \mathbb{Q}$ és $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}^*$ olyanok, hogy $r = a/b$, $s = c/d$ és $t = e/f$, akkor az $\mathbb{Z}$ feletti összeadás és szorzás asszociativitása, valamint a $\mathbb{Z}$ feletti szorzás összeadásra vonatkozó disztributivitása miatt

$$(r+s)+t = ((a/b)+(c/d)) + (e/f) = (a \cdot d + b \cdot c)/(b \cdot d) + (e/f) =$$
$$= ((a \cdot d + b \cdot c) \cdot f + (b \cdot d) \cdot e)/((b \cdot d) \cdot f) = (a \cdot d \cdot f + b \cdot c \cdot f + b \cdot d \cdot e)/(b \cdot (d \cdot f)) =$$
$$= (a \cdot (d \cdot f) + b \cdot (c \cdot f + d \cdot e))/(b \cdot (d \cdot f)) =$$
$$= (a/b) + (c \cdot f + d \cdot e)/(d \cdot f) = (a/b) + ((c/d) + (e/f)) = r + (s+t),$$

tehát a $\mathbb{Q}$ feletti összeadás asszociatív.

Ha $r, s \in \mathbb{Q}$ és $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ olyanok, hogy $r = a/b$ és $s = c/d$, akkor a $\mathbb{Z}$ feletti szorzás és összeadás kommutatvitása miatt

$$r + s = (a/b) + (c/d) = (a \cdot d + b \cdot c)/(b \cdot d) = (c \cdot b + d \cdot a)/(d \cdot b) = (c/d) + (a/b) = s + r,$$

tehát a $\mathbb{Q}$ feletti összeadás kommutatív.

Legyen $\mathbf{0} := 0/1$. Ha $r \in \mathbb{Q}$ és $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ olyan, hogy $r = a/b$, akkor

$$r + \mathbf{0} = (a/b) + (0/1) = (a \cdot 1 + b \cdot 0)/(b \cdot 1) = a/b = r,$$

ezért $\mathbf{0}$ a $\mathbb{Q}$ feletti összeadás neutrális eleme. Nyilvánvaló, hogy minden $b \in \mathbb{Z}^*$ esetén $\mathbf{0} = 0/b$.

Legyen $r \in \mathbb{Q}$ és $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ olyan, hogy $r = a/b$. Ekkor az $s := (-a)/b$ elemre

$$r + s = (a/b) + ((-a)/b) = (a \cdot b + b \cdot (-a))/(b \cdot b) = 0/(b^2) = \mathbf{0},$$

mert $\mathbb{Z}$-ben $b \cdot (-a) = -(a \cdot b)$ teljesül. Ez azt jelenti, hogy s az r-nek inverze a $\mathbb{Q}$ feletti összeadás szerint.

b) Ha $r, s, t \in \mathbb{Q}$ és $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}^*$ olyanok, hogy $r = a/b$, $s = c/d$ és $t = e/f$, akkor az $\mathbb{Z}$ feletti szorzás asszociativitás miatt

$$(r \cdot s) \cdot t = ((a/b) \cdot (c/d)) \cdot (e/f) = ((a \cdot c)/(b \cdot d)) \cdot (e/f) = ((a \cdot c) \cdot e)/((b \cdot d) \cdot f) =$$
$$= (a \cdot (c \cdot e))/(b \cdot (d \cdot f)) = (a/b) \cdot ((c \cdot e)/(d \cdot f)) = (a/b) \cdot ((c/d) \cdot (e/f)) = r \cdot (s \cdot t),$$

tehát a $\mathbb{Q}$ feletti szorzás asszociatív.

Ha $r, s \in \mathbb{Q}$ és $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ olyanok, hogy $r = a/b$ és $s = c/d$, akkor a $\mathbb{Z}$ feletti szorzás kommutativitása miatt

$$r \cdot s = (a/b) \cdot (c/d) = (a \cdot c)/(b \cdot d) = (c \cdot a)/(d \cdot b) = (c/d) \cdot (a/b) = s \cdot r,$$

tehát a $\mathbb{Q}$ feletti szorzás kommutatív.

Legyen $\mathbf{1} := 1/1$. Ha $r \in \mathbb{Q}$ és $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ olyan, hogy $r = a/b$, akkor

$$r \cdot \mathbf{1} = (a/b) \cdot (1/1) = (a \cdot 1)/(b \cdot 1) = a/b = r,$$

ezért $\mathbf{1}$ a $\mathbb{Q}$ feletti szorzás neutrális eleme. Nyilvánvaló, hogy minden $a \in \mathbb{Z}^*$ esetén $\mathbf{1} = a/a$. A $\mathbf{1} = \mathbf{0}$ egyenlőség azt jelentené, hogy $1/1 = 0/1$, vagyis $1 = 1 \cdot 1 = 0 \cdot 1 = 0$, holott $\mathbb{Z}$-ben a multiplikatív neutrális elem nem egyenlő az additív neutrális elemmel. Ezért $\mathbf{1} \neq \mathbf{0}$.

Legyen $r \in \mathbb{Q}$ olyan, hogy $r \neq \mathbf{0}$. Vegyünk olyan $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ párt, amelyre $r = a/b$. Világos, hogy $r \neq \mathbf{0}$ miatt $a \neq 0$, ezért jól értelmezett az $s := b/a \in \mathbb{Q}$ elem. Nyilvánvaló, hogy $\mathbb{Z}$ szorzásának kommutativitása szerint

$$r \cdot s = (a/b) \cdot (b/a) = (a \cdot b)/(b \cdot a) = \mathbf{1},$$

tehát s az r racionális szám inverze a $\mathbb{Q}$ feletti szorzás szerint.

c) Ha $r, s, t \in \mathbb{Q}$ és $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}^*$ olyanok, hogy $r = a/b$, $s = c/d$ és $t = e/f$, akkor az $\mathbb{Z}$ feletti összeadás és szorzás asszociativitása és kommutativitása, valamint a $\mathbb{Z}$ feletti szorzás összeadásra vonatkozó disztributivitása miatt

$$(r + s) \cdot t = ((a/b) + (c/d)) \cdot (e/f) = ((a \cdot d + b \cdot c)/(b \cdot d)) \cdot (e/f) =$$
$$= ((a \cdot d + b \cdot c) \cdot e)/((b \cdot d) \cdot f) = (a \cdot d \cdot e + b \cdot c \cdot e)/(b \cdot d \cdot f) \overset{(*)}{=}$$
$$\overset{(*)}{=} ((a \cdot d \cdot e + b \cdot c \cdot e) \cdot f)/(b \cdot d \cdot f \cdot f) = ((a \cdot e) \cdot (d \cdot f) + (b \cdot f) \cdot (c \cdot e))/((b \cdot f) \cdot (d \cdot f)) =$$
$$= ((a \cdot e)/(b \cdot f)) + ((c \cdot e)/(d \cdot f)) = ((a/b) \cdot (e/f))) + ((c/d) \cdot (e/f)) = r \cdot t + s \cdot t,$$

ahol a $\overset{(*)}{=}$ egyenlőségnél azt használtuk fel, hogy $(a', b') \in \mathbb{Z} \times \mathbb{Z}^*$ és $f \in \mathbb{Z}^*$ esetén $(a' \cdot f)/(b' \cdot f) = a'/b'$, hiszen a $\mathbb{Z}$ feletti szorzás asszociativitása és kommutativitása miatt $(a' \cdot f) \cdot b' = a' \cdot (b' \cdot f)$. Tehát a $\mathbb{Q}$ feletti szorzás disztributív a $\mathbb{Q}$ feletti össszeadásra nézve. ■

16.1.6. Állítás. *Minden $r \in \mathbb{Q}$ esetén léteznek olyan $a, b \in \mathbb{Z}$, hogy $b \neq 0$ és $r = \mathrm{J}_{\mathbb{Z}}(a) \cdot (\mathrm{J}_{\mathbb{Z}}(b))^{-1}$, ahol $(\mathrm{J}_{\mathbb{Z}}(b))^{-1}$ jelöli a $\mathrm{J}_{\mathbb{Z}}(b)$ racionális szám multiplikatív inverzét.*

Bizonyítás. Legyen $r \in \mathbb{Q}$, és vegyünk olyan $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ párt, hogy $r = a/b$. Ekkor $b \neq 0$ miatt a $\mathrm{J}_{\mathbb{Z}}(b) := b/1$ racionális szám nem egyenlő $\mathbb{Q}$ additív neutrális elemével, így jól értelmezett a $(\mathrm{J}_{\mathbb{Z}}(b))^{-1} \in \mathbb{Q}$ multiplikatív inverz, amelyre $(\mathrm{J}_{\mathbb{Z}}(b))^{-1} = 1/b$ teljesül. Ezért

$$\mathrm{J}_{\mathbb{Z}}(a)) \cdot (\mathrm{J}_{\mathbb{Z}}(b))^{-1} = (a/1) \cdot (1/b) = (a \cdot 1)/(1 \cdot b) = a/b = r. \blacksquare$$

Tehát az előző állítás szerint minden $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ párra

$$a/b = \mathrm{J}_{\mathbb{Z}}(a) \cdot (\mathrm{J}_{\mathbb{Z}}(b))^{-1},$$

és ez az egyenlőség indokolja az a/b jelölést.

Most rendezést fogunk bevezetni a racionális számok halmaza felett. Ehhez először megjegyezzük, hogy ha $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, akkor $a/b = (-a)/(-b)$, hiszen bármely $a, b \in \mathbb{Z}$ esetén az $a \cdot (-b) = (-a) \cdot b$ egyenlőségek érvényesek $\mathbb{Z}$-ben (14.1.4. b) pont). A $\mathbb{Z}$ feletti természetes rendezés lineáris, ezért $b > 0$ vagy $b < 0$, és az utóbbi esetben 7.12.12. alapján $0 = (-b) + b < (-b) + 0 = -b$. Ebből következik, hogy minden $r \in \mathbb{Q}$ esetén van olyan $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, hogy $r = a/b$ és $b > 0$, vagyis $b \in \mathbb{Z}^*_+$.

16.1.7. Lemma. *Ha $(a, b), (a', b'), (c, d), (c', d') \in \mathbb{Z} \times \mathbb{Z}^*_+$, $a/b = a'/b'$, $c/d = c'/d'$ és $a \cdot d \leq c \cdot b$, akkor $a' \cdot d' \leq c' \cdot b'$. Ha $r, s \in \mathbb{Q}$, akkor*

$$(\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*_+)(\forall (c, d) \in \mathbb{Z} \times \mathbb{Z}^*_+) \ (\ (\ ((r = a/b) \wedge (s = c/d)) \Rightarrow (a \cdot d \leq c \cdot b) \ ) \ ) \Leftrightarrow$$
$$\Leftrightarrow (\exists (a, b) \in \mathbb{Z} \times \mathbb{Z}^*_+)(\exists (c, d) \in \mathbb{Z} \times \mathbb{Z}^*_+) \ (\ (r = a/b) \wedge (s = c/d) \wedge (a \cdot d \leq c \cdot b) \ ).$$

Bizonyítás. A második állítás nyilvánvalóan ekvivalens az elsővel. Az első állítás bizonyításához felhasználjuk, hogy a hipotézis szerint $a \cdot b' = a' \cdot b$, $c \cdot d' = c' \cdot d$ és $a \cdot d \leq c \cdot b$. Szorozva az egyenlőtlenséget a $b' \in \mathbb{Z}^*_+$ számmal, és felhasználva a $\mathbb{Z}$ feletti szorzás asszociativitását és kommutativitását, valamint a 7.12.13. állítást kapjuk, hogy

$$(a' \cdot d) \cdot b = (a' \cdot b) \cdot d = (a \cdot b') \cdot d = (a \cdot d) \cdot b' \leq (c \cdot b) \cdot b' = (c \cdot b') \cdot b,$$

tehát $b \in \mathbb{Z}^*_+$ és 7.12.13. alapján $a' \cdot d \leq c \cdot b'$. Ezt az egyenlőtlenséget beszorozva a $d' \in \mathbb{Z}^*_+$ számmal, és felhasználva a $\mathbb{Z}$ feletti szorzás asszociativitását és kommutativitását, valamint a 7.12.13. állítást kapjuk, hogy

$$(a' \cdot d') \cdot d = (a' \cdot d) \cdot d' \leq (c \cdot b') \cdot d' = (c \cdot d') \cdot b' = (c' \cdot d) \cdot b' = (c' \cdot b') \cdot d,$$

tehát $d \in \mathbb{Z}^*_+$ és 7.12.13. alapján $a' \cdot d' \leq c' \cdot b'$. $\blacksquare$

16.1.8. Állítás. *A $\mathbb{Q}$ halmazon értelmezzük a következő relációt*

$$T := \{(r, s) \in \mathbb{Q} \times \mathbb{Q} \mid (\exists (a, b) \in \mathbb{Z} \times \mathbb{Z}^*_+)(\exists (c, d) \in \mathbb{Z} \times \mathbb{Z}^*_+)(\ (r = a/b) \wedge (s = c/d) \wedge (a \cdot d \leq c \cdot b) \ )\}.$$

Ekkor T lineáris rendezés $\mathbb{Q}$ felett, és minden $a, b \in \mathbb{Z}$ számra

$$a \leq b \ \Leftrightarrow \ (\mathrm{J}_{\mathbb{Z}}(a), \mathrm{J}_{\mathbb{Z}}(b)) \in T.$$

Bizonyítás. Ha $r \in \mathbb{Q}$, akkor van olyan $(a, b) \in \mathbb{Z} \times \mathbb{Z}_+^*$, hogy $r = a/b$, és ekkor a $\mathbb{Z}$ feletti természetes rendezés reflexivitása miatt $a \cdot b \le a \cdot b$, ami definíció szerint azt jelenti, hogy $(r, r) \in T$. Tehát a T reláció reflexív $\mathbb{Q}$ felett.

Legyenek $r, s \in \mathbb{Q}$ és tegyük fel, hogy $(r, s) \in T$ és $(s, r) \in T$. Ekkor léteznek olyan $(a, b) \in \mathbb{Z} \times \mathbb{Z}_+^*$, $(c, d) \in \mathbb{Z} \times \mathbb{Z}_+^*$, $(c', d') \in \mathbb{Z} \times \mathbb{Z}_+^*$ és $(a', b') \in \mathbb{Z} \times \mathbb{Z}_+^*$ elemek, hogy $r = a/b = a'/b'$, $s = c/d = c'/d'$, $a \cdot d \le c \cdot b$ és $c' \cdot b' \le a' \cdot d'$. Ekkor $a \cdot b' = a' \cdot b$ és $c \cdot d' = c' \cdot d$ is teljesül. A $c' \cdot b' \le a' \cdot d'$ egyenlőtlenséget szorozva d-vel (7.12.13.), és felhasználva a $\mathbb{Z}$ feletti szorzás assszociativitását és kommutativitását kapjuk, hogy

$$(c \cdot b') \cdot d' = (c \cdot d') \cdot b' = (c' \cdot d) \cdot b' = (c' \cdot b') \cdot d \le (a' \cdot d') \cdot d = (a' \cdot d) \cdot d',$$

tehát $d' \in \mathbb{Z}_+^*$ és 7.12.13. folytán $c \cdot b' \le a' \cdot d$. Ezt az egyenlőtlenséget szorozva b-vel (7.12.13.), és ismét felhasználva a $\mathbb{Z}$ feletti szorzás assszociativitását és kommutativitását kapjuk, hogy

$$(c \cdot b) \cdot b' = (c \cdot b') \cdot b \le (a' \cdot d) \cdot b = (a' \cdot b) \cdot d = (a \cdot b') \cdot d = (a \cdot d) \cdot b',$$

ezért $b' \in \mathbb{Z}_+^*$ és 7.12.13. folytán $c \cdot b \le a \cdot d$. Ugyanakkor $a \cdot d \le c \cdot b$ is igaz, így $a \cdot d = c \cdot b$, ami azt jelenti, hogy $r = a/b = c/d = s$. Tehát a T reláció antiszimmetrikus.

Legyenek $r, s, t \in \mathbb{Q}$ olyanok, hogy $(r, s) \in T$ és $(s, t) \in T$. Ekkor vehetünk olyan $(a, b), (c, d), (c', d'), (e, f) \in \mathbb{Z} \times \mathbb{Z}_+^*$ párokat, amelyekre $r = a/b$, $s = c/d = c'/d'$, $t = e/f$, valamint $a \cdot d \le c \cdot b$ és $c' \cdot f \le e \cdot d'$. Azt kell megmutatni, hogy $(r, t) \in T$, vagyis $a \cdot f \le e \cdot b$. Ehhez felhasználjuk azt, hogy $c \cdot d' = c' \cdot d$ is teljesül. Kétszer alkalmazva a 7.12.13. állítást, valamint a $\mathbb{Z}$ feletti szorzás asszociativitását és kommutativitását kapjuk, hogy

$$\begin{aligned}(a \cdot f) \cdot (d \cdot d') &= (a \cdot d) \cdot (d' \cdot f) \le (c \cdot b) \cdot (d' \cdot f) = (c \cdot d') \cdot (b \cdot f) = \\ &= (c' \cdot d) \cdot (b \cdot f) = (c' \cdot f) \cdot (d \cdot b) \le (e \cdot d') \cdot (d \cdot b) = (e \cdot b) \cdot (d \cdot d'),\end{aligned}$$

hiszen a feltevések és 7.12.13. alapján $d \cdot d' \in \mathbb{Z}_+$ és $d \cdot b \in \mathbb{Z}_+$. Tehát $(a \cdot f) \cdot (d \cdot d') \le (e \cdot b) \cdot (d \cdot d')$, ezért $d \cdot d' \in \mathbb{Z}_+^*$ és 7.12.13. alapján $a \cdot f \le e \cdot b$, így $(r, s) \in T$. Tehát a T reláció tranzitív.

Legyenek $r, s \in \mathbb{Q}$ tetszőlegesek, és vegyünk olyan $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}_+^*$ párokat, amelyekre $r = a/b$ és $s = c/d$. A $\mathbb{Z}$ feletti rendezés linearitása miatt $a \cdot d \le c \cdot b$ vagy $c \cdot b \le a \cdot d$. Az első esetben $(r, s) \in T$, a második esetben $(s, r) \in T$. Tehát T *lineáris rendezés* $\mathbb{Q}$ felett.

Ha $a, b \in \mathbb{Z}$, akkor az $(\mathrm{J}_\mathbb{Z}(a), \mathrm{J}_\mathbb{Z}(b)) := (a/1, b/1) \in T$ reláció ekvivalens azzal, hogy $a = a \cdot 1 = b \cdot 1 = b$. ■

16.1.9. Definíció. *A 16.1.8. állításban értelmezett $\mathbb{Q}$ feletti T lineáris rendezést a $\le$ vagy $\le_\mathbb{Q}$ szimbólummal jelöljük és $\mathbb{Q}$ feletti (természetes)* **rendezésnek** *nevezzük. Továbbá, a*

$$\mathbb{Q}_+ := \{r \in \mathbb{Q} \mid \mathbf{0} \le r\},$$
$$\mathbb{Q}_+^* := \{r \in \mathbb{Q} \mid \mathbf{0} < r\}$$

jelöléseket alkalmazzuk.

16.1.10. Állítás. (**A $\mathbb{Q}$ feletti rendezés kapcsolata a műveletekkel**)

a) *Minden $r, s, t \in \mathbb{Q}$ esetén, ha $r \le s$, akkor $r + t \le s + t$.*

b) *Minden $r, s, t \in \mathbb{Q}$ esetén, ha $r \le s$ és $\mathbf{0} \le t$, akkor $r \cdot t \le s \cdot t$.*

Bizonyítás. Tegyük fel, hogy $r, s, t \in \mathbb{Q}$, $r \leq s$ és legyenek $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}_+^*$ olyan párok, amelyekre $r = a/b$, $s = c/d$ és $t = e/f$. Ekkor $r \leq s$ miatt $a \cdot d \leq c \cdot b$.

a) A $\mathbb{Q}$ feletti összeadás definíciója szerint

$$r + t = (a/b) + (e/f) := ((a \cdot f) + (e \cdot b))/(b \cdot f),$$
$$s + t = (c/d) + (e/f) := ((c \cdot f) + (e \cdot d))/(d \cdot f),$$

tehát az $r + t \leq s + t$ egyenlőtlenség bizonyításához azt kell igazolni, hogy

$$((a \cdot f) + (e \cdot b)) \cdot (d \cdot f) \leq ((c \cdot f) + (e \cdot d)) \cdot (b \cdot f).$$

Ez viszont igaz, mert $f \cdot f \in \mathbb{Z}_+$ és 7.12.13., valamint a $\mathbb{Z}$ feletti szorzás $\mathbb{Z}$ feletti összeadásra vonatkozó disztibutivitása és a $\mathbb{Z}$ feletti szorzás asszociativitása és kommutativitása folytán

$$((a \cdot f)+(e \cdot b)) \cdot (d \cdot f)=(a \cdot f) \cdot (d \cdot f)+(e \cdot b) \cdot (d \cdot f)=(a \cdot d) \cdot (f \cdot f)+(e \cdot b) \cdot (d \cdot f) \leq$$
$$\leq (c \cdot b) \cdot (f \cdot f)+(e \cdot b) \cdot (d \cdot f)=(c \cdot f) \cdot (b \cdot f)+(e \cdot d) \cdot (b \cdot f)=((c \cdot f)+(e \cdot d)) \cdot (b \cdot f).$$

b) Tegyük fel, hogy még $\mathbf{0} \leq t$ is teljesül, tehát $0/1 \leq e/f$, vagyis $0 = 0 \cdot f \leq e \cdot 1 = e$. A $\mathbb{Q}$ feletti szorzás definíciója szerint

$$r \cdot t = (a/b) \cdot (e/f) := (a \cdot e)/(b \cdot f),$$
$$s \cdot t = (c/d) \cdot (e/f) := (c \cdot e)/(d \cdot f),$$

tehát az $r \cdot t \leq s \cdot t$ egyenlőtlenség bizonyításához azt kell igazolni, hogy

$$(a \cdot e) \cdot (d \cdot f) \leq (c \cdot e) \cdot (b \cdot f).$$

Ez viszont igaz, mert $r \leq s$ miatt $a \cdot d \leq c \cdot b$, és $e \cdot f \in \mathbb{Z}_+$, így 7.12.13. alapján, valamint a $\mathbb{Z}$ feletti szorzás asszociativitása és kommutativitása folytán

$$(a \cdot e) \cdot (d \cdot f) = (a \cdot d) \cdot (e \cdot f) \leq (c \cdot b) \cdot (e \cdot f) = (c \cdot e) \cdot (b \cdot f)$$

teljesül. ■

16.2. Testek értelmezése és alaptulajdonságai

16.2.1. Definíció. *A $(K, +, \cdot)$ hármast* **testnek** *nevezzük, ha $+$ és $\cdot$ olyan műveletek a K halmaz felett, amelyek rendelkeznek a következő tulajdonságokkal.*

($\mathrm{K_I}$) *A $+$ művelet asszociatív, kommutatív, neutrális-elemes és inverzelemes, tehát a $(K, +)$ pár kommutatív csoport. (A $+$ művelet szerinti neutrális elemet $\mathbf{0}$ jelöli, és minden $x \in K$ esetén $-x$ jelöli az x inverzét a $+$ művelet szerint.)*

($\mathrm{K_{II}}$) *A $\cdot$ művelet asszociatív, kommutatív, létezik neutrális eleme, amely $\mathbf{0}$-val nem egyenlő, és K minden $\mathbf{0}$-tól különböző elemének létezik inverze a $\cdot$ művelet szerint. (A $\cdot$ művelet szerinti neutrális elemet $\mathbf{1}$ jelöli, és minden $x \in K \setminus \{\mathbf{0}\}$ elemre x^{-1} jelöli az x inverzét a $\cdot$ művelet szerint.)*

($\mathrm{K_{III}}$) *A $\cdot$ művelet disztributív a $+$ műveletre nézve.*

A testeket gyakran egyetlen szimbólummal, az alaphalmaz jelével jelöljük, és a műveleteit a $+$ és $\cdot$ szimbólummal jelöljük, ha ez nem okoz félreértést.

Példák. a) A $(\mathbb{Q}, +, \cdot)$ hármas test (16.1.5.); ez a *racionális számok teste.* Ezzel szemben a $(\mathbb{Z}, +, \cdot)$ hármasra $(\mathrm{K_I})$ és $(\mathrm{K_{III}})$ teljesül, azonban $(\mathrm{K_{II}})$ nem. Az $(\mathbb{N}, +, \cdot)$ hármasra csak $(\mathrm{K_{III}})$ teljesül, de $(\mathrm{K_I})$ és $(\mathrm{K_{II}})$ nem.

b) Legyen $p \in \mathbb{N}^*$ tetszőleges, és a $\mathbb{Z}$ halmazon vezessük be a következő relációt:

$$\approx_p := \{(m,n) \in \mathbb{Z} \times \mathbb{Z} | \text{"}n - m \text{ osztható } p\text{-vel"}\}.$$

Ekkor $\approx_p$ ekvivalencia-reláció $\mathbb{Z}$ felett; legyen $\mathbb{Z}_p := \mathbb{Z}/\approx_p$ és jelölje π_p a $\mathbb{Z} \to \mathbb{Z}_p$ kanonikus szürjekciót. A $\mathbb{Z}_p$ halmaz felett egyértelműen léteznek azok a $+$ és $\cdot$ műveletek, amelyekre minden $m, n \in \mathbb{Z}$ esetén $\pi_p(m+n) = \pi_p(m)+\pi_p(n)$ és $\pi_p(m\cdot n) = \pi_p(m)\cdot\pi_p(n)$ teljesül. Ekkor a $(\mathbb{Z}_p, +, \cdot)$ hármasra $(\mathrm{K_I})$ és $(\mathrm{K_{III}})$ teljesül, továbbá $(\mathrm{K_{II}})$ pontosan akkor teljesül, ha p *prímszám.* Ha p *prímszám*, akkor a $\mathbb{Z}_p$ testet $\mathbb{F}_p$-vel is szokás jelölni, és az $(\mathbb{F}_p, +, \cdot)$ testet a p *-edik maradékosztálytestnek* nevezzük.

Legyen K test és $x \in K$. Ekkor a $(\mathrm{K_{III}})$ miatt $x \cdot \mathbf{0} + x \cdot \mathbf{0} = x \cdot (\mathbf{0} + \mathbf{0}) = x \cdot \mathbf{0}$, így az egyenlőség mindkét oldalához hozzáadva $-(x \cdot \mathbf{0})$-t és felhasználva a $+$ művelet asszociativitását kapjuk, hogy $x \cdot \mathbf{0} = \mathbf{0}$. Ismét a $(\mathrm{K_{III}})$ és az előző állítás miatt kapjuk, hogy $x + (-\mathbf{1}) \cdot x = \mathbf{1} \cdot x + (-\mathbf{1}) \cdot x = (\mathbf{1} + (-\mathbf{1})) \cdot x = \mathbf{0} \cdot x = \mathbf{0}$, amiből következik, hogy $(-\mathbf{1}) \cdot x = -x$.

16.2.2. Állítás. *Ha K test és $x \in K$, akkor egyértelműen létezik az az $(x^n)_{n\in\mathbb{N}}$ sorozat, amely K-ban halad, és minden $n \in \mathbb{N}$ számra eleget tesz a következő feltételeknek:*

$$x^0 = \mathbf{1};$$
$$x^{n+1} = x^n \cdot x.$$

Bizonyítás. Adott $x \in K$ esetén elég az iterációs tételt alkalmazni az $\mathbf{1} \in K$ kezdőpontra és a $K \to K;\ x' \mapsto x' \cdot x$ függvényre. ■

Tehát, ha K test és $x \in K$, akkor minden $n \in \mathbb{N}$ számra x^n jól értelmezett, és ezt az x elem *n-edik hatványának* nevezzük; ekkor n szerinti teljes indukcióval könnyen belátható, hogy minden $m \in \mathbb{N}$ esetén:

$$x^{m+n} = x^m \cdot x^n,$$
$$x^{m\cdot n} = (x^m)^n$$

teljesül. Ezek a *hatványozás azonosságai.*

16.3. Test feletti véges műveletek

16.3.1. Állítás. *Legyen $(K, +, \cdot)$ test, I nem üres véges halmaz, $(J_i)_{i\in I}$ nem üres véges halmazok rendszere, és $(f_i)_{i\in I}$ olyan függvényrendszer, hogy minden $i \in I$ esetén $J_i \subseteq \mathrm{Dom}(f_i)$ és $\mathrm{Im}(f_i) \subseteq K$. Ekkor a $J := \prod\limits_{i\in I} J_i$ halmaz nem üres és véges, továbbá fennáll a*

$$\mathrm{P}_{i\in I}\left(\sum_{j\in J_i} f_i(j)\right) = \sum_{\sigma\in J}\left(\mathrm{P}_{i\in I} f_i(\sigma(i))\right)$$

egyenlőség.

Bizonyítás. A 8.8.3. tétel nyilvánvaló következménye, az $S := K$, $\top := \cdot$, és $\perp := +$ választással. ■

16.3.2. Állítás. *Legyen I véges halmaz és $j, k \in I$ olyan elemek, hogy $j \neq k$. Jelölje $\tau_{j,k} \in \mathfrak{S}(I)$ azt a permutációt, amelyre $\tau_{j,k}(j) = k$ és $\tau_{j,k}(k) = j$ és minden $i \in I$ esetén, ha $i \neq j$ és $i \neq k$, akkor $\tau_{j,k}(i) = i$. Legyen $(K, +, \cdot)$ test és $f : \mathfrak{S}(I) \to K$ függvény.*

a) *Ha minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma \circ \tau_{j,k}) = -f(\sigma)$, vagy minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\tau_{j,k} \circ \sigma) = -f(\sigma)$, akkor*

$$\sum_{\sigma \in \mathfrak{S}(I)} f(\sigma) = 0.$$

b) *Ha minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma) \neq 0$, és minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\sigma \circ \tau_{j,k}) = f(\sigma)^{-1}$, vagy minden $\sigma \in \mathfrak{S}(I)$ permutációra $f(\tau_{j,k} \circ \sigma) = f(\sigma)^{-1}$, akkor*

$$\prod_{\sigma \in \mathfrak{S}(I)} f(\sigma) = 1.$$

Bizonyítás. a) A 13.2.2. állítást kell alkalmazni a $(K, +)$ kommutatív monoidra.

b) A 13.2.2. állítást kell alkalmazni a $(K^*, \cdot)$ kommutatív monoidra. ■

16.4. Test karakterisztikája és prímtestek

16.4.1. Állítás. *Ha K test, akkor létezik egyetlen olyan $j : \mathbb{Z} \to K$ nem azonosan* $\mathbf{0}$ *függvény, amelyre teljesül az, hogy minden $q, p \in \mathbb{Z}$ esetén:*

$$j(q + p) = j(q) + j(p), \quad j(q \cdot p) = j(q) \cdot j(p)$$

teljesül.

Bizonyítás. Először az iterációs tételt alkalmazva a $\mathbf{0} \in K$ kezdőpontra és a $K \to K$; $x \mapsto x + \mathbf{1}$ függvényre kapjuk annak a K-ban haladó $\mathbf{s}$ sorozatnak a létezését, amelyre teljesül az, hogy $\mathbf{s}(0) = \mathbf{0}$ és minden $n \in \mathbb{N}$ számra $\mathbf{s}(n+1) = \mathbf{s}(n) + \mathbf{1}$. Ekkor n szerinti teljes indukcióval könnyen belátható, hogy minden $m, n \in \mathbb{N}$ számra $\mathbf{s}(m+n) = \mathbf{s}(m) + \mathbf{s}(n)$ és $\mathbf{s}(m \cdot n) = \mathbf{s}(m) \cdot \mathbf{s}(n)$. Ebből következik, hogy ha $(m, n), (m', n') \in \mathbb{N} \times \mathbb{N}$ és $m + n' = m' + n$, akkor $\mathbf{s}(m) - \mathbf{s}(n) = \mathbf{s}(m') - \mathbf{s}(n')$, így létezik egyetlen olyan $j : \mathbb{Z} \to K$ függvény, amelyre minden $(m, n) \in \mathbb{N} \times \mathbb{N}$ esetén $j(m - n) = \mathbf{s}(m) - \mathbf{s}(n)$ teljesül.

A $\mathbb{Z}$ műveleteinek tulajdonságai és a j függvény definíciója alapján közvetlenül belátható, hogy minden $q, p \in \mathbb{Z}$ esetén $j(q + p) = j(q) + j(p)$ és $j(q \cdot p) = j(q) \cdot j(p)$ teljesül.

Ha $j' : \mathbb{Z} \to K$ szintén olyan függvény, minden $q, p \in \mathbb{Z}$ esetén $j'(q + p) = j'(q) + j'(p)$ és $j'(q \cdot p) = j'(q) \cdot j'(p)$ teljesül, akkor a $\mathbf{s}' := j'|_{\mathbb{N}} : \mathbb{N} \to K$ leszűkített függvényre $\mathbf{s}'(0) = \mathbf{0}$ teljesül, és ha j' nem azonosan $\mathbf{0}$, akkor $j'(1) = \mathbf{1}$, ezért minden $n \in \mathbb{N}$ esetén $\mathbf{s}'(n+1) = \mathbf{s}'(n) + \mathbf{1}$ is teljesül. Ezért $\mathbf{s}' = \mathbf{s}$, következésképpen minden $(m, n) \in \mathbb{N} \times \mathbb{N}$ párra $j(m - n) = \mathbf{s}(m) - \mathbf{s}(n) = \mathbf{s}'(m) - \mathbf{s}'(n) = j'(m - n)$, tehát $j' = j$. ■

16.4.2. Definíció. *Ha $(K, +, \cdot)$ test, akkor a $\mathbb{Z}$ és K közötti* **kanonikus leképezésnek** *nevezzük azt a $\mathbb{Z} \to K$ nem azonosan* $\mathbf{0}$ *függvényt, amelyre teljesül az, hogy minden $q, p \in \mathbb{Z}$ esetén $j(q + p) = j(q) + j(p)$ és $j(q \cdot p) = j(q) \cdot j(p)$. Továbbá, ha K test és $j : \mathbb{Z} \to K$ a kanonikus leképezés, akkor minden $p \in \mathbb{Z}$ és $x \in K$ esetén $px := j(p) \cdot x$.*

16.4.3. Állítás. *Ha K test és $x, y \in K$, akkor minden $n \in \mathbb{N}$ esetén*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

teljesül. (**Binomiális formula K-ra**)

Bizonyítás. Rögzített $x, y \in K$ esetén n szerinti teljes indukcióval bizonyítunk. Ha $n = 0$, akkor $(x+y)^0 := 1$ és $\sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k} = 1$. Legyen $n \in \mathbb{N}$ olyan, amelyre igaz a formula. Ekkor a K feletti hatványozás értelmezése és a K feletti műveletek tulajdonságai, valamint az indukciós hipotézis miatt

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)^n(x+y) = \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right)(x+y) = \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k}\right) + \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}\right) = \\
&= \left(\sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} y^{n-k}\right) + x^{n+1} + \left(\sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k}\right) + y^{n+1} = \\
&= \left(\sum_{j=1}^{n} \binom{n}{j-1} x^j y^{n+1-j}\right) + x^{n+1} + \left(\sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k}\right) + y^{n+1} = \\
&= x^{n+1} + \left(\sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) x^k y^{n+1-k}\right) + y^{n+1} = \\
&= x^{n+1} + \left(\sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k}\right) + y^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{(n+1)-k},
\end{aligned}$$

vagyis az egyenlőség teljesül az $n+1$ számra is. ■

Ha K test, akkor a $\mathbb{Z}$ és K közötti kanonikus leképezés nem feltétlenül injektív; például az $\mathbb{F}_p$ test esetében ez a függvény p szerint periodikus. A racionális számok $\mathbb{Q}$ teste esetében a $\mathbb{Z} \to \mathbb{Q}$ kanonikus leképezés injektív. Könnyen látható, hogy ha K test, akkor a $j : \mathbb{Z} \to K$ kanonikus leképezés pontosan akkor injektív, ha minden $n \in \mathbb{N}^*$ esetén $j(n) \neq \mathbf{0}$; ilyenkor azt mondjuk, hogy a K test *nulla karakterisztikájú.*

1. A K test *karakterisztikáját* a következőképpen értelmezzük.

– Ha $j : \mathbb{Z} \to K$ a kanonikus leképezés, és van olyan $n \in \mathbb{N}^*$, amelyre $j(n) = \mathbf{0}$, akkor a K karakterisztikája a

$$\operatorname{char}(K) := \min\{n \in \mathbb{N}^* | j(n) = \mathbf{0}\}$$

szám.

– Ha $j : \mathbb{Z} \to K$ a kanonikus leképezés, és minden $n \in \mathbb{N}^*$ esetén $j(n) \neq \mathbf{0}$, akkor a K karakterisztikája (definíció szerint) 0.

Mutassuk meg, hogy minden nem nulla karakterisztikájú test karakterisztikája *prímszám*, és minden p prímszámra az $\mathbb{F}_p$ maradékosztály-test karakterisztikája egyenlő p-vel. Ha K véges test, akkor $\operatorname{Card}(K)$ prímszámhatvány.

16.4.4. Állítás. *Legyen K olyan test, amelyre a $j : \mathbb{Z} \to K$ kanonikus leképezés injektív. Ekkor egyértelműen létezik az a $J : \mathbb{Q} \to K$ leképezés, amely j-nek kiterjesztése, és olyan, hogy minden $r, s \in \mathbb{Q}$ esetén:*

$$J(r+s) = J(r) + J(s), \quad J(r \cdot s) = J(r) \cdot J(s).$$

Ez a J leképezés is injektív.

Bizonyítás. Legyenek $(q,p),(q',p') \in \mathbb{Z} \times \mathbb{Z}^*$ olyan párok, hogy $q \cdot p' = q' \cdot p$. Ekkor $j(q) \cdot j(p') = j(q') \cdot j(p)$, és a j injektivitása miatt $j(p), j(p') \in K \setminus \{0\}$, következésképpen $j(q) \cdot j(p)^{-1} = j(q') \cdot j(p')^{-1}$. Ebből a $\mathbb{Q}$ *definíciója* szerint létezik egyetlen olyan $J : \mathbb{Q} \to K$ függvény, amelyre minden $(q,p) \in \mathbb{Z} \times \mathbb{Z}^*$ párra $J(q/p) = j(q) \cdot j(p)^{-1}$ teljesül. A $j(1) = \mathbf{1}$ egyenlőség miatt J a j függvény kiterjesztése, és egyszerű számolással ellenőrizhető, hogy a $\mathbb{Q}$-ban értelmezett $+$ és $\cdot$ műveletek *definíciója* miatt minden $r, s \in \mathbb{Q}$ esetén $J(r+s) = J(r) + J(s)$ és $J(r \cdot s) = J(r) \cdot J(s)$.

Ha $J' : \mathbb{Q} \to K$ szintén olyan kiterjesztése j-nek, hogy minden $r, s \in \mathbb{Q}$ esetén $J'(r+s) = J'(r) + J'(s)$ és $J'(r \cdot s) = J'(r) \cdot J'(s)$ teljesül, akkor minden $(q,p) \in \mathbb{Z} \times \mathbb{Z}^*$ párra $J'(q/p) = j(q) \cdot j(p)^{-1} = J(q/p)$, így $J' = J$.

A J függvény injektivitása ekvivalens azzal, hogy minden $r \in \mathbb{Q}^*$ számra $J(r) \neq \mathbf{0}$. Ez viszont nyilvánvalóan igaz J-re, mert ha $r \in \mathbb{Q}^*$, akkor létezik olyan $(q,p) \in \mathbb{Z} \times \mathbb{Z}^*$ pár, hogy $r = q/p$ és $q \neq 0$; ekkor $J(r) = j(q) \cdot j(p)^{-1} \neq \mathbf{0}$, hiszen j injektivitása miatt $j(q) \neq \mathbf{0}$. ■

16.4.5. Definíció. *Ha K olyan test, hogy a $j : \mathbb{Z} \to K$ kanonikus leképezés injektív, akkor a $\mathbb{Q}$ és K közötti* **kanonikus leképezésnek** *nevezzük a $J : \mathbb{Q} \to K$ függvényt, amely j-nek kiterjesztése, és olyan, hogy minden $r, s \in \mathbb{Q}$ esetén $J(r+s) = J(r) + J(s)$ és $J(r \cdot s) = J(r) \cdot J(s)$ teljesül.*

Tehát ha K olyan test, amelyre a $\mathbb{Z}$ és K közötti kanonikus leképezés injektív, akkor K a racionális számtest "bővítésének" tekinthető, vagyis $\mathbb{Q}$ a "legkisebb" olyan test, hogy a $\mathbb{Z}$ és $\mathbb{Q}$ közötti kanonikus leképezés injektív. Ilyenkor a kevésbé pontos $\mathbb{Q} \subseteq K$ jelölést is alkalmazzuk, vagyis $\mathbb{Q}$-t azonosítjuk a $\mathbb{Q} \to K$ kanonikus injekció által e függvény értékkészletével.

2. A K test *résztestének* nevezünk minden olyan $L \subseteq K$ nem üres halmazt, amelyre minden $x, y \in L$ esetén $x + y \in L$, $x \cdot y \in L$ teljesül, továbbá minden $x \in L$ esetén $-x \in L$, és ha $x \neq \mathbf{0}$, akkor $x^{-1} \in L$. A K test *testbővítésének* nevezünk minden olyan testet, amelynek K részteste. Mutassuk meg, hogy ha L részteste K-nak, akkor az L halmaz a K műveleteinek $L \times L$-re vett leszűkítésével ellátva szintén test, és az L test additív (illetve multiplikatív) neutrális eleme ugyanaz, mint a K test additív (illetve multiplikatív) neutrális eleme. Egy test résztestei tetszőleges nem üres rendszerének a metszete is résztest. Speciálisan a K test *összes* résztesteinek metszete a K tartalmazás tekintetében legkisebb részteste.

3. A K testet *prímtestnek* nevezzük, ha K minden részteste egyenlő K-val, vagyis K-nak nincs nem triviális részteste. Egy test pontosan akkor prímtest, ha izomorf $\mathbb{Q}$-val, vagy létezik olyan p prímszám, hogy izomorf $\mathbb{F}_p$-vel.

(*Útmutatás.* Ha P jelöli a K legkisebb résztestét, akkor P prímtest, és ha P karakterisztikája 0, akkor P izomorf $\mathbb{Q}$-val, ha pedig P karakterisztikája a p prímszám, akkor P izomorf $\mathbb{F}_p$-vel.)

5. Ha a K test karakterisztikája a p prímszám, akkor minden $x, y \in K$ esetén:

$$(x+y)^p = x^p + y^p$$

teljesül.

(*Útmutatás.* Az $(x+y)^p$ kifejezést a binomiális tétellel kifejtjük, és észrevesszük, hogy minden $k \in \mathbb{N}^*$ számra, ha $k < p$, akkor $j(\binom{p}{k}) \cdot \mathbf{1} = \mathbf{0}$, ahol $j : \mathbb{Z} \to K$ a kanonikus leképezés.)

16.5. Hányadostest

16.6. Polinomok és polinomiális függvények test felett

12. (*Polinomok.*) Legyen K test és jelölje $K^{(\mathbb{N})}$ azon K-ban haladó P sorozatok halmazát, amelyekre az $\{n{\in}\mathbb{N} | P(n){\neq}0\}$ halmaz véges. A $K^{(\mathbb{N})}$ halmazon bevezetjük a következő $+$ és $\cdot$ műveleteket.

(i) $P, Q \in K^{(\mathbb{N})}$ esetén legyen $P+Q$ az a sorozat, amelyre minden $n \in \mathbb{N}$ esetén

$$(P+Q)(n) := P(n) + Q(n).$$

(ii) $P, Q \in K^{(\mathbb{N})}$ esetén legyen $P \cdot Q$ az a sorozat, amelyre minden $n \in \mathbb{N}$ esetén

$$(P \cdot Q)(n) := \sum_{k=0}^{n} P(k) \cdot Q(n-k).$$

Minden $P, Q \in K^{(\mathbb{N})}$ elemre $P+Q, P \cdot Q \in K^{(\mathbb{N})}$ teljesül, tehát $+$ és $\cdot$ valóban műveletek $K^{(\mathbb{N})}$ felett. A $(K^{(\mathbb{N})}, +, \cdot)$ hármast a K *test feletti egyváltozós polinomok gyűrűjének* nevezzük, és $K^{(\mathbb{N})}$ elemeit K feletti (*egyváltozós*) *polinomoknak* nevezzük. Ha P polinom K felett és $n \in K$, akkor a $P(n) \in K$ elemet a P n-*edik együtthatójának* nevezzük.

a) A $K^{(\mathbb{N})}$ feletti $+$ művelet kommutatív csoportművelet és a $K^{(\mathbb{N})}$ feletti $\cdot$ művelet asszociatív, kommutatív, neutrális-elemes, és disztributív a $+$ műveletre nézve. Ha $\mathbf{0}$ (illetve $\mathbf{1}$) jelöli a neutrális elemet a $+$ (illetve $\cdot$) művelet szerint, akkor teljesül az, hogy minden $n \in \mathbb{N}$ esetén $\mathbf{0}(n) = 0$ és

$$\mathbf{1}(n) = \begin{cases} 1 & \text{, ha } n = 0 \\ 0 & \text{, ha } n \neq 0. \end{cases}$$

Azonban a $(K^{(\mathbb{N})}, +, \cdot)$ hármas nem test!

b) Ha $P, Q \in K^{(\mathbb{N})}$, és $P \neq \mathbf{0}$ és $Q \neq \mathbf{0}$, akkor $P \cdot Q \neq \mathbf{0}$. Ezt a tényt úgy fejezzük ki, hogy a $K^{(\mathbb{N})}$ *zérusosztómentes* a $\cdot$ műveletre nézve.

c) Legyen $X \in K^{(\mathbb{N})}$ az a polinom, amelyre minden $n \in \mathbb{N}$ esetén:

$$X(n) = \begin{cases} 1 & \text{, ha } n = 1 \\ 0 & \text{, ha } n \neq 1. \end{cases}$$

Ekkor minden $k, n \in \mathbb{N}$ számra:

$$X^k(n) = \begin{cases} 1 & \text{, ha } n = k \\ 0 & \text{, ha } n \neq k, \end{cases}$$

ezért minden $P \in K^{(\mathbb{N})}$ polinomra:

$$P = \sum_{k \in [P \neq 0]} P(k) \cdot X^k$$

teljesül, ahol $[P \neq 0] := \{n \in \mathbb{N} | P(n) \neq 0\}$ (és a konvenció szerint az üres halmazra vett összeg egyenlő 0-val).

d) Minden $c \in K$ elemre legyen $\mathbf{c} \in K^{(\mathbb{N})}$ az a polinom, amelyre minden $n \in \mathbb{N}$ esetén:

$$\mathbf{c}(n) = \begin{cases} c & \text{, ha } n = 0 \\ 0 & \text{, ha } n \neq 0. \end{cases}$$

Ekkor az $f : K \to K^{(\mathbb{N})}$; $c \mapsto \mathbf{c}$ leképezés olyan injekció, hogy minden $a, b \in K$ esetén $f(a+b) = f(a) + f(b)$ és $f(a \cdot b) = f(a) \cdot f(b)$ teljesül; ezáltal a K halmaz, a műveleteivel együtt azonosul a $K^{(\mathbb{N})}$ egy részhalmazával, és a továbbiakban $c \in K$ esetén a $\mathbf{c}$ polinom helyett is a c jelet alkalmazzuk.

e) Minden $P \in K^{(\mathbb{N})}$ polinomra legyen $P_K : K \to K$ az a függvény, amelyre minden $x \in K$ esetén

$$P_K(x) := \sum_{k \in [P \neq 0]} P(k) \cdot x^k.$$

Ekkor a $K^{(\mathbb{N})} \to \mathscr{F}(K; K)$; $P \mapsto P_K$ leképezés olyan *injekció*, amelyre teljesül az, hogy minden $P, Q \in K^{(\mathbb{N})}$ polinomra és $x \in K$ elemre

$$(P + Q)_K(x) = P_K(x) + Q_K(x), \quad (P \cdot Q)_K(x) = P_K(x) \cdot Q_K(x).$$

A P_K alakú $K \to K$ függvényeket K feletti *polinomiális függvényeknek* nevezzük.

f) Egy $P \in K^{(\mathbb{N})}$ polinomot *nulladfokúnak* nevezünk, ha minden $n \in \mathbb{N}^*$ számra $P(n) = 0$. Ha P nem nulladfokú polinom K felett, akkor létezik egyetlen olyan $n \in \mathbb{N}$, amelyre $P(n) \neq 0$ és minden $k \in \mathbb{N}$ esetén, ha $k > n$, akkor $P(k) = 0$; ezt az n számot a P polinom *fokának* nevezzük és $\deg(P)$-vel jelöljük. Ha P nulladfokú polinom K felett, akkor $\deg(P) := 0$. Ha $P, Q \in K^{(\mathbb{N})}$, akkor $\deg(P+Q) = \max(\deg(P), \deg(Q))$, továbbá, ha $P \neq \mathbf{0}$ és $Q \neq \mathbf{0}$, akkor $\deg(P \cdot Q) = \deg(P) + \deg(Q)$.

g) Ha $P, Q \in K^{(\mathbb{N})}$ és $Q \neq \mathbf{0}$, akkor egyértelműen léteznek olyan $R, S \in K^{(\mathbb{N})}$, hogy $P = S \cdot Q + R$ és $\deg(R) < \deg(Q)$ (*euklidészi polinomosztás*).

16.7. Polinomok gyökei és algebrailag zárt testek

16.7.1. Definíció. *Ha K test, akkor a $P \in K[X]$ polinom* **gyökének** *nevezünk minden olyan $c \in K$ elemet, amelyre $P_K(c) = 0$ teljesül.*

16.7.2. Állítás. *Ha K test és $P \in K[X]$, akkor a $c \in K$ elem pontosan akkor gyöke P-nek, ha létezik olyan $Q \in K[X]$, amelyre $P = (X - c) * Q$ (vagyis $X - c$ osztója P-nek a $K[X]$ polinomgyűrűben).*

Bizonyítás. A feltétel elégséges, mert $P_K = (\mathrm{id}_K - c) \cdot Q_K$. A szükségesség bizonyításához eloszjuk P-t az elsőfokú $X - c$ polinommal, tehát vesszük azokat a $Q, R \in K[X]$ polinomokat, amelyekre $P = (X-c)*Q+R$ és $\deg(R) < \deg(X-c) = 1$, vagyis $\deg(R) = 0$ (14.7.8.). Ekkor $P_K = (\mathrm{id}_K - c) \cdot Q_K + R_K$, és $0 = P_K(c) = (c-c)Q_K(c) + R_K(c)$, tehát $R_K(c) = 0$, amiből $\deg(R) = 0$ alapján nyilvánvalóan következik, hogy $R = 0$, így $P = (X - c) * Q$. ■

16.7.3. Következmény. *Ha K test és $P \in K[X]$ nem nulla polinom, akkor P gyökeinek halmaza véges, és számossága kisebb-egyenlő P fokánál.*

Bizonyítás. A P polinom fokszáma szerinti teljes indukcióval bizonyítunk.

Tegyük fel, hogy $\deg P = 0$ és $P \neq 0$, tehát $P(0) \neq 0$ és minden $k \geq 1$ természetes számra $P(k) = 0$. Ha $c \in K$ gyöke a P polinomnak, akkor $0 = P_K(c) = \sum_{k=0}^{\infty} P(k)c^k = P(0)c^0 + \sum_{k=1}^{\infty} P(k)c^k = P(0)$, ami $P(0) \neq 0$ miatt lehetetlen. Ezért P gyökeinek halmaza üres, vagyis véges és 0 számosságú, tehát kisebb-egyenlő számosságú P fokánál.

Legyen $n \in \mathbb{N}$ olyan, hogy minden $Q \in K[X]$ nem nulla polinomra, ha $\deg(Q) = n$, akkor Q gyökeinek halmaza véges, és számossága kisebb-egyenlő Q fokánál. Legyen $P \in K[X]$ olyan polinom, hogy $\deg(P) = n + 1$ és jelölje N_P a P polinom gyökeinek halmazát. Ha $\mathrm{N}_P = \emptyset$, akkor N_P véges és $\mathrm{Card}(\mathrm{N}_P) = 0 \leq \deg(P)$. Ha $\mathrm{N}_P \neq \emptyset$, akkor legyen $c \in \mathrm{N}_P$ rögzített elem. Az előző állítás szerint vehetünk olyan $Q \in K[X]$ polinomot, hogy $P = (X - c) * Q$. Mivel $P \neq 0$, így $Q \neq 0$, tehát a 14.7.5. állítás alapján $n + 1 = \deg P = \deg(X - c) + \deg(Q) = 1 + \deg(Q)$. Ez azt jelenti, hogy $\deg(Q) = n$, így az indukciós hipotézis szerint a Q polinom gyökeinek N_Q halmaza véges és $\mathrm{Card}(\mathrm{N}_Q) \leq \deg(Q)$. Ha $x \in \mathrm{N}_P$, akkor $0 = P_K(x) = (x - c)Q_L(x)$, így K zérusosztómentessége folytán $x = c$ vagy $x \in \mathrm{N}_Q$. Tehát $\mathrm{N}_P \subseteq \{c\} \cup \mathrm{N}_Q$, amiből következik, hogy N_P véges és $\mathrm{Card}(\mathrm{N}_P) \leq \mathrm{Card}(\mathrm{N}_Q) + 1 = n + 1 = \deg(P)$. Ez azt jelenti, hogy az állítás igaz az $n + 1$ számra is. ■

16.7.4. Következmény. *Ha K test, $P, Q \in K[X]$ polinomok, és létezik olyan $E \subseteq K$ halmaz, amelyre $P_K = Q_K$ az E halmazon, és E végtelen, vagy véges és $\mathrm{Card}(E) > \max(\deg(P), \deg(Q))$, akkor $P = Q$.*

Bizonyítás. A hipotézis szerint $(P - Q)_K = P_K - Q_K = 0$ az E halmazon, vagyis E részhalmaza a $P - Q$ polinom gyökei halmazának. Ha $P \neq Q$, vagyis $P - Q \neq 0$, akkor 16.7.3. szerint $P - Q$ gyökeinek halmaza véges, így E véges. Ezért végtelen E esetén szükségképpen $P = Q$. Ha E véges és $\mathrm{Card}(E) > \max(\deg(P), \deg(Q))$, akkor $\mathrm{Card}(E) > \deg(P - Q)$, mivel 14.7.6. szerint $\deg(P - Q) \leq \max(\deg(P), \deg(Q))$. Ezért 16.7.3. alapján ebben az esetben is $P - Q = 0$ teljesül. ■

16.7.5. Következmény. *A K test pontosan akkor végtelen, ha a*

$$K[X] \to \mathscr{F}(K;K); \quad P \mapsto P_K$$

leképezés injektív.

Bizonyítás. Ha K végtelen test, akkor $P, Q \in K[X]$ és $P_K = Q_K$ esetén az előző következmény alapján $P = Q$, vagyis a $K[X] \to \mathscr{F}(K;K)$; $P \mapsto P_K$ leképezés injektív.

Megfordítva, ha K véges test, akkor a $P := \prod_{k \in K} (X - k) \in K[X]$ polinomra $P_K =$

$\prod_{k \in K} (\mathrm{id}_K - k) = 0$ teljesül, ezért a $K[X] \to \mathscr{F}(K;K)$; $P \mapsto P_K$ leképezés nem injektív, hiszen $0_K = 0$ is nyilvánvalóan teljesül, és $\prod_{k \in K} (X - k) \neq 0$, hiszen $\deg\Big(\prod_{k \in K} (X-k)\Big) = \mathrm{Card}(K) \geq 2$. ■

Tehát ha K végtelen test, akkor a $K[X]$ polinomgyűrű azonosítható a $K \to K$ polinomiális függvények gyűrűjével.

16.7.6. Definíció. *Azt mondjuk, hogy a K test* **algebrailag zárt**, *ha minden K feletti, nem nulladfokú polinomnak létezik gyöke K-ban.*

A $\mathbb{Q}$ és $\mathbb{R}$ testek nem algebrailag zártak. (Később igazoljuk, hogy semmilyen rendezett test nem lehet algebrailag zárt, azonban $\mathbb{C}$ algebrailag zárt.)

16.7.7. Állítás. *Véges test nem algebrailag zárt.*

Bizonyítás. Ha K véges test, akkor a

$$P := \mathbf{1} + \prod_{k \in K} (X - k)$$

polinom $\mathrm{Card}(K)$-ad fokú, és nincs gyöke K-ban, mert minden $x \in K$ esetén

$$P_K(x) = 1 + \prod_{k \in K} (x - k) = 1. \ ■$$

16.8. Lagrange-féle interpolációs polinomok

16.8.1. Állítás. *Legyen K test, és $(\alpha_i)_{i \in I}$ nem üres, véges, injektív rendszer K-ban, valamint $(\beta_i)_{i \in I}$ (ugyanolyan indexhalmazú) K-ban haladó rendszer. Ekkor*

$$P := \sum_{k \in I} \beta_k \cdot \left(\prod_{\substack{j \in I \\ j \neq k}} \frac{X - \alpha_j}{\alpha_k - \alpha_j} \right)$$

az az egyértelműen meghatározott K feletti polinom, amelyre $\deg(P) \leq \mathrm{Card}(I)$ *és minden $i \in I$ esetén $P_K(\alpha_i) = \beta_i$.*

Bizonyítás. ■

16.8.2. Állítás. *Legyen $n \in \mathbb{N}^*$ és $(\alpha_k)_{1 \leq k \leq n}$ injektív rendszer a K testben, valamint $(\beta_k)_{1 \leq k \leq n}$ tetszőleges rendszer K-ban. Ekkor létezik egyetlen olyan K feletti P polinom, amely legfeljebb n-ed fokú és olyan, hogy minden $k \in \mathbb{N}$, $1 \leq k \leq n$ számra $P_K(\alpha_k) = \beta_k$ teljesül; ez a következő:*

$$P = \sum_{k=1}^{n} \beta_k \cdot \left(\prod_{\substack{j=1 \\ j \neq k}}^{n} \frac{X - \alpha_j}{\alpha_k - \alpha_j} \right).$$

(**Lagrange-féle interpolációs polinom**)

Bizonyítás. Minden $1 \leq k \leq n$ természetes számra legyen

$$P_k := \prod_{\substack{j=1 \\ j \neq k}}^{n} \frac{X - \alpha_j}{\alpha_k - \alpha_j}.$$

Világos, hogy minden
■

i) Legyen $n \in \mathbb{N}^*$ és $(\alpha_k)_{1 \leq k \leq n}$ *injektív* rendszer K-ban, valamint $(\beta_k)_{1 \leq k \leq n}$ *tetszőleges* rendszer K-ban. Ekkor létezik egyetlen olyan K feletti P polinom, amely n-ed fokú és olyan, hogy minden $k \in \mathbb{N}$, $1 \leq k \leq n$ számra $P_K(\alpha_k) = \beta_k$ teljesül; ez a következő:

$$P = \sum_{k=1}^{n} \beta_k \cdot \frac{(X - \alpha_1) \cdot \dots \cdot (X - \alpha_{k-1}) \cdot (X - \alpha_{k+1}) \cdot \dots \cdot (X - \alpha_n)}{(\alpha_k - \alpha_1) \cdot \dots \cdot (\alpha_k - \alpha_{k-1}) \cdot (\alpha_k - \alpha_{k+1}) \cdot \dots \cdot (\alpha_k - \alpha_n)}$$

(**Lagrange-féle interpolációs polinom**).

16.9. Algebrailag zárt testek és az Euler–Lagrange-tétel

17. fejezet

Vektorterek

17.1. Vektorterek és lineáris operátorok értelmezése

17.1.1. Definíció. *Az* $(E, +, .)$ *hármast* **vektortérnek** *vagy* **lineáris térnek** *nevezzük a* K *test felett, ha* $+ : E \times E \to E$ *és* $. : K \times E \to E$ *olyan függvények, amelyek rendelkeznek a következő tulajdonságokkal:*

($\mathrm{EV_I}$) *Az* E *halmaz feletti* $+$ *művelet asszociatív, kommutatív, neutrális-elemes és inverzelemes, vagyis az* $(E, +)$ *pár kommutatív csoport.*

($\mathrm{EV_{II}}$) *Minden* $\alpha, \beta \in K$ *és* $x, y \in E$ *esetén*

$$\alpha.(\beta.x) = (\alpha \cdot \beta).x; \tag{$\mathrm{EV_{II_1}}$}$$

$$(\alpha + \beta).x = \alpha.x + \beta.x; \tag{$\mathrm{EV_{II_2}}$}$$

$$\alpha.(x + y) = \alpha.x + \alpha.y; \tag{$\mathrm{EV_{II_3}}$}$$

$$1.x = x. \tag{$\mathrm{EV_{II_4}}$}$$

Ha $(E, +, .)$ *vektortér a* K *test felett, akkor a* $+$ *művelet szerinti neutrális elemet rendszerint a* $\mathbf{0}$ *vagy* 0 *szimbólummal jelöljük, továbbá minden* $x \in E$ *esetén* $-x$ *jelöli az* x *elem inverzét a* $+$ *művelet szerint. A valós* (*illetve komplex*) *számok teste feletti vektortereket* **valós** (*illetve* **komplex**) **vektortereknek** *nevezzük.*

17.1.2. Állítás. *Legyen* T *halmaz,* K *test és* $E := \mathscr{F}(T; K)$*. Minden* $x, y \in E$ *és* $\alpha \in K$ *esetén legyenek* $x + y$ *és* $\alpha.x$ *azok a* $T \to K$ *függvények, amelyekre minden* $t \in T$ *esetén*

$$(x + y)(t) := x(t) + y(t),$$
$$(\alpha.x)(t) := \alpha \cdot x(t).$$

Ekkor az

$$E \times E \to E; \quad (x, y) \mapsto x + y,$$
$$K \times E \to E; \quad (\alpha, x) \mapsto \alpha.x$$

leképezések rendelkeznek az ($\mathrm{EV_I}$) *és* ($\mathrm{EV_{II}}$) *tulajdonságokkal, tehát* $(E, +, .)$ *vektortér a* K *test felett. Az* $(E, +)$ *kommutatív csoport neutrális eleme a* $T \to K$ *azonosan* 0 *függvény, és* $x \in E$ *esetén az* x *inverze a* $+$ *művelet szerint a* $T \to K;\ t \mapsto -x(t)$ *függvény.*

Bizonyítás. Nyilvánvalóan következik a testeket definiáló tulajdonságokból. ■

Tehát látjuk, hogy ha T halmaz és K test, akkor a $(\mathscr{F}(T;K),+,.)$ hármas vektortér K felett, ahol $+$ és $.$ az előző állításban bevezetett leképezések; az ilyen alakú vektortereket **teljes függvénytereknek** nevezzük.

17.1.3. Definíció. *A K test feletti $(E,+,.)$ vektortér* **lineáris alterének** *nevezünk minden olyan $F \subseteq E$ nem üres halmazt, amelyre minden $x, y \in F$ és $\alpha \in K$ esetén $x + y \in F$ és $\alpha.x \in F$ teljesül.*

A definíciók alapján nyilvánvaló, hogy ha F lineáris altere a K test feletti $(E,+,.)$ vektortérnek, akkor az $(F,+|_{F\times F},.|_{K\times F})$ hármas szintén vektortér a K test felett.

Világos, hogy vektortér lineáris alterei tetszőleges nem üres rendszerének a metszete is lineáris altér, továbbá a vektortér alaphalmaza is lineáris altér. Ebből következik, hogy vektortér alaphalmazának minden részhalmaza benne van egy tartalmazás tekintetében legkisebb lineáris altérben, ti. az adott részhalmazt tartalmazó lineáris alterek metszetében; ezt a lineáris alteret nevezzük a részhalmaz által *generált lineáris altérnek*.

17.1.4. Definíció. *A teljes függvényterek lineáris altereit* **függvénytereknek** *nevezzük. Ha K test, akkor az $(\mathscr{F}(\mathbb{N};K),+,.)$ teljes függvénytér lineáris altereit* **sorozattereknek** *nevezzük.*

Példák (vektorterekre).

1) Ha K test, akkor a $(K,+,\cdot)$ hármas vektortér K felett, tehát a vektortér-fogalom a test-fogalom általánosításának tekinthető.

2) Az $(\mathbb{R},+,\cdot|_{\mathbb{Q}\times\mathbb{R}})$ hármas vektortér a $\mathbb{Q}$ test felett. A $(\mathbb{C},+,\cdot|_{\mathbb{R}\times\mathbb{C}})$ hármas valós vektortér. Általánosan, ha K test és L részteste K-nak (II. fejezet, 1. pont, **2**. gyakorlat), akkor $(K,+,\cdot|_{L\times K})$ vektortér az L test felett.

3) Legyen K test és $n \in \mathbb{N}$. Ekkor $K^n := \mathscr{F}(n;K)$, tehát $(K^n,+,.)$ egy teljes függvénytér. Ha x és y K-beli elem n-esek és $\alpha \in K$, akkor $x+y$ és $\alpha.x$ azok a K-beli elem n-esek, amelyekre minden $k \in n$ esetén $(x+y)(k) := x(k)+y(k)$ és $(\alpha.x)(k) := \alpha \cdot x(k)$.

4) Legyen K test és $m, n \in \mathbb{N}$. Ekkor $\mathrm{M}_{m,n}(K) := \mathscr{F}(m\times n;K)$, tehát $(\mathrm{M}_{m,n}(K),+,.)$ egy teljes függvénytér. Ha $\mathfrak{a}, \mathfrak{b} \in \mathrm{M}_{m,n}(K)$ és $\alpha \in K$, akkor $\mathfrak{a}+\mathfrak{b}$ és $\alpha.\mathfrak{a}$ azok a K-beli együtthatós $m \times n$-es mátrixok, amelyekre minden $(i,j) \in m \times n$ esetén $(\mathfrak{a}+\mathfrak{b})_{i,j} = \mathfrak{a}_{i,j}+\mathfrak{b}_{i,j}$ és $(\alpha.\mathfrak{a})_{i,j} = \alpha\cdot\mathfrak{a}_{i,j}$.

5) Ha K test, akkor a

$$K^{(\mathbb{N})} := \{\mathbf{s} \in K^{\mathbb{N}} |\text{ az } \{n \in \mathbb{N} | \mathbf{s}(n) \neq 0\} \text{ halmaz véges}\}$$

halmaz lineáris altere a $(K^{\mathbb{N}},+,.)$ sorozattérnek.

6) Ha T halmaz, akkor a $T \to \mathbb{K}$ korlátos függvények $\mathscr{F}^b(T;\mathbb{K})$ halmaza lineáris altere az $(\mathscr{F}(T;\mathbb{K}),+,.)$ függvénytérnek. Speciálisan, $\mathscr{F}^b(\mathbb{N};\mathbb{K})$ azonos a $\mathbb{K}$-ban haladó korlátos sorozatok halmazával; ezt $l^\infty_{\mathbb{K}}$ jelöli. Világos, hogy $l^\infty_{\mathbb{K}}$ lineáris altere a $\mathbb{K}$-ban haladó sorozatok terének.

7) A $\mathbb{K}$-ban haladó konvergens sorozatok halmaza lineáris altere $\mathbb{K}$-ban haladó sorozatok terének.

8) Ha $T \subseteq \mathbb{K}$ tetszőleges halmaz, akkor a $T \to \mathbb{K}$ folytonos függvények $\mathscr{C}(T;\mathbb{K})$ halmaza, valamint a $T \to \mathbb{K}$ korlátos és folytonos függvények $\mathscr{C}^b(T;\mathbb{K})$ halmaza lineáris altere a $(\mathscr{F}(T;\mathbb{K}),+,.)$ függvénytérnek.

9) Ha $\Omega \subseteq \mathbb{K}$ nyílthalmaz, akkor az $\Omega \to \mathbb{K}$ differenciálható függvények halmaza lineáris

altere a $(\mathscr{F}(\Omega;\mathbb{K}),+,.)$ függvénytérnek.

10) Legyen $p \geq 1$ valós szám és

$$l^p_{\mathbb{K}} := \left\{\mathbf{s} \in \mathbb{K}^{\mathbb{N}} \;\middle|\; \text{a } \sum_{k\in\mathbb{N}} |\mathbf{s}(k)|^p \text{ sor konvergens}\right\}.$$

Az $l^p_{\mathbb{K}}$ halmaz elemeit *p-edik hatványon abszolút szummálható* sorozatoknak nevezzük. Az $l^p_{\mathbb{K}}$ halmaz lineáris altere a $\mathbb{K}$-ban haladó sorozatok terének.

Ettől kezdve a vektortereket rendszerint egyetlen szimbólummal, az alaphalmaz jelével jelöljük, és a bennük értelmezett összeadást a $+$, és a hozzájuk tartózó test elemeivel való szorzást a . szimbólummal jelöljük, ha ez nem okoz félreértést.

17.1.5. Állítás. *Legyen T halmaz, F vektortér a K test felett, és $E := \mathscr{F}(T;F)$. Minden $x,y \in E$ és $\alpha \in K$ esetén legyenek $x+y$ és $\alpha.x$ azok a $T \to F$ függvények, amelyekre minden $t \in T$ esetén*

$$(x+y)(t) := x(t) + y(t),$$
$$(\alpha.x)(t) := \alpha \cdot x(t).$$

Ekkor az $(E,+,.)$ hármas vektortér a K test felett.

Bizonyítás. Nyilvánvalóan következik a vektorterek definíciójából. ■

A továbbiakban egy halmazon értelmezett, vektortérbe ható összes függvények halmazát vektortérnek tekintjük az előző állításban bevezetett vektortér-struktúrával ellátva.

17.1.6. Definíció. *Legyenek E és F vektorterek a K test felett. Azt mondjuk, hogy az $u : E \to F$ függvény* **lineáris operátor**, *ha rendelkezik a következő tulajdonságokkal:*

– **additív**, *azaz minden $x,y \in E$ esetén*

$$u(x+y) = u(x) + u(y),$$

– K-**homogén**, *azaz minden $x \in E$ és $\alpha \in K$ esetén*

$$u(\alpha.x) = \alpha.u(x).$$

Az $E \to F$ lineáris operátorok halmazát $\mathbf{L}(E;F)$ jelöli. Az $\mathbf{L}(E;K)$ halmazt az E^* szimbólummal rövidítjük, és ezt az E vektortér **duálisának** *nevezzük. Az E^* elemeit, vagyis az $E \to K$ lineáris operátorokat E feletti* **lineáris funkcionáloknak**, *vagy* **lineáris formáknak** *nevezzük.*

17.1.7. Állítás. *Ha E és F vektorterek a K test felett, akkor $\mathbf{L}(E;F)$ lineáris altere az $\mathscr{F}(E;F)$ függvénytérnek.*

Bizonyítás. Legyenek $u, u' \in \mathbf{L}(E;F)$. Ha $x, x' \in E$, akkor az $\mathscr{F}(E;F)$ függvénytérben bevezetett összeadás definíciója, valamint u és u' additivitása, és F összeadásának asszociativitása és kommutativitása folytán valamint az $\mathscr{F}(E;F)$ függvénytérben bevezetett összeadás definíciója szerint

$$(u+u')(x+x') = u(x+x') + u'(x+x') = (u(x)+u(x')) + (u'(x)+u'(x')) =$$
$$= (u(x)+u'(x)) + (u(x')+u'(x')) = (u+u')(x) + (u+u')(x'),$$

tehát az $u+u' : E \to F$ leképezés additív. Továbbá, ha $x \in E$ és $\lambda \in K$, akkor

$$(u+u')(\lambda.x) = u(\lambda.x) + u'(\lambda.x) = \lambda.u(x) + \lambda.u'(x) = \lambda.(u(x)+u'(x)) = \lambda.(u+u')(x),$$

tehát az $u+u' : E \to F$ leképezés K-homogén. Ez azt jelenti, hogy $u, u' \in \mathbf{L}(E;F)$ esetén $u+u' \in \mathbf{L}(E;F)$.

Legyenek $u \in \mathbf{L}(E;F)$ és $\lambda \in K$. Ha $x, x' \in E$, akkor az $\mathscr{F}(E;F)$ függvénytérben bevezetett testbeli elemmel való szorzás definíciója, valamint u és u' K-homogenitása és az F vektortérre vonatkozó ($\mathrm{EV}_{\mathrm{II}_3}$) tulajdonság folytán

$$(\lambda.u)(x+x') = \lambda.u(x+x') = \lambda.(u(x)+u(x')) = \lambda.u(x) + \lambda.u(x') = (\lambda.u)(x) + (\lambda.u)(x'),$$

tehát a $\lambda.u : E \to F$ leképezés additív. Továbbá, ha $x \in E$ és $\sigma \in K$, akkor az $\mathscr{F}(E;F)$ függvénytérben bevezetett testbeli elemmel való szorzás definíciója, valamint u K-homogenitása, a K test szorzásának kommutativitása, és az F vektortérre vonatkozó ($\mathrm{EV}_{\mathrm{II}_1}$) tulajdonság folytán

$$(\lambda.u)(\sigma.x) = \lambda.u(\sigma.x) = \lambda.(\sigma.u(x)) = (\lambda\sigma).u(x) = (\sigma\lambda).u(x) = \sigma.(\lambda.u(x)) = \sigma.(\lambda.u)(x),$$

tehát a $\lambda.u : E \to F$ leképezés K-homogén. Ez azt jelenti, hogy $u \in \mathbf{L}(E;F)$ és $\lambda \in K$ esetén $\lambda.u \in \mathbf{L}(E;F)$. ■

17.1.8. Definíció. *A K test feletti E és F vektortereket* **lineárisan izomorfaknak** (*vagy csak egyszerűen* **izomorfaknak**) *nevezzük, ha létezik $E \to F$ lineáris bijekció. Azt mondjuk, hogy a K test feletti E vektortér* **véges dimenziós**, *ha létezik olyan $n \in \mathbb{N}$, hogy a K^n és E vektorterek izomorfak.*

Ha E és F vektorterek és $u \in \mathbf{L}(E;F)$, akkor $u(0) = 0$, mert u additív, tehát csoport-morfizmus az $(E,+)$ és $(F,+)$ kommutatív csoportok között, így megtartja a neutrális elemeket (13.1.3.), továbbá u pontosan akkor *injektív*, ha $\mathrm{Ker}(u) = \{0\}$ (13.1.8.), vagyis minden $x \in E$ esetén, ha $x \neq 0$, akkor $u(x) \neq 0$. Ezeket a tulajdonságokat a továbbiakban külön hivatkozás nélkül fogjuk alkalmazni.

17.1.9. Állítás. *Ha E, F és G vektorterek a K test felett, továbbá $u \in \mathbf{L}(E;F)$ és $v \in \mathbf{L}(F;G)$, akkor $v \circ u \in \mathbf{L}(E;G)$.*

Bizonyítás. Ha $x, x' \in E$, akkor u és v additivitása folytán

$$(v \circ u)(x+x') = v(u(x+x')) = v(u(x)+u(x')) = v(u(x)) + v(u(x')) = (v \circ u)(x) + (v \circ u)(x'),$$

tehát a $v \circ u : E \to G$ leképezés additív.

Ha $x \in E$ és $\lambda \in K$, akkor u és v K-homogenitása folytán

$$(v \circ u)(\lambda.x) = v(u(\lambda.x)) = v(\lambda.u(x)) = \lambda.v(u(x)) = (\lambda.(v \circ u))(x),$$

tehát a $v \circ u : E \to G$ leképezés K-homogén. ■

17.1.10. Állítás. *Ha E vektortér, akkor az $E \to E$ lineáris operátorok $\mathbf{L}(E;E)$ halmaza az összedás és függvénykompozíció műveletekkel ellátva egységelemes gyűrű.*

Bizonyítás. A pontonkénti összeadás kommutatív csoportművelet $\mathbf{L}(E;E)$ felett, és a függvénykompozíció asszociatív. Továbbá, a függvénykompozíció nyilvánvalóan jobbról disztributív az $\mathbf{L}(E;E)$ feletti összeadásra nézve, mert minden $u,v,w \in \mathbf{L}(E;E)$ és $x \in E$ esetén az $\mathbf{L}(E;E)$ feletti összeadás definíciója szerint

$$((v+w)\circ u)(x)=(v+w)(u(x))=v(u(x))+w(u(x))=(v\circ u)(x)+(w\circ u)(x)=(v\circ u+w\circ u)(x),$$

tehát $(v+w)\circ u = v\circ u + w\circ u$. Végül, a függvénykompozíció balról is disztributív az az $\mathbf{L}(E;E)$ feletti összeadásra nézve, mert minden $u,v,w \in \mathbf{L}(E;E)$ és $x \in E$ esetén az $\mathbf{L}(E;E)$ feletti összeadás definíciója és u additivitása folytán

$$\begin{aligned}(u\circ(v+w))(x) = u((v+w)(x)) = u(v(x)+w(x)) = u(v(x))+u(w(x)) = \\ = (u\circ v)(x)+(u\circ w)(x) = (u\circ v+u\circ w)(x),\end{aligned}$$

tehát $u\circ(v+w) = u\circ v + u\circ w$. Nyilvánvaló, hogy az id_E operátor egységeleme az $\mathbf{L}(E;E)$ gyűrűnek. ■

Az előző állításban előállított gyűrűket rendszerint *operátorgyűrűknek* nevezzük.

17.1.11. Állítás. *Legyenek E, F, G, és H vektorterek a K test felett, továbbá $v \in \mathbf{L}(G;E)$ és $w \in \mathbf{L}(F;H)$, akkor a*

$$\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H); \quad u \mapsto w\circ u\circ v$$

leképezés lineáris operátor, és ha a $v : G \to E$ és $w : F \to H$ leképezések lineáris bijekciók, akkor $\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H)$ is lineáris bijekció.

Bizonyítás. Jelölje Φ a szóban forgó $\mathbf{L}(E;F) \to \mathbf{L}(G;H)$ leképezést.

Ha $u,u' \in \mathbf{L}(E;F)$, akkor minden $x \in G$ esetén, az operátorterekben bevezetett összeadás definíciója és w additivitása folytán

$$\begin{aligned}\Phi(u+u')(x) = (w\circ(u+u')\circ v)(x) = w((u+u')(v(x))) = w(u(v(x))+u'(v(x))) = \\ = w(u(v(x)))+w(u'(v(x))) = (w\circ u\circ v)(x)+(w\circ u'\circ v)(x) = \\ = \Phi(u)(x)+\Phi(u')(x) = (\Phi(u)+\Phi(u'))(x),\end{aligned}$$

ezért $\Phi(u+u') = \Phi(u)+\Phi(u')$, vagyis a $\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H)$ leképezés additív.

Ha $u \in \mathbf{L}(E;F)$ és $\lambda \in K$, akkor minden $x \in G$ esetén, az operátorterekben bevezetett testbeli elemmel való szorzás definíciója és w K-homogenitása folytán

$$\begin{aligned}\Phi(\lambda.u)(x) = (w\circ(\lambda.u)\circ v)(x) = w((\lambda.u)(v(x))) = w(\lambda.u(v(x))) = \\ = \lambda.w(u(v(x))) = \lambda.(w\circ u\circ v)(x) = (\lambda.\Phi(u))(x),\end{aligned}$$

ezért $\Phi(\lambda.u) = \lambda.\Phi(u)$, vagyis a $\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H)$ leképezés K-homogén.

Ezzel beláttuk, hogy a $\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H)$ leképezés lineáris operátor.

Legyen most $u \in \mathbf{L}(E;F)$ olyan, hogy $\Phi(u) = 0$. Ekkor minden $x \in G$ esetén

$$(w\circ u)(v(x)) = w(u(v(x))) = \Phi(u)(x) = 0,$$

ezért ha v *szürjektív* akkor $w\circ u = 0$. Ekkor minden $y \in E$ vektorra $w(u(y)) = 0$, tehát ha w *injektív*, akkor $u(y) = 0$, vagyis $u = 0$. Ez azt jelenti, hogy ha v szürjektív és w injektív, akkor a $\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H)$ lineáris operátor injektív.

Ha v és w lineáris bijekciók, akkor $u' \in \mathbf{L}(G;H)$ esetén $w^{-1} \circ u' \circ v^{-1} \in \mathbf{L}(E;F)$ olyan lineáris operátor, amelyre

$$\Phi\left(w^{-1} \circ u' \circ v^{-1}\right) = w \circ \left(w^{-1} \circ u' \circ v^{-1}\right) \circ v = u',$$

tehát a $\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H)$ lineáris operátor szürjektív.

Ezzel beláttuk, hogy ha a $v : G \to E$ és $w : F \to H$ leképezések lineáris bijekciók, akkor $\Phi : \mathbf{L}(E;F) \to \mathbf{L}(G;H)$ is lineáris bijekció. ■

Példák (lineáris operátorokra).

1) Legyen K test és $n \in \mathbb{N}$. Minden $u \in (K^n)^*$ lineáris funkcionálhoz egyértelműen létezik olyan $p \in K^n$, hogy minden $x \in K^n$ esetén fennáll az

$$u(x) = \sum_{k \in n} p(k)x(k)$$

egyenlőség. Megfordítva, minden $p \in K^n$ esetén a

$$K^n \to K; \quad x \mapsto \sum_{k \in n} p(k)x(k)$$

leképezés lineáris funkcionál a K^n vektortér felett. Ebből következik, hogy a $(K^n)^*$ és K^n vektorterek között létezik egy kitüntetett bijekció, amelyről könnyen belátható, hogy lineáris. Tehát a $(K^n)^*$ és K^n vektorterek kitüntetett módon (vagy a matematikában szokásos terminológia szerint: *kanonikusan*) izomorfak.

2) Legyen K test és $m, n \in \mathbb{N}$. Minden $\mathfrak{a} \in M_{m,n}(K)$ mátrixra jelölje $u_{\mathfrak{a}}$ azt a $K^n \to K^m$ függvényt, amely minden $x \in K^n$ elem n-eshez a

$$\left(\sum_{j \in n} \mathfrak{a}(i,j)x(j)\right)_{i \in m} \in K^m$$

elemet rendeli. Ekkor minden $\mathfrak{a} \in M_{m,n}(K)$ mátrixra $u_{\mathfrak{a}} \in \mathbf{L}(K^n; K^m)$, és az

$$M_{m,n}(K) \to \mathbf{L}(K^n; K^m); \quad \mathfrak{a} \mapsto u_{\mathfrak{a}}$$

leképezés kitüntetett lineáris bijekció a $M_{m,n}(K)$ és $\mathbf{L}(K^n; K^m)$ vektorterek között. Ez azt jelenti, hogy az $m \times n$-es K-beli együtthatós mátrixok vektortere kanonikusan azonosítható a $K^n \to K^m$ lineáris operátorok vektorterével.

3) Legyen minden $\mathbf{a} \in l^1_{\mathbb{K}}$ abszolút szummálható sorozatra

$$u_{\mathbf{a}} : l^\infty_{\mathbb{K}} \to \mathbb{K}; \quad \mathbf{s} \mapsto \sum_{k=0}^{\infty} \mathbf{a}(k)\mathbf{s}(k).$$

Ekkor minden $\mathbf{a} \in l^1_{\mathbb{K}}$ elemre $u_{\mathbf{a}} \in (l^\infty_{\mathbb{K}})^*$, és az

$$l^1_{\mathbb{K}} \to (l^\infty_{\mathbb{K}})^*; \quad \mathbf{a} \mapsto u_{\mathbf{a}}$$

leképezés *lineáris injekció*. Ez azt jelenti, hogy az $l^1_{\mathbb{K}}$ sorozattér az imént felírt lineáris injekció által kanonikusan azonosítható az $(l^\infty_{\mathbb{K}})^*$ duális egyik lineáris alterével (ti. az $\{u_{\mathbf{a}} | \mathbf{a} \in l^1_{\mathbb{K}}\}$ halmazzal).

4) Legyen minden $\mathbf{a} \in l^\infty_{\mathbb{K}}$ (korlátos) számsorozatra

$$u_{\mathbf{a}} : l^1_{\mathbb{K}} \to K; \quad \mathbf{s} \mapsto \sum_{k=0}^{\infty} \mathbf{a}(k)\mathbf{s}(k).$$

Ekkor minden $\mathbf{a} \in l^\infty_{\mathbb{K}}$ elemre $u_{\mathbf{a}} \in (l^1_{\mathbb{K}})^*$, és az

$$l^\infty_{\mathbb{K}} \to (l^1_{\mathbb{K}})^*; \quad \mathbf{a} \mapsto u_{\mathbf{a}}$$

leképezés *lineáris injekció*. Ez azt jelenti, hogy az $l^\infty_{\mathbb{K}}$ sorozattér az imént felírt lineáris injekció által kanonikusan azonosítható az $(l^1_{\mathbb{K}})^*$ duális egyik lineáris alterével (ti. az $\{u_{\mathbf{a}} | \mathbf{a} \in l^\infty_{\mathbb{K}}\}$ halmazzal).

5) Legyen $p \geq 1$ tetszőleges valós szám, és minden $\mathbf{a} \in l^\infty_{\mathbb{K}}$ (korlátos) számsorozatra

$$u_{\mathbf{a}} : l^p_{\mathbb{K}} \to l^p_{\mathbb{K}}; \quad \mathbf{s} \mapsto \mathbf{a} \cdot \mathbf{s}.$$

Ekkor minden $\mathbf{a} \in l^\infty_{\mathbb{K}}$ elemre $u_{\mathbf{a}} \in \mathbf{L}(l^p_{\mathbb{K}}; l^p_{\mathbb{K}})$, és az

$$l^\infty_{\mathbb{K}} \to \mathbf{L}(l^p_{\mathbb{K}}; l^p_{\mathbb{K}}); \quad \mathbf{a} \mapsto u_{\mathbf{a}}$$

leképezés *lineáris injekció*. Ez azt jelenti, hogy az $l^\infty_{\mathbb{K}}$ sorozattér az imént felírt lineáris injekció által azonosítható az $l^p_{\mathbb{K}} \to l^p_{\mathbb{K}}$ lineáris operátorok vektorterének egyik lineáris alterével (ti. az $\{u_{\mathbf{a}} | \mathbf{a} \in l^\infty_{\mathbb{K}}\}$ halmazzal).

6) Legyen T halmaz és K test. Minden $t \in T$ pontra legyen

$$\varepsilon_t : \mathscr{F}(T; K) \to K; \quad f \mapsto f(t).$$

Ekkor minden $t \in T$ esetén $\varepsilon_t \in (\mathscr{F}(T; K))^*$, és a

$$T \to (\mathscr{F}(T; K))^*; \quad t \mapsto \varepsilon_t$$

leképezés *injekció*. Ez azt jelenti, hogy a T halmaz az imént felírt injekció által kanonikusan azonosul az $(\mathscr{F}(T; K))^*$ duális tér egyik részhalmazával, ti. az $\{\varepsilon_t | t \in T\}$ halmazzal. Ha T véges, akkor az $\{\varepsilon_t | t \in T\}$ halmaz által generált lineáris altér $(\mathscr{F}(T; K))^*$-ban *egyenlő* $(\mathscr{F}(T; K))^*$-gal. Az ε_t alakú lineáris funcionálokat az $\mathscr{F}(T; K)$ függvénytér felett *helyettesítő funcionáloknak* nevezzük.

7) a) A $K^{(T)} := \{f \in \mathscr{F}(T; K) |$ a $\{t \in T | f(t) \neq 0\}$ halmaz véges$\}$ halmaz lineáris altere az $\mathscr{F}(T; K)$ függvénytérnek.

b) Minden $t \in T$ esetén jelölje δ_t azt az elemet $K^{(T)}$-ben, amelyre teljesül az, hogy minden $t' \in T$ elemre

$$\delta_t(t') := \begin{cases} 1 & , \text{ha } t' = t \\ 0 & , \text{ha } t' \neq t. \end{cases}$$

Ekkor a $(\delta_t)_{t \in T}$ rendszer *bázis* a $K^{(T)}$ vektortérben (**2**. gyakorlat), és a

$$T \to K^{(T)}; \quad t \mapsto \delta_t$$

leképezés *injekció*, tehát a T halmaz kanonikusan azonosul a $K^{(T)}$ vektortér egyik bázishalmazával. Ezért a $K^{(T)}$ vektortér felfogható a T halmaz olyan "bővítésének", amely vektortér K felett, és amelynek minden eleme "T-beli elemek formális lineáris kombinációja". Ez utóbbi állítás azt a triviális tényt fejezi ki, hogy minden $x \in K^{(T)}$ elemre fennáll az

$$x = \sum_{t \in [x \neq 0]} x(t).\delta_t$$

egyenlőség, ahol $[x \neq 0] := \{t' \in T | x(t') \neq 0\}$ (és az üres halmazra vett összeg definíció szerint egyenlő 0-val), és ha itt $t \in T$ esetén a δ_t szimbólum helyett az őt egyértelműen meghatározó t szimbólumot írjuk, akkor ez a kifejezés átmegy az

$$x = \sum_{t \in [x \neq 0]} x(t).t$$

formális egyenlőségbe. Ezért a $K^{(T)}$ elemeit szokás a T-beli pontok K-beli együtthatókkal vett *formális lineáris kombinációinak* nevezni.

c) A $K^{(T)}$ vektortér rendelkezik a következő tulajdonsággal: ha F tetszőleges vektortér a K test felett, és $f : T \to F$ tetszőleges függvény, akkor létezik egyetlen olyan $\tilde{f} : K^{(T)} \to F$ lineáris operátor, hogy minden $t \in T$ esetén $\tilde{f}(\delta_t) = f(t)$ teljesül.

d) A c)-ben megfogalmazott tulajdonság lineáris izomorfia erejéig egyértelműen meghatározza a $K^{(T)}$ vektorteret. Pontosabban; ha (E, j) olyan pár, hogy E vektortér K felett, és $j : T \to E$ olyan függvény, hogy minden K feletti F vektortérhez és minden $f : T \to F$ függvényhez létezik egyetlen olyan $\tilde{f} : K^{(T)} \to F$ lineáris operátor, hogy $\tilde{f} \circ j = f$; akkor létezik egyetlen olyan $u : K^{(T)} \to E$ lineáris bijekció, amelyre minden $t \in T$ esetén $u(\delta_t) = j(t)$ teljesül.

(A $K^{(T)}$ vektorteret a T halmaz által generált *szabad vektortérnek* nevezzük.)

17.2. Lineáris alterek és faktorterek

17.2.1. Definíció. *Legyen E vektortér a K test felett. Az $M \subseteq E$ halmazt* **lineáris altérnek** *nevezzük E-ben, ha $M \neq \emptyset$, $M + M \subseteq M$ és $K.M \subseteq M$.*

Nyilvánvaló, hogy ha M lineáris altere a K test feletti E vektortérnek, akkor $\mathbf{0} \in M$, mert $M \neq \emptyset$ miatt vehetünk egy $x \in M$ vektort, és akkor $\mathbf{0} = 0.x \in K.M \subseteq M$. Az is triviális, hogy $\{\mathbf{0}\}$ a tartalmazás szerint legkisebb és E a tartalmazás szerint legnagyobb lineáris altere az E vektortérnek.

Fontos példát láthatunk lineáris alterekre a következő állításban.

17.2.2. Állítás. *Ha E és F vektorterek a K test felett, és $u, v : E \to F$ lineáris operátorok, akkor az $\{x \in E | u(x) = v(x)\}$ halmaz és a*

$$\mathrm{Ker}(u) := \{x \in E | u(x) = 0\}$$

halmaz lineáris altér E-ben, valamint $\mathrm{Im}(u)$ *lineáris altér F-ben.*

Bizonyítás. Legyen $M := \{x \in E | u(x) = v(x)\}$. Ha $x, x' \in M$, akkor u és v additivitása miatt $u(x + x') = u(x) + u(x') = v(x) + v(x') = v(x + x')$, tehát $x + x' \in M$, ami azt jelenti, hogy $M + M \subseteq M$. Ha $x \in M$ és $\lambda \in K$, akkor az u és v leképezések K-homogenitása miatt $u(\lambda.x) = \lambda.u(x) = \lambda.v(x) = v(\lambda.x)$, tehát $\lambda.x \in M$, ami azt jelenti, hogy $K.M \subseteq M$. Mivel $u(0) = 0 = v(0)$, így $0 \in M$, vagyis $M \neq \emptyset$, tehát M lineáris altere E-nek.

Az előző bekezdés szerint $\mathrm{Ker}(u)$ lineáris altere E-nek, mert $\mathrm{Ker}(u) = \{x \in E | u(x) =$

$v(x)\}$, ahol v a 0 értékű $E \to F$ konstansfüggvény.

Ha $y, y' \in \mathrm{Im}(u)$, akkor léteznek olyan $x, x' \in E$, hogy $y = u(x)$ és $y' = u(x')$, ezért u additivitása folytán $y + y' = u(x) + u(x') = u(x + x') \in \mathrm{Im}(u)$, ami azt jelenti, hogy $\mathrm{Im}(u) + \mathrm{Im}(u) \subseteq \mathrm{Im}(u)$. Ha $y \in \mathrm{Im}(u)$ és $\lambda \in K$, akkor létezik olyan $x \in E$, hogy $y = u(x)$, ezért az u leképezés K-homogenitása folytán $\lambda.y = \lambda.u(x) = u(\lambda.x) \in \mathrm{Im}(u)$, ami azt jelenti, hogy $K.\mathrm{Im}(u) \subseteq \mathrm{Im}(u)$. Világos, hogy $E \neq \emptyset$ miatt $\mathrm{Im}(u) \neq \emptyset$, így $\mathrm{Im}(u)$ lineáris altere F-nek. ■

17.2.3. Állítás. *Legyen E vektortér a K test felett. Az $M \subseteq E$ halmaz pontosan akkor lineáris altere E-nek, ha minden M-ben haladó $(x_i)_{i\in I}$ véges rendszerre és $(\alpha_i)_{i\in I} \in K^I$ rendszerre $\sum_{i\in I} \alpha_i.x_i \in M$.*

Bizonyítás. A lineáris alterek definíciója és 8.5.4. a) miatt nyilvánvaló, hogy a feltétel elégséges. A szükségességet az I indexhalmaz számossága szerinti teljes indukcióval bizonyítjuk.

Az üres indexhalmazra vett összeg E-ben definíció szerint egyenlő $\mathbf{0}$-val, ami eleme az M lineáris altérnek.

Legyen $n \in \mathbb{N}$ olyan, hogy az állítás minden n számosságú I indexhalmazra igaz. Legyen I olyan véges halmaz, hogy $\mathrm{Card}(I) = n+1$, és vegyünk tetszőleges M-ben haladó $(x_i)_{i\in I}$ rendszert és tetszőleges K-ban haladó $(\alpha_i)_{i\in I}$ rendszert. Legyen $i_* \in I$ rögzített elem. Ekkor az indukciós hipotézis alapján $\sum_{i\in I\setminus\{i_*\}} \alpha_i.x_i \in M$, ezért 8.5.4. b) alapján

$$\sum_{i\in I} \alpha_i.x_i = \alpha_{i_*}.x_{i_*} + \sum_{i\in I\setminus\{i_*\}} \alpha_i.x_i \in K.M + M \subseteq M + M \subseteq M. \blacksquare$$

17.2.4. Állítás. *Legyen E vektortér a K test felett és $H \subseteq E$. Jelölje $\mathrm{sp}(H)$ azon $x \in E$ vektorok halmazát, amelyekhez létezik olyan H-ban haladó $(x_i)_{i\in I}$ véges rendszer és olyan $(\alpha_i)_{i\in I} \in K^I$ rendszer, hogy $x = \sum_{i\in I} \alpha_i.x_i$. Ekkor $\mathrm{sp}(H)$ olyan lineáris altere E-nek, hogy $H \subseteq \mathrm{sp}(H)$, és az E vektortér minden H-t tartalmazó M lineáris alterére $\mathrm{sp}(H) \subseteq M$ (vagyis $\mathrm{sp}(H)$ a tartalmazás tekintetében legkisebb H-t tartalmazó lineáris altere E-nek).*

Bizonyítás. Világos, hogy $\mathbf{0} \in \mathrm{sp}(H)$, mert az üres indexhalmazra vett összeg E-ben definíció szerint egyenlő $\mathbf{0}$-val, és 8.5.4. a) miatt nyilvánvaló, hogy $H \subseteq \mathrm{sp}(H)$.

Legyenek $x, y \in \mathrm{sp}(H)$. Megmutatjuk, hogy $x + y \in \mathrm{sp}(H)$. A definíció szerint vehetünk olyan H-ban haladó $(x_i)_{i\in I}$ véges rendszert és olyan $(\alpha_i)_{i\in I} \in K^I$ rendszert, hogy $x = \sum_{i\in I} \alpha_i.x_i$, valamint olyan H-ban haladó $(y_j)_{j\in J}$ véges rendszert és olyan $(\beta_j)_{j\in J} \in K^J$ rendszert, hogy $y = \sum_{j\in J} \beta_j.y_j$. Ekkor az $I \bigsqcup J := (\{0\} \times I) \cup (\{1\} \times J)$ diszjunkt unió minden k eleméhez értelmezzük a $\gamma_k \in K$ és $z_k \in H$ elemeket a következőképpen:

- minden $i \in I$ esetén, ha $k = (0, i)$, akkor $\gamma_k := \alpha_i$ és $z_k := x_i$;
- minden $j \in J$ esetén, ha $k = (1, j)$, akkor $\gamma_k := \beta_j$ és $z_k := y_j$.

Ekkor 8.5.5. alkalmazásával kapjuk, hogy

$$\sum_{k\in I\bigsqcup J} \gamma_k.z_k = \sum_{k\in\{0\}\times I} \gamma_k.z_k + \sum_{k\in\{1\}\times J} \gamma_k.z_k = \sum_{i\in I} \gamma_{(0,i)}.z_{(0,i)} + \sum_{j\in J} \gamma_{(1,j)}.z_{(0,j)} =$$

$$= \sum_{i\in I} \alpha_i.x_i + \sum_{j\in J} \beta_j.y_j = x + y,$$

és természetesen $\sum_{k\in I\bigsqcup J} \gamma_k.z_k \in \mathrm{sp}(H)$.

Legyen $x \in \mathrm{sp}(H)$ és $\alpha \in K$. Megmutatjuk, hogy $\alpha.x \in \mathrm{sp}(H)$. A definíció szerint vehetünk olyan H-ban haladó $(x_i)_{i\in I}$ véges rendszert és olyan $(\alpha_i)_{i\in I} \in K^I$ rendszert, hogy $x = \sum_{i\in I} \alpha_i.x_i$. Ekkor $\alpha.x = \sum_{i\in I}(\alpha\alpha_i).x_i \in \mathrm{sp}(H)$.

Tehát beláttuk, hogy $\mathrm{sp}(H)$ olyan lineáris altere E-nek, amelyre $H \subseteq \mathrm{sp}(H)$. Ha M olyan lineáris altere E-nek, hogy $H \subseteq M$, akkor az előző állítás alapján $\mathrm{sp}(H) \subseteq M$. ■

17.2.5. Definíció. *Ha E vektortér és $H \subseteq E$ tetszőleges halmaz, akkor az előző állításban értelmezett* $\mathrm{sp}(H)$ *halmazt a H* **által generált lineáris altérnek** *nevezzük.*

Egyébként nyilvánvaló, hogy ha E vektortér és $H \subseteq E$, akkor $\mathrm{sp}(H)$ egyenlő az E vektortér H halmazt tartalmazó lineáris altereinek metszetével.

17.2.6. Állítás. *Legyen E vektortér a K test felett és $M \subseteq E$ lineáris altér. Ekkor az*

$$\mathrm{R}_M \ := \ \{ \ (x,y) \in E \times E \mid y - x \in M \ \}$$

halmaz ekvivalencia E felett; az E/R_M faktorhalmazt E/M-fel, és az $E \to E/M$ kanonikus szürjekciót a $\pi_{E/M}$ szimbólummal jelöljük. Ekkor egyértelműen léteznek olyan $+ : (E/M) \times (E/M) \to E/M$ és $. : K \times (E/M) \to E/M$ leképezések, amelyekre az $(E/M, +, .)$ hármas vektortér a K test felett és a $\pi_{E/M} : E \to E/M$ függvény lineáris operátor.

Bizonyítás. (Egzisztencia.) Ha $x \in E$, akkor $x - x = 0 \in M$, ezért $(x,x) \in \mathrm{R}_M$, tehát az R_M reláció reflexív E felett. Ha $(x,y) \in \mathrm{R}_M$, akkor $y - x \in M$, ezért $x - y = -(y-x) \subseteq -M \subseteq M$, így $(y,x) \in \mathrm{R}_M$, tehát az R_M reláció szimmetrikus. Ha $(x,y) \in \mathrm{R}_M$ és $(y,z) \in \mathrm{R}_M$, akkor $y - x \in M$, $z - y \in M$, ezért $z - x = (z-y) + (y-x) \in M + M \subseteq M$, tehát az R_M reláció tranzitív. Ez azt jelenti, hogy R_M ekvivalencia E felett.

Ha $x, x', y, y' \in M$ olyanok, hogy $(x,x') \in \mathrm{R}_M$ és $(y,y') \in \mathrm{R}_M$, akkor $x - x' \in M$ és $y - y' \in M$, következésképpen $(x+y) - (x'+y') = (x-x') + (y-y') \in M + M \subseteq M$, tehát $(x+y, x'+y') \in \mathrm{R}_M$. Ez azt jelenti, hogy az R_M ekvivalenciára és a $+$ műveletre teljesül a (FAC) feltétel, vagyis az E feletti összeadás faktorizálható R_M szerint (11.5.1.). Tehát egyértelműen létezik létezik az E/M faktorhalmaz felett az a $+/\mathrm{R}_M$ művelet, amelyre minden $x, y \in E$ esetén $\pi_{E/M}(x)(+/\mathrm{R}_M)\pi_{E/M}(y) = \pi_{E/M}(x+y)$. A 11.5.3. állítás szerint $+/\mathrm{R}_M$ kommutatív csoportművelet az E/M faktorhalmaz felett. A továbbiakban $+$ jelöli a $+/\mathrm{R}_M$ műveletet is, ami nem okoz félreértést, mert a műveletek operandusainak típusából mindig világos lesz, hogy melyik műveletről van szó.

Legyen $\lambda \in K$. Ha $(x,x') \in \mathrm{R}_M$, azaz $x - x' \in M$, akkor $\lambda.x - \lambda.x' = \lambda.(x - x') \in \lambda.M \subseteq M$, ezért $(\lambda.x, \lambda.x') \in \mathrm{R}_M$. Ebből következik, hogy létezik egyetlen olyan

$$K \times (E/M) \to E/M; \quad (\lambda, \xi) \mapsto \lambda.\xi$$

függvény, amelyre teljesül az, hogy minden $\lambda \in K$ és $x \in E$ esetén $\lambda.\pi_{E/M}(x) = \pi_{E/M}(\lambda.x)$.

Legyenek $\lambda, \sigma \in K$ és $\xi \in E/M$. Ha $x \in E$ olyan, hogy $\xi = \pi_{E/M}(x)$, akkor

$$(\lambda\sigma).\xi = (\lambda\sigma).\pi_{E/M}(x) = \pi_{E/M}((\lambda\sigma).x) = \pi_{E/M}(x)(\lambda.(\sigma.x)) = \lambda.\pi_{E/M}(x)(\sigma.x) = \lambda.(\sigma.\xi),$$

valamint

$$(\lambda + \sigma).\xi = (\lambda + \sigma).\pi_{E/M}(x) = \pi_{E/M}((\lambda + \sigma).x) = \pi_{E/M}(\lambda.x + \sigma.x) =$$
$$= \pi_{E/M)}(\lambda.x) + \pi_{E/M)}(\sigma.x) = \lambda.\pi_{E/M}(x) + \sigma.\pi_{E/M} = \lambda.\xi + \sigma.x,$$

ahol kihasználtuk a $\pi_{E/M} : E \to E/M$ függvény additivitását.

Legyen $\lambda \in K$ és $\xi, \zeta \in E/M$. Ha $x, y \in E$ olyanok, hogy $\xi = \pi_{E/M}(x)$ és $\zeta = \pi_{E/M}(y)$, akkor

$$\lambda.(\xi + \zeta) = \lambda.(\pi_{E/M}(x) + \pi_{E/M}(y)) = \lambda.\left(\pi_{E/M}(x + y)\right) = \pi_{E/M}(\lambda.(x + y)) =$$
$$= \pi_{E/M}(\lambda.x + \lambda.y) = \pi_{E/M}(\lambda.x) + \pi_{E/M}(\lambda.y) = \lambda.\pi_{E/M}(x) + \lambda.\pi_{E/M}(y) = \lambda.\xi + \lambda.\zeta,$$

ahol kétszer kihasználtuk a $\pi_{E/M} : E \to E/M$ függvény additivitását.

Ha $\xi \in E/M$ és $x \in E$ olyan, hogy $\xi = \pi_{E/M}(x)$, akkor

$$1.\xi = 1.\pi_{E/M}(x) = \pi_{E/M}(1.x) = \pi_{E/M}(x) = \xi.$$

Ez azt jelenti, hogy az $(E/M, +, .)$ hármas vektortér a K test felett, és a $\pi_{E/M} : E \to E/M$ leképezés K-lineáris.

(Unicitás.) Tegyük fel, hogy $\tilde{+} : (E/M) \times (E/M) \to E/M$ és $\tilde{.} : K \times (E/M) \to E/M$ olyan függvények, hogy az $(E/M, \tilde{+}, \tilde{.})$ hármas vektortér a K test felett, és a $\pi_{E/M} : E \to E/M$ függvény K-lineáris.

Legyenek $\xi, \zeta \in E/M$. Ha $x, y \in E$ olyanok, hogy $\xi = \pi_{E/M}(x)$ és $\zeta = \pi_{E/M}(y)$, akkor

$$\xi \tilde{+} \zeta = \pi_{E/M}(x) \tilde{+} \pi_{E/M}(y) = \pi_{E/M}(x + y) = \pi_{E/M}(x) + \pi_{E/M}(y) = \xi + \zeta,$$

amiből következik, hogy $\tilde{+} = +$.

Legyen $\lambda \in K$ és $\xi \in E/M$. Ha $x \in E$ olyan, hogy $\xi = \pi_{E/M}(x)$, akkor

$$\lambda \tilde{.} \xi = \lambda \tilde{.} \pi_{E/M}(x) = \pi_{E/M}(\lambda.x) = \lambda.\xi,$$

amiből következik, hogy $\tilde{.} = .$ is teljesül. ■

17.2.7. Definíció. *Ha E vektortér a K test felett és $M \subseteq E$ lineáris altér, akkor az előző állításban értelmezett E/M vektorteret az E vektortér M altér szerinti* **lineáris faktorterének**, *vagy egyszerűen* **faktorterének** *nevezzük, és az $E \to E/M$ kanonikus szürjekciót $\pi_{E/M}$-mel jelöljük.*

17.2.8. Állítás. *Legyenek E és F vektorterek a K test felett, M lineáris altere E-nek és $u : E \to F$ lineáris operátor. A következő állítások ekvivalensek.*

(i) *Létezik egyetlen olyan $v : E/M \to F$ lineáris operátor, hogy $v \circ \pi_{E/M} = u$.*

(ii) *Létezik olyan $v : E/M \to F$ lineáris operátor, hogy $v \circ \pi_{E/M} = u$.*

(iii) *$M \subseteq \mathrm{Ker}(u)$.*

Bizonyítás. (i)⇒(ii) Triviális.

(ii)⇒(iii) Ha $v : E/M \to F$ olyan lineáris operátor, hogy $v \circ \pi_{E/M} = u$, akkor $M = \mathrm{Ker}\left(\pi_{E/M}\right) \subseteq \mathrm{Ker}(u)$.

(iii)⇒(i) Tegyük fel, hogy $M \subseteq \mathrm{Ker}(u)$. Ha $\xi \in E/M$ és $x, x' \in E$ olyan vektorok, hogy $\pi_{E/M}(x) = \xi = \pi_{E/M}(x')$, akkor $x - x' \in \mathrm{Ker}\left(\pi_{E/M}\right) = M \subseteq \mathrm{Ker}(u)$, így $u(x) = u(x')$.

Ezért létezik egyetlen olyan $v : E/M \to F$ függvény, amelyre $v \circ \pi_{E/M} = u$. Ez a v függvény lineáris operátor, mert

– ha $\xi, \xi' \in E/M$ és $x, x' \in E$ olyan vektorok, hogy $\xi = \pi_{E/M}(x)$ és $\xi' = \pi_{E/M}(x')$, akkor $\pi_{E/M}$ és u additivitása, valamint $v \circ \pi_{E/M} = u$ miatt

$$\begin{aligned} v(\xi + \xi') &= v\left(\pi_{E/M}(x) + \pi_{E/M}(x')\right) = v\left(\pi_{E/M}(x + x')\right) = u(x + x') = \\ &= u(x) + u(x') = v\left(\pi_{E/M}(x)\right) + v(\pi_{E/M}(x')) = v(\xi) + v(\xi'), \end{aligned}$$

tehát v additív;

– ha $\xi \in E/M$ és $\lambda \in K$, továbbá $x \in E$ olyan vektor, hogy $\xi = \pi_{E/M}(x)$, akkor a $\pi_{E/M}$ és u operátorok K-homogenitása, valamint $v \circ \pi_{E/M} = u$ miatt

$$v(\lambda.\xi) = v\left(\lambda.\pi_{E/M}(x)\right) = v\left(\pi_{E/M}(\lambda.x)\right) = u(\lambda.x) = \lambda.u(x) = \lambda.v\left(\pi_{E/M}(x)\right) = \lambda.v(\xi),$$

tehát v K-homogén. ■

17.2.9. Következmény. *Ha E és F vektorterek és $u : E \to F$ lineáris operátor, akkor az u függvény által meghatározott E feletti R_u ekvivalencia egyenlő a $\mathrm{Ker}(u)$ altér által meghatározott E feletti ekvivalenciával, és az $\dot{u}$ kanonikus faktorizált lineáris izomorfizmus az $E/\mathrm{Ker}(u)$ lineáris faktortér és $\mathrm{Im}(u) \subseteq F$ lineáris altér között.*

Bizonyítás. A definíció szerint $\mathrm{R}_u = \{(x, y) \in E \times E | u(x) = u(y)\} = \{(x, y) \in E \times E | x - y \in \mathrm{Ker}(u)\}$, ezért az u függvény által meghatározott E feletti R_u ekvivalencia egyenlő a $\mathrm{Ker}(u)$ altér által meghatározott E feletti ekvivalenciával. Az $\dot{u} : E/\mathrm{Ker}(u) \to \mathrm{Im}(u)$ függvény olyan bijekció, amelyre $\dot{u} \circ \pi_{E/\mathrm{Ker}(u)} = u$, ezért az előző állítást alkalmazva az $M := \mathrm{Ker}(u)$ lineáris altérre kapjuk, hogy létezik olyan $v : E/\mathrm{Ker}(u) \to F$ lineáris operátor, amelyre $v \circ \pi_{E/\mathrm{Ker}(u)} = u$, így a $\pi_{E/\mathrm{Ker}(u)} : E \to E/\mathrm{Ker}(u)$ függvény szürjektivitása miatt $\dot{u} = v$. Tehát az $\dot{u} : E/\mathrm{Ker}(u) \to \mathrm{Im}(u)$ kanonikus faktorizált *lineáris* bijekció az $E/\mathrm{Ker}(u)$ lineáris faktortér és $\mathrm{Im}(u) \subseteq F$ lineáris altér között, vagyis lineáris izomorfizmus. ■

17.2.10. Állítás. *Legyen E vektortér a K test felett és $M, N \subseteq E$ lineáris alterek. Ekkor létezik egyetlen olyan $u : (M + N)/M \to N/(M \cap N)$ lineáris operátor, amelyre az alábbi diagram kommutatív:*

$$\begin{tikzcd}
(M+N)/M \arrow[r, "u"] & N/(M \cap N) \\
M+N \arrow[u, "\pi_{(M+N)/M}"] & \\
M \times N \arrow[u, "\mathrm{s}"] \arrow[r, "\mathrm{pr}_N"'] & N \arrow[uu, "\pi_{N/(M\cap N)}"']
\end{tikzcd}$$

ahol $\mathrm{s} : M \times N \to M + N$ *az E vektortér összeadás-függvényének leszűkítése $M \times N$-re és* $\mathrm{pr}_N : M \times N \to N$ *a második projekció. Ez az u leképezés izomorfizmus az $(M + N)/M$ és $N/(M \cap N)$ lineáris faktorterek között.*

Bizonyítás. Az s függvény ráképez $M + N$-re, és a $\pi_{(M+N)/M}$ függvény ráképez az $(M + N)/M$ faktortérre, így a $\pi_{(M+N)/M} \circ \mathrm{s} : M \times N \to (M + N)/M$ leképezés szürjektív, ezért az u függvény egyértelműen van meghatározva azzal a feltétellel, hogy a fenti diagram kommutatív (azaz $u \circ \left(\pi_{(M+N)/M} \circ \mathrm{s}\right) = \pi_{N/(M \cap N)} \circ \mathrm{pr}_N$).

Az u leképezés létezésének bizonyításához legyen $\xi \in (M+N)/M$ rögzítve. Ekkor $\pi_{(M+N)/M}$ szürjektivitása miatt (nem egyértelműen) létezik olyan $(x_M, x_N) \in M+N$ pár, hogy $\pi_{(M+N)/M}(x_M + x_N) = \xi$, tehát $\pi_{(M+N)/M}(x_N) = \xi$, hiszen $x_M \in M = \operatorname{Ker}(\pi_{(M+N)/M})$. Ha $(x'_M, x'_N) \in M+N$ szintén olyan pár, hogy $\pi_{(M+N)/M}(x'_N) = \xi$, akkor $\pi_{(M+N)/M}(x_N - x'_N) = 0$, tehát $x_N - x'_N \in \operatorname{Ker}(\pi_{(M+N)/M}) = M$, ugyanakkor $x_N - x'_N \in N$, tehát $x_N - x'_N \in M \cap N$, ezért $\pi_{N/(M\cap N)}(x_N) = \pi_{N/(M\cap N)}(x'_N)$. Ez azt jelenti, hogy létezik egyetlen olyan $u : (M+N)/M \to N/(M\cap N)$ függvény, amelyre teljesül az, hogy minden $\xi \in (M+N)/M$ és $x_N \in N$ esetén, ha $\pi_{(M+N)/M}(x_N) = \xi$, akkor $u(\xi) = \pi_{N/(M\cap N)}(x_N)$. Erre az u leképezésre a definíció szerint $u \circ (\pi_{(M+N)/M} \circ \mathrm{s}) = \pi_{N/(M\cap N)} \circ \mathrm{pr}_N$ nyilvánvalóan teljesül.

Az u leképezés additív, mert ha $\xi, \xi' \in (M+N)/M$ és $x_N, x'_N \in N$ olyanok, hogy $\pi_{(M+N)/M}(x_N) = \xi$ és $\pi_{(M+N)/M}(x'_N) = \xi'$, akkor $\pi_{(M+N)/M}(x_N)$ additivitása folytán az $x_N + x'_N \in N$ vektorra $\pi_{(M+N)/M}(x_N + x'_N) = \pi_{(M+N)/M}(x_N) + \pi_{(M+N)/M}(x'_N) = \xi + \xi'$, tehát $\pi_{N/(M\cap N)}$ additivitásából következik, hogy $u(\xi + \xi') = \pi_{N/(M\cap N)}(x_N + x'_N) = \pi_{N/(M\cap N)}(x_N) + \pi_{N/(M\cap N)}(x'_N) = u(\xi) + u(\xi')$.

Az u leképezés K-homogén, mert ha $\lambda \in K$, valamint $\xi \in (M+N)/M$ és $x_N \in N$ olyanok, hogy $\pi_{(M+N)/M}(x_N) = \xi$, akkor $\pi_{(M+N)/M}$ K-homogenitása folytán a $\lambda.x_N \in N$ vektorra $\pi_{(M+N)/M}(\lambda.x_N) = \lambda.\pi_{(M+N)/M}(x_N) = \lambda.\xi$, tehát $\pi_{N/(M\cap N)}$ K-homogenitásából következik, hogy $u(\lambda.\xi) = \pi_{(M+N)/M}(\lambda.x_N) = \lambda.\pi_{(M+N)/M}(x_N) = \lambda.u(\xi)$.

Ezzel beláttuk, hogy az $u : (M+N)/M \to N/(M\cap N)$ leképezés lineáris operátor. Az u operátor szürjektív, mert $\eta \in N/(M\cap N)$ esetén $\pi_{N/(M\cap N)}$ szürjektivitása miatt van olyan $x_N \in N$, hogy $\eta = \pi_{N/(M\cap N)}(x_N)$, és ekkor $\xi := \pi_{(M+N)/M}(x_N) \in (M+N)/M$ olyan elem, amelyre a definíció szerint $u(\xi) = \eta$. Továbbá, u injektív is, mert ha $\xi \in (M+N)/M$ olyan, hogy $u(\xi) = 0$, és $x_N \in N$ olyan vektor, hogy $\pi_{(M+N)/M}(x_N) = \xi$, akkor $0 = u(\xi) = \pi_{N/(M\cap N)}(x_N)$, tehát $x_N \in \operatorname{Ker}(\pi_{N/(M\cap N)}) = M \cap N$, vagyis $x_N \in M = \operatorname{Ker}(\pi_{(M+N)/M})$, ezért $\xi = \pi_{(M+N)/M}(x_N) = 0$. Tehát u lineáris bijekció, vagyis izomorfizmus az $(M+N)/M$ és $N/(M\cap N)$ lineáris faktorterek között. ■

17.2.11. Definíció. *Ha E vektortér és $M, N \subseteq E$ lineáris alterek, akkor az $(M+N)/M$ és $N/(M\cap N)$ lineáris faktorterek közötti* **kanonikus izomorfizmusnak** *nevezzük azt az $u : (M+N)/M \to N/(M\cap N)$ lineáris bijekciót, amelyre az előző állításban felírt diagram kommutatív.*

17.3. Vektorterek szorzata és direkt összege

17.3.1. Állítás. *Legyen $(E_i)_{i\in I}$ olyan rendszer, amelynek minden tagja vektortér a K test felett. Legyen $E := \prod_{i\in I} E_i$ és értelmezzük a következő leképezéseket:*

$$E \times E \to E; \quad ((x_i)_{i\in I}, (y_i)_{i\in I}) \mapsto (x_i + y_i)_{i\in I}$$
$$K \times E \to E; \quad (\lambda, (x_i)_{i\in I}) \mapsto (\lambda.x_i)_{i\in I}.$$

Ekkor az E halmaz ezekkel a leképezésekkel ellátva vektortér a K test felett.

Bizonyítás. Az E szorzathalmaz feletti $+$ művelet a komponens-vektorterek feletti összeadás műveletek rendszerének szorzata, ezért kommutatív csoportművelet (**??**), vagyis az E feletti $+$ műveletre (EV$_{\mathrm{I}}$ teljesül. Az (EV$_{\mathrm{II}}$ tulajdonság bizonyításához legyenek $\alpha, \beta \in K$ és $x := (x_i)_{i\in I}$, $y := (y_i)_{i\in I} \in E$. Mivel minden $i \in I$ esetén az E_i

vektortérre (EV$_{\text{II}}$ teljesül, így fennállnak a következő egyenlőségek:

$$\alpha.(\beta.x) = \alpha.((\beta.x_i)_{i\in I}) = (\alpha.(\beta.x_i))_{i\in I} = ((\alpha\cdot\beta).x_i)_{i\in I} = (\alpha\cdot\beta).x;$$
$$(\alpha+\beta).x = ((\alpha+\beta).x_i)_{i\in I} = (\alpha.x_i + \beta.x_i)_{i\in I} = (\alpha.x_i)_{i\in I} + (\beta.x_i)_{i\in I} = \alpha.x + \beta.x;$$
$$\alpha.(x+y)=\alpha.(x_i+y_i)_{i\in I}=(\alpha.(x_i+y_i))_{i\in I}=(\alpha.x_i+\alpha.y_i)_{i\in I}=(\alpha.x_i)_{i\in I}+(\alpha.y_i)_{i\in I}=\alpha.x+\alpha.y;$$
$$1.x = (1.x_i)_{i\in I} = (x_i)_{i\in I} = x,$$

amit bizonyítani kellett. ■

17.3.2. Definíció. *Ha $(E_i)_{i\in I}$ vektorterek rendszere, akkor az előző állításban értelmezett E vektorteret $(E_i)_{i\in I}$ vektortér-rendszer* **lineáris szorzatterének**, *vagy egyszerűen* **szorzatterének** *nevezzük.*

Vegyük észre, hogy ha T halmaz és F vektortér, akkor az $\mathscr{F}(T;F)$ függvénytér *egyenlő* annak az $(F_t)_{t\in T}$ vektortér-rendszernek a lineáris szorzatával, amelyre minden $t\in T$ esetén $F_t := F$.

17.3.3. Állítás. *Ha E és F vektorterek a K test felett, akkor az $u : E \to F$ függvény pontosan akkor lineáris operátor, ha a $\mathrm{gr}(u) := \{(x,u(x))|x\in E\}$ grafikon lineáris altere az $E\times F$ lineáris szorzattérnek.*

Bizonyítás. Tegyük fel, hogy a $\mathrm{gr}(u)\subseteq E\times F$ halmaz lineáris altere az $E\times F$ lineáris szorzattérnek. Ekkor $x,y\in E$ esetén $(x+y,u(x)+u(y)) = (x,u(x))+(y,u(y))\in\mathrm{gr}(u)$, ugyanakkor $(x+y,u(x+y))\in\mathrm{gr}(u)$, ezért $u(x)+u(y)=u(x+y)$, hiszen u függvény. Ez azt jelenti, hogy u additív. Továbbá, ha $x\in E$ és $\lambda\in K$, akkor $(\lambda.x,\lambda.u(x)) = \lambda.(x,u(x))\in\mathrm{gr}(u)$, ugyanakkor $(\lambda.x,u(\lambda.x))\in\mathrm{gr}(u)$, ezért $u(\lambda.x)=\lambda.u(x)$, hiszen u függvény. Ez azt jelenti, hogy u K-homogén. Tehát u lineáris operátor.

Megfordítva, tegyük fel, hogy u lineáris operátor. Ha $(x,y),(x',y')\in\mathrm{gr}(u)$, akkor $y=u(x)$ és $y'=u(x')$, mert $\mathrm{gr}(u)$ definíciója szerint $(x,u(x)),(x',u(x'))\in\mathrm{gr}(u)$ is teljesül és u függvény, ezért u additivitásából következik, hogy $(x,y)+(x',y') = (x,u(x))+(x',u(x')) = (x+x',u(x)+u(x')) = (x+x',u(x+x'))\in\mathrm{gr}(u)$. Ez azt jelenti, hogy $\mathrm{gr}(u)+\mathrm{gr}(u)\subseteq\mathrm{gr}(u)$. Ha $(x,y)\in\mathrm{gr}(u)$ és $\lambda\in K$, akkor $y=u(x)$, mert $\mathrm{gr}(u)$ definíciója szerint $(x,u(x))\in\mathrm{gr}(u)$ is teljesül és u függvény, ezért az u függvény K-homogenitásából következik, hogy $\lambda.(x,y)=(\lambda.x,\lambda.y)=(\lambda.x,\lambda.u(x))=(\lambda.x,u(\lambda.x))\in\mathrm{gr}(u)$. Ez azt jelenti, hogy $K.\mathrm{gr}(u)\subseteq\mathrm{gr}(u)$. Mivel $E\neq\emptyset$, így $\mathrm{gr}(u)\neq\emptyset$, tehát $\mathrm{gr}(u)$ lineáris altere az $E\times F$ lineáris szorzattérnek. ■

17.3.4. Állítás. *Legyen $(E_i)_{i\in I}$ olyan rendszer, amelynek minden tagja vektortér a K test felett. Ekkor a*

$$\bigoplus_{i\in I} E_i := \left\{(x_i)_{i\in I}\in\prod_{i\in I}E_i \;\middle|\; \text{az } \{i\in I|x_i\neq 0\} \text{ halmaz véges}\right\}$$

halmaz lineáris altere az $(E_i)_{i\in I}$ vektortér-rendszer szorzatterének.

Bizonyítás. Ha $\mathbf{0}$ jelöli azt az I-n értelmezett függvényt, amely minden $i\in I$ indexhez az E_i vektortér additív neutrális elemét rendeli, akkor nyilvánvalóan $\mathbf{0}\in\bigoplus_{i\in I}E_i$, tehát $\bigoplus_{i\in I}E_i\neq\emptyset$.

Legyenek $(x_i)_{i\in I}$, $(y_i)_{i\in I}\in\prod_{i\in I}E_i$. Minden $i\in I$ esetén, ha $x_i=0$ és $y_i=0$, akkor

$x_i + y_i = 0$, következésképpen $\{i \in I | x_i + y_i \neq 0\} \subseteq \{i \in I | x_i \neq 0\} \cup \{i \in I | y_i \neq 0\}$, és ha $(x_i)_{i\in I}$, $(y_i)_{i\in I} \in \bigoplus_{i\in I} E_i$, akkor itt a jobb oldalon két véges halmaz uniója áll, ezért $\{i \in I | x_i + y_i \neq 0\}$ véges halmaz, vagyis $(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \in \bigoplus_{i\in I} E_i$. Ez azt jelenti, hogy

$$\left(\bigoplus_{i\in I} E_i\right) + \left(\bigoplus_{i\in I} E_i\right) \subseteq \bigoplus_{i\in I} E_i.$$

Legyenek $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ és $\lambda \in K$. Minden $i \in I$ esetén, ha $x_i = 0$, akkor $\lambda.x_i = 0$, következésképpen $\{i \in I | \lambda.x_i \neq 0\} \subseteq \{i \in I | x_i \neq 0\}$, és ha $(x_i)_{i\in I} \in \bigoplus_{i\in I} E_i$, akkor itt a jobb oldalon véges halmaz áll, vagyis $\lambda.(x_i)_{i\in I} = (\lambda.x_i)_{i\in I} \in \bigoplus_{i\in I} E_i$. Ez azt jelenti, hogy

$$K.\left(\bigoplus_{i\in I} E_i\right) \subseteq \bigoplus_{i\in I} E_i.$$

Tehát $\bigoplus_{i\in I} E_i$ lineáris altere az $(E_i)_{i\in I}$ vektortér-rendszer szorzatterének. ■

17.3.5. Definíció. *Ha $(E_i)_{i\in I}$ vektorterek rendszere, akkor az előző állításban értelmezett $\bigoplus_{i\in I} E_i$ vektorteret az $(E_i)_{i\in I}$ vektortér-rendszer* **külső direkt összegének** *nevezzük.*

Tehát a külső direkt összeg a szorzattér lineáris altere. Ha az $\{i \in I | E_i \neq \{0\}\}$ halmaz véges (például I véges halmaz), akkor az $(E_i)_{i\in I}$ vektortér-rendszer külső direkt összege nyilvánvalóan *egyenlő* az $(E_i)_{i\in I}$ vektortér-rendszer szorzatterével.

17.3.6. Állítás. *Legyenek $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ olyan (egyenlő indexhalmazú) rendszerek, amelyek minden tagja vektortér a K test felett. Legyen $(u_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $u_i : E_i \to F_i$ lineáris operátor. Ekkor a*

$$\mathop{\times}_{i\in I} u_i : \prod_{i\in I} E_i \to \prod_{i\in I} F_i$$

szorzatfüggvény olyan lineáris operátor az $E := \prod_{i\in I} E_i$ és $F := \prod_{i\in I} F_i$ lineáris szorzatterek között, hogy

$$\left(\mathop{\times}_{i\in I} u_i\right)\left\langle \bigoplus_{i\in I} E_i \right\rangle \subseteq \bigoplus_{i\in I} F_i.$$

Bizonyítás. Legyenek $\lambda \in K$ és $x := (x_i)_{i\in I}$, $x' := (x'_i)_{i\in I} \in E$. Ekkor felhasználva azt, hogy minden $i \in I$ esetén $u_i : E_i \to F_i$ additív, kapjuk, hogy

$$\left(\mathop{\times}_{i\in I} u_i\right)(x + x') = \left(\mathop{\times}_{i\in I} u_i\right)((x_i + x'_i)_{i\in I}) = (u_i(x_i + x'_i))_{i\in I} = (u_i(x_i))_{i\in I} + (u_i(x'_i))_{i\in I} =$$

$$= (u_i(x_i) + u_i(x'_i))_{i\in I} = \left(\mathop{\times}_{i\in I} u_i\right)(x) + \left(\mathop{\times}_{i\in I} u_i\right)(x'),$$

tehát a $\mathop{\times}_{i\in I} u_i$ szorzatfüggvény additív, továbbá felhasználva azt, hogy minden $i \in I$ esetén $u_i : E_i \to F_i$ K-homogén, kapjuk, hogy

$$\left(\mathop{\times}_{i\in I} u_i\right)(\lambda.x) = \left(\mathop{\times}_{i\in I} u_i\right)((\lambda.x_i)_{i\in I}) = (u_i(\lambda.x_i))_{i\in I} =$$

$$= (\lambda.u_i(x_i))_{i\in I} = \lambda.(u_i(x_i))_{i\in I} = \lambda.\Big(\bigtimes_{i\in I} u_i\Big)(x),$$

tehát a $\bigtimes_{i\in I} u_i$ szorzatfüggvény K-homogén.

Ha $x := (x_i)_{i\in I} \in \bigoplus_{i\in I} E_i$, akkor $\{i \in I | x_i \neq \mathbf{0}_i\}$ véges halmaz (ahol minden $I \ni i$-re $\mathbf{0}_i$ az additív neutrális elem E_i-ben), ugyanakkor $\{i \in I | u_i(x_i) \neq \mathbf{0}'_i\} \subseteq \{i \in I | x_i \neq \mathbf{0}_i\}$ (ahol minden $I \ni i$-re $\mathbf{0}'_i$ az additív neutrális elem F_i-ben), hiszen minden $i \in I$ indexre $u_i(\mathbf{0}_i) = \mathbf{0}'_i$, ezért $\{i \in I | u_i(x_i) \neq \mathbf{0}'_i\}$ is véges halmaz, vagyis $\Big(\bigtimes_{i\in I} u_i\Big)(x) \in \bigoplus_{i\in I} F_i$. ■

17.3.7. Definíció. *Legyenek $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ (egyenlő indexhalmazú) vektortér-rendszerek, és $(u_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $u_i : E_i \to F_i$ lineáris operátor. Ekkor a*

$$\bigoplus_{i\in I} u_i : \bigoplus_{i\in I} E_i \to \bigoplus_{i\in I} F_i; \quad (x_i)_{i\in I} \mapsto (u_i(x_i))_{i\in I}$$

lineáris operátort az $(u_i)_{i\in I}$ **operátor-rendszer direkt összegének** *nevezzük.*

17.4. Algebrai komplementerek

17.4.1. Definíció. *Ha E vektortér, akkor az $M \subseteq E$ lineáris altér* **algebrai komplementerének** *nevezünk minden olyan $N \subseteq E$ lineáris alteret, amelyre $M + N = E$ és $M \cap N = \{\mathbf{0}\}$.*

Az "algebrai komplementer" kifejezés helyett röviden a "komplementer" szót is használjuk mindaddig, amíg nem vezetünk be másfajta komplementer-fogalmat.

Ha E vektortér és $M, N \subseteq E$ lineáris alterek, akkor az "N komplementere M-nek" és az "M komplementere N-nek" kijelentések ekvivalensek, mert $M \cap N = N \cap M$ és a $+$ művelet kommutativitása miatt $M + N = N + M$.

Nyilvánvaló, hogy ha E vektortér és $M, N \subseteq E$ lineáris alterek, akkor a

$$\pi_{E/M}|_N : N \to E/M$$

leképezés lineáris operátor az N lineáris altér és az E/M lineáris faktortér között, valamint az

$$M \times N \to E; \quad (x, y) \mapsto x + y$$

leképezés lineáris operátor az $M \times N$ lineáris szorzattér és E között. A következő állítás szerint ezeknek a lineáris operátoroknak a tulajdonságaival kifejezhető az, hogy két altér egymás komplementere.

17.4.2. Állítás. *Legyen E vektortér, és legyenek $M, N \subseteq E$ lineáris alterek. A következő állítások ekvivalensek.*

(i) *N komplementere M-nek.*

(ii) *A $\pi_{E/M}|_N : N \to E/M$ leképezés bijekció.*

(iii) *Az $M \times N \to E$; $(x, y) \mapsto x + y$ leképezés bijekció.*

Bizonyítás. (i)⇒(ii) Tegyük fel, hogy N komplementere M-nek. Ha $x \in N$ olyan, hogy $\left(\pi_{E/M}|_N\right)(x) = \mathbf{0}$, akkor $x \in M$, ezért $M \cap N = \{\mathbf{0}\}$ miatt $x = \mathbf{0}$. Ez azt jelenti, hogy a $\pi_{E/M}|_N$ lineáris operátor injektív. Ha $z \in E/M$, akkor $\pi_{E/M}$ szürjektivitása miatt van olyan $x \in E$, hogy $z = \pi_{E/M}(x)$, tehát $E = M + N$ következtében léteznek olyan

$x_M \in M$ és $x_N \in N$, hogy $x = x_M + x_N$, így $z = \pi_{E/M}(x) = \pi_{E/M}(x_M) + \pi_{E/M}(x_N) = \pi_{E/M}(x_N) = \left(\pi_{E/M}|_N\right)(x_N)$. Ez azt jelenti, hogy a $\pi_{E/M}|_N$ leképezés szürjektív.

(ii)⇒(iii) Tegyük fel, hogy a $\pi_{E/M}|_N : N \to E/M$ leképezés bijekció. Ha $(x,y) \in M \times N$ olyan, hogy $x + y = \mathbf{0}$, akkor $\mathbf{0} = \pi_{E/M}(x+y) = \pi_{E/M}(y) = \left(\pi_{E/M}|_N\right)(y)$, tehát $\pi_{E/M}|_N$ injektivitása miatt $y = \mathbf{0}$, és így $x = -y = \mathbf{0}$, vagyis $(x,y) = (\mathbf{0},\mathbf{0})$. Ez azt jelenti, hogy az $M \times N \to E$; $(x,y) \mapsto x + y$ lineáris operátor injektív. Ha $z \in E$, akkor $\pi_{E/M}(z) \in E/M$, ezért a $\pi_{E/M}|_N : N \to E/M$ leképezés szürjektivitása miatt létezik olyan $y \in N$, hogy $\pi_{E/M}(y) = \left(\pi_{E/M}|_N\right)(y) = \pi_{E/M}(z)$, tehát $z - y \in M$, így $z = (z-y) + y \in M + N$. Ez azt jelenti, hogy az $M \times N \to E$; $(x,y) \mapsto x+y$ leképezés szürjektív.

(iii)⇒(i) Tegyük fel, hogy az $s : M \times N \to E$; $(x,y) \mapsto x + y$ leképezés bijekció. Ha $x \in M \cap N$, akkor $s(x,\mathbf{0}) = x = s(\mathbf{0},x)$, így az s leképezés injektivitásából következik, hogy $(x,\mathbf{0}) = (\mathbf{0},x)$, tehát $x = \mathbf{0}$. Ez azt jelenti, hogy $M \cap N = \{\mathbf{0}\}$. Másfelől nyilvánvaló, hogy $\mathrm{Im}(s) = M + N$, ezért az s leképezés szürjektivitása miatt $M + N = E$. ■

17.4.3. Következmény. *Legyen E vektortér és $M \subseteq E$ lineáris altér. Ha N és N' olyan lineáris alterek E-ben, amelyek M-nek komplementerei, akkor az N és N' vektorterek lineárisan izomorfak egymással.*

Bizonyítás. Az előző állítás szerint $\pi_{E/M}|_N : N \to E/M$ és $\pi_{E/M}|_{N'} : N' \to E/M$ lineáris izomorfizmusok, ezért $\left(\pi_{E/M}|_{N'}\right)^{-1} \circ \left(\pi_{E/M}|_N\right) : N \to N'$ lineáris izomorfizmus. ■

17.4.4. Állítás. *Ha E vektortér a K test felett és $M \subseteq E$ lineáris altér, akkor létezik M-nek komplementere.*

Bizonyítás. Jelölje $\mathfrak{S}_M$ azon $N \subseteq E$ lineáris alterek halmazát, amelyekre $M \cap N = \{0\}$. Az $\mathfrak{S}_M$ halmaz felett a tartalmazás-reláció *induktív* rendezés, hiszen ha $(N_i)_{i\in I}$ olyan nem üres rendszer $\mathfrak{S}_M$-ben, amelyre minden $I \ni i,j$-re $N_i \subseteq N_j$ vagy $N_j \subseteq N_i$, akkor $N := \bigcup_{i\in I} N_i \in \mathfrak{S}_M$ és minden $I \ni i$-re $N_i \subseteq N$. Ezért a Zorn-lemma alapján vehetünk olyan $N \in \mathfrak{S}_M$ elemet, amely tartalmazás tekintetében maximális. Ekkor $M \cap N = \{0\}$ és állítjuk, hogy $M + N = E$, vagyis N komplementere M-nek. Valóban, ha létezik $x \in E \setminus (M + N)$, akkor $y \in M \cap (N + K.x)$ esetén van olyan $z \in N$ és $\lambda \in K$, hogy $y = z + \lambda.x$. Ekkor $\lambda.x = y - z \in M + N$, ezért $x \notin M + N$ alapján $\lambda = 0$, így $y - z = 0$, vagyis $y = z \in M \cap N$, azaz $y = 0$. Ez azt jelenti, hogy $N + K.x \in \mathfrak{S}_M$, ugyanakkor $N + K.x$ tartalmazza N-t és nem egyenlő N-nel, mert $x \notin N$. Ez viszont ellentmond N maximalitásának. ■

17.4.5. Következmény. *Ha E vektortér, $M \subseteq E$ lineáris altér, és $L \subseteq E$ olyan lineáris altér, amelyre $M \cap L = \{\mathbf{0}\}$, akkor létezik M-nek olyan N komplementere E-ben, amelyre $L \subseteq N$.*

Bizonyítás. A 17.4.4. állítás szerint az $M + L \subseteq E$ lineáris altérnek létezik komplementere E-ben: legyen V ilyen lineáris altér. Ekkor $N := L + V$ olyan lineáris altere E-nek, amelyre $M + N = M + (L + V) = (M + L) + V = E$. Tegyük fel, hogy $x \in M \cap N$. Ekkor léteznek olyan $x_L \in L$ és $x_V \in V$ vektorok, amelyekre $x = x_L + x_V$. Világos, hogy ekkor $x_V \in V$ és $x_V = x - x_L \in M - L \subseteq M + L$, tehát $x_V \in (M + L) \cap V$. Mivel V komplementere $M + L$-nek, így $(M + L) \cap V = \{\mathbf{0}\}$, következésképpen $x_V = \mathbf{0}$. Ezért $x = x_L \in M \cap L = \{\mathbf{0}\}$, tehát $x = \mathbf{0}$. Ez azt jelenti, hogy $M \cap N = \{\mathbf{0}\}$, vagyis N komplementere M-nek E-ben, ugyanakkor $L \subseteq N$ is teljesül. ■

17.4.6. Állítás. *Legyenek E és F vektorterek, továbbá $u : E \to F$ lineáris szürjekció.*

a) *Ha az $N \subseteq E$ lineáris altér algebrai komplementere* $\mathrm{Ker}(u)$*-nak, akkor az $u|_N : N \to F$ lineáris operátor bijekció, és az $(u|_N)^{-1} : F \to E$ leképezés u-nak olyan lineáris jobbinverze, amelyre* $\mathrm{Im}\,((u|_N)^{-1}) = N$.

b) *Ha $\mathfrak{N}$ jelöli a* $\mathrm{Ker}(u)$ *altér E-beli algebrai komplementereinek halmazát, és $\mathscr{J}$ jelöli az u leképezés lineáris jobbinverzeinek halmazát, akkor az $\mathfrak{N} \to \mathscr{J}$; $N \mapsto (u|_N)^{-1}$ leképezés bijekció.*

Bizonyítás. a) A 17.4.4. állítás szerint vehetünk olyan $N \subseteq E$ lineáris alteret, amely komplementere $\mathrm{Ker}(u)$-nak. Ekkor az $u|_N : N \to F$ lineáris operátor bijekció. Valóban, ha $x \in \mathrm{Ker}(u|_N)$, akkor $x \in N \cap \mathrm{Ker}(u) = \{\mathbf{0}\}$, tehát $x = 0$, így $u|_N$ injekció. Ha $y \in F$, akkor u szürjektivitása miatt van olyan $x \in E$, hogy $u(x) = y$, és ekkor $N + \mathrm{Ker}(u) = E$ miatt léteznek olyan $x_N \in N$ és $x' \in \mathrm{Ker}(u)$ vektorok, amelyekre $x = x_N + x'$, tehát $(u|_N)(x_N) = u(x_N) = u(x) = y$, így $u|_N$ ráképez F-re. Tehát az $(u|_N)^{-1} : F \to E$ lineáris operátor injekció, és világos, hogy $u \circ (u|_N)^{-1} = \mathrm{id}_F$, vagyis $(u|_N)^{-1}$ lineáris jobbinverze u-nak, és triviális, hogy $\mathrm{Im}\,((u|_N)^{-1}) = N$.

b) Ha N és N' algebrai komplementerei $\mathrm{Ker}(u)$-nak, akkor $(u|_N)^{-1} = (u|_{N'})^{-1}$ esetén $N = \mathrm{Im}\,((u|_N)^{-1}) = \mathrm{Im}\,((u|_{N'})^{-1}) = N'$, tehát az $\mathfrak{N} \to \mathscr{J}$; $N \mapsto (u|_N)^{-1}$ leképezés injekció. E leképezés szürjektivitásának bizonyításához legyen $v \in \mathscr{J}$, vagyis $v : F \to E$ lineáris jobbinverze u-nak.

Ekkor $\mathrm{Im}(v)$ algebrai komplementere $\mathrm{Ker}(u)$-nak. Valóban, ha $x \in \mathrm{Im}(v) \cap \mathrm{Ker}(u)$, akkor van olyan $y \in F$, hogy $x = v(y)$, ezért $0 = u(x) = u(v(y)) = y$, tehát $\mathrm{Im}(v) \cap \mathrm{Ker}(u) = \{0\}$. Továbbá, minden $x \in E$ esetén $x = v(u(x)) + (x - v(u(x)))$, és $v(u(x)) \in \mathrm{Im}(v)$, valamint $u(x - v(u(x))) = u(x) + u(v(u(x))) = 0$, vagyis $x - v(u(x)) \in \mathrm{Ker}(u)$, tehát $E = \mathrm{Im}(v) + \mathrm{Ker}(u)$.

Tehát $N := \mathrm{Im}(v) \in \mathfrak{N}$. Állítjuk, hogy $v = (u|_N)^{-1}$. Valóban, $u \circ v = \mathrm{id}_F$ miatt $(u|_N) \circ v = \mathrm{id}_F$, amiből következik, hogy $v = (u|_N)^{-1} \circ ((u|_N) \circ v) = (u|_N)^{-1} \circ \mathrm{id}_F = (u|_N)^{-1}$. Ez azt jelenti, hogy a $\mathfrak{N} \to \mathscr{J}$; $N \mapsto (u|_N)^{-1}$ leképezés szürjekció. ■

17.4.7. Következmény. *Vektorterek között ható lineáris szürjekciónak létezik lineáris jobbinverze.*

Bizonyítás. Az előző állítás és 17.4.4. közvetlen következménye. ■

Könnyen belátható, hogy a 17.4.4. és 17.4.7. állítások *ekvivalensek*, mert ha E vektortér és $M \subseteq E$ lineáris altér, akkor a $\pi_{E/M} : E \to E/M$ lineáris szürjekció bármely $v : E/M \to E$ lineáris jobbinverzére teljesül az, hogy $\mathrm{Im}(v)$ az M altér komplementere.

17.5. Bázisok és dimenzió

17.5.1. Definíció. *Legyen E vektortér a K test felett.* **Lineáris függetlennek** *nevezünk E-ben minden olyan $L \subseteq E$ halmazt, amelyre teljesül a következő állítás.*

– *Minden $X \subseteq L$ véges halmazra, és minden $\lambda : X \to K$ függvényre, ha $\sum_{x \in X} \lambda(x).x = 0$, akkor minden $x \in X$ esetén $\lambda(x) = 0$.*

Egy E-ben haladó $(e_i)_{i \in I}$ rendszert **lineárisan függetlennek** *nevezzük E-ben, ha injektív és az $\{e_i | i \in I\}$ halmaz lineárisan független E-ben.*

Nyilvánvaló, hogy lineárisan független halmaznak nem lehet eleme a vektortér additív neutrális eleme.

A definíció alapján világos, hogy E vektortér a K test felett, akkor az E-ben haladó $(e_i)_{i\in I}$ rendszer pontosan akkor lineárisan független, ha minden $(\lambda_i)_{i\in I} \in K^{(I)}$ rendszerre: a $\sum_{i\in I} \lambda_i.e_i = 0$ egyenlőségből következik, hogy minden $i \in I$ indexre $\lambda_i = 0$.

17.5.2. Definíció. *Legyen E vektortér a K test felett.* **Generátorhalmaznak** *nevezünk E-ben minden olyan $G \subseteq E$ halmazt, amelyre teljesül a következő állítás.*

– *Minden $e \in E$ elemhez van olyan $X \subseteq G$ véges halmaz, és van olyan $\lambda : X \to K$ függvény, hogy $e = \sum_{x\in X} \lambda(x).x$.*

Egy E-ben haladó $(e_i)_{i\in I}$ rendszert **generátorrendszernek** *nevezünk, ha az $\{e_i|i \in I\}$ halmaz generátorhalmaz E-ben.*

A definíció alapján világos, hogy E vektortér a K test felett, akkor az E-ben haladó $(e_i)_{i\in I}$ rendszer pontosan akkor generátorrendszer, ha minden $e \in E$ esetén van olyan $(\lambda_i)_{i\in I} \in K^{(I)}$, hogy $e = \sum_{i\in I} \lambda_i.e_i$.

17.5.3. Definíció. *Legyen E vektortér.* **Bázishalmaznak** *nevezünk E-ben minden olyan részhalmazt, amely lineárisan független generátorhalmaz. Egy E-ben haladó $(e_i)_{i\in I}$ rendszert* **bázisnak** *nevezünk, ha $\{e_i|i \in I\}$ bázishalmaz E-ben. Azt mondjuk, hogy az E vektortér* **véges dimenziós**, *ha létezik E-ben véges bázishalmaz.*

A 17.2.4. állítás alapján világos, hogy ha E vektortér, akkor a $G \subseteq E$ halmaz pontosan akkor generátorhalmaz E-ben, ha $\mathrm{sp}(G) = E$.

A definíciók alapján nyilvánvaló, hogy vektortér lineárisan független részhalmazának minden részhalmaza lineárisan független, és minden olyan részhalmaza generátorhalmaz, amely tartalmaz generátorhalmazt.

Példa. Legyen T halmaz, K test, és tekintsük a $K^{(T)}$ vektorteret. Minden $t \in T$ esetén legyen $\mathbf{e}_t \in K^{(T)}$ az a függvény, amelyre minden $t' \in T$ esetén

$$\mathbf{e}_t(t') := \begin{cases} 1 & \text{, ha } t' = t, \\ 0 & \text{, ha } t' \neq t. \end{cases}$$

Ekkor $(\mathbf{e}_t)_{t\in T}$ bázisrendszer a $K^{(T)}$ vektortérben. Valóban, ha $I \subseteq T$ véges halmaz, valamint $\lambda : I \to K$ olyan függvény, hogy $\mathbf{0} = \sum_{i\in I} \lambda(i).\mathbf{e}_i$, akkor minden $i \in I$ esetén $0 = \mathbf{0}(i) = \lambda(i)$, tehát az $(\mathbf{e}_t)_{t\in T}$ rendszer lineárisan független. Továbbá, ha $x \in K^{(T)}$, akkor világos, hogy $x = \sum_{t\in[x\neq 0]} x(t).\mathbf{e}_t$, ezért $(\mathbf{e}_t)_{t\in T}$ generátorrendszer is $K^{(T)}$-ben.

17.5.4. Állítás. *Legyenek E, F vektorterek a K test felett, és $u : E \to F$ lineáris operátor.*

a) *Ha $L \subseteq E$ lineárisan független halmaz és u injektív, akkor $u\langle L\rangle \subseteq F$ lineárisan független halmaz.*

b) *Ha $G \subseteq E$ generátorhalmaz és u szürjektív, akkor $u\langle G\rangle \subseteq F$ generátorhalmaz.*

c) *Ha $B \subseteq E$ bázishalmaz és u bijektív, akkor $u\langle B\rangle \subseteq F$ bázishalmaz.*

Bizonyítás. A c) állítás nyilvánvalóan következik az a) és b) állításokból, valamint a definíciókból.

a) Legyen $L \subseteq E$ lineárisan független halmaz és $u : E \to F$ injektív lineáris operátor. Legyen $Y \subseteq u\langle L\rangle$ véges halmaz és $\lambda : Y \to K$ olyan függvény, hogy $\sum_{y\in Y} \lambda(y).y = \mathbf{0}$.

Az u függvény injektivitásából következik, hogy $X := \overset{-1}{u}\langle Y\rangle \subseteq L$ olyan véges halmaz, hogy $u|_X : X \to Y$ bijekció, ezért az F-beli összeadás általános kommutativitása (8.6.1.), valamint u linearitása miatt

$$\mathbf{0} = \sum_{y\in Y} \lambda(y).y = \sum_{x\in X} \lambda(u(x)).u(x) = u\left(\sum_{x\in X} \lambda(u(x)).x\right),$$

amiből ismét u injektivitását alkalmazva kapjuk, hogy $\sum_{x\in X} \lambda(u(x)).x = \mathbf{0}$. Az L halmaz lineárisan független E-ben, $X \subseteq L$ véges halmaz, és $\lambda \circ u : X \to K$ függvény, ezért a $\sum_{x\in X} (\lambda \circ u)(x).x = \mathbf{0}$ egyenlőségből következik, hogy minden $x \in X$ esetén $(\lambda \circ u)(x) = 0$. Mivel $Y = u\langle X\rangle$, így minden $y \in Y$ esetén $\lambda(y) = 0$, tehát $u\langle L\rangle \subseteq F$ lineárisan független halmaz.

b) Legyen $G \subseteq E$ generátorhalmaz és $u : E \to F$ szürjektív lineáris operátor. Rögzítsünk egy $y_0 \in F$ elemet, és u szürjektivitását alkalmazva válasszunk olyan $x_0 \in E$ vektort, amelyre $u(x_0) = y_0$. A G halmaz generátorhalmaz E-ben, így létezik olyan $X \subseteq G$ véges halmaz és olyan $\lambda : X \to K$ függvény, hogy $x_0 = \sum_{x\in X} \lambda(x).x$. Ekkor u linearitása miatt

$$y_0 = u(x_0) = u\left(\sum_{x\in X} \lambda(x).x\right) = \sum_{x\in X} \lambda(x).u(x).$$

Legyen $Y := u\langle X\rangle$, amely véges részhalmaza $u\langle G\rangle$-nek. Könnyen ellenőrizhető, hogy az $\left(\overset{-1}{u}\langle\{y\}\rangle \cap X\right)_{y\in Y}$ halmazrendszer partíciója X-nek, így az F-beli összeadás általános asszociativitását (8.7.1.) alkalmazva kapjuk, hogy

$$\sum_{x\in X} \lambda(x).u(x) = \sum_{y\in Y}\left(\sum_{x\in \overset{-1}{u}\langle\{y\}\rangle\cap X} \lambda(x).u(x)\right) = \sum_{y\in Y}\left(\sum_{x\in \overset{-1}{u}\langle\{y\}\rangle\cap X} \lambda(x)\right).y.$$

Ez azt jelenti, hogy $Y \subseteq u\langle G\rangle$ véges halmaz és a

$$\lambda' : Y \to K; \quad y \mapsto \sum_{x\in \overset{-1}{u}\langle\{y\}\rangle\cap X} \lambda(x)$$

függvényre $y_0 = \sum_{y\in Y} \lambda'(y).y$ teljesül, tehát $u\langle G\rangle$ generátorhalmaz F-ben. ■

Az alkalmazások szempontjából érdemes megfogalmazni az előző állítást vektorhalmazok helyett vektorrendszerekre.

17.5.5. Következmény. *Legyenek E, F vektorterek a K test felett, és $u : E \to F$ lineáris operátor.*

a) *Ha* $(e_i)_{i\in I}$ *lineárisan független rendszer* E*-ben és* u *injektív, akkor* $(u(e_i))_{i\in I}$ *lineárisan független rendszer* F*-ben.*

b) *Ha* $(e_i)_{i\in I}$ *generátorrendszer* E*-ben és* u *szürjektív, akkor* $(u(e_i))_{i\in I}$ *generátorrendszer* F*-ben.*

c) *Ha* $(e_i)_{i\in I}$ *bázis* E*-ben és* u *bijektív, akkor* $(u(e_i))_{i\in I}$ *bázis* F*-ben.*

Bizonyítás. Mindhárom esetben áttérünk az $(e_i)_{i\in I}$ rendszerről az $\{e_i | i \in I\} \subseteq E$ halmazra, és erre a vektorhalmazra alkalmazzuk a 17.5.4. állítást. ■

17.5.6. Lemma. *Legyen* E *vektortér a* K *test felett és* $(L_i)_{i\in I}$ *az* E *vektortér lineárisan független részhalmazainak olyan rendszere, hogy minden* $i, j \in I$ *esetén* $L_i \subseteq L_j$ *vagy* $L_j \subseteq L_i$*. Ekkor az* $\bigcup_{i\in I} L_i$ *halmaz lineárisan független* E*-ben.*

Bizonyítás. Legyen $X \subseteq \bigcup_{i\in I} L_i$ véges halmaz és $\lambda : X \to K$ olyan függvény, amelyre $\sum_{x\in X} \lambda(x).x = \mathbf{0}$. Azt kell igazolni, hogy minden $x \in X$ esetén $\lambda(x) = 0$. Természetesen feltehetjük, hogy $X \neq \emptyset$, különben minden $x \in X$ esetén $\lambda(x) = 0$ triviálisan igaz.

A 8.1.20. b) állítás szerint az $X \subseteq \bigcup_{i\in I} L_i$ nem üres véges halmazhoz vehetünk olyan $i \in I$ indexet, hogy $X \subseteq L_i$. Az L_i halmaz lineárisan független E-ben, ezért minden $x \in X$ esetén $\lambda(x) = 0$. ■

17.5.7. Lemma. *Legyen* E *vektortér a* K *test felett,* $L \subseteq E$ *lineárisan független halmaz, és* $y \in E \setminus L$*. Az* $L \cup \{y\}$ *halmaz pontosan akkor lineárisan független, ha* $y \notin \mathrm{sp}(L)$*.*

Bizonyítás. (I) Tegyük fel, hogy $y \notin \mathrm{sp}(L)$, és legyen $X \subseteq L \cup \{y\}$ olyan véges halmaz és $\lambda : X \to K$ olyan függvény, hogy $\sum_{x\in X} \lambda(x).x = \mathbf{0}$. Megmutatjuk, hogy minden $x \in X$ esetén $\lambda(x) = 0$, tehát $L \cup \{y\}$ lineárisan független halmaz.

Ha $y \notin X$, akkor $X \subseteq L$, így L lineáris függetlensége miatt minden $x \in X$ esetén $\lambda(x) = 0$. Tegyük fel, hogy $y \in X$. Ha $X \setminus \{y\} = \emptyset$, vagyis $X = \{y\}$, akkor 8.5.4. a) alapján $\mathbf{0} = \sum_{x\in X} \lambda(x).x = \lambda(y).y$, következésképpen $\lambda(y) = 0$, mert $y \neq \mathbf{0}$, hiszen $y \notin \mathrm{sp}(L)$ és $\mathbf{0} \in \mathrm{sp}(L)$. Tegyük fel, hogy $X \setminus \{y\} \neq \emptyset$. Ekkor 8.5.4. b) alapján

$$\mathbf{0} = \sum_{x\in X} \lambda(x).x = \lambda(y).y + \sum_{x\in X\setminus\{y\}} \lambda(x).x.$$

Ebből, és az $X \setminus \{y\} \subseteq L$ összefüggésből következik, hogy $\lambda(y) \neq 0$ esetén

$$y = \sum_{x\in X\setminus\{y\}} \left(\frac{-\lambda(x)}{\lambda(y)}\right).x \in \mathrm{sp}(L)$$

teljesülne, holott $y \notin \mathrm{sp}(L)$. Ezért $\lambda(y) = 0$, következésképpen $\mathbf{0} = \sum_{x\in X\setminus\{y\}} \lambda(x).x$, így L lineáris függetlensége és $X \setminus \{y\} \subseteq L$ miatt minden $x \in X \setminus \{y\}$ vektorra $\lambda(x) = 0$. Ez azt jelenti, hogy minden $x \in X$ esetén $\lambda(x) = 0$, tehát az $L \cup \{y\}$ halmaz lineárisan független.

(II) Tegyük fel, hogy $y \in \mathrm{sp}(L)$. Megmutatjuk, hogy $L \cup \{y\}$ nem lineárisan független halmaz. Valóban, van olyan $X \subseteq L$ véges halmaz és olyan $\lambda : X \to K$ függvény, hogy $y = \sum_{x \in X} \lambda(x).x$. Ekkor $y \notin L$ és $X \subseteq L$ miatt $y \notin X$, és a

$$\lambda' : X \cup \{y\} \to K; \qquad x \mapsto \begin{cases} \lambda(x) & \text{, ha } x \in X, \\ -1 & \text{, ha } x = y \end{cases}$$

függvényre 8.5.4. b) alapján teljesül az, hogy

$$\mathbf{0} = (-1).y + \sum_{x \in X} \lambda(x).x = \sum_{x \in X \cup \{y\}} \lambda'(x).x,$$

ezért az $L \cup \{y\}$ halmaz nem lineárisan független. ■

17.5.8. Tétel. *Legyen E vektortér. Minden $L \subseteq E$ lineárisan független halmazhoz, és minden $G \subseteq E$ generátorhalmazhoz, $L \subseteq G$ esetén létezik olyan $B \subseteq E$ bázishalmaz E-ben, amelyre $L \subseteq B \subseteq G$ teljesül. Létezik E-ben bázishalmaz.*

Bizonyítás. Legyen $\mathfrak{S}$ az L halmazt tartalmazó és G által tartalmazott E-beli lineárisan független halmazok halmaza, és $\leq$ a tartalmazás-reláció az $\mathfrak{S}$ halmaz felett. Ekkor $L \in \mathfrak{S}$, tehát $\mathfrak{S} \neq \emptyset$, és a 17.5.6. lemma szerint $(\mathfrak{S}, \leq)$ *induktívan* rendezett halmaz, ezért a Kuratowski–Zorn-lemma alapján létezik $\mathfrak{S}$-nek maximális eleme a $\leq$ rendezés szerint: legyen $B \in \mathfrak{S}$ ilyen elem.

Megmutatjuk, hogy B generátorhalmaz E-ben. Indirekt, tegyük fel, hogy $E \setminus \mathrm{sp}(B) \neq \emptyset$, és vegyünk egy $y \in E \setminus \mathrm{sp}(B)$ vektort. A G halmaz generátorhalmaz, így létezik olyan $X \subseteq G$ véges halmaz és olyan $\lambda : X \to K$ függvény, hogy $y = \sum_{x \in X} \lambda(x).x$. Ha $X \subseteq \mathrm{sp}(B)$ teljesülne, akkor 17.2.4. alapján $y \in \mathrm{sp}(B)$ is igaz volna, holott $y \notin \mathrm{sp}(B)$. Ezért van olyan $x \in X$, hogy $x \notin \mathrm{sp}(B)$, így $x \notin B$ még inkább teljesül. A B halmaz lineáris függetlensége, $x \notin B$, és 17.5.7. alapján ekkor $B \cup \{x\}$ lineárisan független halmaz, és $L \subseteq B \subseteq B \cup \{x\} \subseteq G$, tehát $B \cup \{x\} \in \mathfrak{S}$, ugyanakkor $B \cup \{x\}$ valódi részként tartalmazza B-t, ami ellentmond B maximalitásának a $\leq$ rendezés szerint.

Ezzel igazoltuk, hogy B olyan bázishalmaz E-ben, amelyre $L \subseteq B \subseteq G$.

Az $L := \emptyset$ és $G := E$ választással azonnal kapjuk, hogy létezik E-ben bázishalmaz. ■

Az előző tétel fontos következménye az, hogy vektortérben minden lineárisan független halmaz kiegészíthető egy előre adott generátorhalmaz elemeivel bázishalmazzá. Pontosabban a következő állításról van szó.

17.5.9. Következmény. *Legyen E vektortér. Minden $L \subseteq E$ lineárisan független halmazhoz, és minden $G \subseteq E$ generátorhalmazhoz létezik olyan $L' \subseteq G$ halmaz, hogy $L \cap L' = \emptyset$ és $L \cup L'$ bázishalmaz E-ben.*

Bizonyítás. Az $L \cup G$ halmaz olyan generátorhalmaz E-ben, amely tartalmazza az L lineárisan független halmazt, tehát az előző tétel alapján van olyan B bázishalmaz E-ben, hogy $L \subseteq B \subseteq L \cup G$. Ekkor az $L' := B \setminus L$ halmaz nyilvánvalóan olyan, amelynek a létezését állítottuk. ■

17.5.10. Lemma. *Ha E vektortér és $B \subseteq E$ véges bázishalmaz E-ben, akkor minden $B' \subseteq E$ bázishalmaz véges és* $\mathrm{Card}(B') \leq \mathrm{Card}(B)$.

Bizonyítás. (I) Jelölje $\mathfrak{A}(n)$ a következő kijelentést:

"Minden E vektortérre, és minden $B \subseteq E$ bázishalmazra, ha a B halmaz kisebb-egyenlő számosságú n-nél, akkor minden $B' \subseteq E$ bázishalmaz kisebb-egyenlő számosságú n-nél."

Teljes indukcióval bebizonyítjuk, hogy $(\forall n)((n \in \mathbb{N}) \Rightarrow \mathfrak{A}(n))$ tétel.

Ha E vektortér és $B \subseteq E$ olyan bázishalmaz, amely kisebb-egyenlő számosságú 0-nál, akkor $B = \emptyset$, ezért $E = \mathrm{sp}(B) = \{\mathbf{0}\}$, így minden $B' \subseteq E$ bázishalmazra $B' = \emptyset$, mert B' lineárisan független halmaz, tehát $\mathbf{0} \notin B'$. Ez azt jelenti, hogy $\mathfrak{A}(0)$ igaz.

Legyen $n \in \mathbb{N}$ olyan szám, amelyre $\mathfrak{A}(n)$ teljesül, és rögzítsünk egy E vektorteret, egy olyan $B \subseteq E$ véges bázishalmazt, amely kisebb-egyenlő számosságú $n+1$-nél, és egy $B' \subseteq E$ bázishalmazt. Azt kell igazolni, hogy B' kisebb-egyenlő számosságú az $n+1$ számnál.

Ha $B' = \emptyset$, akkor az állítás nyilvánvalóan igaz. Tegyük fel, hogy B' nem üres, és legyen $z \in B'$ rögzített vektor. Ekkor B' lineáris függetlensége miatt $\{z\} \subseteq E$ lineárisan független halmaz és $B \subseteq E$ generátorhalmaz, ezért 17.5.9. alapján létezik olyan $H \subseteq B$ halmaz, amelyre $H \cap \{z\} = \emptyset$, vagyis $z \notin H$, és $H \cup \{z\}$ bázishalmaz E-ben.

Ha $H = B$ teljesülne, akkor a H halmazra vonatkozó hipotézis szerint $B \cup \{z\}$ lineárisan független lenne és $z \notin H = B$, így 17.5.7. alapján $z \notin \mathrm{sp}(B) = E$, holott $z \in E$. Ezért $H \neq B$, tehát $\mathrm{Card}(H) < \mathrm{Card}(B) \leq n+1$, amiből következik, hogy $\mathrm{Card}(H) \leq n$.

Értelmezzük az

$$N := \mathrm{sp}(H), \quad N' := \mathrm{sp}(B' \setminus \{z\})$$

lineáris altereket E-ben, és megmutatjuk, hogy N és N' mindketten komplementerei E-ben a $K.z$ lineáris altérnek.

A $H \cup \{z\}$ halmaz lineárisan független és $z \notin H$, így 17.5.7. alapján $z \notin \mathrm{sp}(H) = N$. Ebből következik, hogy $(K.z) \cap N = \{\mathbf{0}\}$, mert $y \in (K.z) \cap N$ esetén van olyan $\alpha \in K$, hogy $\alpha.z = y \in N$, és ekkor szükségképpen $\alpha = 0$, tehát $y = \mathbf{0}$, különben $z = \alpha^{-1}.y \in N$ teljesülne.

Ugyanakkor $(K.z) + N = E$ is igaz, mert $y \in E$ esetén van olyan $X \subseteq H \cup \{z\}$ halmaz és olyan $\lambda : X \to K$ függvény, hogy $y = \sum_{x \in X} \lambda(x).x$, hiszen $H \cup \{z\}$ generátorhalmaz E-ben, és ekkor

– ha $z \notin X$, akkor $X \subseteq H$, tehát $y \in \mathrm{sp}(H) = N \subseteq (K.z) + N$,

– ha $z \in X$, akkor $y = \lambda(z).z + \sum_{x \in X \setminus \{z\}} \lambda(x).x \in (K.z) + N$, hiszen ekkor $X \setminus \{z\} \subseteq H$, tehát $\sum_{x \in X \setminus \{z\}} \lambda(x).x \in \mathrm{sp}(H) = N$.

Ezzel megmutattuk, hogy N komplementere E-ben a $K.z$ lineáris altérnek.

A $B' = (B' \setminus \{z\}) \cup \{z\}$ halmaz lineárisan független és $z \notin B' \setminus \{z\}$, így 17.5.7. alapján $z \notin \mathrm{sp}(B' \setminus \{z\}) = N'$. Ebből következik, hogy $(K.z) \cap N' = \{\mathbf{0}\}$, mert $y \in (K.z) \cap N'$ esetén van olyan $\alpha \in K$, hogy $\alpha.z = y \in N'$, és ekkor szükségképpen $\alpha = 0$, tehát $y = \mathbf{0}$, különben $z = \alpha^{-1}.y \in N'$ teljesülne.

Ugyanakkor $(K.z) + N' = E$ is igaz, mert $y \in E$ esetén van olyan $X \subseteq B'$ véges halmaz és olyan $\lambda : X \to K$ függvény, hogy $y = \sum_{x \in X} \lambda(x).x$, hiszen B' generátorhalmaz E-ben, és ekkor

– ha $z \notin X$, akkor $X \subseteq B' \setminus \{z\}$, tehát $y \in \mathrm{sp}(B' \setminus \{z\}) = N' \subseteq (K.z) + N'$,

– ha $z \in X$, akkor $y = \lambda(z).z + \sum_{x \in X \setminus \{z\}} \lambda(x).x \in (K.z) + N'$, hiszen ekkor $X \setminus \{z\} \subseteq B' \setminus \{z\}$, tehát $\sum_{x \in X \setminus \{z\}} \lambda(x).x \in \mathrm{sp}(B' \setminus \{z\}) = N'$.

Ezzel megmutattuk, hogy N' komplementere E-ben a $K.z$ lineáris altérnek.

Most hivatkozhatunk a 17.4.3. állításra, amely szerint az N' és N vektorterek lineárisan izomorfak: legyen $u : N' \to N$ lineáris bijekció. A definíció szerint $B' \setminus \{z\}$ bázishalmaz N'-ben, ezért 17.5.4. c) alapján $u\langle B' \setminus \{z\}\rangle$ bázishalmaz N-ben. Ugyanakkor, szintén a definíció szerint, H bázishalmaz N-ben, és tudjuk, hogy H véges és $\mathrm{Card}(H) \leq n$. Ezért az indukciós hipotézis, vagyis $\mathfrak{A}(n)$ alapján kapjuk, hogy az $u\langle B' \setminus \{z\}\rangle$ halmaz kisebb-egyenlő számosságú n-nél. Tehát $u\langle B' \setminus \{z\}\rangle$ véges is, és mivel az $u|_{B' \setminus \{z\}}$ leképezés bijekció $B' \setminus \{z\}$ és $u\langle B' \setminus \{z\}\rangle$ között, így $B' \setminus \{z\}$ is véges halmaz és $\mathrm{Card}(B' \setminus \{z\}) = \mathrm{Card}(u\langle B' \setminus \{z\}\rangle) \leq n$. Ezért a $B' = (B' \setminus \{z\}) \cup \{z\}$ halmaz is véges és $\mathrm{Card}(B') = \mathrm{Card}(B' \setminus \{z\}) + 1 \leq n + 1$, amit bizonyítani kellett.

(II) Legyen E vektortér és $B \subseteq E$ véges bázishalmaz E-ben. Legyen $B' \subseteq E$ tetszőleges bázishalmaz E-ben. Ekkor az $n := \mathrm{Card}(B)$ természetes számra $\mathfrak{A}(n)$ igaz, tehát (I) alapján B' véges és $\mathrm{Card}(B') \leq n = \mathrm{Card}(B)$. ■

17.5.11. Állítás. *Véges dimenziós vektortér mindegyik bázishalmaza véges, és bármely két bázishalmaza ekvipotens egymással.*

Bizonyítás. Legyen E véges dimenziós vektortér és B_0 rögzített véges bázishalmaz E-ben. Legyen B tetszőleges bázishalmaz E-ben. Ekkor az előző lemma szerint B véges és $\mathrm{Card}(B) \leq \mathrm{Card}(B_0)$. De ekkor B véges bázishalmaz E-ben és B_0 bázishalmaz E-ben, így ismét az előző lemma alapján $\mathrm{Card}(B_0) \leq \mathrm{Card}(B)$. Ez azt jelenti, hogy B véges és $\mathrm{Card}(B) = \mathrm{Card}(B_0)$. Tehát az E vektortér minden bázishalmaza véges, és mindegyik bázishalmazának a számossága egyenlő a $\mathrm{Card}(B_0)$ számmal. ■

17.5.12. Definíció. *Ha E véges dimenziós vektortér, akkor* $\dim(E)$ *jelöli azt a természetes számot, amelyre* $\dim(E) = \mathrm{Card}(B)$ *teljesül, ahol B tetszőleges bázishalmaz E-ben; továbbá a* $\dim(E)$ *számot az E vektortér* **dimenziójának** *nevezzük.*

Most megmutatjuk, hogy minden vektortér lineárisan izomorf egy függvénytérrel.

17.5.13. Állítás. *Legyen E vektortér a K test felett. Ha B bázishalmaz E-ben, akkor a*

$$u_B : K^{(B)} \to E; \quad x \mapsto \sum_{b \in B} x(b).b$$

leképezés izomorfizmus a $K^{(B)}$ és E vektorterek között.

Bizonyítás. Az u_B leképezés additív, mert $x, y \in K^{(B)}$ esetén

$$u_B(x+y) = \sum_{b \in B}(x+y)(b).b \overset{(1)}{=} \sum_{b \in B}(x(b).b + y(b).b) \overset{(2)}{=} \sum_{b \in B} x(b).b + \sum_{b \in B} y(b).b = u_B(x) + u_B(y),$$

ahol az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk a $K^{(B)}$ feletti összeadás definícióját és a vektorterekre vonatkozó $(\mathrm{EV}_{\mathrm{II}_2})$ tulajdonságot (17.1.1.), továbbá a $\overset{(2)}{=}$ egyenlőségnél a 12.5.7. állítást alkalmaztuk az $(E, +)$ kommutatív monoidra és az $(x(b).b)_{b \in B}$ és $(y(b).b)_{b \in B}$ rendszerekre.

Az u_B leképezés K-homogén, mert $x \in K^{(B)}$ és $\lambda \in K$ esetén

$$u_B(\lambda.x) = \sum_{b \in B} (\lambda.x)(b).b \overset{(3)}{=} \sum_{b \in B} (\lambda.(x(b).b)) \overset{(4)}{=} \lambda. \sum_{b \in B} x(b).b = \lambda.u_B(x),$$

ahol a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk a $K^{(B)}$-beli függvények K elemeivel való szorzásának definícióját és a vektorterekre vonatkozó $(\mathrm{EV}_{\mathrm{II}_1})$ tulajdonságot (17.1.1.), továbbá a $\overset{(4)}{=}$ egyenlőségnél a 12.5.16. állítást alkalmaztuk az $(S, \perp) := (S', \perp') := (E, +)$ kommutatív monoidra és a $\pi : E \to E;\ z \mapsto \lambda.z$ leképezésre, felhasználva az $(\mathrm{EV}_{\mathrm{II}_3})$ tulajdonságot (17.1.1.).

Ezzel megmutattuk, hogy $u_B : K^{(B)} \to E$ lineáris operátor.

Az u_B lineáris operátor injektív. Legyen ugyanis $x \in K^{(B)}$ olyan, hogy $u_B(x) = \mathbf{0}$. Ekkor a $B_* := \{b \in B | x(b) \neq 0\}$ halmaz véges és $\sum_{b \in B_*} x(b).b = \sum_{b \in B} x(b).b = \mathbf{0}$, tehát B lineáris függetlensége folytán minden $b \in B_*$ esetén $x(b) = 0$, vagyis $B_* = \emptyset$, azaz $x = \mathbf{0}$.

Az u_B lineáris operátor szürjektív. Valóban, ha $y \in E$, akkor van olyan $B_y \subseteq B$ véges halmaz és olyan $\lambda : B_y \to K$ függvény, hogy $y = \sum_{b \in B_z} \lambda(z).b$, hiszen B generátorhalmaz E-ben. Ha x jelöli a λ függvény 0-val vett kiterjesztését B_y-ról, B-re, akkor $x \in K^{(B)}$ és $u_B(x) = \sum_{b \in B} x(b).b = \sum_{b \in B_y} \lambda(b).b = y$.

Ezzel megmutattuk, hogy az $u_B : K^{(B)} \to E$ lineáris operátor bijekció. ■

17.5.14. Tétel. *Ha E vektortér a K test felett, valamint B és B' bázishalmazok E-ben, akkor B és B' ekvipotens halmazok.*

Bizonyítás. Az előző állítás szerint a $K^{(B)}$ és $K^{(B')}$ vektorterek lineárisan izomorfak, hiszen mindketten lineárisan izomorfak E-vel, ezért azt kell megmutatni, hogy ha T és T' olyan halmazok, amelyekre a $K^{(T)}$ és $K^{(T')}$ vektorterek lineárisan izomorfak, akkor T és T' ekvipotensek.

Ennek bizonyításához legyenek T és T' halmazok, valamint legyen $u : K^{(T)} \to K^{(T')}$ lineáris bijekció. Tekintsük a

$$f : T \to \mathscr{P}(T'); \quad t \mapsto \{t' \in T' \mid u(\mathbf{e}_t)(t') \neq 0\}$$

leképezést, ahol minden $t \in T$ esetén $\mathbf{e}_t$ az az elem $K^{(T)}$, amelyre minden $s \in T \setminus \{t\}$ esetén $\mathbf{e}_t(s) = 0$, és $\mathbf{e}_t(t) = 1$. Fennáll a

$$T' = \bigcup_{t \in T} f(t)$$

egyenlőség. Valóban, legyen $t' \in T'$, és $y \in K^{(T')}$ olyan elem, amelyre $y(t') \neq 0$. Az u leképezés szürjektivitása folytán létezik olyan $x \in K^{(T)}$, hogy $u(x) = y$; ekkor az u leképezés linearitása és $x = \sum_{t \in [x \neq 0]} x(t).\mathbf{e}_t$ miatt

$$y = u(x) = \sum_{t \in [x \neq 0]} x(t).u(\mathbf{e}_t),$$

így $y(t') \neq 0$ következtében van olyan $t \in T$, amelyre $u(\mathbf{e}_t)(t') \neq 0$, így $t' \in f(t)$. Világos, hogy minden $t \in T$ esetén $f(t) \subseteq T'$ *véges* halmaz. Ebből azonnal következik, hogy ha T véges, akkor T' is véges. A T és T' szerepét felcserélve ebből kapjuk, hogy két alternatíva van: vagy T és T' mindketten végesek, vagy mindketten végtelenek.

(I) Tegyük fel, hogy T és T' mindketten végtelenek. Az u leképezés injektivitása miatt minden $t \in T$ esetén $u(\mathbf{e}_t) \neq 0$, tehát $f(t) \neq \emptyset$. Ezért a $(\{t\} \times f(t))_{t\in T}$ halmazrendszer nem üres véges halmazok diszjunkt rendszere, így 10.3.10. szerint $\bigcup_{t\in T}(\{t\} \times f(t))$ ekvipotens T-vel. Azonban ez a halmaz nagyobb-egyenlő számosságú az $\bigcup_{t\in T} f(t)$ halmaznál, vagyis T'-nél, tehát T nagyobb-egyenlő számosságú T'-nél. A T és T' halmazok szerepét felcserélve, hasonló érveléssel kapjuk, hogy T' is nagyobb-egyenlő számosságú T-nél, így a Schröder–Bernstein-tételt (6.5.5.) alkalmazva kapjuk, hogy T és T' ekvipotensek.

(II) Tegyük fel, hogy T és T' mindketten végesek. Ekkor

$$\mathrm{Card}(T) = \dim(K^{(T)}) = \dim(K^{(T')}) = \mathrm{Card}(T'),$$

ezért T és T' ekvipotensek (8.1.6.). ■

17.5.15. Következmény. *Ha E vektortér, $L \subseteq E$ lineárisan független halmaz és $B \subseteq E$ bázishalmaz, akkor L kisebb-egyenlő számosságú B-nél.*

Bizonyítás. 17.5.9. alapján van olyan $L' \subseteq E$ lineárisan független halmaz, hogy $L \cap L' = \emptyset$ és $L \cup L'$ bázishalmaz. Ekkor az előző tétel szerint $L \cup L'$ és B ekvipotens halmazok, és természetesen L kisebb-egyenlő számosságú $L \cup L'$-nél, így B-nél is. ■

17.5.16. Következmény. *Ha E és F vektorterek, F véges dimenziós, és létezik $E \to F$ lineáris injekció, akkor E is véges dimenziós.*

Bizonyítás. Ha B bázishalmaz E-ben és $u : E \to F$ lineáris injekció, akkor $u\langle B\rangle$ lineárisan független halmaz F-ben (17.5.4. a) pont), így 17.5.15. alapján véges, tehát $B = u^{-1}\langle u\langle B\rangle\rangle$ is véges halmaz (8.1.11.). ■

17.5.17. Definíció. *Minden E vektortérre* $\dim(E)$ *jelöli a* $\mathrm{Card}(B)$ *számosságot, ahol B tetszőleges bázishalmaza E-nek, és ezt a számosságot az E vektortér* **dimenziójának** *nevezzük. Ha E vektortér és $M \subseteq E$ lineáris altér, akkor az E/M lineáris faktortér dimenzióját az M altér* **kodimenziójának** *nevezzük, és a* $\mathrm{codim}(M)$ *szimbólummal jelöljük.*

17.5.18. Állítás. *Az E vektortér pontosan akkor végtelen dimenziós, ha minden $n \in \mathbb{N}$ esetén létezik olyan $L \subseteq E$ halmaz, amely lineárisan független, véges, és* $\mathrm{Card}(L) = n$.

Bizonyítás. Tegyük fel, hogy E végtelen dimenziós, és legyen $B \subseteq E$ végtelen bázishalmaz. Ekkor vehetünk olyan $D \subseteq B$ halmazt, amely megszámlálhatóan végtelen (10.1.2.). Legyen $\sigma : \mathbb{N} \to D$ bijekció, és minden $n \in \mathbb{N}$ esetén legyen $L_n := \{\sigma(k) | k < n\}$. Ekkor minden $n \in \mathbb{N}$ esetén L_n lineárisan független, mert részhalmaza a B bázishalmaznak, továbbá L_n véges és $\mathrm{Card}(L_n) = n$.

Tegyük fel, hogy E véges dimenziós. Ha $L \subseteq E$ lineárisan független halmaz, akkor 17.5.10. alapján L kisebb-egyenlő számosságú $\dim(E)$-nél, vagyis $n \in \mathbb{N}$ és $n > \dim(E)$ esetén nincs olyan $L \subseteq E$ lineárisan független, véges halmaz, amelyre $\mathrm{Card}(L) = n$. ■

17.5.19. Tétel. *Két vektortér, ugyanazon test felett pontosan akkor lineárisan izomorf, ha a dimenzióik megegyeznek.*

Bizonyítás. Lineárisan izomorf vektorterek 17.5.4. c) alapján egyenlő dimenziójúak. Legyenek E és F egyenlő dimenziójú vektorterek a K test felett, és legyen B (illetve C) bázis E-ben (illetve F-ben). Ha $f : B \to C$ bijekció, akkor a

$$K^{(B)} \to K^{(C)}; \quad x \mapsto x \circ f^{-1}$$

leképezés nyilvánvalóan lineáris bijekció, tehát $K^{(B)}$ és $K^{(C)}$ lineárisan izomorf vektorterek. Ugyanakkor 17.5.13. szerint E lineárisan izomorf $K^{(B)}$-vel és F lineárisan izomorf $K^{(C)}$-vel, így az E és F vektorterek lineárisan izomorfak. ■

17.5.20. Állítás. *Ha E végtelen dimenziós vektortér a K test felett, akkor az E és* $(\dim(E)) \times K$ *halmazok ekvipotensek.*

Bizonyítás. Legyen B bázis E-ben, tehát $\dim(E) = \mathrm{Card}(B)$. Ekkor 17.5.13. szerint az E és $K^{(B)}$ vektorterek izomorfak, ezért az E és $K^{(B)}$ halmazok ekvipotensek. Ez azt jelenti, hogy az állítás azzal ekvivalens, hogy végtelen B halmaz esetén a $K^{(B)}$ és $B \times K$ halmazok ekvipotensek.

Jelölje $\mathfrak{X}$ a B halmaz véges részhalmazinak halmazát. Világos, hogy minden $\lambda \in K^{(B)}$ esetén $[\lambda \neq 0] := \{b \in B | \lambda(b) \neq 0\} \in \mathfrak{X}$ és $\lambda|_{[\lambda \neq 0]} \in (K \setminus \{0\})^{[\lambda \neq 0]}$, tehát jól értelmezett a

$$f : K^{(B)} \to \bigcup_{X \in \mathfrak{X}} (K \setminus \{0\})^X; \quad \lambda \mapsto \lambda|_{[\lambda \neq 0]}$$

leképezés. Megmutatjuk, hogy f *bijekció.*

Ha $\lambda, \lambda' \in K^{(B)}$ és $\lambda|_{[\lambda \neq 0]} = \lambda'|_{[\lambda' \neq 0]}$, akkor $X := [\lambda \neq 0] = \mathrm{Dom}\left(\lambda|_{[\lambda \neq 0]}\right) = \mathrm{Dom}\left(\lambda'|_{[\lambda' \neq 0]}\right) = [\lambda' \neq 0]$, és minden $b \in X$ esetén $\lambda(b) = \lambda'(b)$, míg $b \in B \setminus X$ esetén $\lambda(b) = 0 = \lambda'(b)$, tehát $\lambda = \lambda'$, így az f függvény injektív.

Ha $X \in \mathfrak{X}$ és $\sigma \in (K \setminus \{0\})^X$, akkor λ-val jelölve a $\sigma : X \to K \setminus \{0\}$ függvény 0-val vett kiterjesztését X-ről B-re kapjuk, hogy $\lambda \in K^{(B)}$ és $[\lambda \neq 0] = X$ és $\lambda|_X = \sigma$, vagyis $f(\lambda) = \sigma$, tehát az f függvény szürjektív.

Ezzel beláttuk, hogy $K^{(B)}$ és $\bigcup_{X \in \mathfrak{X}} (K \setminus \{0\})^X$ ekvipotens halmazok. Most két esetet különböztetünk meg.

1) Tegyük fel, hogy K végtelen. Ekkor $K \setminus \{0\}$ is végtelen halmaz, így minden X nem üres véges halmazra $(K \setminus \{0\})^X$ ekvipotens $K \setminus \{0\}$-val (10.3.8.), vagyis K-val. Tehát minden $X \in \mathfrak{X}$ esetén $(K \setminus \{0\})^X$ kisebb-egyenlő számosságú K-nál, így a 10.3.9. állítás szerint az $\bigcup_{X \in \mathfrak{X}} (K \setminus \{0\})^X$ halmaz kisebb-egyenlő számosságú $\mathfrak{X} \times K$-nál, így $B \times K$-nál is, hiszen B végtelensége folytán $\mathfrak{X}$ és B ekvipotensek (10.3.12.).

2) Tegyük fel, hogy K véges. Ekkor minden X véges halmazra $(K \setminus \{0\})^X$ véges halmaz (8.1.21.), tehát minden $X \in \mathfrak{X}$ esetén $(K \setminus \{0\})^X$ kisebb-egyenlő számosságú $\mathbb{N}$-nél, így a 10.3.9. állítás szerint az $\bigcup_{X \in \mathfrak{X}} (K \setminus \{0\})^X$ halmaz kisebb-egyenlő számosságú $\mathfrak{X} \times \mathbb{N}$-nél. Ugyanakkor B végtelensége folytán $\mathfrak{X}$ és B ekvipotensek (10.3.12.), így 10.3.3. szerint $\mathfrak{X} \times \mathbb{N}$ ekvipotens B-vel, így kisebb-egyenlő számosságú $B \times K$-nál.

Ezzel beláttuk, hogy $K^{(B)}$ kisebb-egyenlő számosságú $B \times K$-nál.

Minden $b \in B$ esetén jelölje $\mathbf{e}_b \in K^{(B)}$ azt a függvényt, amelyre minden $b' \in B$ esetén $\mathbf{e}_b(b') := \delta_{b,b'}$. Ekkor a

$$B \times (K \setminus \{0\}) \to K^{(B)}; \quad (b, \lambda) \mapsto \lambda.\mathbf{e}_b$$

leképezés nyilvánvalóan injekció, így $B \times (K \setminus \{0\})$ kisebb-egyenlő számosságú $K^{(B)}$-nél. Ha K végtelen, akkor $K \setminus \{0\}$ és K ekvipotensek, így $B \times K$ kisebb-egyenlő számosságú $K^{(B)}$-nél. Ha K véges, akkor $K \setminus \{0\} \neq \emptyset$ és B végtelensége miatt, 10.3.3. alapján $B \times (K \setminus \{0\})$ és $B \times K$ is ekvipotens B-vel, így $B \times K$ kisebb-egyenlő számosságú $K^{(B)}$-nél.

A Schröder–Bernstein-tétel (6.5.5.) szerint a $K^{(B)}$ és $B \times K$ halmazok ekvipotensek. ■

17.6. Véges dimenziós vektorterek

17.6.1. Állítás. *Legyen $(E_i)_{i \in I}$ véges dimenziós vektorterek véges rendszere.*

a) *Ha $(B_i)_{i \in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén B_i bázishalmaz az E_i vektortérben, akkor $\bigcup_{i \in I} \mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle$ bázishalmaz a $\bigoplus_{i \in I} E_i$ vektortérben, ahol $\mathbf{0}$ az additív neutrális elem a $\bigoplus_{i \in I} E_i$ vektortérben.*

b) *Ha $\left((e_{i,j})_{J_i} \right)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(e_{i,j})_{j \in J_i}$ bázis az E_i vektortérben, és $\mathscr{I} := \{(i,j) | (i \in I) \wedge (j \in J_i)\}$, akkor az $(e_{i,j})_{(i,j) \in \mathscr{I}}$ rendszer bázis a $\bigoplus_{i \in I} E_i$ vektortérben.*

c) *A $\bigoplus_{i \in I} E_i$ vektortér véges dimenziós vektortér és*

$$\dim \left(\bigoplus_{i \in I} E_i \right) = \sum_{i \in I} \dim(E_i).$$

Bizonyítás. Legyen $E := \bigoplus_{i \in I} E_i$, és jelölje $\mathbf{0}$ az additív neutrális elemet az E vektortérben. Minden $i \in I$ esetén az $\mathrm{in}_{i,\mathbf{0}} : E_i \to E$ leképezés injektív lineáris operátor, így 17.5.4. a) szerint $\mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle$ lineárisan független halmaz E-ben. Továbbá, az $(\mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle)_{i \in I}$ halmazrendszer diszjunkt, mert ha $i, j \in I$ és $i \neq j$, akkor $(x_k)_{k \in I} \in \mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle \cap \mathrm{in}_{j,\mathbf{0}}\langle B_j \rangle$ esetén van olyan $b_i \in B_i$ és $b_j \in B_j$, hogy $(x_k)_{k \in I} = \mathrm{in}_{i,\mathbf{0}}(b_i) = \mathrm{in}_{j,\mathbf{0}}(b_j)$, és ekkor $x_i = b_i$, ugyanakkor $x_i = 0_i$ (ahol 0_i az additív neutrális elem az E_i vektortérben), mert az $\mathrm{in}_{j,\mathbf{0}}(b_j)$ rendszer i-edik komponense 0_i, hiszen $i \neq j$, tehát $b_i = 0_i$, ami lehetetlen.

Megmutatjuk, hogy a $B := \bigcup_{i \in I} \mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle$ véges halmaz (8.1.13.) bázishalmaz az E vektortérben.

Legyen K az a test, amely felett E vektortér, és legyen $\lambda \in K^B$ olyan függvény, hogy $\sum_{\mathbf{b} \in B} \lambda(\mathbf{b}).\mathbf{b} = \mathbf{0}$. Ekkor a monoidok véges műveleteinek általános asszociativitása (12.5.10.) és kommutativitása (12.5.9.) alapján

$$\mathbf{0} = \sum_{\mathbf{b} \in B} \lambda(\mathbf{b}).\mathbf{b} = \sum_{i \in I} \Bigg(\sum_{\mathbf{b} \in \mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle} \lambda(\mathbf{b}).\mathbf{b} \Bigg) = \sum_{i \in I} \Bigg(\sum_{b \in B_i} \lambda(\mathrm{in}_{i,\mathbf{0}}(b)).\mathrm{in}_{i,\mathbf{0}}(b) \Bigg) =$$
$$= \sum_{i \in I} \mathrm{in}_{i,\mathbf{0}} \Bigg(\sum_{b \in B_i} (\lambda \circ \mathrm{in}_{i,\mathbf{0}})(b).b \Bigg) = \Bigg(\sum_{b \in B_i} (\lambda \circ \mathrm{in}_{i,\mathbf{0}})(b).b \Bigg)_{i \in I}.$$

Ezért minden $i \in I$ indexre $\sum_{b \in B_i} (\lambda \circ \mathrm{in}_{i,\mathbf{0}})(b).b = 0_i$, így B_i lineáris függetlensége folytán minden $b \in B_i$ esetén $(\lambda \circ \mathrm{in}_{i,\mathbf{0}})(b) = 0$. Ez azt jelenti, hogy $\lambda = 0$, vagyis B lineárisan független részhalmaza az E vektortérnek.

Legyen $(x_i)_{i \in I} \in E$. Minden $i \in I$ esetén $x_i \in E_i$ és B_i generátorhalmaz az E_i vektortérben, így létezik olyan $\lambda_i \in K^{B_i}$ függvény, hogy $x_i = \sum_{b \in B_i} \lambda_i(b).b$, tehát az $\mathrm{in}_{i,\mathbf{0}} : E_i \to E$ leképezés linearitása folytán

$$\mathrm{in}_{i,\mathbf{0}}(x_i) = \mathrm{in}_{i,\mathbf{0}}\Big(\sum_{b \in B_i} \lambda_i(b).b\Big) = \sum_{b \in B_i} \lambda_i(b).\mathrm{in}_{i,\mathbf{0}}(b) \in \mathrm{sp}(\mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle) \subseteq \mathrm{sp}(B).$$

Ebből azonnal következik, hogy $(x_i)_{i \in I} = \sum_{i \in I} \mathrm{in}_{i,\mathbf{0}}(x_i) \in \mathrm{sp}(B)$, ezért B generátorhalmaz az E vektortérben.

Tehát B bázishalmaz az E vektortérben, így E véges dimenziós, továbbá az $(\mathrm{in}_{i,\mathbf{0}}\langle B_i \rangle)_{i \in I}$ halmazrendszer diszjunktságát felhasználva, 9.1.4. alkalmazásával kapjuk, hogy

$$\dim(E) = \mathrm{Card}(B) = \sum_{i \in I} \mathrm{Card}(B_i) = \sum_{i \in I} \dim(E_i) \ \blacksquare$$

Ezzel az a) és c) állításokat igazoltuk. A c) állítás nyilvánvalóan következik a)-ból, ha az $\left((e_{i,j})_{J_i}\right)_{i \in I}$ rendszerről áttérünk arra a $(B_i)_{i \in I}$ halmazrendszerre, amelyre minden $i \in I$ esetén $B_i := \{e_{i,j} | j \in J_i\}$. $\blacksquare$

17.6.2. Következmény. *Ha M lineáris altere az E véges dimenziós vektortérnek, akkor*

$$\dim(E/M) = \dim(E) - \dim(M).$$

Bizonyítás. Legyen $j : E/M \to E$ lineáris jobbinverze a $\pi_{E/M} : E \to E/M$ kanonikus szürjekciónak (17.4.7.). Ekkor $E = M \oplus \mathrm{Im}(j)$, mert

– ha $x \in M \cap \mathrm{Im}(j)$, akkor van olyan $\xi \in E/M$, amelyre $x = j(\xi)$, tehát $M = \mathrm{Ker}(\pi_{E/M})$ és $\pi_{E/M} \circ j = \mathrm{id}_{E/M}$ miatt $\xi = \pi_{E/M}(j(\xi)) = \pi_{E/M}(x) = \mathbf{0}$, ezért $x = j(\mathbf{0}) = \mathbf{0}$, ami azt jelenti, hogy $M \cap \mathrm{Im}(j) = \{\mathbf{0}\}$;

– ha $x \in E$ tetszőleges, akkor $x = (x - j(\pi_{E/M}(x))) + j(\pi_{E/M}(x))$ és $\pi_{E/M} \circ j = \mathrm{id}_{E/M}$ miatt $x - j(\pi_{E/M}(x)) \in \mathrm{Ker}(\pi_{E/M}) = M$, valamint $j(\pi_{E/M}(x)) \in \mathrm{Im}(j)$, ami azt jelenti, hogy $M + \mathrm{Im}(j) = E$.

Ezért 17.6.1. szerint $\dim(E) = \mathrm{Im}(M) + \dim(\mathrm{Im}(j))$. Ugyanakkor $j : E/M \to \mathrm{Im}(j)$ lineáris bijekció, ezért 17.5.19. miatt $\dim(E/M) = \dim(\mathrm{Im}(j)) = \dim(E) - \dim(M)$. $\blacksquare$

17.6.3. Következmény. *Ha M és N véges dimenziós lineáris alterei az E vektortérnek, akkor*

$$\dim(M + N) + \dim(M \cap N) = \dim(M) + \dim(N).$$

Bizonyítás. A 17.2.10. állítás szerint az $(M + N)/M$ és $N/(M \cap N)$ lineáris faktorterek izomorfak, így az előző állítást alkalmazva (E helyett az $M + N$ véges dimenziós vektortérre), 17.5.19. alapján kapjuk, hogy

$$\dim(M+N) - \dim(M) = \dim((M+N)/M) = \dim(N/(M \cap N)) = \dim(N) - \dim(M \cap N),$$

amiből átrendezéssel nyerjük a bizonyítandó egyenlőséget. $\blacksquare$

17.6.4. Állítás. *Ha E és F olyan véges dimenziós vektorterek, hogy* $\dim(E) = \dim(F)$, *akkor minden $u : E \to F$ lineáris operátorra a következő állítások ekvivalensek.*

(i) *Az u operátor bijekció.*

(ii) *Az u operátor injekció.*

(iii) *Az u operátor szürjekció.*

Bizonyítás. (i)⇒(ii) Triviális.

(ii)⇒(iii) A (ii) feltétel szerint u izomorfizmus az E és $\mathrm{Im}(u)$ vektorterek között, tehát 17.5.19. szerint $\dim(E) = \dim(\mathrm{Im}(u))$. A 17.4.4. állítás szerint $\mathrm{Im}(u)$-nak létezik algebrai komplementere F-ben, tehát vehetünk olyan $N \subseteq F$ lineáris alteret, amelyre $\mathrm{Im}(u) + N = F$ és $\mathrm{Im}(u) \cap N = \{0\}$. Ezért 17.6.3. alkalmazásával kapjuk, hogy

$$\dim(F) = \dim(\mathrm{Im}(u)+N) = \dim(\mathrm{Im}(u))+\dim(N)-\dim(\mathrm{Im}(u)\cap N) = \dim(E)+\dim(N),$$

tehát $\dim(E) = \dim(F)$ miatt $\dim(N) = 0$, vagyis $N = \{0\}$, azaz $F = \mathrm{Im}(u)$, így u szürjektív.

(iii)⇒(i) Jelölje $\dot{u}$ az $E/\mathrm{Ker}(u) \to \mathrm{Im}(u)$ kanonikus bijekciót, amely izomorfizmus az $E/\mathrm{Ker}(u)$ és $\mathrm{Im}(u)$ vektorterek között (17.2.9.). Ekkor (iii) és $\dim(E) = \dim(F)$, valamint 17.6.2. és 17.5.19. szerint

$$\dim(E) - \dim(\mathrm{Ker}(u)) = \dim(E/\mathrm{Ker}(u)) = \dim(\mathrm{Im}(u)) = \dim(F) = \dim(E),$$

ezért $\dim(\mathrm{Ker}(u)) = 0$, vagyis $\mathrm{Ker}(u) = \{0\}$, azaz u injektív. ■

17.7. Lineáris operátor kiterjesztése

17.7.1. Tétel. *Ha E és F vektorterek, $M \subseteq E$ lineáris altér, és $u : M \to F$ lineáris operátor, akkor létezik olyan $\widetilde{u} : E \to F$ lineáris operátor, amelyre $u \subseteq \tilde{u}$.*

Bizonyítás. Legyen N tetszőleges komplementere M-nek, és tekintsük az

$$s : M \times N \to E; \quad (x, y) \mapsto x + y$$
$$p : M \times N \to M; \quad (x, y) \mapsto x$$

leképezéseket. Ezek lineáris operátorok és 17.4.2. szerint s bijekció, mert N komplementere M-nek E-ben. Továbbá, $x \in M$ esetén $s^{-1}(x) = (x, \mathbf{0})$, így az $u \circ p \circ s^{-1} : E \to F$ operátor u-nak lineáris kiterjesztése. ■

17.7.2. Következmény. *Legyenek E, F és G vektorterek a K test felett, valamint $u : E \to F$ és $v : E \to G$ lineáris operátorok. Akkor és csak akkor létezik olyan $w : F \to G$ lineáris operátor, amelyre $w \circ u = v$, vagyis a*

$$\begin{tikzcd} E \arrow[r, "u"] \arrow[dr, "v"'] & F \arrow[d, "w"] \\ & G \end{tikzcd}$$

diagram kommutatív, ha $\mathrm{Ker}(u) \subseteq \mathrm{Ker}(v)$.

Bizonyítás. Ha $w : F \to G$ olyan lineáris operátor, hogy $w \circ u = v$, akkor $x \in \mathrm{Ker}(u)$ esetén $v(x) = w(u(x)) = w(0) = 0$, tehát $\mathrm{Ker}(u) \subseteq \mathrm{Ker}(v)$.

Megfordítva, tegyük fel, hogy $\mathrm{Ker}(u) \subseteq \mathrm{Ker}(v)$. Ha $x, x' \in E$ olyan vektorok, hogy $u(x) = u(x')$, akkor u additivitása folytán $u(x - x') = u(x) - u(x') = 0$, tehát $x - x' \in \mathrm{Ker}(u)$, így a hipotézis szerint $x - x' \in \mathrm{Ker}(v)$, így v additivitása miatt $v(x) = v(x')$. Ezért 6.4.12. szerint egyértelműen létezik az a $w_* : \mathrm{Im}(u) \to G$ leképezés, amelyre minden $x \in E$ esetén $w_*(u(x)) = v(x)$ teljesül, vagyis $w_* \circ u = v$.

Megmutatjuk, hogy a w_* leképezés *lineáris operátor* az $\mathrm{Im}(u) \subseteq F$ lineáris altér és a G vektortér között.

Ha $y, y' \in \mathrm{Im}(u)$, és $x, x' \in E$ olyan vektorok, hogy $u(x) = y$ és $u(x') = y'$, akkor u és v additivitása folytán

$$w_*(y + y') = w_*(u(x) + u(x')) = w_*(u(x + x')) = (w_* \circ u)(x + x') = v(x + x') =$$
$$= v(x) + v(x') = (w_* \circ u)(x) + (w_* \circ u)(x') = w_*(u(x)) + w_*(u(x')) = w_*(y) + w_*(y'),$$

tehát w_* additív.

Ha $y \in \mathrm{Im}(u)$ és $\lambda \in K$, akkor véve olyan $x \in E$ vektort, hogy $y = u(x)$, az u és v leképezések K-homogenitásából kapjuk, hogy

$$w_*(\lambda.y) = w_*(\lambda.u(x)) = w_*(u(\lambda.x)) = (w_* \circ u)(\lambda.x) = v(\lambda.x) = \lambda.v(x) =$$
$$= \lambda.(w_* \circ u)(x) = \lambda.w_*(u(x)) = \lambda.w_*(y),$$

tehát w_* K-homogén.

A 17.7.1. tétel alapján létezik olyan $w : F \to G$ lineáris operátor, hogy $w_* \subseteq w$: ekkor nyilvánvalóan $w \circ u = w_* \circ u = v$ teljesül. ■

17.7.3. Következmény. *Legyenek E és F vektorterek a K test felett. Ha $(e_i)_{i \in I}$ lineárisan független rendszer E-ben és $(f_i)_{i \in I}$ tetszőleges (ugyanolyan indexhalmazú) rendszer F-ben, akkor létezik olyan $u : E \to F$ lineáris operátor, hogy minden $i \in I$ esetén $u(e_i) = f_i$, és ha $u' : E \to F$ szintén olyan lineáris operátor, hogy minden $i \in I$ esetén $u'(e_i) = f_i$, akkor $u = u'$ az $(e_i)_{i \in I}$ rendszer által generált lineáris altéren.*

Bizonyítás. Jelölje M az $\{e_i | i \in I\}$ halmaz által generált lineáris alteret E-ben, és értelmezzük a

$$v : K^{(I)} \to M; \quad (\lambda_i)_{i \in I} \mapsto \sum_{i \in I} \lambda_i.e_i$$

leképezést, amely nyilvánvalóan lineáris operátor. Az $(e_i)_{i \in I}$ rendszer lineáris függetlensége miatt v injektív, és az M altér definíciója szerint v szürjektív is, tehát $v : K^{(I)} \to M$ lineáris bijekció. Továbbá világos, hogy minden $i \in I$ esetén $v(\mathbf{e}_i) = e_i$, ahol $\mathbf{e}_i \in K^{(I)}$ az a rendszer, amelyre minden $I \ni j$-re $\mathbf{e}_i(j) = \delta_{i,j}$.

Értelmezzük a

$$w : K^{(I)} \to F; \quad (\lambda_i)_{i \in I} \mapsto \sum_{i \in I} \lambda_i.f_i$$

leképezést, amely nyilvánvalóan lineáris operátor. Ekkor $w \circ v^{-1} : M \to F$ olyan lineáris operátor, amelyre minden $i \in I$ esetén $(w \circ v^{-1})(e_i) = w(\mathbf{e}_i) = f_i$. A 17.7.1. tétel szerint létezik olyan $u : E \to F$ lineáris operátor, amely kiterjesztése $w \circ v^{-1}$-nek. Világos, hogy u olyan objektum, amelynek a létezését állítottuk.

Ha $u' : E \to F$ szintén olyan lineáris operátor, hogy minden $i \in I$ esetén $u'(e_i) = f_i$, akkor $\{e_i | i \in I\} \subseteq \{x \in E | u(x) = u'(x)\} = \mathrm{Ker}(u - u')$, ezért $\mathrm{sp}(\{e_i | i \in I\}) \subseteq \mathrm{Ker}(u - u')$, vagyis $u = u'$ az $\mathrm{sp}(\{e_i | i \in I\}) \subseteq E$ lineáris altéren. ■

17.7.4. Következmény. *Ha E vektortér a K test felett, akkor E^* szétválasztó E felett, tehát minden $x \in E \setminus \{0\}$ vektorhoz létezik olyan $u \in E^*$, hogy $u(x) \neq 0$.*

Bizonyítás. Ha $x \in E \setminus \{0\}$, akkor az (x) egy tagú rendszer lineárisan független E-ben, ezért erre a rendszerre, valamint a K_s vektortér (1) egy tagú rendszerére alkalmazva az előző állítást kapjuk olyan $u : E \to K_s$ lineáris operátor (vagyis E^*-beli elem) létezését, amelyre $u(x) = 1$. ■

17.7.5. Következmény. *Vektorterek között ható lineáris injekciónak létezik lineáris balinverze.*

Bizonyítás. Legyenek E és F vektorterek, továbbá $u : E \to F$ lineáris injekció. Ekkor $u^{-1} : \mathrm{Im}(u) \to E$ lineáris operátor és $\mathrm{Im}(u)$ lineáris altere F-nek, így 17.7.1. szerint létezik olyan $v : F \to E$ lineáris operátor, amely u^{-1}-nek kiterjesztése. Ekkor $v = u^{-1}$ az $\mathrm{Im}(u)$ halmazon, következésképpen $v \circ u = u^{-1} \circ u = \mathrm{id}_E$, tehát v lineáris balinverze u-nak. ■

17.8. Lineáris operátor sajátértékei és sajátvektorai

17.8.1. Definíció. *Legyen E vektortér a K test felett és $u : E \to E$ lineáris operátor.*
– *Az u lineáris operátor* **sajátértékének** *nevezünk minden olyan $\lambda \in K$ elemet, amelyhez létezik olyan $x \in E \setminus \{0\}$, hogy $u(x) = \lambda.x$ teljesül (vagyis a $\lambda.\mathrm{id}_E - u$ lineáris operátor nem injektív).*
– *Az u lineáris operátor sajátértékeinek halmazát $\mathrm{S}(u)$ jelöli, és minden $\lambda \in \mathrm{S}(u)$ esetén $\mathrm{E}_\lambda(u) := \{x \in E | u(x) = \lambda.x\}$ $(= \mathrm{Ker}(\lambda.\mathrm{id}_E - u))$, amit a λ sajátértékhez tartozó* **sajátaltérnek** *nevezünk, és $\mathrm{E}_\lambda(u) \setminus \{0\}$ elemeit az u operátor λ sajátértékéhez tartozó* **sajátvektoroknak** *nevezzük.*

17.8.2. Állítás. *Legyen E vektortér a K test felett, és $u : E \to E$ lineáris operátor.*

a) *Legyen $(\lambda_i)_{i \in I}$ tetszőleges nem üres injektív rendszer $\mathrm{S}(u)$-ban, és $(x_i)_{i \in I}$ olyan rendszer E-ben, amelyre minden $i \in I$ esetén $x_i \in \mathrm{E}_{\lambda_i}(u) \setminus \{0\}$. Ekkor az $(x_i)_{i \in I}$ rendszer lineárisan független E-ben.*

b) *Ha $\lambda, \lambda' \in \mathrm{S}(u)$ és $\lambda \neq \lambda'$, akkor $\mathrm{E}_\lambda(u) \cap \mathrm{E}_{\lambda'}(u) = \{0\}$.*

c) *Minden $\lambda \in \mathrm{S}(u)$ esetén $\mathrm{E}_\lambda(u) \cap \sum\limits_{\lambda' \in \mathrm{S}(u) \setminus \{\lambda\}} \mathrm{E}_{\lambda'}(u) = \{0\}$.*

Bizonyítás. a) Indirekt bizonyítunk, tehát feltesszük, hogy az $(x_i)_{i \in I}$ rendszer lineárisan összefügg E-ben, vagyis létezik olyan $S \subseteq I$ nem üres véges halmaz, hogy az $(x_i)_{i \in S}$ rendszer lineárisan összefüggő. Jelölje $\mathfrak{S}$ azon $S \subseteq I$ nem üres véges halmazok halmazát, amelyekre az $(x_i)_{i \in S}$ rendszer lineárisan összefüggő, és legyen $n := \min\{\mathrm{Card}(S) | S \in \mathfrak{S}\}$. Legyen $S \in \mathfrak{S}$ olyan halmaz, amelyre $n = \mathrm{Card}(S)$, és vegyünk olyan $(\alpha_i)_{i \in S}$ rendszert K-ban, amelyre $\sum\limits_{i \in S} \alpha_i.x_i = 0$ és van olyan $i \in S$, hogy $\alpha_i \neq 0$. Ebből már látható, hogy $n > 1$, különben az S halmaz egyetlen i elemére $\alpha_i.x_i = 0$ teljesülne, ami $\alpha_i \neq 0$ és $x_i \neq 0$ miatt lehetetlen. Rögzítsünk olyan $j \in S$ elemet, amelyre $\alpha_j \neq 0$, és legyen $S' := S \setminus \{j\}$, valamint minden $S' \ni i$-re $\alpha'_i := \alpha_i / \alpha_j$. Ekkor $x_j = -\sum\limits_{i \in S'} \alpha'_i.x_i$ és minden $i \in S$ esetén $x_i \in \mathrm{E}_{\lambda_i}(u)$, ezért u linearitása folytán

$$-\sum_{i \in S'} (\lambda_j \alpha'_i).x_i = \lambda_j.x_j = u(x_j) = -\sum_{i \in S'} \alpha'_i.u(x_i) = -\sum_{i \in S'} (\alpha'_i \lambda_i).x_i,$$

tehát $\sum_{i\in S'} \alpha'_i(\lambda_i - \lambda_j).x_i = 0$. Az $(\lambda_i)_{i\in I}$ rendszer injektivitása miatt minden $S' \ni i$-re $\lambda_i - \lambda_j \neq 0$, és $-\sum_{i\in S'} \alpha'_i.x_i = x_j \neq 0$ miatt van olyan $i \in S'$, hogy $\alpha'_i \neq 0$. Ez azt jelenti, hogy az $(x_i)_{i\in S'}$ rendszer lineárisan összefüggő és $n > 1$ miatt $S' \neq \emptyset$, tehát $S' \in \mathfrak{S}$, ami $\mathrm{Card}(S') = n - 1$ miatt ellentmond az n szám minimalitásának.

b) Ha $\lambda, \lambda' \in \mathrm{S}(u)$ és $\lambda \neq \lambda'$, akkor $x \in \mathrm{E}_\lambda(u) \cap \mathrm{E}_{\lambda'}(u)$ esetén $\lambda.x = u(x) = \lambda'.x$, tehát $(\lambda - \lambda').x = 0$, ezért $x = 0$.

c) Legyen $\lambda \in \mathrm{S}(u)$ és $x \in \mathrm{E}_\lambda(u) \cap \sum_{\lambda' \in \mathrm{S}(u)\setminus\{\lambda\}} \mathrm{E}_{\lambda'}(u)$. Ekkor van olyan $S \subseteq \mathrm{S}(u)\setminus\{\lambda\}$ véges halmaz és olyan $(x_{\lambda'})_{\lambda'\in S}$ rendszer, hogy $x = \sum_{\lambda'\in S} x_{\lambda'}$ és minden $S \ni \lambda'$-re $x_{\lambda'} \in \mathrm{E}_{\lambda'}(u)$. Legyen $x_\lambda := x$, és tekintsük az $(x_{\lambda'})_{\lambda'\in S\cup\{\lambda\}}$ rendszert, amely az előzőek szerint lineárisan összefüggő. Ha $x \neq 0$ volna, akkor S megválasztható lenne úgy, hogy minden $\lambda' \in S$ esetén $x_{\lambda'} \neq 0$, tehát b) alapján az $(x_{\lambda'})_{\lambda'\in S\cup\{\lambda\}}$ rendszer injektív volna, így a) szerint az $(x_{\lambda'})_{\lambda'\in S\cup\{\lambda\}}$ rendszer lineárisan független lenne, ami lehetetlen. Ezért $x = 0$. ■

17.8.3. Következmény. *Ha E véges dimenziós vektortér, akkor minden $u : E \to E$ lineáris operátorra* $\mathrm{S}(u)$ *véges halmaz és* $\mathrm{Card}(\mathrm{S}(u)) \leq \dim(E)$.

Bizonyítás. Legyen $u : E \to E$ lineáris operátor. Az S(u) halmaz definíciója szerint minden $\lambda \in \mathrm{S}(u)$ esetén $\mathrm{E}_\lambda(u) \setminus \{0\} \neq \emptyset$, így a kiválasztási axióma alkalmazásával vehetünk egy

$$(x_\lambda)_{\lambda\in\mathrm{S}(u)} \in \prod_{\lambda\in\mathrm{S}(u)} (\mathrm{E}_\lambda(u) \setminus \{0\})$$

rendszert. Ha $\lambda, \lambda' \in \mathrm{S}(u)$ és $\lambda \neq \lambda'$, akkor $x_\lambda \neq x_{\lambda'}$, különben az előző állítás b) pontja szerint $x_\lambda = x_{\lambda'} \in \mathrm{E}_\lambda(u) \cap \mathrm{E}_{\lambda'}(u) = \{0\}$ teljesülne. Tehát az $\mathrm{S}(u) \to E;\ \lambda \mapsto x_\lambda$ függvény injekció, így az előző állítás a) pontja szerint $L := \{x_\lambda | \lambda \in \mathrm{S}(u)\}$ lineárisan független halmaz E-ben, tehát L véges és $\mathrm{Card}(L) \leq \dim(E)$ (17.5.15.). Mivel L és S(u) ekvipotens halmazok (hiszen az $\mathrm{S}(u) \to L;\ \lambda \mapsto x_\lambda$ függvény bijekció), így $\mathrm{S}(u)$ is véges halmaz és $\mathrm{Card}(\mathrm{S}(u)) \leq \dim(E)$. ■

17.9. Biduális és duális bázisok

17.9.1. Állítás. *Ha E vektortér a K test felett, akkor minden $x \in E$ esetén az*

$$E^* \to K; \quad u \mapsto u(x)$$

leképezés lineáris funkcionál E^* felett, és az

$$\mathrm{j}_E : E \to E^{**}; \quad x \mapsto (u \mapsto u(x))$$

leképezés injektív lineáris operátor.

Bizonyítás. Legyen $x \in E$ rögzített. Ha $u, v \in E^*$, akkor az E^* duálisban bevezetett összeadás definíciója szerint $(u + v)(x) = u(x) + v(x)$, amiből következik, hogy az $E^* \to K;\ u \mapsto u(x)$ leképezés additív. Ha $u \in E^*$ és $\lambda \in K$, akkor az E^* duálisban bevezett, K-beli elemmel való szorzás definíciója szerint $(\lambda.u)(x) = \lambda u(x)$, amiből következik, hogy az $E^* \to K;\ u \mapsto u(x)$ leképezés K-homogén. Tehát az $E^* \to K;\ u \mapsto u(x)$ leképezés K-lineáris.

Ha $x, y \in E$, akkor minden $u \in E^*$ esetén u additivitása miatt $\mathrm{j}_E(x+y)(u) = u(x+y) = u(x) + u(y) = \mathrm{j}_E(x)(u) + \mathrm{j}_E(y)(u) = (\mathrm{j}_E(x) + \mathrm{j}_E(y))(u)$, amiből következik, hogy a j_E leképezés additív. Ha $x \in E$ és $\lambda \in K$, akkor minden $u \in E^*$ esetén u K-homogenitása miatt $\mathrm{j}_E(\lambda.x)(u) = u(\lambda.x) = \lambda u(x) = \lambda \mathrm{j}_E(x)(u) = (\lambda.\mathrm{j}_E(x))(u)$, amiből következik, hogy a j_E leképezés K-homogén. Tehát a j_E leképezés K-lineáris.

Ha $x \in E$ és $x \neq 0$, akkor 17.7.4. szerint létezik olyan $u \in E^*$, hogy $\mathrm{j}_E(x)(u) = u(x) \neq 0$, tehát $\mathrm{j}_E(x) \neq 0$, ami azt jelenti, hogy a $\mathrm{j}_E : E \to E^{**}$ lineáris operátor injektív. ■

17.9.2. Definíció. *Ha E vektortér a K test felett, akkor az előző állításban értelmezett*

$$\mathrm{j}_E : E \to E^{**}$$

leképezést az E és E^{**} vektorterek közötti **kanonikus lineáris operátornak** *nevezzük.*

17.9.3. Állítás. *Legyen E vektortér a K test felett, és $(e_i)_{i\in I}$ algebrai bázis E-ben. Ekkor létezik egyetlen olyan $(u_i)_{i\in I}$ rendszer E^*-ban, amelyre minden $i, j \in I$ esetén $u_j(e_i) = \delta_{i,j}$. Ez az $(u_i)_{i\in I}$ rendszer rendelkezik a következő tulajdonságokkal.*

a) *Az $(u_i)_{i\in I}$ rendszer lineárisan független az E^* algebrai duálisban.*

b) *Minden $x \in E$ esetén $(u_i(x))_{i\in I} \in K^{(I)}$ (tehát csak véges sok $i \in I$ indexre teljesül az, hogy $u_i(x) \neq 0$), és $x = \sum_{i\in I} u_i(x).e_i$.*

c) *Ha $I \neq \emptyset$, akkor $\bigcap_{i\in I} \mathrm{Ker}(u_i) = \{\mathbf{0}\}$.*

Bizonyítás. (*Unicitás.*) Legyenek $(u_i)_{i\in I}$ és $(v_i)_{i\in I}$ olyan rendszerek E^*-ban, amelyekre minden $i, j \in I$ esetén $u_j(e_i) = \delta_{i,j} = v_j(e_i)$. Ekkor minden $j \in I$ esetén az $u_j, v_j \in E^*$ lineáris funkcionálok előírt, és egyenlő értékeket vesznek fel egy algebrai bázis minden tagján, így egyenlőek.

(*Egzisztencia.*) Legyen $j \in I$ rögzített, és vezessük be az $N_j := \mathrm{sp}(\{e_i | i \in I \setminus \{j\}\})$ lineáris alteret E-ben.

Megmutatjuk, hogy $(K.e_j) \oplus N_j = E$. Tegyük fel, hogy $x \in (K.e_j) \cap N_j$. Ekkor van olyan $\lambda \in K$, hogy $x = \lambda.e_j$, és van olyan $(\lambda_i)_{i\in I\setminus\{j\}} \in K^{(I\setminus\{j\})}$, amelyre $x = \sum_{i\in I\setminus\{j\}} \lambda_i.e_i$. Ekkor a $\lambda_j := -\lambda$ választással $\sum_{i\in I} \lambda_i.e_i = (-\lambda).e_j + \sum_{i\in I\setminus\{j\}} \lambda_i.e_i = 0$, ezért az $(e_i)_{i\in I}$ rendszer lineáris függetlensége miatt minden $i \in I$ esetén $\lambda_i = 0$, így $0 = \lambda_j = -\lambda$ is teljesül, tehát $\lambda = 0$, ezért $x = \mathbf{0}$. Ez azt jelenti, hogy $(K.e_j) \cap N_j = \{\mathbf{0}\}$. Ha $x \in E$ tetszőleges, akkor létezik olyan $(\lambda_i)_{i\in I} \in K^{(I)}$ rendszer, amelyre $x = \sum_{i\in I} \lambda_i.e_i$, hiszen $(e_i)_{i\in I}$ algebrai generátorrendszer E-ben, és ekkor $x = \lambda_j.e_j + \sum_{i\in I\setminus\{j\}} \lambda_i.e_i \in (K.e_j) + N_j$. Ez azt jelenti, hogy $(K.e_j) + N_j = E$, ezért $(K.e_j) \oplus N_j = E$.

Jelölje s_j az E vektortér összeadás-függvényének leszűkítését $(K.e_j) \times N_j$-re, amelyről tudjuk, hogy lineáris bijekció (17.4.2.). Jelölje α_j a $K \to K.e_j$; $\lambda \mapsto \lambda.e_j$ leképezést, amely lineáris bijekció. Végül, jelölje p_j a $(K.e_j) \times N_j \to K.e_j$ első projekciót, amely lineáris leképezés. Ekkor $u_j := \alpha_j^{-1} \circ p_j \circ s_j^{-1} : E \to K$ lineáris leképezés, vagyis $u_j \in E^*$, és könnyen látható, hogy $u_j(e_j) = 1$ (hiszen $s_j^{-1}(e_j) = (e_j, \mathbf{0})$, így $p_j\left(s_j^{-1}(e_j)\right) = e_j$, tehát $\alpha_j^{-1}\left(p_j\left(s_j^{-1}(e_j)\right)\right) = 1$), továbbá minden $i \in I \setminus \{j\}$ esetén $u_j(e_i) = 0$ (hiszen

$s_j^{-1}(e_i) = (\mathbf{0}, e_i)$, így $p_j\left(s_j^{-1}(e_i)\right) = \mathbf{0}$, tehát $\alpha_j^{-1}\left(p_j\left(s_j^{-1}(e_i)\right)\right) = 0)$. Ez azt jelenti, hogy minden $i \in I$ esetén $u_j(e_i) = \delta_{i,j}$.

Tehát az $(u_j)_{j\in I} := \left(\alpha_j^{-1} \circ p_j \circ s_j^{-1}\right)_{j\in I}$ rendszer E^*-ban halad, és minden $i, j \in I$ esetén $u_j(e_i) = \delta_{i,j}$. Ezzel az előírt tulajdonságú, E^*-ban haladó $(u_i)_{i\in I}$ rendszer létezését is igazoltuk.

a) Legyen $(\lambda_j)_{j\in I} \in K^{(I)}$ olyan rendszer, hogy $\sum_{j\in I} \lambda_j.u_j = \mathbf{0}$. Ekkor minden $i \in I$ esetén

$$0 = \left(\sum_{j\in I} \lambda_j.u_j\right)(e_i) = \sum_{j\in I} \lambda_j.u_j\,(e_i) = \sum_{j\in I} \lambda_j.\delta_{i,j} = \lambda_i,$$

tehát az $(u_i)_{i\in I}$ funkcionálrendszer lineárisan független E^*-ban.

b) Legyen $x \in E$, és vegyünk olyan $(\lambda_i)_{i\in I} \in K^{(I)}$ rendszert, amelyre $x = \sum_{i\in I} \lambda_i.e_i$. Ekkor minden $j \in I$ esetén u_j linearitása miatt

$$u_j(x) = u_j\left(\sum_{i\in I} \lambda_i.e_i\right) = \sum_{i\in I} \lambda_i.u_j\,(e_i) = \sum_{i\in I} \lambda_i.\delta_{i,j} = \lambda_j,$$

következésképpen $(u_i(x))_{i\in I} = (\lambda_i)_{i\in I} \in K^{(I)}$ és $x = \sum_{i\in I} u_i(x)e_i$.

c) Ebből következik, hogy ha $I \neq \emptyset$, akkor $x \in \bigcap_{i\in I} \operatorname{Ker}(u_i)$ esetén minden $i \in I$ esetén $u_i(x) = 0$, tehát $x = \sum_{i\in I} u_i(x)e_i = \mathbf{0}$, vagyis $\bigcap_{i\in I} \operatorname{Ker}(u_i) = \{\mathbf{0}\}$. ■

17.9.4. Definíció. *Ha E vektortér, és $(e_i)_{i\in I}$ bázis E-ben, akkor az $(e_i)_{i\in I}$ rendszer* **duálisának** *nevezzük azt az E^*-ban haladó $(u_i)_{i\in I}$ rendszert, amelyre minden $i, j \in I$ esetén $u_j(e_i) = \delta_{i,j}$, és ezt a duális rendszert az $(e_i^*)_{i\in I}$ szimbólummal is jelöljük.*

Ha E vektortér a K test felett, és $(e_i)_{i\in I}$ algebrai bázis E-ben, akkor az $(u_i)_{i\in I}$ duális rendszer lineárisan független E^*-ban (17.9.3. a) pont), így $\dim(E) = \operatorname{Card}(I) \leq \dim(E^*)$, de $(u_i)_{i\in I}$ nem szükségképpen generátorrendszer E^*-ban, tehát nem szükségképpen algebrai bázis E^*-ban, vagyis $\dim(E) < \dim(E^*)$ lehetséges. °(Például, rögzítve bármilyen $\|\cdot\|$ normát $\mathbb{K}^{(\mathbb{N})}$ felett, a $\|\cdot\|$ szerint folytonos $\mathbb{K}^{(\mathbb{N})}$ feletti lineáris funcionálok $\left(\mathbb{K}^{(\mathbb{N})}\right)'$ vektortere a funkcionálnormával ellátva végtelen dimenziós Banach-tér, ezért a Baire-féle kategóriatétel alapján ez a vektortér nem megszámlálhatóan végtelen dimenziós, így $\left(\mathbb{K}^{(\mathbb{N})}\right)' \subseteq \left(\mathbb{K}^{(\mathbb{N})}\right)^*$ miatt $\left(\mathbb{K}^{(\mathbb{N})}\right)^*$ is nem megszámlálhatóan végtelen dimenziós vektortér, ugyanakkor $\dim\left(\mathbb{K}^{(\mathbb{N})}\right) = \operatorname{Card}(\mathbb{N})$)$_\circ$.

17.9.5. Állítás. *Legyen F vektortér a K test felett, T halmaz, és jelölje $(e_t)_{t\in T}$ a $K^{(T)}$ vektortér kanonikus bázisát. Ekkor a*

$$\Phi : \mathbf{L}(K^{(T)}; F) \to F^T; \quad u \mapsto (u\,(e_t))_{t\in T}$$

leképezés lineáris bijekció az $\mathbf{L}(K^{(T)}; F)$ operátortér és az F^T szorzattér között, és

$$\Phi^{-1} : F^T \to \mathbf{L}(K^{(T)}; F); \quad f \mapsto \left(x \mapsto \sum_{t\in T} x(t)f(t)\right).$$

Bizonyítás. A Φ leképezés nyilvánvalóan K-lineáris, és injektív, mert ha $u \in \mathrm{Ker}(\Phi)$, akkor minden $t \in T$ esetén $u(e_t) = 0$, tehát minden $x \in K^{(T)}$ esetén, az u operátor K-linearitása folytán $u(x) = u\left(\sum_{t \in T} x(t).e_t\right) = \sum_{t \in T} x(t).u(e_t) = \mathbf{0}$, tehát $u = \mathbf{0}$. A Φ leképezés szürjektív is, mert ha $f \in F^T$ (vagyis $f : T \to F$ tetszőleges függvény), akkor az

$$u : K^{(T)} \to F; \quad x \mapsto \sum_{t \in T} x(t)f(t)$$

leképezés nyilvánvalóan lineáris, és minden $t' \in T$ esetén $u(e_{t'}) = \sum_{t \in T} e_{t'}(t)f(t) = \sum_{t \in T} \delta_{t',t} f(t) = f(t')$, tehát $f = \Phi(u)$. ■

17.9.6. Következmény. *Legyen K test, T halmaz, és jelölje $(e_t)_{t \in T}$ a $K^{(T)}$ vektortér kanonikus bázisát. Ekkor a*

$$\Phi : \left(K^{(T)}\right)^* \to K^T; \quad u \mapsto (u(e_t))_{t \in T}$$

leképezés lineáris bijekció, és

$$\Phi^{-1} : K^T \to \left(K^{(T)}\right)^*; \quad f \mapsto \left(x \mapsto \sum_{t \in T} x(t)f(t)\right).$$

Bizonyítás. A 17.9.5. állítás nyilvánvaló következménye az $F := K$ speciális esetben. ■

17.9.7. Következmény. *Ha E véges dimenziós vektortér a K test felett, akkor az E^* algebrai duális is véges dimenziós, és* $\dim_K(E) = \dim_K(E^*)$.

Bizonyítás. Ha E véges dimenziós vektortér K felett és T algebrai bázishalmaz E-ben, akkor T véges és E lineárisan izomorf K^T-vel (17.5.13.), így az állítás nyilvánvalóan 17.9.6. és 17.1.11. következménye. ■

17.9.8. Következmény. *Ha E véges dimenziós vektortér, akkor az E^{**} biduális véges dimenziós vektortér, és $\dim_K(E) = \dim_K(E^{**})$, továbbá a $\mathrm{j}_E : E \to E^{**}$ kanonikus lineáris operátor izomorfizmus az E és E^{**} vektorterek között.*

Bizonyítás. A 17.9.7. állítás szerint E^* véges dimenziós és $\dim_K(E) = \dim_K(E^*)$, így alkalmazva a 17.9.7. állítást E^*-ra, kapjuk, hogy az E^{**} biduális véges dimenziós vektortér, és $\dim_K(E^*) = \dim_K(E^{**})$. Tehát E^{**} véges dimenziós vektortér, és $\dim_K(E) = \dim_K(E^{**})$. A $\mathrm{j}_E : E \to E^{**}$ lineáris operátor injektív (17.9.1.), ezért 17.6.4. alapján j_E lineáris bijekció az E és E^{**} vektorterek között. ■

17.9.9. Állítás. *Legyen E vektortér a K test felett, és $(u_i)_{i \in I}$ tetszőleges E^*-ban haladó rendszer. Ha $u \in E^*$ nem $\mathbf{0}$ lineáris funkcionál, akkor a következő állítások evivalensek.*

(i) *Létezik olyan $(\lambda_i)_{i \in I} \in K^{(I)}$ rendszer, amelyre $u = \sum_{i \in I} \lambda_i.u_i$ (ami azzal ekvivalens, hogy $u \in \mathrm{sp}\left(\{u_i | i \in I\}\right)$).*

(ii) *Létezik olyan $J \subseteq I$ nem üres véges halmaz, hogy $\bigcap_{i \in J} \mathrm{Ker}\,(u_i) \subseteq \mathrm{Ker}(u)$.*

Bizonyítás. (i)⇒(ii) Legyen $(\lambda_i)_{i\in I} \in K^{(I)}$ olyan rendszer, amelyre $u = \sum_{i\in I} \lambda_i.u_i$, és legyen $J := \{i \in I | \lambda_i \neq 0\}$. Ekkor $J \subseteq I$ véges halmaz, és nem üres, mert $u \neq \mathbf{0}$. Nyilvánvaló, hogy $\bigcap_{i\in J} \mathrm{Ker}\,(u_i) \subseteq \mathrm{Ker}(u)$ teljesül.

(ii)⇒(i) Legyen $J \subseteq I$ olyan nem üres véges halmaz, hogy $\bigcap_{i\in J} \mathrm{Ker}\,(u_i) \subseteq \mathrm{Ker}(u)$, és értelmezzük a

$$w : E \to K^J; \quad x \mapsto (u_j(x))_{j\in J}$$

leképezést, amely nyilvánvalóan lineáris operátor. Világos, hogy $\mathrm{Ker}(w) = \bigcap_{i\in J} \mathrm{Ker}\,(u_i)$, ezért a hipotézis szerint $\mathrm{Ker}(w) \subseteq \mathrm{Ker}(u)$, amiből 17.7.2. alapján következik olyan $v \in \left(K^J\right)^*$ létezése, amelyre $u = v \circ w$, tehát a következő diagram kommutatív

$$\begin{tikzcd} E \arrow[r, "w"] \arrow[dr, "u"'] & K^J \arrow[d, "v"] \\ & K \end{tikzcd}$$

A 17.9.6. állítás szerint van olyan $(\lambda_i)_{i\in J} \in K^J$, amelyre minden $(x_j)_{j\in J} \in K^J$ esetén $v\left((x_j)_{j\in J}\right) = \sum_{j\in J} \lambda_j x_j$. Ekkor minden $x \in E$ vektorra

$$u(x) = v(w(x)) = v\left((u_j(x))_{j\in J}\right) = \sum_{j\in J} \lambda_j u_j(x),$$

következésképpen $u = \sum_{i\in I} \lambda_i.u_i$. ■

17.9.10. Állítás. *Legyen E véges dimenziós vektortér a K test felett, $n := \dim_K(E)$, és $(e_i)_{i\in n}$ algebrai bázis az E vektortérben, akkor az $(u_i)_{i\in n}$ duális rendszer algebrai bázis az E^* algebrai duálisban.*

Bizonyítás. Az állítás triviálisan igaz, ha $n = 0$. A 17.9.3. állítás c) pontja szerint $n \neq 0$ esetén $\bigcap_{i\in n} \mathrm{Ker}(u_i) = \{\mathbf{0}\}$, így 17.9.9. alapján $(u_i)_{i\in n}$ generátorrendszer E^*-ban. Mivel pedig a 17.9.3. állítás a) pontja szerint $(u_i)_{i\in n}$ lineárisan független is így $(u_i)_{i\in n}$ algebrai bázis E^*-ban. ■

17.9.11. Következmény. *Legyen E véges dimenziós vektortér a K test felett, $n := \dim_K(E)$, és $(u_i)_{i\in n}$ algebrai bázis az E^* vektortérben. Ekkor létezik egyetlen olyan $(e_i)_{i\in n}$ rendszer E-ben, amelyre minden $i, j \in n$ esetén $u_i(e_j) = \delta_{i,j}$. Ez az $(e_i)_{i\in n}$ rendszer algebrai bázis az E vektortérben.*

Bizonyítás. Jelölje $(z_i)_{i\in n}$ az $(u_i)_{i\in n}$ rendszer duálisát, tehát $(z_i)_{i\in n}$ az az E^{**}-ban haladó rendszer, amelyre minden $i, j \in n$ esetén $z_i(u_j) = \delta_{i,j}$. 17.9.8. szerint a $\mathrm{j}_E : E \to E^{**}$ kanonikus lineáris operátor szürjektív, ezért létezik olyan $(e_i)_{i\in n}$ rendszer E-ben, amelyre minden $i \in n$ esetén $z_i = \mathrm{j}_E(e_i)$. Mivel $\mathrm{j}_E : E \to E^{**}$ lineáris bijekció, és 17.9.10. szerint $(z_i)_{i\in n}$ algebrai bázis E^{**}-ban, így 17.5.5. c) alapján $(e_i)_{i\in n}$ algebrai bázis E-ben. Továbbá, minden $i, j \in n$ esetén, a j_E operátor definíciója szerint $u_i(e_j) = \mathrm{j}_E(e_j)(u_i) = z_j(u_i) = \delta_{i,j}$. Ha $(e'_i)_{i\in n}$ szintén olyan rendszer E-ben, amelyre minden $i, j \in n$ esetén $u_i(e'_j) = \delta_{i,j} = u_i(e_j)$, akkor minden $j \in n$ indexre $\mathrm{j}_E(e'_j) \in E^{**}$ olyan, hogy $\mathrm{j}_E(e'_j) = \mathrm{j}_E(e_j)$ az $\{u_i | i \in n\}$ algebrai bázishalmazon, ezért $\mathrm{j}_E(e'_j) = \mathrm{j}_E(e_j)$, így az j_E operátor injektivitása folytán $e'_j = e_j$. ■

A következő tétel pontos formulát ad végtelen dimenziós vektortér duálisának dimenziójára. Ehhez szükségünk lesz egy lemmára.

17.9.12. Lemma. *Legyen K test, és minden $\lambda \in K$ esetén legyen $\mathbf{s}_\lambda := (\lambda^n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$. Ekkor az $(\mathbf{s}_\lambda)_{\lambda\in K}$ rendszer lineárisan független a $K^{\mathbb{N}}$ vektortérben.*

Bizonyítás. Legyen $\Lambda \subseteq K$ nem üres véges halmaz és $(c_\lambda)_{\lambda\in\Lambda} \in K^\Lambda$ tetszőleges olyan rendszer, hogy $\sum\limits_{\lambda\in\Lambda} c_\lambda.\mathbf{s}_\lambda = 0$. Azt kell igazolni, hogy minden $\lambda \in \Lambda$ esetén $c_\lambda = 0$.

A hipotézis szerint minden $n \in \mathbb{N}$ esetén $\sum\limits_{\lambda\in\Lambda} c_\lambda.\lambda^n = 0$ teljesül. Legyen $m := \mathrm{Card}(\Lambda)$ és $\sigma : m \to \Lambda$ bijekció. Ekkor minden $n \in \mathbb{N}$ esetén

$$0 = \sum_{\lambda\in\Lambda} c_\lambda.\lambda^n = \sum_{i=0}^{m-1} c_{\sigma(i)}.\sigma(i)^n.$$

Legyen minden $i \leq m-1$ természetes számra $a_i := \sigma(i)$ és $x_i := c_{\sigma(i)}$. Ekkor $(a_i)_{i\in m} \in K^m$ és $(x_i)_{i\in m} \in K^m$ olyan rendszerek, hogy minden $k \leq m-1$ természetes számra $\sum\limits_{i=0}^{m-1} x_i.a_i^k = 0$, ami úgy is írható, hogy

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ a_0 & a_1 & \dots & a_{m-1} \\ a_0^2 & a_1^2 & \dots & a_{m-1}^2 \\ \vdots & & & \vdots \\ a_0^{m-1} & a_1^{m-1} & \dots & a_{m-1}^{m-1} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{m-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Az itt álló $m \times m$-es mátrix Vandermonde-mátrix (15.2.14.), amelynek determinánsára

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_0 & a_1 & \dots & a_{m-1} \\ a_0^2 & a_1^2 & \dots & a_{m-1}^2 \\ \vdots & & & \vdots \\ a_0^{m-1} & a_1^{m-1} & \dots & a_{m-1}^{m-1} \end{pmatrix} = \underset{\substack{(i,j)\in m\times m \\ i<j}}{\mathrm{P}} (a_j - a_i)$$

teljesül (15.2.15.) tehát az $(a_i)_{i\in m}$ rendszer (vagyis a σ függvény) injektivitása folytán ez a determináns nem 0, ami azt jelenti, hogy ez a mátrix, mint $K^m \to K^m$ lineáris operátor *injektív* (??). Ezért minden $i \leq m-1$ természetes számra $x_i = 0$, ami azt jelenti, hogy minden $\lambda \in \Lambda$ esetén $c_\lambda = 0$, hiszen a σ függvény ráképez Λ-ra. ■

17.9.13. Tétel. (**Erdős–Kaplansky-tétel.**) *Ha E végtelen dimenziós vektortér a K test felett, akkor*

$$\dim(E^*) = \mathrm{Card}(E^*) = (\mathrm{Card}(K))^{\dim(E)}.$$

(**Megjegyzés.** *Itt kardinális hatványról van szó, azaz* $(\mathrm{Card}(K))^{\dim(E)} := \mathrm{Card}(K^{\dim(E)})$.)

Bizonyítás. (I) Először megmutatjuk, hogy

$$\mathrm{Card}(K) \leq \dim(E^*) \leq \mathrm{Card}(E^*) = (\mathrm{Card}(K))^{\dim(E)}.$$

Legyen B bázis az E vektortérben, tehát $\dim(E) = \mathrm{Card}(B)$. A 17.5.13. állítás szerint a $K^{(B)}$ és E vektorterek izomorfak, így $\left(K^{(B)}\right)^*$ és E^* is izomorfak. A 17.9.6. állítás szerint a $\left(K^{(B)}\right)^*$ és K^B vektorterek izomorfak, ezért 17.5.19. alapján $\dim(E^*) = \dim\left(K^B\right)$. Mivel B végtelen halmaz, így vehetünk egy $\sigma : \mathbb{N} \to B$ injekciót (10.1.2.). Vezessük be az

$$u : K^{\mathbb{N}} \to K^B; \quad \mathbf{s} \mapsto \left(\mathbf{s} \circ \sigma^{-1}\right)^\circ$$

leképezést, ahol $\mathbf{s} \in K^{\mathbb{N}}$ esetén $\left(\mathbf{s} \circ \sigma^{-1}\right)^\circ$ jelöli az $\mathbf{s} \circ \sigma^{-1} : \mathrm{Im}(\sigma) \to K$ függvény 0-val vett kiterjesztését $\mathrm{Im}(\sigma)$-ról B-re. Világos, hogy u lineáris injekció, ezért a $K^{\mathbb{N}}$ és $\mathrm{Im}(\sigma)$ vektorterek izomorfak, tehát $\dim(K^{\mathbb{N}}) = \dim(\mathrm{Im}(\sigma)) \leq \dim\left(K^B\right) = \dim(E^*)$. Az előző lemma szerint $\mathrm{Card}(K) \leq \dim(K^{\mathbb{N}})$, következésképpen $\mathrm{Card}(K) \leq \dim(E^*)$. Ugyanakkor $\dim(E^*) = \dim\left(K^B\right) \leq \mathrm{Card}(K^B) = (\mathrm{Card}(K))^{\mathrm{Card}(B)} = (\mathrm{Card}(K))^{\dim(E)}$. Ugyanakkor E^* ekvipotens K^B-vel, ezért $\mathrm{Card}(E^*) = \mathrm{Card}(K^B)$.

(II) A 17.5.20. állítást alkalmazva az E^* végtelen dimenziós vektortérre kapjuk, hogy E^* ekvipotens a $\dim(E^*) \times K$ halmazzal. Az (I) bekezdés szerint K kisebb-egyenlő számosságú $\dim(E^*$-nál, ezért $\dim(E^*) \times K$ kisebb-egyenlő számosságú $\dim(E^*) \times \dim(E^*)$-nál, ami a számosságaritmetika alaptétele szerint ekvipotens $\dim(E^*)$-gal. Tehát $\mathrm{Card}(E^*) \leq \dim(E^*)$ is teljesül, így a Schröder–Bernstein-tétel (6.5.5.) alkalmazásával kapjuk a bizonyítandó egyenlőségeket. ■

17.9.14. Következmény. *Ha E végtelen dimenziós vektortér, akkor* $\dim(E) < \dim(E^*)$, *és a $\mathrm{j}_E : E \to E^{**}$ kanonikus lineáris operátor nem szürjektív.*

Bizonyítás. Mivel minden test legalább két elemű, így K-val jelölve azt a testet, amely felett E végtelen dimenziós vektortér, az Erdős–Kaplansky-tétel alkalmazásával kapjuk, hogy

$$\dim(E^*) = (\mathrm{Card}(K))^{\dim(E)} \geq 2^{\dim(E)} = \mathrm{Card}(\mathscr{P}(E)),$$

és természetesen $\dim(E) \leq \mathrm{Card}(E)$, és a Cantor-tétel alapján $\mathrm{Card}(\mathscr{P}(E)) > \mathrm{Card}(E)$, ezért $\dim(E^*) > \dim(E)$.

Ebből következik, hogy minden végtelen dimenziós E vektortérre $\dim(E^*) < \dim(E^{**})$, tehát $\dim(E) < \dim(E^{**})$, így a $\mathrm{j}_E : E \to E^{**}$ kanonikus lineáris operátor nem lehet szürjektív, különben lineáris izomorfizmus volna, így 17.5.19. szerint $\dim(E) = \dim(E^{**})$ teljesülne. ■

17.10. Lineáris operátor mátrixai

17.10.1. Állítás. *Legyenek E és F vektorterek a K test felett, $\mathbf{e} := (e_j)_{j \in J}$ bázis E-ben és $\mathbf{f} := (f_i)_{i \in I}$ bázis F-ben. Ekkor minden $u \in \mathbf{L}(E; F)$ operátorhoz létezik egyetlen olyan $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) = (m_{i,j})_{(i,j) \in I \times J} \in \mathrm{M}_{I,J}(K)$ mátrix, amelyre teljesülnek a következők:*

a) *minden $j \in J$ esetén $(m_{i,j})_{i \in I} \in K^{(I)}$, vagyis az $\{i \in I | m_{i,j} \neq 0\}$ halmaz véges, tehát $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) \in \dot{\mathrm{M}}_{I,J}(K)$ (15.1.5.);*

b) *minden $j \in J$ esetén $u(e_j) = \sum_{i \in I} m_{i,j} . f_i$.*

Továbbá, az $\dot{\mathrm{M}}_{I,J}(K) = \{(m_{i,j})_{(i,j)\in I\times J} \in \mathrm{M}_{I,J}(K) \mid (\forall j \in J) : (m_{i,j})_{i\in I} \in K^{(I)}\}$ *halmaz lineáris altere az* $\mathrm{M}_{I,J}(K)$ *vektortérnek, és az*

$$\mathbf{L}(E;F) \to \dot{\mathrm{M}}_{I,J}(K); \quad u \mapsto \mathrm{M}_{\mathbf{f},\mathbf{e}}(u) \tag{$*$}$$

leképezés izomorfizmus az $\mathbf{L}(E;F)$ *és* $\dot{\mathrm{M}}_{I,J}(K)$ *vektorterek között.*

Bizonyítás. Legyen $u \in \mathbf{L}(E;F)$. Minden $j \in J$ esetén $u(e_j) \in F$, és mivel $(f_i)_{i\in I}$ bázis F-ben, így létezik egyetlen olyan $(m_{i,j})_{i\in I} \in K^{(I)}$ rendszer, amelyre $u(e_j) = \sum_{i\in I} m_{i,j}.f_i$. Ezzel a b) feltételnek eleget tevő $(m_{i,j})_{(i,j)\in I\times J} \in \mathrm{M}_{I,J}(K)$ mátrix egyértelmű létezését beláttuk, és világos, hogy erre a) is teljesül, tehát ez a mátrix eleme $\dot{\mathrm{M}}_{I,J}(K)$-nak.

Legyen $m := (m_{i,j})_{(i,j)\in I\times J} \in \dot{\mathrm{M}}_{I,J}(K)$ és $m' := \left(m'_{i,j}\right)_{(i,j)\in I\times J} \in \dot{\mathrm{M}}_{I,J}(K)$. Ekkor minden $j \in J$ esetén $\{i \in I | m_{i,j} + m'_{i,j} \neq 0\} \subseteq \{i \in I | m_{i,j} \neq 0\} \cup \{i \in I | m'_{i,j} \neq 0\}$, ezért $\{i \in I | m_{i,j} + m'_{i,j} \neq 0\}$ véges halmaz. Mivel $m + m' = \left(m_{i,j} + m'_{i,j}\right)_{(i,j)\in I\times J}$, így $m + m' \in \dot{\mathrm{M}}_{I,J}(K)$.

Legyen $m := (m_{i,j})_{(i,j)\in I\times J} \in \dot{\mathrm{M}}_{I,J}(K)$ és $\lambda \in K$. Ekkor minden $j \in J$ esetén $\{i \in I | \lambda m_{i,j} \neq 0\} \subseteq \{i \in I | m_{i,j} \neq 0\}$, ezért $\{i \in I | \lambda m_{i,j} \neq 0\}$ véges halmaz. Mivel $\lambda.m = (\lambda m_{i,j})_{(i,j)\in I\times J}$, így $\lambda.m \in \dot{\mathrm{M}}_{I,J}(K)$.

Mivel a K feletti $I\times J$-es 0 mátrix nyilvánvalóan eleme $\dot{\mathrm{M}}_{I,J}(K)$-nak, vagyis $\dot{\mathrm{M}}_{I,J}(K) \neq \emptyset$, így $\dot{\mathrm{M}}_{I,J}(K)$ lineáris altere az $\mathrm{M}_{I,J}(K)$ vektortérnek.

Most megmutatjuk, hogy a $(*)$ leképezés *bijekció*. Ez a leképezés injektív, mert ha $u, u' \in \mathbf{L}(E;F)$ olyanok, hogy $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) = (m_{i,j})_{(i,j)\in I\times J} = \mathrm{M}_{\mathbf{f},\mathbf{e}}(u')$, akkor minden $j \in J$ indexre $u(e_j) = \sum_{i\in I} m_{i,j}.f_i = u'(e_j)$, következésképpen $u = u'$ az $\{e_j | j \in J\}$ halmazon, amely generátorhalmaz E-ben, így u és u' linearitása folytán $u = u'$. A $(*)$ leképezés szürjektivitásának bizonyításához legyen $(m_{i,j})_{i\in I} \in \dot{\mathrm{M}}_{I,J}(K)$ rögzítve. Ekkor minden $j \in J$ esetén $(m_{i,j})_{i\in I} \in K^{(I)}$, ezért jól értelmezett a $\sum_{i\in I} m_{i,j}.f_i \in F$ vektor, tehát 17.7.3. alapján egyértelműen létezik olyan $u \in \mathbf{L}(E;F)$, amelyre minden $j \in J$ esetén $u(e_j) = \sum_{i\in I} m_{i,j}.f_i$, vagyis b) teljesül. Ez azt jelenti, hogy $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) = (m_{i,j})_{(i,j)\in I\times J}$, tehát a $(*)$ leképezés szürjektív.

Végül igazoljuk a $(*)$ leképezés linearitását. Legyenek $u, u' \in \mathbf{L}(E;F)$ és $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) = (m_{i,j})_{(i,j)\in I\times J}$, valamint $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u') = \left(m'_{i,j}\right)_{(i,j)\in I\times J}$. Ha $j \in J$, akkor

$$(u+u')(e_j) = u(e_j) + u'(e_j) = \left(\sum_{i\in I} m_{i,j}.f_i\right) + \left(\sum_{i\in I} m'_{i,j}.f_i\right) = \sum_{i\in I}(m_{i,j} + m'_{i,j}).f_i,$$

és a mátrixok összeadásának definíciója szerint $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) + \mathrm{M}_{\mathbf{f},\mathbf{e}}(u') = \left(m_{i,j} + m'_{i,j}\right)_{(i,j)\in I\times J}$. Minden $j \in J$ esetén $\{i \in I | m_{i,j} + m'_{i,j} \neq 0\} \subseteq \{i \in I | m_{i,j} \neq 0\} \cup \{i \in I | m'_{i,j} \neq 0\}$, és itt a jobb oldalon véges halmaz áll, ezért $\left(m_{i,j} + m'_{i,j}\right)_{(i,j)\in I\times J} \in \dot{\mathrm{M}}_{I,J}(K)$. Ebből látható, hogy $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u+u') = \mathrm{M}_{\mathbf{f},\mathbf{e}}(u) + \mathrm{M}_{\mathbf{f},\mathbf{e}}(u')$, tehát a $(*)$ leképezés additív.

Legyenek $u \in \mathbf{L}(E;F)$ és $\lambda \in K$, valamint $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) = (m_{i,j})_{(i,j)\in I\times J}$. Ha $j \in J$, akkor

$$(\lambda.u)(e_j) = \lambda.u(e_j) = \lambda.\sum_{i\in I} m_{i,j}.f_i = \sum_{i\in I}(\lambda m_{i,j}).f_i,$$

és mátrix K-beli elemmel vett szorzásának definíciója szerint $\lambda.\mathrm{M}_{\mathbf{e},\mathbf{f}}(u) = (\lambda m_{i,j})_{(i,j)\in I\times J}$. Minden $j \in J$ esetén $\{i \in I | \lambda m_{i,j} \neq 0\} \subseteq \{i \in I | m_{i,j} \neq 0\}$, és itt a jobb oldalon véges halmaz áll, ezért $(\lambda m_{i,j})_{(i,j)\in I\times J} \in \dot{\mathrm{M}}_{I,J}(K)$. Ebből látható, hogy $\mathrm{M}_{\mathbf{f},\mathbf{e}}(\lambda u) = \lambda \mathrm{M}_{\mathbf{f},\mathbf{e}}(u)$, tehát a $(*)$ leképezés K-homogén. ■

17.10.2. Definíció. *Legyenek E és F vektorterek a K test felett. Ha I és J halmazok, valamint $\mathbf{e} = (e_j)_{j\in J}$ bázis E-ben és $\mathbf{f} = (f_i)_{i\in I}$ bázis F-ben, akkor minden $u \in \mathbf{L}(E;F)$ lineáris operátorra $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u)$ jelöli azt az $(m_{i,j})_{(i,j)\in I\times J} \in \dot{\mathrm{M}}_{I,J}(K)$ mátrixot, amelyre teljesül az, hogy minden $j \in J$ esetén $u(e_j) = \sum_{i\in I} m_{i,j}.f_i$, és azt mondjuk, hogy $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u)$ az u* **operátor mátrixa** *az* **e** *és* **f** **bázisok szerint**. *Ha* **e** *bázis az E vektortérben és $u \in \mathbf{L}(E;E)$, akkor azt mondjuk, hogy $\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$ az u* **operátor mátrixa** *az* **e bázisban**.

17.10.3. Állítás. *Legyenek E, F és G vektorterek a K test felett. Ha* **e** *bázis E-ben,* **f** *bázis F-ben és* **g** *bázis G-ben, akkor minden $u \in \mathbf{L}(E;F)$ és $v \in \mathbf{L}(F;G)$ lineáris operátorra*

$$\mathrm{M}_{\mathbf{g},\mathbf{e}}(v \circ u) = \mathrm{M}_{\mathbf{g},\mathbf{f}}(v) \cdot \mathrm{M}_{\mathbf{f},\mathbf{e}}(u).$$

Bizonyítás. Legyenek $\mathbf{e} = (e_j)_{j\in J}$, $\mathbf{f} = (f_i)_{i\in I}$ és $\mathbf{g} = (g_l)_{l\in L}$. Legyen továbbá $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) = (m_{i,j})_{(i,j)\in I\times J}$ és $\mathrm{M}_{\mathbf{g},\mathbf{f}}(v) = (n_{l,i})_{(l,i)\in L\times I}$. Ekkor minden $j \in J$ esetén

$$\begin{aligned}(v \circ u)(e_j) = v(u(e_j)) = v\Big(\sum_{i\in I} m_{i,j}.f_i\Big) = \sum_{i\in I} m_{i,j}.v(f_i) = \sum_{i\in I} m_{i,j}.\Big(\sum_{l\in L} n_{l,i}.g_l\Big) = \\ = \sum_{i\in I}\Big(\sum_{l\in L}(m_{i,j}n_{l,i}).g_l\Big) = \sum_{l\in L}\Big(\sum_{i\in I}(n_{l,i}m_{i,j}).g_l\Big) = \sum_{l\in L}\Big(\sum_{i\in I} n_{l,i}m_{i,j}\Big).g_l.\end{aligned}$$

Mivel $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) \in \dot{\mathrm{M}}_{I,J}(K)$ és $\mathrm{M}_{\mathbf{g},\mathbf{f}}(u) \in \dot{\mathrm{M}}_{L,I}(K)$, így 15.1.9. szerint

$$\Big(\sum_{i\in I} n_{l,i}m_{i,j}\Big)_{(l,j)\in L\times J} = \mathrm{M}_{\mathbf{g},\mathbf{f}}(v) \cdot \mathrm{M}_{\mathbf{f},\mathbf{e}}(u) \in \dot{\mathrm{M}}_{L,J}(K).$$

Ebből következik, hogy $\mathrm{M}_{\mathbf{g},\mathbf{e}}(v \circ u) = \mathrm{M}_{\mathbf{g},\mathbf{f}}(v) \cdot \mathrm{M}_{\mathbf{f},\mathbf{e}}(u)$. ■

17.10.4. Tétel. *Ha E vektortér a K test felett és $\mathbf{e} = (e_j)_{j\in J}$ bázis E-ben, akkor az*

$$\mathbf{L}(E;E) \to \dot{\mathrm{M}}_I(K); \quad u \mapsto \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$$

leképezés izomorfizmus az $\mathbf{L}(E;E)$ operátorgyűrű és az $\dot{\mathrm{M}}_I(K)$ mátrixgyűrű között.

Bizonyítás. A 17.10.1. állítás alapján a szóban forgó leképezés morfizmus az $\mathbf{L}(E;E)$ és $\dot{\mathrm{M}}_I(K)$ gyűrűk összeadása szerint, és az előző állítás alapján a szóban forgó leképezés morfizmus az $\mathbf{L}(E;E)$ és $\dot{\mathrm{M}}_I(K)$ gyűrűk szorzása szerint. Ugyanakkor ez a leképezés bijekció (17.10.1.), így izomorfizmus az $\mathbf{L}(E;E)$ operátorgyűrű és az $\dot{\mathrm{M}}_I(K)$ mátrixgyűrű között. ■

17.10.5. Következmény. *Ha E vektortér a K test felett és $\mathbf{e} = (e_j)_{j\in J}$ bázis E-ben, akkor minden $u \in \mathbf{L}(E;E)$ esetén $u \in \mathbf{GL}(E)$ pontosan akkor teljesül, ha az $\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$ mátrix invertálható az $\dot{\mathrm{M}}_I(K)$ egységelemes mátrixgyűrűben, és ha $u \in \mathbf{GL}(E)$, akkor*

$$(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))^{-1} = \mathrm{M}_{\mathbf{e},\mathbf{e}}(u^{-1}).$$

Bizonyítás. Az előző tétel és a 14.1.5. definíció után álló megjegyzés nyilvánvaló következménye, hiszen $\mathbf{GL}(E)$ az $\mathbf{L}(E;E)$ gyűrű invertálható elemeinek halmaza. ■

17.10.6. Következmény. *Legyenek E és F vektorterek a K test felett, továbbá $\mathbf{e} = (e_j)_{j\in J}$ és $\mathbf{e}' = (e'_j)_{j\in J}$ bázisok E-ben, valamint $\mathbf{f} := (f_i)_{i\in I}$ és $\mathbf{f}' := (f'_i)_{i\in I}$ bázisok F-ben. Legyenek $v \in \mathbf{L}(E;E)$ és $w \in \mathbf{L}(F;F)$ azok a lineáris operátorok, amelyekre minden $j \in J$ esetén $v(e_j) = e'_j$, és minden $i \in I$ esetén $w(f_i) = f'_i$. Ekkor $v \in \mathbf{GL}(E)$ és $w \in \mathbf{GL}(F)$, továbbá minden $u \in \mathbf{L}(E;F)$ lineáris operátorra*

$$\mathrm{M}_{\mathbf{f}',\mathbf{f}'}(w)\cdot \mathrm{M}_{\mathbf{f}',\mathbf{e}'}(u)\cdot (\mathrm{M}_{\mathbf{e}',\mathbf{e}'}(v))^{-1} = \mathrm{M}_{\mathbf{f},\mathbf{e}}(u),$$
$$(\mathrm{M}_{\mathbf{f},\mathbf{f}}(w))^{-1}\cdot \mathrm{M}_{\mathbf{f},\mathbf{e}}(u)\cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(v) = \mathrm{M}_{\mathbf{f}',\mathbf{e}'}(u).$$

Bizonyítás. A v és w operátorok nyilvánvalóan lineáris bijekciók, és természetesen minden $j \in J$ esetén $v^{-1}(e'_j) = e_j$, és minden $i \in I$ esetén $w^{-1}(f'_i) = f_i$.
Legyen $\mathrm{M}_{\mathbf{f},\mathbf{e}}(u) = (m_{i,j})_{(i,j)\in I\times J}$. Ekkor minden $j \in J$ esetén

$$\left(w\circ u\circ v^{-1}\right)(e'_j) = w(u(e_j)) = w\Big(\sum_{i\in I} m_{i,j}.f_i\Big) = \sum_{i\in I} m_{i,j}.w(f_i) = \sum_{i\in I} m_{i,j}.f'_i,$$

ami azt jelenti, hogy $\mathrm{M}_{\mathbf{f}',\mathbf{e}'}(w\circ u\circ v^{-1}) = (m_{i,j})_{(i,j)\in I\times J} = \mathrm{M}_{\mathbf{f},\mathbf{e}}(u)$. Ebből 17.10.3. és 17.10.5. alapján kapjuk az első bizonyítandó egyenlőséget.
Legyen $\mathrm{M}_{\mathbf{f}',\mathbf{e}'}(u) = \left(m'_{i,j}\right)_{(i,j)\in I\times J}$. Ekkor minden $j \in J$ esetén

$$\left(w^{-1}\circ u\circ v\right)(e_j) = w(u(e'_j)) = w^{-1}\Big(\sum_{i\in I} m'_{i,j}.f'_i\Big) = \sum_{i\in I} m'_{i,j}.w^{-1}(f'_i) = \sum_{i\in I} m'_{i,j}.f_i,$$

ami azt jelenti, hogy $\mathrm{M}_{\mathbf{f},\mathbf{e}}(w^{-1}\circ u\circ v) = \left(m'_{i,j}\right)_{(i,j)\in I\times J} = \mathrm{M}_{\mathbf{f}',\mathbf{e}'}(u)$. Ebből 17.10.3. és 17.10.5. alapján kapjuk a második bizonyítandó egyenlőséget. ■

17.10.7. Következmény. *Legyen E vektortér a K test felett, továbbá $\mathbf{e} = (e_i)_{i\in I}$ és $\mathbf{f} = (f_i)_{i\in I}$ bázisok E-ben. Legyen $v \in \mathbf{L}(E;E)$ az a lineáris operátor, amelyre minden $i \in I$ esetén $v(e_i) = f_i$. Ekkor $v \in \mathbf{GL}(E)$, és minden $u \in \mathbf{L}(E;E)$ lineáris operátorra*

$$\mathrm{M}_{\mathbf{f},\mathbf{f}}(u) = (\mathrm{M}_{\mathbf{e},\mathbf{e}}(v))^{-1}\cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(v), \mathrm{M}_{\mathbf{e},\mathbf{e}}(u) = \mathrm{M}_{\mathbf{f},\mathbf{f}}(v)\cdot \mathrm{M}_{\mathbf{f},\mathbf{f}}(u)\cdot (\mathrm{M}_{\mathbf{f},\mathbf{f}}(v))^{-1}.$$

Bizonyítás. Legyen $\mathrm{M}_{\mathbf{f},\mathbf{f}}(u) = (n_{i,j})_{(i,j)\in I\times I}$. Ekkor minden $j \in I$ esetén

$$(v^{-1}\circ u\circ v)(e_j) = v^{-1}(u(f_j)) = v^{-1}\Big(\sum_{i\in I} n_{i,j}.f_i\Big) = \sum_{i\in I} n_{i,j}.v^{-1}(f_i) = \sum_{i\in I} n_{i,j}.e_i,$$

tehát $\mathrm{M}_{\mathbf{e},\mathbf{e}}(v^{-1}\circ u\circ v) = (n_{i,j})_{(i,j)\in I\times I} = \mathrm{M}_{\mathbf{f},\mathbf{f}}(u)$, és 17.10.3. és 17.10.5. alapján a bal oldalon $(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v))^{-1}\cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(v)$ áll.
Legyen $\mathrm{M}_{\mathbf{e},\mathbf{e}}(u) = (m_{i,j})_{(i,j)\in I\times I}$. Ekkor minden $j \in I$ esetén

$$(v\circ u\circ v^{-1})(f_j) = v(u(e_j)) = v\Big(\sum_{i\in I} m_{i,j}.e_i\Big) = \sum_{i\in I} m_{i,j}.v(e_i) = \sum_{i\in I} m_{i,j}.f_i,$$

tehát $\mathrm{M}_{\mathbf{f},\mathbf{f}}(v\circ u\circ v^{-1}) = (m_{i,j})_{(i,j)\in I\times I} = \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$, és 17.10.3. és 17.10.5. alapján a bal oldalon $\mathrm{M}_{\mathbf{f},\mathbf{f}}(v)\cdot \mathrm{M}_{\mathbf{f},\mathbf{f}}(u)\cdot (\mathrm{M}_{\mathbf{f},\mathbf{f}}(v))^{-1}$ áll. ■

17.10.8. Következmény. *Legyenek E és F vektorterek a K test felett, $u \in \mathbf{L}(E;E)$, és tegyük fel, hogy $v \in \mathbf{L}(E;F)$ lineáris bijekció. Ha $\mathbf{e}$ bázis E-ben és $\mathbf{f}$ bázis F-ben, akkor*

$$\mathrm{M}_{\mathbf{e},\mathbf{f}}\left(v^{-1}\right)\mathrm{M}_{\mathbf{f},\mathbf{f}}\left(v\circ u\circ v^{-1}\right)\mathrm{M}_{\mathbf{f},\mathbf{e}}(v)=\mathrm{M}_{\mathbf{e},\mathbf{e}}(u).$$

Bizonyítás. A 17.10.3. állítás szerint

$$\mathrm{M}_{\mathbf{f},\mathbf{f}}\left(v\circ u\circ v^{-1}\right)\mathrm{M}_{\mathbf{f},\mathbf{e}}(v)=\mathrm{M}_{\mathbf{f},\mathbf{e}}\left(\left(v\circ u\circ v^{-1}\right)\circ v\right)=\mathrm{M}_{\mathbf{f},\mathbf{e}}(v\circ u),$$

és ismét alkalmazva a 17.10.3. állítást kapjuk, hogy

$$\mathrm{M}_{\mathbf{e},\mathbf{f}}\left(v^{-1}\right)\mathrm{M}_{\mathbf{f},\mathbf{e}}(v\circ u)=\mathrm{M}_{\mathbf{e},\mathbf{e}}\left(v^{-1}\circ(v\circ u)\right)=\mathrm{M}_{\mathbf{e},\mathbf{e}}(u).$$

Ebből a két egyenlőségből, a mátrixszorzás asszociativitása 15.1.9. alapján kapjuk a bizonyítandó egyenlőséget. ■

17.11. Lineáris operátor determinánsa és nyoma

17.11.1. Lemma. *Legyen E véges dimenziós vektortér a K test felett, és legyen $n := \dim(E) > 0$. Ha $\mathbf{e} = (e_i)_{i\in n}$ és $\mathbf{f} = (f_i)_{i\in n}$ bázisok E-ben, akkor minden $u : E \to E$ lineáris operátorra*

$$\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right)=\det\left(\mathrm{M}_{\mathbf{f},\mathbf{f}}(u)\right).$$

Bizonyítás. Ha v jelöli azt az $E \to E$ lineáris operátort, amelyre minden $i \in n$ esetén $v(e_i) = f_i$, akkor a 17.10.7. állítás szerint $v \in \mathbf{GL}(E)$, és

$$\mathrm{M}_{\mathbf{f},\mathbf{f}}(u)=\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v)\right)^{-1}\cdot\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\cdot\mathrm{M}_{\mathbf{e},\mathbf{e}}(v),$$

amiből 15.2.4. és 15.2.5. alapján kapjuk, hogy

$$\det\left(\mathrm{M}_{\mathbf{f},\mathbf{f}}(u)\right)=\left(\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v)\right)\right)^{-1}\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right)\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v)\right)=\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right). \blacksquare$$

Az előző lemma szerint értelmes a következő definíció.

17.11.2. Definíció. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) > 0$. Minden $u : E \to E$ lineáris operátorra*

$$\det(u):=\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right),$$

ahol $\mathbf{e}$ tetszőleges bázis az E vektortérben. Ha $u : E \to E$ lineáris operátor, akkor a $\det(u) \in K$ elemet az u **lineáris operátor determinánsának** *nevezzük.*

17.11.3. Állítás. *Legyen E véges dimenziós vektortér a K test felett, és tegyük fel, hogy $n := \dim(E) > 0$.*

a) *Minden $u : E \to E$ lineáris operátorra és $\lambda \in K$ elemre*

$$\det(\lambda.u)=\lambda^n\det(u).$$

b) *Minden $u, v : E \to E$ lineáris operátorra*

$$\det(v\circ u)=\det(v)\det(u).$$

c) *Minden $u \in \mathbf{GL}(E)$ esetén $\det(u) \in K \setminus \{0\}$ és*

$$\det\left(u^{-1}\right)=\left(\det(u)\right)^{-1}.$$

d) *Ha F vektortér és $v : E \to F$ lineáris bijekció, akkor minden $u : E \to E$ lineáris operátorra*

$$\det\left(v\circ u\circ v^{-1}\right)=\det(u).$$

Bizonyítás. a) Legyen $\mathbf{e}$ bázis az E vektortérben. A 17.10.1. állítás szerint az $\mathbf{L}(E;E) \to \mathrm{M}_n(K)$; $u \mapsto \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$ leképezés K-homogén, tehát, ha $u \in \mathbf{L}(E;E)$ és $\lambda \in L$, akkor $\mathrm{M}_{\mathbf{e},\mathbf{e}}(\lambda.u) = \lambda.\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$, így a lineáris operátor determinánsának definíciója szerint

$$\det(\lambda.u) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(\lambda.u)\right) = \det\left(\lambda.\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) = \lambda^n \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) = \lambda^n \det(u),$$

ahol felhasználtuk a 15.2.2. állítást.

b) Legyen $\mathbf{e}$ bázis az E vektortérben. A 17.10.3. állítás szerint $u, v \in \mathbf{L}(E;E)$ esetén $\mathrm{M}_{\mathbf{e},\mathbf{e}}(v \circ u) = \mathrm{M}_{\mathbf{e},\mathbf{e}}(v) \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$, ezért a lineáris operátor determinánsának definíciója szerint

$$\begin{aligned}\det(v \circ u) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v \circ u)\right) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v) \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) = \\ = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v)\right) \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) = \det(v)\det(u),\end{aligned}$$

ahol felhasználtuk a 15.2.4. állítást.

c) Legyen $\mathbf{e}$ bázis az E vektortérben. A 17.10.5. állítás szerint $u \in \mathbf{GL}(E)$ esetén az $\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$ mátrix invertálható az $\mathrm{M}_n(K)$ egységelemes mátrixgyűrűben és $(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))^{-1} = \mathrm{M}_{\mathbf{e},\mathbf{e}}(u^{-1})$, ezért 15.2.5. alapján a $\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) \in K$ elem invertálható K-ban, vagyis nem 0, tehát a lineáris operátor determinánsának definíciója szerint

$$\det\left(u^{-1}\right) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u^{-1})\right) = \det\left((\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))^{-1}\right) = \left(\det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right)\right)^{-1} = (\det(u))^{-1}.$$

d) A hipotézis szerint $\dim(F) = n$, hiszen E és F lineárisan izomorfak és $\dim(E) = n$. Legyen $\mathbf{e} := (e_i)_{i\in n}$ bázis az E vektortérben és $\mathbf{f} := (f_i)_{i\in n}$ bázis az F vektortérben. A 17.10.8. állítás szerint

$$\mathrm{M}_{\mathbf{e},\mathbf{f}}\left(v^{-1}\right) \mathrm{M}_{\mathbf{f},\mathbf{f}}\left(v \circ u \circ v^{-1}\right) \mathrm{M}_{\mathbf{f},\mathbf{e}}(v) = \mathrm{M}_{\mathbf{e},\mathbf{e}}(u),$$

ugyanakkor az itt álló mátrixok mindegyike $n \times n$-es, K-beli együtthatós mátrix, így 15.2.4. alapján kapjuk, hogy

$$\det\left(\mathrm{M}_{\mathbf{e},\mathbf{f}}\left(v^{-1}\right)\right) \det\left(\mathrm{M}_{\mathbf{f},\mathbf{f}}\left(v \circ u \circ v^{-1}\right)\right) \det\left(\mathrm{M}_{\mathbf{f},\mathbf{e}}(v)\right) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right).$$

A definíció szerint $\det\left(v \circ u \circ v^{-1}\right) = \det\left(\mathrm{M}_{\mathbf{f},\mathbf{f}}\left(v \circ u \circ v^{-1}\right)\right)$ és $\det(u) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right)$, ezért ez azt jelenti, hogy

$$\det\left(\mathrm{M}_{\mathbf{e},\mathbf{f}}\left(v^{-1}\right)\right) \det\left(v \circ u \circ v^{-1}\right) \det\left(\mathrm{M}_{\mathbf{f},\mathbf{e}}(v)\right) = \det(u) \qquad (*).$$

A 17.10.3. állítás szerint $\mathrm{M}_{\mathbf{e},\mathbf{f}}\left(v^{-1}\right) \mathrm{M}_{\mathbf{f},\mathbf{e}}(v) = \mathrm{M}_{\mathbf{e},\mathbf{e}}\left(v^{-1} \circ v\right) = \mathrm{M}_{\mathbf{e},\mathbf{e}}\left(\mathrm{id}_E\right)$, ezért 15.2.4. alkalmazásával

$$\det\left(\mathrm{M}_{\mathbf{e},\mathbf{f}}\left(v^{-1}\right)\right) \det\left(\mathrm{M}_{\mathbf{f},\mathbf{e}}(v)\right) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}\left(\mathrm{id}_E\right)\right) = 1$$

adódik, amit a $(*)$ egyenlőségbe helyettesítve kapjuk a bizonyítandó összefüggést. ■

17.11.4. Lemma. *Legyen E véges dimenziós vektortér a K test felett, és legyen $n := \dim(E) > 0$. Ha $\mathbf{e} = (e_i)_{i\in n}$ és $\mathbf{f} = (f_i)_{i\in n}$ bázisok E-ben, akkor minden $u : E \to E$ lineáris operátorra*

$$\mathrm{tr}\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) = \mathrm{tr}\left(\mathrm{M}_{\mathbf{f},\mathbf{f}}(u)\right).$$

Bizonyítás. A 17.10.7. állítás szerint $\mathrm{M}_{\mathbf{f},\mathbf{f}}(u) = (\mathrm{M}_{\mathbf{e},\mathbf{e}}(v))^{-1} \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(u) \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(v)$, ahol $v : E \to E$ az a lineáris bijekció, amelyre minden $i \in n$ esetén $v(e_i) = f_i$, ezért 15.3.3. alapján

$$\mathrm{tr}\left(\mathrm{M}_{\mathbf{f},\mathbf{f}}(u)\right) = \mathrm{tr}\left((\mathrm{M}_{\mathbf{e},\mathbf{e}}(v))^{-1} \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(u) \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(v)\right) = \mathrm{tr}\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right). \blacksquare$$

Az előző lemma szerint értelmes a következő definíció.

17.11.5. Definíció. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) > 0$. Ekkor minden $u : E \to E$ lineáris operátorra*

$$\mathrm{tr}(u) := \mathrm{tr}\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right),$$

ahol **e** *tetszőleges bázis E-ben, és a $\mathrm{tr}(u) \in K$ elemet az u* **operátor nyomának** *nevezzük.*

Természetesen itt nem önmagával való definícióról van szó, mert a definiáló egyenlőség jobb oldalán test feletti mátrix nyomának definíciója szerepel, amit a 15.3.1.-ban értelmeztünk.

17.11.6. Állítás. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) > 0$. Ekkor az*

$$\mathbf{L}(E) \to K; \quad u \mapsto \mathrm{tr}(u)$$

leképezés olyan lineáris operátor, hogy minden $u, v \in \mathbf{L}(E)$ esetén

$$\mathrm{tr}(u \circ v) = \mathrm{tr}(v \circ u).$$

Bizonyítás. Ha **e** bázis az E vektortérben, akkor a definíció szerint az $\mathbf{L}(E) \to K;\ u \mapsto \mathrm{tr}(u)$ leképezés egyenlő az $\mathbf{L}(E) \to \mathrm{M}_n(K);\ u \mapsto \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$ és az $\mathrm{M}_n(K) \to K$ nyom-forma kompozíciójával, és az előbbi 17.10.1. alapján lineáris operátor, míg az utóbbi 15.3.2. alapján lineáris funkcionál. Ezért az $\mathbf{L}(E) \to K;\ u \mapsto \mathrm{tr}(u)$ leképezés lineáris.

Ha **e** bázis az E vektortérben és $u, v \in \mathbf{L}(E)$, akkor 17.10.3. és 15.3.2. alapján

$$\mathrm{tr}(u \circ v) = \mathrm{tr}\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u \circ v)\right) = \mathrm{tr}\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u) \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(v)\right) =$$
$$= \mathrm{tr}\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v) \cdot \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) = \mathrm{tr}\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(v \circ u)\right) = \mathrm{tr}(v \circ u). \blacksquare$$

17.11.7. Következmény. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) > 0$. Ha $u, v \in \mathbf{L}(E)$ és $v \in \mathbf{GL}(E)$, akkor*

$$\mathrm{tr}(v^{-1} \circ u \circ v) = \mathrm{tr}(u).$$

Bizonyítás. Az előző állítás alkalmazásával kapjuk, hogy

$$\mathrm{tr}(v^{-1} \circ u \circ v) = \mathrm{tr}((v^{-1} \circ u) \circ v) = \mathrm{tr}(v \circ (v^{-1} \circ u)) = \mathrm{tr}((v \circ v^{-1}) \circ u) = \mathrm{tr}(\mathrm{id}_E \circ u) = \mathrm{tr}(u),$$

amit bizonyítani kellett. $\blacksquare$

17.12. Lineáris operátor karakterisztikus polinomja

17.12.1. Állítás. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) > 0$. Ha $u : E \to E$ lineáris operátor, akkor a következő állítások ekvivalensek.*

(i) *Az u operátor bijekció.*

(ii) *Az u operátor injekció.*

(iii) *Az u operátor szürjekció.*

(iv) $\det(u) \neq 0$.

Bizonyítás. Az (i), (ii) és (iii) állítások 17.6.4. szerint ekvivalensek. Ugyanakkor (i) azt jelenti, hogy $u \in \mathbf{GL}(E)$, ami 17.10.5. alapján azzal ekvivalens, hogy $\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$ invertálható elem az $\mathrm{M}_n(K)$ mátrixgyűrűben, ahol $\mathbf{e}$ tetszőleges bázis E-ben. A 15.4.9. állítás alapján $\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)$ invertálhatósága az $\mathrm{M}_n(K)$ mátrixgyűrűben azzal ekvivalens, hogy a $\det(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))$ elemnek létezik inverze K-ban a szorzás szerint, vagyis $\det(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)) \neq 0$, hiszen K test. Mivel a definíció szerint $\det(u) = \det(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))$, így (i) és (iv) ekvivalensek. ∎

A következő állítás előtt emlékeztetünk arra, hogy ha E vektortér a K test felett és $u : E \to E$ lineáris operátor, akkor $\mathrm{S}(u)$ jelöli u *sajátértékeinek* halmazát, tehát $\mathrm{S}(u)$ azon $\lambda \in K$ elemek halmaza, amelyekhez van olyan $x \in E$, hogy $x \neq 0$ és $u(x) = \lambda.x$ (17.8.1.).

17.12.2. Következmény. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) > 0$. Ha $u : E \to E$ lineáris operátor, akkor $\lambda \in \mathrm{S}(u)$ pontosan akkor teljesül, ha* $\det(\lambda.\mathrm{id}_E - u) = 0$.

Bizonyítás. Világos, hogy $\lambda \in K$ esetén $\lambda \in \mathrm{S}(u)$ ekvivalens azzal, hogy a $\lambda.\mathrm{id}_E - u : E \to E$ lineáris operátor nem injektív, ami az előző állítás alapján azzal ekvivalens, hogy $\det(\lambda.\mathrm{id}_E - u) = 0$. ∎

17.12.3. Állítás. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) > 0$. Legyen $\mathbf{e}$ bázis az E vektortérben és $u : E \to E$ lineáris operátor. Ekkor minden $\lambda \in K$ esetén*

$$\det(\lambda.\mathrm{id}_E - u) = \sum_{k=0}^{n} (-1)^{n-k} \Bigg(\sum_{\substack{H \subseteq n,\\ \mathrm{Card}(H)=k}} \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n\setminus H)\times(n\setminus H)}\right) \Bigg) \lambda^k.$$

Bizonyítás. Legyen $\lambda \in K$ rögzítve. Ekkor

$$\det(\lambda.\mathrm{id}_E - u) \overset{(1)}{=} \det(\mathrm{M}_{\mathbf{e},\mathbf{e}}(\lambda.\mathrm{id}_E - u)) \overset{(2)}{=} \det(\lambda.\mathrm{I}_n - \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)) \overset{(3)}{=}$$
$$\overset{(3)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \prod_{i \in n} \left(\lambda \delta_{i,\sigma(i)} - (\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)} \right) \overset{(4)}{=} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_n(\sigma) \prod_{i \in n} \Bigg(\sum_{j \in \{0,1\}} c_{i,j}(\sigma) \Bigg),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél lineáris operátor determinánsának definícióját alkalmaztuk;

– a $\overset{(2)}{=}$ egyenlőségnél az $n \times n$-es egységmátrix jelölésére bevezettük az I_n szimbólumot, és felhasználtuk azt, hogy az $\mathbf{L}(E;E) \to \mathrm{M}_n(K);\ v \mapsto \mathrm{M}_{\mathbf{e},\mathbf{e}}(v)$ leképezés lineáris operátor, és $\mathrm{M}_{\mathbf{e},\mathbf{e}}(\mathrm{id}_E) = \mathrm{I}_n$;

– a $\overset{(3)}{=}$ egyenlőségnél a mátrixok determinánsának definícióját alkalmaztuk;

– a $\overset{(4)}{=}$ egyenlőségnél minden $\sigma \in \mathfrak{S}_n$ permutációra és $(i,j) \in n \times \{0,1\}$ párra bevezettük a $c_{i,j}(\sigma) \in K$ objektumot úgy, hogy

$$c_{i,j}(\sigma) := \begin{cases} \lambda \delta_{i,\sigma(i)} & \text{ha } j = 0, \\ (-\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)} & \text{ha } j = 1. \end{cases}$$

Ha $\sigma \in \mathfrak{S}_n$, akkor

$$\prod_{i\in n}\Big(\sum_{j\in\{0,1\}} c_{i,j}(\sigma)\Big) \overset{(5)}{=} \sum_{\tau\in\{0,1\}^n}\Big(\prod_{i\in n} c_{i,\tau(i)}(\sigma)\Big) \overset{(6)}{=} \sum_{H\subseteq n}\Big(\prod_{i\in n} c_{i,\chi_H(i)}(\sigma)\Big) \overset{(7)}{=}$$

$$\overset{(7)}{=} \sum_{H\subseteq n}\bigg(\Big(\prod_{i\in H} c_{i,1}(\sigma)\Big)\Big(\prod_{i\in n\setminus H} c_{i,0}(\sigma)\Big)\bigg) \overset{(8)}{=}$$

$$\overset{(8)}{=} \sum_{H\subseteq n}\bigg((-1)^{\mathrm{Card}(H)}\Big(\prod_{i\in H}(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)}\Big)\lambda^{n-\mathrm{Card}(H)}\Big(\prod_{i\in n\setminus H}\delta_{i,\sigma(i)}\Big)\bigg) \overset{(9)}{=},$$

$$\overset{(9)}{=} \sum_{H\subseteq n}\bigg((-1)^{n-\mathrm{Card}(H)}\Big(\prod_{i\in n\setminus H}(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)}\Big)\lambda^{\mathrm{Card}(H)}\Big(\prod_{i\in H}\delta_{i,\sigma(i)}\Big)\bigg),$$

ahol

– az $\overset{(5)}{=}$ egyenlőségnél a véges műveletek általános disztributivitásának tételét (8.8.3.) alkalmaztuk a K testbeli szorzásra és összeadásra;

– a $\overset{(6)}{=}$ egyenlőségnél felhasználtuk azt, hogy a $\mathscr{P}(n) \to \{0,1\}^n$; $H \mapsto \chi_H$ leképezés bijekció, és alkalmaztuk véges műveletek általános kommutativitásának tételét (8.6.1.) a $(K,+)$ kommutatív csoportra;

– a $\overset{(7)}{=}$ egyenlőségnél a 12.5.6. állítást alkalmaztuk a $(K,\cdot)$ monoidra;

– a $\overset{(8)}{=}$ egyenlőségnél a $c_{i,j}(\sigma)$ objektumok definícióját alkalmaztuk;

– a $\overset{(9)}{=}$ egyenlőségnél felhasználtuk azt, hogy a $\mathscr{P}(n) \to \mathscr{P}(n)$; $H \mapsto n \setminus H$ leképezés bijekció, és ismét a véges műveletek általános kommutativitásának tételét (8.6.1.) alkalmaztuk a $(K,+)$ kommutatív csoportra.

Tehát

$$\det(\lambda.\mathrm{id}_E - u) =$$

$$= \sum_{\sigma\in\mathfrak{S}_n}\varepsilon_n(\sigma)\Bigg(\sum_{H\subseteq n}\bigg((-1)^{n-\mathrm{Card}(H)}\Big(\prod_{i\in n\setminus H}(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)}\Big)\lambda^{\mathrm{Card}(H)}\Big(\prod_{i\in H}\delta_{i,\sigma(i)}\Big)\bigg)\Bigg) \overset{(10)}{=}$$

$$\overset{(10)}{=} \sum_{H\subseteq n}(-1)^{n-\mathrm{Card}(H)}\lambda^{\mathrm{Card}(H)}\bigg(\sum_{\sigma\in\mathfrak{S}_n}\varepsilon_n(\sigma)\Big(\prod_{i\in n\setminus H}(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)}\Big)\Big(\prod_{i\in H}\delta_{i,\sigma(i)}\Big)\bigg) \overset{(11)}{=}$$

$$\overset{(11)}{=} \sum_{H\subseteq n}(-1)^{n-\mathrm{Card}(H)}\lambda^{\mathrm{Card}(H)}\bigg(\sum_{\substack{\sigma\in\mathfrak{S}_n,\\ H\subseteq[\sigma=\mathrm{id}_n]}}\varepsilon_n(\sigma)\Big(\prod_{i\in n\setminus H}(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)}\Big)\bigg) \overset{(12)}{=}$$

$$\overset{(12)}{=} \sum_{k=0}^{n}(-1)^{n-k}\lambda^k\bigg(\sum_{\substack{H\subseteq n,\\ \mathrm{Card}(H)=k}}\bigg(\sum_{\substack{\sigma\in\mathfrak{S}_n,\\ H\subseteq[\sigma=\mathrm{id}_n]}}\varepsilon_n(\sigma)\Big(\prod_{i\in n\setminus H}(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)}\Big)\bigg)\bigg) \overset{(13)}{=}$$

$$\overset{(13)}{=} \sum_{k=0}^{n}(-1)^{n-k}\bigg(\sum_{\substack{H\subseteq n,\\ \mathrm{Card}(H)=k}}\det\big(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n\setminus H)\times(n\setminus H)}\big)\bigg)\lambda^k,$$

ahol

– a $\overset{(10)}{=}$ egyenlőségnél felcseréltük az összegzések sorrendjét (12.5.7.);

– a $\overset{(11)}{=}$ egyenlőségnél felhasználtuk azt a nyilvánvaló tényt, hogy minden $\sigma \in \mathfrak{S}_n$ és

$H \subseteq n$ esetén

$$\prod_{i \in H} \delta_{i,\sigma(i)} = \begin{cases} 1 & \text{, ha } H \subseteq [\sigma = \mathrm{id}_n], \\ 0 & \text{, egyébként;} \end{cases}$$

– a $\overset{(12)}{=}$ egyenlőségnél felhasználtuk azt, hogy a $(\{H \subseteq E | \mathrm{Card}(H) = k\})_{k \in n+1}$ halmazrendszer diszjunkt és $\bigcup_{k=0}^{n} \{H \subseteq E | \mathrm{Card}(H) = k\} = \mathscr{P}(n)$, így alkalmazható a 12.5.10. tétel;

– a $\overset{(13)}{=}$ egyenlőségnél felhasználtuk azt, hogy ha rögzített $H \subseteq n$ és $\tau \in \mathfrak{S}_{n \setminus H}$ esetén $\widehat{\tau}$ jelöli az

$$n \to n; \quad i \mapsto \begin{cases} \tau(i) & \text{, ha } i \in n \setminus H, \\ i & \text{, ha } i \in H \end{cases}$$

leképezést, akkor $\widehat{\tau} \in \mathfrak{S}_n$ és $H \subseteq [\widehat{\tau} = \mathrm{id}_n]$, továbbá a

$$\mathfrak{S}_{n \setminus H} \to \{\sigma \in \mathfrak{S}_n | H \subseteq [\sigma = \mathrm{id}_n]\}; \quad \tau \mapsto \widehat{\tau}$$

leképezés bijekció, így a K-beli összeadás általános kommutativitása és a mátrixok determinánsának értelmezése alapján

$$\sum_{\substack{\sigma \in \mathfrak{S}_n, \\ H \subseteq [\sigma = \mathrm{id}_n]}} \varepsilon_n(\sigma) \Big(\prod_{i \in n \setminus H} (\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\sigma(i)} \Big) = \sum_{\tau \in \mathfrak{S}_{n \setminus H}} \varepsilon_n(\widehat{\tau}) \Big(\prod_{i \in n \setminus H} (\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\tau(i)} \Big) \overset{(*)}{=}$$

$$\overset{(*)}{=} \sum_{\tau \in \mathfrak{S}_{n \setminus H}} \varepsilon_{n \setminus H}(\tau) \Big(\prod_{i \in n \setminus H} (\mathrm{M}_{\mathbf{e},\mathbf{e}}(u))_{i,\tau(i)} \Big) = \det \left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus H) \times (n \setminus H)} \right),$$

ahol a $\overset{(*)}{=}$ egyenlőségnél felhasználtuk azt, hogy ha $\tau \in \mathfrak{S}_{n \setminus H}$, akkor $\varepsilon_n(\widehat{\tau}) = \varepsilon_{n \setminus H}(\tau)$ (ld. 13.3.10. az $E := n$ és $X := n \setminus H$ választással). ■

17.12.4. Következmény. *Legyen E véges dimenziós vektortér a K végtelen test felett, és $n := \dim(E) > 0$. Ha $\mathbf{e}$ és $\mathbf{f}$ bázisok az E vektortérben, akkor minden $u : E \to E$ lineáris operátorra és $k \leq n$ természetes számra*

$$\sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H) = k}} \det \left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus H) \times (n \setminus H)} \right) = \sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H) = k}} \det \left(\mathrm{M}_{\mathbf{f},\mathbf{f}}(u)|_{(n \setminus H) \times (n \setminus H)} \right).$$

Bizonyítás. Vezessük be a

$$P := \sum_{k=0}^{n} (-1)^{n-k} \Big(\sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H) = k}} \det \left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus H) \times (n \setminus H)} \right) \Big) X^k,$$

$$Q := \sum_{k=0}^{n} (-1)^{n-k} \Big(\sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H) = k}} \det \left(\mathrm{M}_{\mathbf{f},\mathbf{f}}(u)|_{(n \setminus H) \times (n \setminus H)} \right) \Big) X^k$$

polinomokat. Az előző állítás szerint minden $\lambda \in K$ esetén

$$P_K(\lambda) = \det(\lambda.\mathrm{id}_E - u) = Q_K(\lambda),$$

vagyis a P_K és Q_K polinomiális függvények egyenlőek, ezért a K test végtelensége folytán $P = Q$ (16.7.5.), ami az állítást bizonyítja. ■

17.12.5. Definíció. *Legyen E véges dimenziós vektortér a K végtelen test felett, és $n := \dim(E) > 0$. Ekkor minden $k \leq n$ természetes számra az $u : E \to E$ lineáris operátor k-***adik karakterisztikus invariánsának** *nevezzük a*

$$\mathrm{c}_k(u) := \sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H)=k}} \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus H) \times (n \setminus H)}\right) \in K$$

elemet, ahol **e** *tetszőleges bázis az E vektortérben. Továbbá, minden $u : E \to E$ lineáris operátorra a*

$$\mathrm{C}(u) := \sum_{k=0}^{n} (-1)^{n-k} \mathrm{c}_k(u).X^k \in K[X]$$

polinomot az u operátor **karakterisztikus polinomjának** *nevezzük.*

17.12.6. Állítás. *Legyen E vektortér a K végtelen test felett, és $n := \dim(E) > 0$. Ekkor minden $u : E \to E$ lineáris operátorra $\mathrm{c}_n(u) = 1$, és*

$$\mathrm{c}_0(u) = \det(u),$$

$$\mathrm{c}_{n-1}(u) = \mathrm{tr}(u),$$

tehát $n > 1$ esetén

$$\mathrm{C}(u) = (-1)^n \det(u) + \left(\sum_{k=1}^{n-2} (-1)^{n-k} \mathrm{c}_k(u).X^k\right) - \mathrm{tr}(u).X^{n-1} + X^n.$$

Bizonyítás. Nyilvánvaló, hogy ha **e** bázis az E vektortérben, akkor

$$\mathrm{c}_0(u) = \sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H)=0}} \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus H) \times (n \setminus H)}\right) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus \emptyset) \times (n \setminus \emptyset)}\right) = \det(u),$$

valamint

$$\mathrm{c}_n(u) = \sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H)=n}} \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus n) \times (n \setminus n)}\right) = 1.$$

Továbbá, ha $n > 0$, akkor

$$\mathrm{c}_{n-1}(u) = \sum_{\substack{H \subseteq n, \\ \mathrm{Card}(H)=n-1}} \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus H) \times (n \setminus H)}\right) \stackrel{(*)}{=} \sum_{k=0}^{n-1} \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{(n \setminus (n \setminus \{k\})) \times (n \setminus (n \setminus \{k\}))}\right) =$$

$$= \sum_{k=0}^{n-1} \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)|_{\{k\} \times \{k\}}\right) = \sum_{k=0}^{n-1} \left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right)_{k,k} = \mathrm{tr}(u),$$

ahol az $\stackrel{(*)}{=}$ egyenlőségnél kihasználtuk, hogy az

$$n \to \{H \subseteq n | \mathrm{Card}(H) = n-1\}; \quad k \mapsto n \setminus \{k\}$$

leképezés bijekció, így alkalmazható a K feletti összeadásra a véges műveletek általános kommutativitásának tétele (8.6.1.). ■

17.12.7. Tétel. (**Cayley–Hamilton-tétel.**) *Legyen E véges dimenziós vektortér a K végtelen test felett, és $n := \dim(E) > 0$. Ekkor minden $u : E \to E$ lineáris operátorra*

$$\sum_{k=0}^{n}(-1)^{n-k}\mathrm{c}_k(u).u^k = 0.$$

Bizonyítás. Legyen $\mathbf{e}$ bázis az E vektortérben és jelölje $\mathbf{1}$ az $\mathrm{M}_n(K)$ mátrixgyűrű egységelemét. Ekkor a karakterisztikus invariánsok definíciója és az $\mathbf{L}(E) \to \mathrm{M}_n(K);\ v \mapsto \mathrm{M}_{\mathbf{e},\mathbf{e}}(v)$ leképezés tulajdonságai szerint minden $\lambda \in K$ elemre

$$\det\left(\lambda.\mathbf{1} - \mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right) = \det\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}\left(\lambda.\mathrm{id}_E - u\right)\right) = \det\left(\lambda.\mathrm{id}_E - u\right) = \sum_{k=0}^{n}(-1)^{n-k}\mathrm{c}_k(u)\lambda^k.$$

Alkalmazva a mátrixokra vonatkozó Cayley–Hamilton-tételt (15.5.4.) kapjuk, hogy

$$0 = \sum_{k=0}^{n}(-1)^{n-k}\mathrm{c}_k(u).\left(\mathrm{M}_{\mathbf{e},\mathbf{e}}(u)\right)^k = \sum_{k=0}^{n}(-1)^{n-k}\mathrm{c}_k(u).\mathrm{M}_{\mathbf{e},\mathbf{e}}(u^k) =$$
$$= \mathrm{M}_{\mathbf{e},\mathbf{e}}\Big(\sum_{k=0}^{n}(-1)^{n-k}\mathrm{c}_k(u).u^k\Big),$$

amiből az $\mathbf{L}(E) \to \mathrm{M}_n(K);\ v \mapsto \mathrm{M}_{\mathbf{e},\mathbf{e}}(v)$ lineáris operátor injektivitása alapján következik a bizonyítandó operátor-egyenlőség. ■

17.13. Valós vektortér komplexifikációja

17.13.1. Definíció. *Az E valós vektortér* **komplexifikációjának** *nevezzük a (V, j) párt, ha V komplex vektortér, $j : E \to V$ $\mathbb{R}$-lineáris operátor, és teljesül a következő állítás:*

(CO) *Minden F komplex vektortérhez, és minden $u : E \to F$ $\mathbb{R}$-lineáris operátorhoz egyértelműen létezik olyan $v : V \to F$ $\mathbb{C}$-lineáris operátor, hogy az alábbi diagram kommutatív:*

$$\begin{tikzcd} E \arrow[r, "j"] \arrow[dr, "u"'] & V \arrow[d, "v"] \\ & F \end{tikzcd}$$

vagyis $v \circ j = u$.

17.13.2. Állítás. *Ha E valós vektortér és a (V_1, j_1), (V_2, j_2) párok mindketten komplexifikációi E-nek, akkor létezik egyetlen olyan $v : V_1 \to V_2$ $\mathbb{C}$-lineáris izomorfizmus a V_1 és V_2 komplex vektorterek között, amelyre az*

$$\begin{tikzcd} E \arrow[r, "j_1"] \arrow[dr, "j_2"'] & V_1 \arrow[d, "v"] \\ & V_2 \end{tikzcd}$$

diagram kommutatív, vagyis $v \circ j_1 = j_2$.

Bizonyítás. Mivel $j_2 : E \to V_2$ $\mathbb{R}$-lineáris operátor és (V_1, j_1) komplexifikációja E-nek, így (CO) alapján legfeljebb egy olyan $v : V_1 \to V_2$ $\mathbb{C}$-lineáris létezik, amelyre $v \circ j_1 = j_2$, ezért az adott tulajdonságú objektum *egyértelmű* (még az összes $V_1 \to V_2$ $\mathbb{C}$-lineáris operátorok halmazában is).

Mivel $j_1 : E \to V_1$ $\mathbb{R}$-lineáris operátor és (V_2, j_2) komplexifikációja E-nek, így (CO) alapján a létezik egyetlen olyan $v_1 : V_2 \to V_1$ $\mathbb{C}$-lineáris operátor, amelyre az

$$\begin{tikzcd} E \arrow[r, "j_2"] \arrow[dr, "j_1"'] & V_2 \arrow[d, "v_1"] \\ & V_1 \end{tikzcd}$$

diagram kommutatív, vagyis $v_1 \circ j_2 = j_1$.

Mivel $j_2 : E \to V_2$ $\mathbb{R}$-lineáris operátor és (V_1, j_1) komplexifikációja E-nek, így (CO) alapján a létezik egyetlen olyan $v_2 : V_1 \to V_2$ $\mathbb{C}$-lineáris operátor, amelyre az

$$\begin{tikzcd} E \arrow[r, "j_1"] \arrow[dr, "j_2"'] & V_1 \arrow[d, "v_2"] \\ & V_2 \end{tikzcd}$$

diagram kommutatív, vagyis $v_2 \circ j_1 = j_2$.

Ekkor nyilvánvalóan $(v_1 \circ v_2) \circ j_1 = j_1$ és $(v_2 \circ v_1) \circ j_2 = j_2$, továbbá $v_1 \circ v_2 : V_1 \to V_1$ $\mathbb{C}$-lineáris operátor és $v_2 \circ v_1 : V_2 \to V_2$ $\mathbb{C}$-lineáris operátor.

Mivel (V_1, j_1) komplexifikációja E-nek, és $j_1 : E \to V_1$ $\mathbb{R}$-lineáris operátor, így (CO) alapján létezik egyetlen olyan $w_1 : V_1 \to V_1$ $\mathbb{C}$-lineáris operátor, amelyre az

$$\begin{tikzcd} E \arrow[r, "j_1"] \arrow[dr, "j_1"'] & V_1 \arrow[d, "w_1"] \\ & V_1 \end{tikzcd}$$

diagram kommutatív, vagyis $w \circ j_1 = j_1$. Az egyértelműségi feltétel alapján triviális, hogy $w_1 = \mathrm{id}_{V_1}$. Ugyanakkor $(v_1 \circ v_2) \circ j_1 = j_1$ is teljesül, ezért $w_1 = v_1 \circ v_2$, amiből következik, hogy $v_1 \circ v_2 = \mathrm{id}_{V_1}$.

Mivel (V_2, j_2) komplexifikációja E-nek, és $j_2 : E \to V_2$ $\mathbb{R}$-lineáris operátor, így (CO) alapján létezik egyetlen olyan $w_2 : V_2 \to V_2$ $\mathbb{C}$-lineáris operátor, amelyre az

$$\begin{tikzcd} E \arrow[r, "j_2"] \arrow[dr, "j_2"'] & V_2 \arrow[d, "w_2"] \\ & V_2 \end{tikzcd}$$

diagram kommutatív, vagyis $w \circ j_2 = j_2$. Az egyértelműségi feltétel alapján triviális, hogy $w_2 = \mathrm{id}_{V_2}$. Ugyanakkor $(v_2 \circ v_1) \circ j_2 = j_2$ is teljesül, ezért $w_2 = v_2 \circ v_1$, amiből következik, hogy $v_2 \circ v_1 = \mathrm{id}_{V_2}$.

Ez azt jelenti, hogy a $v_2 : V_1 \to V_2$ $\mathbb{C}$-lineáris operátor bijekció, és $v_2^{-1} = v_1$. Továbbá, v_2-re teljesül a $v_2 \circ j_1 = j_2$, amivel az adott tulajdonságú operátor *létezését* igazoltuk. ■

17.13.3. Állítás. *Legyen E valós vektortér, $E_{\mathbb{C}} := E \times E$ és értelmezzük a következő leképezéseket*

$$s : E_{\mathbb{C}} \times E_{\mathbb{C}} \to E_{\mathbb{C}}; \quad ((x,y),(x',y')) \longmapsto (x+x', y+y'),$$
$$m : \mathbb{C} \times E_{\mathbb{C}} \to E_{\mathbb{C}}; \quad (\alpha,(x,y)) \longmapsto (\Re(\alpha).x - \Im(\alpha).y, \Im(\alpha).x + \Re(\alpha).y).$$

Ekkor az $E_{\mathbb{C}}$ halmaz ezekkel a leképezésekkel ellátva olyan komplex vektortér, hogy a

$$\mathrm{j} : E \to E_{\mathbb{C}}; \quad x \longmapsto (x,0)$$

leképezés $\mathbb{R}$-lineáris injekció, és az $(E_{\mathbb{C}}, \mathrm{j})$ pár komplexifikációja az E valós vektortérnek.

Bizonyítás. A definíció szerint az $(E_{\mathbb{C}}, s)$ pár egyenlő az $(E,+)$ kommutatív csoport önmagával vett szorzatával, ezért az $(E_{\mathbb{C}}, s)$ pár is kommutatív csoport.
Legyenek $\alpha, \beta \in \mathbb{C}$ és $(x,y) \in E_{\mathbb{C}}$. Ekkor a definíció szerint

$$\begin{gathered} m(\alpha, m(\beta,(x,y))) = m(\alpha, (\Re(\beta).x - \Im(\beta).y, \Im(\beta).x + \Re(\beta).y)) = \\ = (\Re(\alpha).(\Re(\beta).x - \Im(\beta).y) - \Im(\alpha).(\Im(\beta).x + \Re(\beta).y), \\ \Im(\alpha).(\Re(\beta).x - \Im(\beta).y) + \Re(\alpha).(\Im(\beta).x + \Re(\beta).y)) = \\ = ((\Re(\alpha)\Re(\beta) - \Im(\alpha)\Im(\beta)).x - (\Re(\alpha)\Im(\beta) + \Im(\alpha)\Re(\beta)).y, \\ (\Im(\alpha)\Re(\beta) + \Re(\alpha)\Im(\beta)).x + (-\Im(\alpha)\Im(\beta) + \Re(\alpha)\Re(\beta)).y) = \\ = (\Re(\alpha\cdot\beta).x - \Im(\alpha\cdot\beta).y, \Im(\alpha\cdot\beta).x + \Re(\alpha\cdot\beta).y) = m(\alpha\cdot\beta,(x,y)), \end{gathered}$$

továbbá, a $\Re, \Im : \mathbb{C} \to \mathbb{R}$ függvények additivitása folytán

$$\begin{gathered} m(\alpha+\beta,(x,y)) = (\Re(\alpha+\beta).x - \Im(\alpha+\beta).y, \Im(\alpha+\beta).x + \Re(\alpha+\beta).y) = q \\ = ((\Re(\alpha)+\Re(\beta)).x - (\Im(\alpha)+\Im(\beta)).y, (\Im(\alpha)+\Im(\beta)).x + (\Re(\alpha)+\Re(\beta)).y) = \\ = ((\Re(\alpha).x - \Im(\alpha).y) + (\Re(\beta).x - \Im(\beta).y), (\Im(\alpha).x + \Re(\alpha).y) + (\Im(\beta).x + \Re(\beta).y)) = \\ = s((\Re(\alpha).x - \Im(\alpha).y, \Im(\alpha).x + \Re(\alpha).y), (\Re(\beta).x - \Im(\beta).y, \Im(\beta).x + \Re(\beta).y)) = \\ = s(m(\alpha,(x,y)), m(\beta,(x,y))). \end{gathered}$$

Ha $\alpha \in \mathbb{C}$ és $(x,y), (x',y') \in E_{\mathbb{C}}$, akkor

$$\begin{gathered} m(\alpha, s((x,y),(x',y'))) = m(\alpha,(x+x', y+y')) = \\ = (\Re(\alpha).(x+x') - \Im(\alpha).(y+y'), \Im(\alpha).(x+x') + \Re(\alpha).(y+y')) = \\ =((\Re(\alpha).x - \Im(\alpha).y) + (\Re(\alpha).x' - \Im(\alpha).y'), (\Im(\alpha).x + \Re(\alpha).y) + (\Im(\alpha).x' + \Re(\alpha).y'))= \\ = s((\Re(\alpha).x - \Im(\alpha).y, \Im(\alpha).x + \Re(\alpha).y), (\Re(\alpha).x' - \Im(\alpha).y', \Im(\alpha).x' + \Re(\alpha).y')) = \\ = s(m(\alpha,(x,y)), m(\alpha,(x',y'))). \end{gathered}$$

Ha $\alpha \in \mathbb{R}$ és $(x,y) \in E_{\mathbb{C}}$, akkor

$$m(\alpha,(x,y)) = (\Re(\alpha).x - \Im(\alpha).y, \Im(\alpha).x + \Re(\alpha).y) = (\alpha.x - 0.y, 0.x + \alpha.y) = (\alpha.x, \alpha.y).$$

Ebből látszik, hogy minden $(x,y) \in E_{\mathbb{C}}$ esetén

$$m(1,(x,y)) = (1.x, 1.y) = (x,y),$$

amivel igazoltuk, hogy az $(E_{\mathbb{C}}, s, m)$ hármas komplex vektortér, továbbá minden $\alpha \in \mathbb{R}$ és $x \in E$ esetén

$$\mathrm{j}(\alpha.x) = (\alpha.x, 0) = (\alpha.x, \alpha.0) = m(\alpha,(x,0)) = m(\alpha, \mathrm{j}(x)),$$

valamint minden $x, y \in E$ esetén

$$\mathrm{j}(x+y) = (x+y, 0) = (x+y, 0+0) = s((x,0),(y,0)) = s(\mathrm{j}(x), \mathrm{j}(y)),$$

tehát a

$$\mathrm{j} : E \to E_{\mathbb{C}}; \quad x \longmapsto (x, 0)$$

leképezés $\mathbb{R}$-lineáris operátor. Nyilvánvaló, hogy a j operátor injekció.

Megmutatjuk, hogy az $(E_{\mathbb{C}}, \mathrm{j})$ pár komplexifikációja az E valós vektortérnek. Ehhez legyen F komplex vektortér, és $u : E \to F$ tetszőleges $\mathbb{R}$-lineáris operátor. Értelmezzük az

$$v : E_{\mathbb{C}} \to F; \quad (x,y) \mapsto u(x) + \mathbf{i}.u(y)$$

leképezést. Ez $\mathbb{C}$-lineáris operátor az $E_{\mathbb{C}}$ és F komplex vektorterek között. Valóban, ha $(x,y), (x',y') \in E_{\mathbb{C}}$, akkor az $u : E \to F$ operátor additivitása miatt

$$v(s((x,y),(x',y'))) = v(x+x', y+y') = u(x+x') + \mathbf{i}.u(y+y')) =$$
$$=(u(x) + u(x')) + \mathbf{i}.(u(y) + u(y'))=(u(x) + \mathbf{i}.u(y)) + (u(x') + \mathbf{i}.u(y'))=v(x,y) + v(x',y'),$$

tehát v additív, és ha $\alpha \in \mathbb{C}$ és $(x,y) \in E_{\mathbb{C}}$, akkor az u operátor $\mathbb{R}$-homogenitása miatt

$$\begin{aligned}
v(m(\alpha,(x.y))) &= v(\Re(\alpha).x - \Im(\alpha).y, \Im(\alpha).x + \Re(\alpha).y) = \\
&= u(\Re(\alpha).x - \Im(\alpha).y) + \mathbf{i}.u(\Im(\alpha).x + \Re(\alpha).y) = \\
&= \Re(\alpha).u(x) - \Im(\alpha).u(y) + \mathbf{i}.(\Im(\alpha).u(x) + \Re(\alpha).u(y)) = \\
&= (\Re(\alpha) + \mathbf{i}.\Im(\alpha)).u(x) + \mathbf{i}.(\Re(\alpha) + \mathbf{i}.\Im(\alpha)).u(y) = \\
&= \alpha.u(x) + \mathbf{i}.\alpha.u(y) = \alpha.(u(x) + \mathbf{i}.u(y)) = \alpha.v(x,y),
\end{aligned}$$

tehát a v operátor $\mathbb{C}$-homogén. Világos, hogy minden $x \in E$ esetén

$$(v \circ \mathrm{j})(x) = v(x,0) = u(x) + \mathbf{i}.u(0) = u(x),$$

tehát $v \circ \mathrm{j} = u$. Ez azt jelenti, hogy $v : E_{\mathbb{C}} \to F$ olyan $\mathbb{C}$-lineáris operátor, amelyre a következő diagram kommutatív:

$$\begin{tikzcd}
E \arrow[r, "\mathrm{j}"] \arrow[dr, "u"'] & E_{\mathbb{C}} \arrow[d, "v"] \\
& F
\end{tikzcd} .$$

Tegyük fel, hogy $v' : E_{\mathbb{C}} \to F$ olyan $\mathbb{C}$-lineáris operátor, amelyre $v' \circ \mathrm{j} = u$. A $v' = v$ egyenlőség bizonyításához először megjegyezzük, hogy $y \in E$ esetén $m(\mathbf{i}, (y,0)) = (0,y)$, mert a definíció szerint

$$m(\mathbf{i},(y,0)) = (\Re(\mathbf{i}).y - \Im(\mathbf{i}).0, \Im(\mathbf{i}).y + \Re(\mathbf{i}).0) = (0.y - 1.0, 1.y + 0.0) = (0,y).$$

Ebből következik, hogy minden $(x,y) \in E_{\mathbb{C}}$ esetén

$$s((x,0), m(\mathbf{i},(y,0))) = s((x,0),(0,y)) = (x+0, 0+y) = (x,y),$$

ezért v' additivitása és $\mathbb{C}$-homogenitása miatt

$$v'(x,y) = v'(s((x,0), m(\mathbf{i},(y,0)))) = v'(x,0) + v'(m(\mathbf{i},(y,0))) = v'(x,0) + \mathbf{i}.v'(y,0) =$$
$$= (v' \circ \mathrm{j})(x) + \mathbf{i}.(v' \circ \mathrm{j})(y) = u(x) + \mathbf{i}.u(y) = v(x,y),$$

tehát $v' = v$. Ez azt jelenti, hogy v az egyetlen olyan $E_{\mathbb{C}} \to F$ $\mathbb{C}$-lineáris operátor, amelyre $v \circ \mathrm{j} = u$. Ezért az $(E_{\mathbb{C}}, \mathrm{j})$ pár komplexifikációja az E valós vektortérnek. ■

A két előző állítás alapján mondható, hogy minden valós vektortérnek *létezik* komplexifikációja, és bármely két komplexifikációja kitüntetett módon azonosítható egymással, abban az értelemben, ahogy a 17.13.2. állításban megfogalmaztuk.

17.13.4. Definíció. *Ha E valós vektortér, akkor az előző állításban értelmezett* $(E_{\mathbb{C}}, \mathrm{j})$ *párt az E valós vektortér* **standard additív komplexifikációjának** *nevezzük.*

Később, a vektorterek tenzorszorzatának bevezetése után, szó lesz valós vektortér standard *multiplikatív* komplexifikációjáról is.

17.13.5. Állítás. *Ha a (V, j) pár komplexifikációja az E valós vektortérnek, akkor j injekció, és minden $v \in V$ esetén egyértelműen léteznek olyan $x, y \in E$ vektorok, hogy $v = j(x) + \mathbf{i}.j(y)$.*

Bizonyítás. A 17.13.2. állítás szerint egyértelműen létezik olyan $u : E_{\mathbb{C}} \to V$ $\mathbb{C}$-lineáris bijekció, amelyre $u \circ \mathrm{j} = j$.

Mivel a $\mathrm{j} : E \to E_{\mathbb{C}}$ operátor nyilvánvalóan injektív, így j is injekció. Továbbá, a 17.13.3. állítás bizonyításában láttuk, hogy minden $z \in E_{\mathbb{C}}$ elemre $z = \mathrm{j}(x) + \mathbf{i}.\mathrm{j}(y)$ teljesül, ha $x, y \in E$ azok a vektorok, amelyekre $z = (x, y)$, ezért az u operátor $\mathbb{C}$-linearitása miatt $u(z) = u(\mathrm{j}(x)) + \mathbf{i}.u(\mathrm{j}(y)) = j(x) + \mathbf{i}.j(y)$. Így az u operátor szürjektivitásából következik, hogy minden $v \in V$ esetén léteznek olyan $x, y \in E$ vektorok, amelyekre $v = j(x) + \mathbf{i}.j(y)$. Ha $x, y, x', y' \in E$ olyan vektorok, hogy $j(x) + \mathbf{i}.j(y) = j(x') + \mathbf{i}.j(y')$, akkor az u operátor $\mathbb{C}$-linearitása és $u \circ \mathrm{j} = j$ miatt $u(\mathrm{j}(x) + \mathbf{i}.\mathrm{j}(y)) = u(\mathrm{j}(x') + \mathbf{i}.\mathrm{j}(y'))$, ezért u injektivitásából következik, hogy

$$(x, y) = \mathrm{j}(x) + \mathbf{i}.\mathrm{j}(y) = \mathrm{j}(x') + \mathbf{i}.\mathrm{j}(y') = (x', y'),$$

tehát $x = x'$ és $y = y'$, vagyis minden $v \in V$ esetén *egyértelműen* léteznek olyan $x, y \in E$ vektorok, hogy $v = j(x) + \mathbf{i}.j(y)$. ■

Ezáltal az E valós vektortér azonosul az $E_{\mathbb{C}}$ komplex vektortér egyik $\mathbb{R}$-lineáris alterével.

d) Az $E_{\mathbb{C}}$ komplex vektortér alatt fekvő $(E_{\mathbb{C}})_{(\mathbb{R})}$ valós vektortér kanonikusan azonosítható az E valós vektortér önmagával vett lineáris szorzatterével.

e) A $C : E_{\mathbb{C}} \to E_{\mathbb{C}};\ (x, y) \longmapsto (x, -y)$ leképezés additív és olyan, hogy minden $\lambda \in \mathbb{C}$ és $z \in E_{\mathbb{C}}$ esetén $C(\lambda.z) = \overline{\lambda}.C(z)$; az ilyen tulajdonságú függvényeket *konjugált lineárisaknak* nevezzük. Továbbá, C bijekció és $C \circ C = \mathrm{id}_E$ teljesül. A C leképezést az E_C *kanonikus konjugációjának* nevezzük.

18. fejezet

Affin terek

18.1. Affin terek és affin függvények értelmezése

18.1.1. Definíció. *Az* $(E, \mathbf{E}, \Phi)$ *hármast* **affin térnek** *nevezzük, ha* E *nem üres halmaz,* $\mathbf{E}$ *vektortér és*

$$\Phi : E \times E \to \mathbf{E}$$

olyan függvény, amelyre teljesülnek a következők:

$(\mathrm{AFF_I})$ *Minden* $x \in E$ *esetén az* $E \to \mathbf{E};\ y \mapsto \Phi(x, y)$ *leképezés bijekció.*

$(\mathrm{AFF_{II}})$ *Minden* $x, y, z \in E$ *esetén* $\Phi(x, y) + \Phi(y, z) = \Phi(x, z)$.

Megállapodunk abban, hogy ha $(E, \mathbf{E}, \Phi)$ affin tér, akkor $x, y \in E$ esetén az

$$\overrightarrow{xy} := \Phi(x, y)$$

jelölést alkalmazzuk (ha ez nem vezet félreértésre), és azt mondjuk, hogy "E affin tér az $\mathbf{E}$ vektortér felett". Ezzel a jelöléssel $(\mathrm{AFF_I})$ azt jelenti, hogy minden $x \in E$ esetén az

$$E \to \mathbf{E}; \quad y \mapsto \overrightarrow{xy}$$

leképezés bijekció, és $(\mathrm{AFF_{II}})$ azt jelenti, hogy minden $x, y, z \in E$ esetén

$$\overrightarrow{xy} + \overrightarrow{yz} = \overrightarrow{xz}.$$

Ha E affin tér az $\mathbf{E}$ vektortér felett, akkor $(\mathrm{AFF_{II}})$-ből következik, hogy minden $x \in E$ esetén $\overrightarrow{xx} + \overrightarrow{xx} = \overrightarrow{xx}$, amihez hozzáadva a $-\overrightarrow{xx}$ vektort és felhasználva $\mathbf{E}$ összeadásának asszociativitását kapjuk, hogy $\overrightarrow{xx} = \mathbf{0}$. Ebből ismét $(\mathrm{AFF_{II}})$ alapján adódik, hogy minden $x, y \in E$ esetén $\overrightarrow{xy} + \overrightarrow{yx} = \overrightarrow{xx} = \mathbf{0}$, tehát $\overrightarrow{yx} = -\overrightarrow{xy}$.

Példa. 1) Legyen $\mathbf{E}$ vektortér és tekintsük a

$$\mathbf{E} \times \mathbf{E} \to \mathbf{E}; \quad (\mathbf{x}, \mathbf{y}) \mapsto \overrightarrow{\mathbf{xy}} := \mathbf{y} - \mathbf{x}.$$

leképezést. Ekkor az $(\mathbf{E}, \mathbf{E}, \to)$ hármas affin tér az $\mathbf{E}$ vektortér felett.

2) Legyen $\mathbf{E}$ vektortér, $\mathbf{F} \subseteq \mathbf{E}$ lineáris altér, $\mathbf{a} \in \mathbf{E}$, és tekintsük az $\mathbf{a}+\mathbf{F} := \{\mathbf{a}+\mathbf{x} | \mathbf{x} \in \mathbf{F}\}$ halmazt. Ekkor az $\mathbf{a} + \mathbf{F}$ halmaz

$$(\mathbf{a} + \mathbf{F}) \times (\mathbf{a} + \mathbf{F}) \to \mathbf{F}; \quad (\mathbf{a} + \mathbf{x}, \mathbf{a} + \mathbf{y}) \mapsto \overrightarrow{\mathbf{xy}} := \mathbf{y} - \mathbf{x}.$$

leképezéssel ellátva affin tér az $\mathbf{F}$ vektortér felett.

18.1.2. Állítás. *Legyen E affin tér az $\mathbf{E}$ vektortér felett. Ha $(x_i)_{i\in I}$ nem üres véges rendszer E-ben és $(z_i)_{i\in I}$ olyan K-beli rendszer, hogy $\sum_{i\in I} z_i = 1$, akkor létezik egyetlen olyan $x \in E$ pont, amelyre minden $o \in E$ esetén*

$$\overrightarrow{ox} = \sum_{i\in I} z_i \overrightarrow{ox_i}.$$

Bizonyítás. Legyen minden $o \in E$ esetén

$$x_o := o + \sum_{i\in I} z_i \overrightarrow{ox_i}.$$

Ha $o, o' \in E$, akkor $\overrightarrow{oo'} = \sum_{i\in I} z_i \overrightarrow{oo'}$ miatt

$$x_{o'} = o' + \sum_{i\in I} z_i \overrightarrow{o'x_i} = o + \overrightarrow{oo'} + \sum_{i\in I} z_i \overrightarrow{o'x_i} = o + \sum_{i\in I} z_i (\overrightarrow{oo'} + \overrightarrow{o'x_i}) = o + \sum_{i\in I} z_i \overrightarrow{ox_i} = x_o.$$

Tehát, ha $x := x_o$, ahol $o \in E$ *tetszőleges*, akkor minden $o \in E$ esetén $x = o + \sum_{i\in I} z_i \overrightarrow{ox_i}$, vagyis $\overrightarrow{ox} = \sum_{i\in I} z_i \overrightarrow{ox_i}$. Ezzel a kívánt tulajdonságú pont létezését igazoltuk, és az egyértelműsége nyilvánvaló, mert ha $x, x' \in E$ eleget tesznek a feltételnek, akkor minden $o \in E$ esetén $\overrightarrow{ox} = \overrightarrow{ox'}$, ezért $x = o + \overrightarrow{ox} = o + \overrightarrow{ox'} = x'$. ■

18.1.3. Definíció. *Ha E affin tér az $\mathbf{E}$ vektortér felett, $(x_i)_{i\in I}$ nem üres véges rendszer E-ben, és $(z_i)_{i\in I}$ olyan K-beli rendszer, hogy $\sum_{i\in I} z_i = 1$, akkor*

$$\sum_{i\in I} z_i x_i$$

jelöli azt a pontot E-ben, amelyre minden $o \in E$ esetén

$$\overrightarrow{o\left(\sum_{i\in I} z_i x_i\right)} = \sum_{i\in I} z_i \overrightarrow{ox_i}.$$

18.2. Affin csoport

18.3. Elemi geometria affin tereken

19. fejezet

Multilineáris operátorok és tenzorszorzatok

19.1. Multilineáris operátorok értelmezése

Ha $(E_i)_{i\in I}$ vektorterek rendszere és F vektortér (mind ugyanazon test felett), akkor képezhető a $\prod_{i\in I} E_i$ lineáris szorzattér, és a $\prod_{i\in I} E_i \to F$ függvények halmazának kijelölhető egy nevezetes részhalmaza; a lineáris operátorok $\mathbf{L}\Big(\prod_{i\in I} E_i; F\Big)$ halmaza. Azonban ekkor mód van arra, hogy egy másik függvénytípust is értelmezzünk; a $\prod_{i\in I} E_i \to F$ *multilineáris operátorok* típusát.

A definíció előtt emlékeztetünk arra, hogy ha $(E_i)_{i\in I}$ halmazrendszer, $\mathfrak{a} = (\mathfrak{a}_i)_{i\in I} \in \prod_{i\in I} E_i$, és $k \in I$, akkor $\mathrm{in}_{k,\mathfrak{a}}$ jelöli azt az $E_k \to \prod_{i\in I} E_i$ függvényt, amely minden $x \in E_k$ ponthoz azt a rendszert rendeli a $\prod_{i\in I} E_i$ szorzathalmazból, amelynek i-edik komponense $\mathfrak{a}_i$, ha $i \in I$ és $i \neq k$, továbbá a k-adik komponense x. Fontos az, hogy az $\mathrm{in}_{k,\mathfrak{a}} : E_k \to \prod_{i\in I} E_i$ injekció *nem függ* az $\mathfrak{a}$ pont k-adik komponensétől, tehát ha $\mathfrak{a}' = (\mathfrak{a}'_i)_{i\in I} \in \prod_{i\in I} E_i$ olyan pont, amelyre minden $i \in I \setminus \{k\}$ esetén $\mathfrak{a}_i = \mathfrak{a}'_i$, akkor $\mathrm{in}_{k,\mathfrak{a}} = \mathrm{in}_{k,\mathfrak{a}'}$.

19.1.1. Definíció. *Legyen $(E_i)_{i\in I}$ vektorterek rendszere, és F vektortér a K test felett. Egy $u : \prod_{i\in I} E_i \to F$ függvényt* **multilineáris operátornak** *nevezünk, ha minden $k \in I$ és minden $\mathfrak{a} \in \prod_{i\in I} E_i$ esetén az $u \circ \mathrm{in}_{k,\mathfrak{a}} : E_k \to F$ leképezés lineáris operátor. A $\prod_{i\in I} E_i \to F$ multilineáris operátorok halmazát $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ jelöli. A $\prod_{i\in I} E_i \to K$ multilineáris operátorokat* **multilineáris funkcionáloknak** *nevezzük. Ha E és F vektorterek, akkor $n \in \mathbb{N}$ esetén a $\mathbf{Mult}(E^n; F)$ halmazt az $\mathbf{L}_n(E; F)$ szimbólummal is jelöljük.*

Tehát a többváltozós függvények parciális függvényeinek definíciója (6.7.8.) alapján mondható, hogy vektorterek szorzatán értelmezett, vektortérbe érkező függvény pontosan akkor multilineáris, ha minden parciális függvénye lineáris.

Nyilvánvaló, hogy ha $(E_i)_{i\in I}$ vektorterek rendszere és F vekortér a K test felett, akkor $\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; F\Big)$ lineáris altere az $\mathscr{F}\Big(\prod\limits_{i\in I} E_i; F\Big)$ függvénytérnek, hiszen ha $u, v \in \mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; F\Big)$ és $\lambda \in K$, akkor minden $k \in I$ és $\mathfrak{a} \in \prod\limits_{i\in I} E_i$ esetén

$$\begin{gathered}(u+v)\circ \mathrm{in}_{k,\mathfrak{a}} = u\circ \mathrm{in}_{k,\mathfrak{a}} + v\circ \mathrm{in}_{k,\mathfrak{a}} \in \mathbf{L}(E_k; F),\\ (\lambda.u)\circ \mathrm{in}_{k,\mathfrak{a}} = \lambda.(u\circ \mathrm{in}_{k,\mathfrak{a}}) \in \mathbf{L}(E_k; F),\end{gathered}$$

ahol azt használjuk ki, hogy $\mathbf{L}(E_k; F)$ lineáris altere az $\mathscr{F}(E_k; F)$ függvénytérnek. Ezért a továbbiakban a $\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; F\Big)$ halmazt a pontonként értelmezett műveletekkel ellátva vektortérnek fogjuk tekinteni.

19.1.2. Állítás. *Legyen $(E_i)_{i\in I}$ vektorterek nem üres rendszere, F vektortér, és*

$$\prod_{i\in I} E_i \to \prod_{k\in I} \mathbf{L}\left(E_k; F\right); \quad (x_i)_{i\in I} \mapsto \left(u_{k,(x_i)_{i\in I}}\right)_{k\in I}$$

függvény. Akkor és csak akkor létezik olyan $u \in \mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; F\Big)$, hogy minden $k \in I$ és $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén

$$u\circ \mathrm{in}_{k,(x_i)_{i\in I}} = u_{k,(x_i)_{i\in I}}, \tag{1}$$

ha teljesülnek a következő feltételek.

a) *Minden $j, k \in I$ és $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén*

$$u_{j,(x_i)_{i\in I}}(x_j) = u_{k,(x_i)_{i\in I}}(x_k).$$

b) *Minden $k \in I$ és $(x_i)_{i\in I}, (x'_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén, ha minden $i \in I\setminus\{k\}$ indexre $x_i = x'_i$, akkor*

$$u_{k(x_i)_{i\in I}} = u_{k,\left(x'_i\right)_{i\in I}}.$$

Ha a) *és* b) *teljesül, akkor az* (1) *feltétellel az u multilineáris operátor egyértelműen van meghatározva.*

Bizonyítás. (I) Tegyük fel, hogy $u \in \mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; F\Big)$ olyan multilineáris operátor, amelyre minden $k \in I$ és $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén (1) teljesül. Nyilvánvaló, hogy minden $j, k \in I$ és $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén $\mathrm{in}_{j,(x_i)_{i\in I}}(x_j) = (x_i)_{i\in I} = \mathrm{in}_{k,(x_i)_{i\in I}}(x_k)$, amiből(1) alapján következik, hogy

$$u_{j,(x_i)_{i\in I}}(x_j) = \left(u\circ \mathrm{in}_{j,(x_i)_{i\in I}}\right)(x_j) = u\left((x_i)_{i\in I}\right) = \left(u\circ \mathrm{in}_{k,(x_i)_{i\in I}}\right)(x_k) = u_{k,(x_i)_{i\in I}}(x_k),$$

ezért a) teljesül. nyilvánvaló, hogy minden $k \in I$ és $(x_i)_{i\in I}, (x'_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén, ha minden $i \in I \setminus \{k\}$ indexre $x_i = x'_i$, akkor $\mathrm{in}_{k,(x_i)_{i\in I}} = \mathrm{in}_{k,\left(x'_i\right)_{i\in I}}$, amiből (1) alapján következik, hogy

$$u_{k,(x_i)_{i\in I}} = u \circ \mathrm{in}_{k,(x_i)_{i\in I}} = u \circ \mathrm{in}_{k,\left(x'_i\right)_{i\in I}} = u_{k,\left(x'_i\right)_{i\in I}},$$

ezért b) teljesül.

Ha $u' \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ szintén olyan multilineáris operátor, amelyre minden $k \in I$ és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén $u' \circ \mathrm{in}_{k,(x_i)_{i\in I}} = u_{k,(x_i)_{i\in I}}$, akkor rögzítve egy $k \in I$ indexet kapjuk, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ rendszerre

$$\begin{aligned} u\left((x_i)_{i\in I}\right) &= u\left(\mathrm{in}_{k,(x_i)_{i\in I}}(x_k)\right) = \left(u \circ \mathrm{in}_{k,(x_i)_{i\in I}}\right)(x_k) = \left(u_{k,(x_i)_{i\in I}}\right)(x_k) = \\ &= \left(u' \circ \mathrm{in}_{k,(x_i)_{i\in I}}\right)(x_k) = u'\left(\mathrm{in}_{k,(x_i)_{i\in I}}(x_k)\right) = u'\left((x_i)_{i\in I}\right), \end{aligned}$$

tehát $u = u'$. Ez azt jelenti, hogy az (1) feltétellel az u multilineáris operátor egyértelműen van meghatározva.

(II) Tegyük fel, hogy a) és b) teljesül. Rögzítsünk egy $j \in I$ indexet, és értelmezzük az

$$u : \prod_{i\in I} E_i \to F; \quad (x_i)_{i\in I} \mapsto u_{j,(x_i)_{i\in I}}(x_j)$$

leképezést. Legyen $k \in I$ és $\mathbf{x} = (x_i)_{i\in I} \in \prod_{i\in I} E_i$. Ekkor minden $x \in E_k$ esetén

$$\begin{aligned} (u \circ \mathrm{in}_{k,\mathbf{x}})(x) &= u(\mathrm{in}_{k,\mathbf{x}}(x)) = u_{j,\mathrm{in}_{k,\mathbf{x}}(x)}\left((\mathrm{in}_{k,\mathbf{x}}(x))_j\right) \overset{(1)}{=} \\ &\overset{(1)}{=} u_{k,\mathrm{in}_{k,\mathbf{x}}(x)}\left((\mathrm{in}_{k,\mathbf{x}}(x))_k\right) = u_{k,\mathrm{in}_{k,\mathbf{x}}(x)}(x) \overset{(2)}{=} u_{k,\mathbf{x}}(x), \end{aligned}$$

ahol az $\overset{(1)}{=}$ egyenlőségnél az a) feltételt alkalmaztuk, és a $\overset{(2)}{=}$ egyenlőségnél figyelembe vettük azt, hogy az $\mathrm{in}_{k,\mathbf{x}}(x)$ és $\mathbf{x}$ rendszerek mindegyik k-tól különböző komponense egyenlő, így a b) feltétel alapján $u_{k,\mathrm{in}_{k,\mathbf{x}}(x)} = u_{k,\mathbf{x}}$. Ez azt jelenti, hogy minden $k \in I$ és $\mathbf{x} \in \prod_{i\in I} E_i$ esetén $u \circ \mathrm{in}_{k,\mathbf{x}} = u_{k,\mathbf{x}} \in \mathbf{L}(E_k; F)$, tehát $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ és teljesül az (1) egyenlőség. ■

19.1.3. Állítás. *Legyen $(E_i)_{i\in I}$ vektorterek nem üres rendszere, továbbá F vektortér, valamint $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$. Ha $(G_i)_{i\in I}$ szintén vektortér rendszer, H vektortér, és minden $i \in I$ esetén $v_i : G_i \to E_i$ lineáris operátor, valamint $w : F \to H$ lineáris operátor, akkor a*

$$w \circ u \circ \Big(\underset{i\in I}{\times} v_i\Big) : \prod_{i\in I} G_i \to H; \quad (x_i)_{i\in I} \mapsto w(u((v_i(x_i))_{i\in I}))$$

leképezés multilineáris operátor.

Bizonyítás. Legyen $k \in I$ és $\mathfrak{a} = (\mathfrak{a}_i)_{i \in I} \in \prod_{i \in I} G_i$ rögzített, és vezessük be a $\mathfrak{b} := (v_i(\mathfrak{a}_i))_{i \in I} \in \prod_{i \in I} E_i$ rendszert. Könnyen látható, hogy $\left(\underset{i \in I}{\times} v_i \right) \circ \mathrm{in}_{k,\mathfrak{a}} = \mathrm{in}_{k,\mathfrak{b}} \circ v_k$, vagyis $\underset{i \in I}{\times} v_i$ definíciója szerint minden $x \in G_k$ esetén $\left(v_i \left((\mathrm{in}_{k,\mathfrak{a}}(x))_i \right) \right)_{i \in I} = \mathrm{in}_{k,\mathfrak{b}}(v_k(x))$. Valóban, ha $x \in G_k$ és $i \in I$, akkor

– $i \neq k$ esetén $(\mathrm{in}_{k,\mathfrak{a}}(x))_i = \mathfrak{a}_i$ és $(\mathrm{in}_{k,\mathfrak{b}}(v_k(x)))_i = \mathfrak{b}_i$, ezért $v_i \left((\mathrm{in}_{k,\mathfrak{a}}(x))_i \right) = v_i(\mathfrak{a}_i) = \mathfrak{b}_i = (\mathrm{in}_{k,\mathfrak{b}}(v_k(x)))_i$,

– $i = k$ esetén $(\mathrm{in}_{k,\mathfrak{a}}(x))_k = x$ és $(\mathrm{in}_{k,\mathfrak{b}}(v_k(x)))_k = v_k(x)$, ezért $v_k \left((\mathrm{in}_{k,\mathfrak{a}}(x))_k \right) = v_k(x) = (\mathrm{in}_{k,\mathfrak{b}}(v_k(x)))_k$.

Ez azt jelenti, hogy

$$\left(w \circ u \circ \left(\underset{i \in I}{\times} v_i \right) \right) \circ \mathrm{in}_{k,\mathfrak{a}} = w \circ (u \circ \mathrm{in}_{k,\mathfrak{b}}) \circ v_k \in \mathbf{L}\,(G_k; H)\,,$$

hiszen $v_k \in \mathbf{L}(G_k; E_k)$, és $u \in \mathbf{Mult}\left(\prod_{i \in I} E_i; F \right)$ miatt $u \circ \mathrm{in}_{k,\mathfrak{b}} \in \mathbf{L}(E_k; F)$, valamint $w \in \mathbf{L}(F; H)$. ■

Vigyázzunk arra, hogy ha $(E_i)_{i \in I}$ vektorterek nem üres rendszere, F vektortér, $u \in \mathbf{Mult}\left(\prod_{i \in I} E_i; F \right)$, és $(G_i)_{i \in I}$ szintén (ugyanolyan indexhalmazú) vektortér rendszer, $v : \prod_{i \in I} G_i \to \prod_{i \in I} E_i$ *tetszőleges lineáris operátor*, H vektortér és $w : F \to H$ lineáris operátor, akkor a $w \circ u \circ v : \prod_{i \in I} G_i \to H$ függvény nem feltétlenül multilineáris operátor. Az előző állítás szerint ez a függvény akkor lesz multilineáris operátor, ha a v lineáris operátor $\underset{i \in I}{\times} v_i$ alakú, ahol $(v_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $v_i : G_i \to E_i$ lineáris operátor.

19.1.4. Következmény. *Legyen $(E_i)_{i \in I}$ vektorterek nem üres rendszere, továbbá F vektortér a K test felett. Ekkor minden $u \in \mathbf{Mult}\left(\prod_{i \in I} E_i; K \right)$ és $z \in F$ esetén az*

$$u \dot{\otimes} z : \prod_{i \in I} E_i \to F; \quad (x_i)_{i \in I} \mapsto u\left((x_i)_{i \in I} \right).z$$

leképezés multilineáris operátor, tehát eleme $\mathbf{Mult}\left(\prod_{i \in I} E_i; F \right)$-nek.

Bizonyítás. A $w_z : K \to F$; $\lambda \mapsto \lambda.z$ leképezés lineáris operátor, és $u \dot{\otimes} z = w_z \circ u$, így az állítás nyilvánvalóan következik a 19.1.3. állításból. ■

19.1.5. Következmény. *Legyen $(E_i)_{i \in I}$ vektorterek nem üres rendszere, továbbá F vektortér a K test felett. Legyen $(G_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén G_i lineáris altere E_i-nek. Ekkor minden $u \in \mathbf{Mult}\left(\prod_{i \in I} E_i; F \right)$ esetén $u|_{\prod_{i \in I} G_i} \in \mathbf{Mult}\left(\prod_{i \in I} G_i; F \right)$.*

Bizonyítás. Nyilvánvalóan következik a 19.1.3. állításból, ha minden $i \in I$ esetén $u_i := \mathrm{in}_{G_i,E_i}$, és $H := F$, valamint $w := \mathrm{id}_F$. ■

A következő állítás fontos szerepet játszik a multilineáris operátorokkal kapcsolatos állítások teljes indukciós bizonyításaiban, amikor véges sok vektortér szorzatán értelmezett multilineáris operátorokról van szó.

19.1.6. Lemma. *Legyen $(E_i)_{i\in I}$ vektorterek rendszere, $k \in I$ és $z \in E_k$. Értelmezzük a*

$$\tau_{k,z} : \prod_{i\in I\setminus\{k\}} E_i \to \prod_{i\in I} E_i$$

függvényt úgy, hogy minden $x = (x_i)_{i\in I\setminus\{k\}}$ esetén $\tau_{k,z}(x) \in \prod_{i\in I} E_i$ az a rendszer, amelyre minden $i \in I$ esetén

$$(\tau_{k,z}(x))_i := \begin{cases} x_i & , \textit{ha } i \in I\setminus\{k\}, \\ z & , \textit{ha } i = k. \end{cases}.$$

Ha F vektortér és $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$, akkor $u \circ \tau_{k,z} \in \mathbf{Mult}\Big(\prod_{i\in I\setminus\{k\}} E_i; F\Big)$.

Bizonyítás. Legyen $j \in I\setminus\{k\}$ és $\mathfrak{a} = (\mathfrak{a}_i)_{i\in I\setminus\{k\}} \in \prod_{i\in I\setminus\{k\}} E_i$. Azt kell igazolni, hogy az $(u \circ \tau_{k,z}) \circ \mathrm{in}_{j,\mathfrak{a}} : E_j \to F$ leképezés lineáris operátor.
Ehhez vegyünk egy $x \in E_j$ vektort és tetszőleges $i \in I$ indexet. Ekkor a definíció szerint

$$\left((\tau_{k,z} \circ \mathrm{in}_{j,\mathfrak{a}})(x)\right)_i = \begin{cases} (\mathrm{in}_{j,\mathfrak{a}}(x))_i & , \text{ha } i \neq k \\ z & , \text{ha } i = k, \end{cases}$$

ami azt jelenti, hogy

$$\left((\tau_{k,z} \circ \mathrm{in}_{j,\mathfrak{a}})(x)\right)_i = \begin{cases} \mathfrak{a}_i & , \text{ha } i \neq k \text{ és } i \neq j \\ x & , \text{ha } i \neq k \text{ és } i = j \\ z & , \text{ha } i = k, \end{cases}.$$

De $j \neq k$ miatt az $(i \neq k) \wedge (i = j)$ és $i = j$ kijelentések ekvivalensek, ezért

$$\left((\tau_{k,z} \circ \mathrm{in}_{j,\mathfrak{a}})(x)\right)_i = \begin{cases} \mathfrak{a}_i & , \text{ha } i \neq k \text{ és } i \neq j \\ x & , \text{ha } i = j \\ z & , \text{ha } i = k, \end{cases}.$$

Ha most bevezetjük azt az $\mathfrak{a}' \in \prod_{i\in I} E_i$ rendszert, amelyre minden $i \in I$ esetén

$$\mathfrak{a}'_i := \begin{cases} \mathfrak{a}_i & , \text{ha } i \neq k \\ z & , \text{ha } i = k \end{cases},$$

akkor világos, hogy minden $x \in E_j$ és $i \in I$ esetén

$$(\mathrm{in}_{j,\mathfrak{a}'}(x))_i = \begin{cases} \mathfrak{a}'_i & , \text{ha } i \neq j \\ x & , \text{ha } i = j \end{cases},$$

ami azzal ekvivalens, hogy

$$(\mathrm{in}_{j,\mathfrak{a}'}(x))_i = \begin{cases} \mathfrak{a}_i & \text{, ha } i \neq j \text{ és } i \neq k \\ z & \text{, ha } i \neq j \text{ és } i = k \\ x & \text{, ha } i = j \end{cases}.$$

De $j \neq k$ miatt az $(i \neq j) \wedge (i = k)$ és $i = k$ kijelentések ekvivalensek, ezért minden $x \in E_j$ és $i \in I$ esetén

$$(\mathrm{in}_{j,\mathfrak{a}'}(x))_i = \begin{cases} \mathfrak{a}_i & \text{, ha } i \neq j \text{ és } i \neq k \\ z & \text{, ha } i = k \\ x & \text{, ha } i = j \end{cases}.$$

Ez azt jelenti, hogy $\tau_{k,z} \circ \mathrm{in}_{j,\mathfrak{a}} = \mathrm{in}_{j,\mathfrak{a}'}$, következésképpen

$$(u \circ \tau_{k,z}) \circ \mathrm{in}_{j,\mathfrak{a}} = u \circ \mathrm{in}_{j,\mathfrak{a}'} \in \mathbf{L}(E_j; F),$$

amit bizonyítani kellett. ■

19.2. Multilineáris operátor multihomogenitása

19.2.1. Állítás. **(Multilineáris operátor multihomogenitása)** *Legyen* $(E_i)_{i\in I}$ *vektorterek nem üres, véges rendszere és* F *vektortér a* K *test felett, és* $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$.
Ha $(\lambda_i)_{i\in I} \in K^I$ *és* $(\mathfrak{a}_i)_{i\in I} \in \prod_{i\in I} E_i$, *akkor*

$$u((\lambda_i.\mathfrak{a}_i)_{i\in I}) = \Big(\mathop{\mathrm{P}}_{i\in I} \lambda_i\Big).u((\mathfrak{a}_i)_{i\in I}).$$

Bizonyítás. Az I indexhalmaz számossága szerinti teljes indukcióval bizonyítunk. Ehhez jelölje $\mathscr{A}(n)$ a következő kijelentés rövidítését:
"Vektorterek minden $(E_i)_{i\in I}$ véges rendszerére, ha $\mathrm{Card}(I) = n$, akkor minden F vektortérre, minden $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ függvényre, valamint minden $(\lambda_i)_{i\in I} \in K^I$ és $(\mathfrak{a}_i)_{i\in I} \in \prod_{i\in I} E_i$ rendszerre: $u((\lambda_i.\mathfrak{a}_i)_{i\in I}) = \Big(\mathop{\mathrm{P}}_{i\in I} \lambda_i\Big).u((\mathfrak{a}_i)_{i\in I})$."
Azt kell igazolni, hogy $(\forall n \in \mathbb{N}^*) : \mathscr{A}(n)$ teljesül. Az $\mathscr{A}(1)$ állítás azért igaz, mert $\mathrm{Card}(I) = 1$ és $I = \{i\}$ esetén $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ azonosul $\mathbf{L}(E_i; F)$-fel, és ekkor az egyenlőség az u lineáris operátor homogenitását fejezi ki.
Legyen $n \in \mathbb{N}^*$ olyan, hogy $\mathscr{A}(n)$ teljesül, és legyen $(E_i)_{i\in I}$ vektortereknek olyan véges rendszere, hogy $\mathrm{Card}(I) = n + 1$, valamint legyen F vektortér és $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$.
Kijelölünk egy $k \in I$ indexet, és bevezetjük az $I' := I \setminus \{k\}$ jelölést. Világos, hogy ekkor $(E_i)_{i\in I'}$ vektortereknek olyan véges rendszere, hogy $\mathrm{Card}(I') = n$. Rögzítünk egy $(\lambda_i)_{i\in I} \in K^I$ és egy $\mathfrak{a} := (\mathfrak{a}_i)_{i\in I} \in \prod_{i\in I} E_i$ rendszert. Bevezetjük a $z := \lambda_k.\mathfrak{a}_k \in E_k$ vektort,

és tekintjük a 19.1.6. lemmában értelmezett $\tau_{k,z} : \prod_{i\in I'} E_i \to \prod_{i\in I} E_i$ leképezést, amelyre teljesül az, hogy $u \circ \tau_{k,z} \in \mathbf{Mult}\Big(\prod_{i\in I'} E_i; F\Big)$.

Most alkalmazhatjuk az $\mathscr{A}(n)$ kijelentést az $(E_i)_{i\in I'}$ vektortér rendszerre, az F vektortérre, az $u \circ \tau_{k,z} \in \mathbf{Mult}\Big(\prod_{i\in I'} E_i; F\Big)$ multilineáris operátorra, valamint a $(\lambda_i)_{i\in I'} \in K^{I'}$ és $(\mathfrak{a}_i)_{i\in I'} \in \prod_{i\in I'} E_i$ rendszerekre. Tehát az

$$(u \circ \tau_{k,z})\left((\lambda_i.\mathfrak{a}_i)_{i\in I'}\right) = \Big(\mathrm{P}_{i\in I'} \lambda_i\Big).(u \circ \tau_{k,z})\left((\mathfrak{a}_i)_{i\in I'}\right).$$

egyenlőség az *indukciós hipotézis miatt* teljesül.
Ha $i \in I$, akkor a definíció szerint

$$\left(\tau_{k,z}\left((\lambda_i.\mathfrak{a}_i)_{i\in I'}\right)\right)_i := \begin{cases} \lambda_i.\mathfrak{a}_i & , \text{ha } i \in I', \\ z & , \text{ha } i = k. \end{cases}$$

továbbá $z = \lambda_k.\mathfrak{a}_k \in E_k$, így

$$\tau_{k,z}\left((\lambda_i.\mathfrak{a}_i)_{i\in I'}\right) = (\lambda_i.\mathfrak{a}_i)_{i\in I}.$$

Ha $j \in I$, akkor a definíció szerint

$$\left(\tau_{k,z}\left((\mathfrak{a}_i)_{i\in I'}\right)\right)_j := \begin{cases} \mathfrak{a}_j & , \text{ha } j \in I', \\ z & , \text{ha } j = k, \end{cases}$$

ami azt jelenti, hogy

$$\tau_{k,z}\left((\mathfrak{a}_i)_{i\in I'}\right) = \mathrm{in}_{k,\mathfrak{a}}(z) = \mathrm{in}_{k,\mathfrak{a}}(\lambda_k.\mathfrak{a}_k).$$

Ugyanakkor, az $u \circ \mathrm{in}_{k,\mathfrak{a}} : E_k \to F$ leképezés lineáris, ezért homogén, így

$$(u \circ \mathrm{in}_{k,\mathfrak{a}})(\lambda_k.\mathfrak{a}_k) = \lambda_k.(u \circ \mathrm{in}_{k,\mathfrak{a}})(\mathfrak{a}_k)$$

is teljesül. Végül nyilvánvaló, hogy

$$\mathrm{in}_{k,\mathfrak{a}}(\mathfrak{a}_k) = (\mathfrak{a}_i)_{i\in I}.$$

Felhasználva ezeket az összefüggéseket kapjuk, hogy

$$\begin{aligned} u((\lambda_i.\mathfrak{a}_i)_{i\in I}) &= u\left(\tau_{k,z}\left((\lambda_i.\mathfrak{a}_i)_{i\in I'}\right)\right) = (u \circ \tau_{k,z})\left((\lambda_i.\mathfrak{a}_i)_{i\in I'}\right) = \\ &= \Big(\mathrm{P}_{i\in I'} \lambda_i\Big).(u \circ \tau_{k,z})\left((\mathfrak{a}_i)_{i\in I'}\right) = \Big(\mathrm{P}_{i\in I'} \lambda_i\Big).u\left(\tau_{k,z}((\mathfrak{a}_i)_{i\in I'})\right) = \\ = \Big(\mathrm{P}_{i\in I'} \lambda_i\Big).u\left(\mathrm{in}_{k,\mathfrak{a}}(\lambda_k.\mathfrak{a}_k)\right) &= \Big(\mathrm{P}_{i\in I'} \lambda_i\Big).\left(\lambda_k.u\left(\mathrm{in}_{k,\mathfrak{a}}(\mathfrak{a}_k)\right)\right) = \Big(\mathrm{P}_{i\in I} \lambda_i\Big)u\left((\mathfrak{a}_i)_{i\in I}\right), \end{aligned}$$

tehát $\mathscr{A}(n+1)$ is igaz. ■

19.2.2. Következmény. *Legyen $(E_i)_{i\in I}$ vektorterek nem üres, véges rendszere és F vektortér a K test felett, valamint $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$. Ha $\lambda \in K$ és $\mathfrak{a} \in \prod_{i\in I} E_i$, akkor*

$$u(\lambda.\mathfrak{a}) = \lambda^{\mathrm{Card}(I)}.u(\mathfrak{a}).$$

Bizonyítás. Elegendő a 19.2.1. állítást alkalmazni arra a $(\lambda_i)_{i\in I}$ rendszerre, amelyre minden $i \in I$ esetén $\lambda_i := \lambda$, figyelembe véve, hogy ekkor $\mathrm{P}_{i\in I} \lambda_i = \lambda^{\mathrm{Card}(I)}$. ■

19.3. Multilineáris operátor multiadditivitása

19.3.1. Állítás. **(Multilineáris operátor multiadditivitása)** *Legyen* $(E_i)_{i\in I}$ *vektorterek nem üres, véges rendszere,* F *vektortér, valamint* $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$*. Ha minden* $I \ni i$*-re* $(\mathfrak{a}_{i,j})_{j\in J_i}$ *véges rendszer* E_i*-ben, és* $J := \prod_{i\in I} J_i$*, akkor*

$$u\Big(\Big(\sum_{j\in J_i} \mathfrak{a}_{i,j}\Big)_{i\in I}\Big) = \sum_{\sigma\in J} u((\mathfrak{a}_{i,\sigma(i)})_{i\in I}).$$

Bizonyítás. Az I indexhalmaz számossága szerinti teljes indukcióval bizonyítunk. Ehhez jelölje $\mathscr{A}(n)$ a következő kijelentés rövidítését:

"Vektorterek minden $(E_i)_{i\in I}$ véges rendszerére, ha $\mathrm{Card}(I) = n$, akkor minden F vektortérre, minden $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ függvényre, valamint minden olyan $((\mathfrak{a}_{i,j})_{j\in J_i})_{i\in I}$ rendszerre, amelyre minden $i \in I$ esetén $(\mathfrak{a}_{i,j})_{j\in J_i}$ véges rendszer E_i-ben, teljesül az $u\Big(\Big(\sum_{j\in J_i} \mathfrak{a}_{i,j}\Big)_{i\in I}\Big) = \sum_{\sigma\in J} u((\mathfrak{a}_{i,\sigma(i)})_{i\in I})$ egyenlőség."

Azt kell igazolni, hogy $(\forall n \in \mathbb{N}^*)\mathscr{A}(n)$ teljesül. Az $\mathscr{A}(1)$ állítás azért igaz, mert $\mathrm{Card}(I) = 1$ és $I = \{i\}$ esetén $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ azonosul $\mathbf{L}(E_i; F)$-fel, és ekkor az egyenlőség az u lineáris operátor additivitását fejezi ki.

Legyen $n \in \mathbb{N}^*$ olyan, hogy $\mathscr{A}(n)$ teljesül, és legyen $(E_i)_{i\in I}$ vektortereknek olyan véges rendszere, hogy $\mathrm{Card}(I) = n+1$, valamint legyen F vektortér és $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$.

Kijelölünk egy $k \in I$ indexet, és bevezetjük az $I' := I \setminus \{k\}$ jelölést. Világos, hogy ekkor $(E_i)_{i\in I'}$ vektortereknek olyan véges rendszere, hogy $\mathrm{Card}(I') = n$. Rögzítünk egy olyan $((\mathfrak{a}_{i,j})_{j\in J_i})_{i\in I}$ rendszert, amelyre $i \in I$ esetén $(\mathfrak{a}_{i,j})_{j\in J_i}$ véges rendszer E_i-ben. Bevezetjük a $z := \sum_{j\in J_k} \mathfrak{a}_{k,j} \in E_k$ vektort, és tekintjük a 19.1.6. lemmában értelmezett $\tau_{k,z} : \prod_{i\in I'} E_i \to \prod_{i\in I} E_i$ leképezést, amelyre teljesül az, hogy $u \circ \tau_{k,z} \in \mathbf{Mult}\Big(\prod_{i\in I'} E_i; F\Big)$.

Most alkalmazhatjuk az $\mathscr{A}(n)$ kijelentést az $(E_i)_{i\in I'}$ vektortér rendszerre, az F vektortérre, az $u \circ \tau_{k,z} \in \mathbf{Mult}\Big(\prod_{i\in I'} E_i; F\Big)$ multilineáris operátorra, valamint a $((\mathfrak{a}_{i,j})_{j\in J_i})_{i\in I'}$ rendszerre, amelyre minden $i \in I'$ esetén $(\mathfrak{a}_{i,j})_{j\in J_i}$ véges rendszer E_i-ben. Tehát ha $J' := \prod_{i\in I'} J_i$, akkor az

$$(u \circ \tau_{k,z})\Big(\Big(\sum_{j\in J_i} \mathfrak{a}_{i,j}\Big)_{i\in I'}\Big) = \sum_{\sigma'\in J'} (u \circ \tau_{k,z})((\mathfrak{a}_{i,\sigma'(i)})_{i\in I'}),$$

egyenlőség az *indukciós hipotézis miatt* teljesül.

A $\tau_{k,z} : \prod_{i\in I'} E_i \to \prod_{i\in I} E_i$ leképezés és a z vektor definíciója alapján nyilvánvaló, hogy

$$(u \circ \tau_{k,z})\Big(\Big(\sum_{j\in J_i} \mathfrak{a}_{i,j}\Big)_{i\in I'}\Big) = u\Big(\Big(\sum_{j\in J_i} \mathfrak{a}_{i,j}\Big)_{i\in I}\Big).$$

Legyen most $\sigma' \in J' = \prod_{i\in I'} J_i$. Ha $i \in I$, akkor $\tau_{k,z}$ definíciója szerint

$$\left(\tau_{k,z}\left((\mathfrak{a}_{i,\sigma'(i)})_{i\in I'}\right)\right)_i = \begin{cases} \mathfrak{a}_{i,\sigma'(i)} & \text{, ha } i \neq k \\ z & \text{, ha } i = k, \end{cases}$$

amiből következik, hogy ha az $\mathfrak{a}' \in \prod_{i\in I} E_i$ rendszert úgy értelmezzük, hogy minden $i \in I$ esetén

$$\mathfrak{a}'_i := \begin{cases} \mathfrak{a}_{i,\sigma'(i)} & \text{, ha } i \neq k \\ 0 & \text{, ha } i = k, \end{cases}$$

akkor fennáll az

$$\tau_{k,z}\left((\mathfrak{a}_{i,\sigma'(i)})_{i\in I'}\right) = \mathrm{in}_{k,\mathfrak{a}'}(z)$$

egyenlőség. (Megjegyezzük, hogy itt az $\mathfrak{a}'_k \in E_k$ vektor *bármi* lehetne, hiszen az $\mathrm{in}_{k,\mathfrak{a}'}$ leképezés *független* a $\mathfrak{a}'$ rendszer k-adik komponensétől.) Felhasználva az $u \circ \mathrm{in}_{k,\mathfrak{a}'} : E_k \to F$ leképezés additivitását és a $z := \sum_{j\in J_k} \mathfrak{a}_{k,j}$ definíciót kapjuk, hogy

$$(u \circ \tau_{k,z})\left((\mathfrak{a}_{i,\sigma'(i)})_{i\in I'}\right) = (u \circ \mathrm{in}_{k,\mathfrak{a}'})(z) = (u \circ \mathrm{in}_{k,\mathfrak{a}'})\Big(\sum_{j\in J_k} \mathfrak{a}_{k,j}\Big) = \sum_{j\in J_k} (u \circ \mathrm{in}_{k,\mathfrak{a}'})(\mathfrak{a}_{k,j}).$$

Vezessük be azt a $\varrho_k : J' \times J_k \to J$ függvényt, amelyre minden $(\sigma', j) \in J' \times J_k$ esetén minden $i \in I$ indexre

$$(\varrho_k(\sigma', j))(i) := \begin{cases} \sigma'(i) & \text{, ha } i \neq k \\ j & \text{, ha } i = k \end{cases}.$$

Világos, hogy ekkor minden $j \in J_k$ esetén

$$\mathrm{in}_{k,\mathfrak{a}'}(\mathfrak{a}_{k,j}) = \left(\mathfrak{a}_{i,(\varrho_k(\sigma',j))(i)}\right)_{i\in I}.$$

Ez azt jelenti, hogy

$$u\bigg(\Big(\sum_{j\in J_i} \mathfrak{a}_{i,j}\Big)_{i\in I}\bigg) = \sum_{\sigma'\in J'} \bigg(\sum_{j\in J_k} u\left(\left(\mathfrak{a}_{i,(\varrho_k(\sigma',j))(i)}\right)_{i\in I}\right)\bigg) =$$
$$= \sum_{(\sigma',j)\in J'\times J_k} u\left(\left(\mathfrak{a}_{i,(\varrho_k(\sigma',j))(i)}\right)_{i\in I}\right).$$

Nyilvánvaló, hogy a $\varrho_k : J' \times J_k \to J$ függvény bijekció, ezért

$$\sum_{(\sigma',j)\in J'\times J_k} u\left(\left(\mathfrak{a}_{i,(\varrho_k(\sigma',j))(i)}\right)_{i\in I}\right) = \sum_{\sigma\in J} u((\mathfrak{a}_{i,\sigma(i)})_{i\in I}),$$

így $\mathscr{A}(n+1)$ is igaz. ■

19.3.2. Definíció. *Ha* $(E_i)_{i\in I}$ *vektorterek nem üres, véges rendszere, valamint* $\mathfrak{a} := (\mathfrak{a}_i)_{i\in I} \in \prod_{i\in I} E_i$ *és* $\mathfrak{b} := (\mathfrak{b}_i)_{i\in I} \in \prod_{i\in I} E_i$, *akkor minden* $H \subseteq I$ *halmazra*

$$(\mathfrak{a}, \mathfrak{b})_H \in \prod_{i\in I} E_i$$

az a rendszer, amelyre minden $i \in I$ esetén

$$((\mathfrak{a},\mathfrak{b})_H)_i := \begin{cases} \mathfrak{a}_i & , \textit{ha } i \in H \\ \mathfrak{b}_i & , \textit{ha } i \notin H \end{cases}.$$

19.3.3. Következmény. *Legyen $(E_i)_{i\in I}$ vektorterek nem üres, véges rendszere, F vektortér, és $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$. Ekkor*

$$u(\mathfrak{a}+\mathfrak{b}) = u(\mathfrak{a}) + u(\mathfrak{b}) + \sum_{\substack{H\subseteq I \\ \emptyset\neq H\neq I}} u((\mathfrak{a},\mathfrak{b})_H).$$

Bizonyítás. Legyen minden $i \in I$ esetén $J_i := \{0,1\}$, és $\mathfrak{c}_{i,0} := \mathfrak{b}_i$ és $\mathfrak{c}_{i,1} := \mathfrak{a}_i$. Ekkor minden $i \in I$ esetén $(\mathfrak{c}_{i,j})_{j\in J_i}$ véges rendszer E_i-ben, és világos, hogy

$$\sum_{j\in J_i} \mathfrak{c}_{i,j} = \mathfrak{b}_i + \mathfrak{a}_i = \mathfrak{a}_i + \mathfrak{b}_i = (\mathfrak{a}+\mathfrak{b})_i,$$

tehát alkalmazva a 19.3.1. állítást kapjuk, hogy

$$u(\mathfrak{a}+\mathfrak{b}) = u\Big(\Big(\sum_{j\in J_i} \mathfrak{c}_{i,j}\Big)_{i\in I}\Big) = \sum_{\sigma\in\{0,1\}^I} u\left((\mathfrak{c}_{i,\sigma(i)})_{i\in I}\right),$$

hiszen $\prod_{i\in I} J_i = \{0,1\}^I$. Tudjuk, hogy a $\mathscr{P}(I) \to \{0,1\}^I;\ H \mapsto \chi_H$ leképezés *bijekció*, ezért

$$u(\mathfrak{a}+\mathfrak{b}) = \sum_{H\in\mathscr{P}(I)} u\big(\big(\mathfrak{c}_{i,\chi_H(i)}\big)_{i\in I}\big).$$

Minden $H \subseteq I$ esetén $\big(\mathfrak{c}_{i,\chi_H(i)}\big)_{i\in I}$ az az eleme $\prod_{i\in I} E_i$-nek, amelynek minden $i \in I$ esetén az i-edik komponense $\mathfrak{c}_{i,1} = \mathfrak{a}_i$, ha $i \in H$, és $\mathfrak{c}_{i,0} = \mathfrak{b}_i$, ha $i \notin H$, tehát a definíció szerint

$$\big(\mathfrak{c}_{i,\chi_H(i)}\big)_{i\in I} = (\mathfrak{a},\mathfrak{b})_H.$$

Ez azt jelenti, hogy

$$u(\mathfrak{a}+\mathfrak{b}) = \sum_{H\in\mathscr{P}(I)} u\left((\mathfrak{a},\mathfrak{b})_H\right) =$$

$$= u\left((\mathfrak{a},\mathfrak{b})_I\right) + u\left((\mathfrak{a},\mathfrak{b})_\emptyset\right) + \sum_{\substack{H\subseteq I \\ \emptyset\neq H\neq I}} u\left((\mathfrak{a},\mathfrak{b})_H\right),$$

amiből $(\mathfrak{a},\mathfrak{b})_I = \mathfrak{a}$ és $(\mathfrak{a},\mathfrak{b})_\emptyset = \mathfrak{b}$ miatt következik a bizonyítandó egyenlőség. ■

Vigyázzunk arra, hogy $\mathbf{L}\Big(\prod_{i\in I} E_i; F\Big)$ és $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ általában *teljesen különböző* lineáris alterek az $\mathscr{F}\Big(\prod_{i\in I} E_i; F\Big)$ függvénytérben; ha I legalább két elemű, akkor csak a 0 operátor a közös elemük. Ha $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$, akkor u általában nem homogén és nem is additív: ezek helyett u-ra multihomogenitás (19.2.1.) és multiadditivitás (19.3.1.) érvényes.

19.4. Példák multilineáris operátorokra

1) Ha $(E_i)_{i\in I}$ olyan vektortér rendszer, amelyre $\mathrm{Card}(I) = 1$, akkor a $\prod_{i\in I} E_i$ vektortér kanonikusan azonosul E-vel, ahol $E := E_i$ (az I indexhalmaz egyetlen i elemére), és ekkor minden F vektortérre $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ azonosul $\mathbf{L}(E; F)$-fel.

2) Legyenek E, F és G vektorterek. Egy $u : E \times F \to G$ leképezés pontosan akkor multilineáris, ha minden $f \in F$ esetén az $u(\cdot, f) : E \to G$ leképezés lineáris operátor, és minden $e \in E$ esetén az $u(e, \cdot) : F \to G$ leképezés lineáris operátor. Az $E \times F \to G$ multilineáris operátorokat *bilineáris* operátoroknak nevezzük.

3) Ha E vektortér a K test felett, akkor a

$$K \times E \to E; \quad (\alpha, x) \mapsto \alpha.x$$

leképezés bilineáris operátor. Speciálisan, ha K test, akkor a

$$K \times K \to K; \quad (\alpha, \beta) \mapsto \alpha \cdot \beta$$

leképezés is bilineáris operátor. Ennek általánosításaként könnyen látható, hogy ha K test és I nem üres véges halmaz, akkor a

$$\mathrm{P}_I : K^I \to K; \quad (\lambda_i)_{i\in I} \mapsto \mathop{\mathrm{P}}_{i\in I} \lambda_i$$

leképezés multilineáris operátor, mert ha $k \in I$ és $\mathbf{a} = (a_i)_{i\in I} \in K^I$, akkor minden $x \in K$ esetén $(\mathrm{P}_I \circ \mathrm{in}_{k,\mathbf{a}})(x) = \mathop{\mathrm{P}}_{i\in I} x_i$, ahol minden $i \in I$ indexre

$$x_i := \begin{cases} a_i & \text{, ha } i \neq k, \\ x & \text{, ha } i \neq k, \end{cases}$$

következésképpen

$$(\mathrm{P}_I \circ \mathrm{in}_{k,\mathbf{a}})(x) = \Big(\mathop{\mathrm{P}}_{i\in I\setminus\{k\}} x_i\Big) \cdot x_k = \Big(\mathop{\mathrm{P}}_{i\in I\setminus\{k\}} a_i\Big) \cdot x,$$

tehát a $\mathrm{P}_I \circ \mathrm{in}_{k,\mathbf{a}} : K \to K$ függvény egyenlő a $\mathop{\mathrm{P}}_{i\in I\setminus\{k\}} a_i \in K$ elemmel való szorzás lineáris operátorával, így $\mathrm{P}_I \in \mathbf{Mult}\left(K^I; K\right)$.

4) Ha A algebra, akkor az

$$A \times A \to A; \quad (a, b) \mapsto a \cdot b$$

belső szorzás bilineáris operátor.

5) Ha E, F és G vektorterek, akkor az

$$\mathbf{L}(E; F) \times \mathbf{L}(F; G) \to \mathbf{L}(E; G); \quad (u, v) \mapsto v \circ u$$

leképezés bilineáris operátor.

6) Ha E és F vektorterek, akkor az

$$\mathbf{L}(E; F) \times E \to F; \quad (u, x) \mapsto u(x)$$

leképezés bilineáris operátor.

7) Legyen $(E_i)_{i\in I}$ nem üres, véges vektortér-rendszer a K test felett, és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$. Ekkor a

$$\dot{\bigotimes_{i\in I}} x_i : \prod_{i\in I} E_i^* \to K; \quad (u_i)_{i\in I} \mapsto \prod_{i\in I} u_i(x_i)$$

leképezés multilineáris funkcionál, tehát $\dot{\bigotimes_{i\in I}} x_i \in \mathbf{Mult}\Big(\prod_{i\in I} E_i^*; K\Big)$. Valóban, ha $k \in I$ és $(u_i)_{i\in I} \in \prod_{i\in I} E_i^*$, akkor minden $E_k^* \ni u$-ra

$$\Big(\Big(\dot{\bigotimes_{i\in I}} x_i\Big) \circ \mathrm{in}_{k,(u_i)_{i\in I}}\Big)(u) = \Big(\prod_{i\in I\setminus\{k\}} u_i(x_i)\Big) \cdot u(x_k),$$

amiből látható, hogy $\Big(\dot{\bigotimes_{i\in I}} x_i\Big) \circ \mathrm{in}_{k,(u_i)_{i\in I}} : E_k^* \to K$ lineáris funkcionál. Megállapodunk abban, hogy a $\Big\{ \dot{\bigotimes_{i\in I}} x_i \;\Big|\; (x_i)_{i\in I} \in \prod_{i\in I} E_i \Big\}$ halmaz által generált $\mathbf{Mult}\Big(\prod_{i\in I} E_i^*; K\Big)$-beli lineáris alteret a $\dot{\bigotimes_{i\in I}} E_i$ szimbólummal jelöljük, és az $(E_i)_{i\in I}$ vektortér rendszer *konkrét tenzorszorzatának* nevezzük. Az

$$m : \prod_{i\in I} E_i \to \dot{\bigotimes_{i\in I}} E_i; \quad (x_i)_{i\in I} \mapsto \dot{\bigotimes_{i\in I}} x_i$$

leképezés multilineáris operátor, mert ha $k \in I$ és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ rögzítettek, akkor minden $x \in E_k$ és $(u_i)_{i\in I} \in \prod_{i\in I} E_i^*$ esetén a definíció szerint

$$\Big(\Big(m \circ \mathrm{in}_{k,(x_i)_{i\in I}}\Big)(x)\Big)\big((u_i)_{i\in I}\big) = \Big(\prod_{i\in I\setminus\{k\}} u_i(x_i)\Big) \cdot u_k(x),$$

amiből látható, hogy $m \circ \mathrm{in}_{k,(x_i)_{i\in I}} : E_k \to \dot{\bigotimes_{i\in I}} E_i$ lineáris operátor.

8) Legyen $(E_i)_{i\in I}$ nem üres, véges vektortér-rendszer a K test felett, és $(u_i)_{i\in I} \in \prod_{i\in I} E_i^*$. Ekkor a

$$\dot{\bigotimes_{i\in I}} u_i : \prod_{i\in I} E_i \to K; \quad (x_i)_{i\in I} \mapsto \prod_{i\in I} u_i(x_i)$$

leképezés multilineáris funkcionál, tehát $\dot{\bigotimes_{i\in I}} u_i \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$. Valóban, ha $k \in I$ és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$, akkor minden $E_k \ni x$-re

$$\Big(\Big(\dot{\bigotimes_{i\in I}} u_i\Big) \circ \mathrm{in}_{k,(x_i)_{i\in I}}\Big)(x) = \Big(\prod_{i\in I\setminus\{k\}} u_i(x_i)\Big) \cdot u_k(x),$$

amiből látható, hogy $\Big(\dot{\bigotimes_{i\in I}} u_i\Big) \circ \mathrm{in}_{k,(x_i)_{i\in I}} : E_k \to K$ lineáris funkcionál. Megállapodunk abban, hogy a $\Big\{ \dot{\bigotimes_{i\in I}} u_i \;\Big|\; (u_i)_{i\in I} \in \prod_{i\in I} E_i^* \Big\}$ halmaz által generált $\mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$-beli lineáris alteret a $\dot{\bigotimes\limits_{i\in I}} E_i^*$ szimbólummal jelöljük, és az $(E_i^*)_{i\in I}$ vektortér rendszer *konkrét tenzorszorzatának* nevezzük. Az

$$m : \prod_{i\in I} E_i^* \to \dot{\bigotimes_{i\in I}} E_i^*; \quad (u_i)_{i\in I} \mapsto \dot{\bigotimes_{i\in I}} u_i$$

leképezés multilineáris operátor, mert ha $k \in I$ és $(u_i)_{i\in I} \in \prod\limits_{i\in I} E_i^*$ rögzítettek, akkor minden $u \in E_k^*$ és $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén a definíció szerint

$$\Big(\Big(m \circ \mathrm{in}_{k,(u_i)_{i\in I}}\Big)(u)\Big)\,((x_i)_{i\in I}) = \Big(\mathop{\mathrm{P}}_{i\in I\setminus\{k\}} u_i(x_i)\Big) \cdot u(x_k),$$

amiből látható, hogy $m \circ \mathrm{in}_{k,(u_i)_{i\in I}} : E_k^* \to \dot{\bigotimes\limits_{i\in I}} E_i^*$ lineáris operátor.

19.5. Multilineáris operátorok véges dimenziós terek között

19.5.1. Állítás. *Legyen $(E_i)_{i\in I}$ nem üres, véges vektortér-rendszer és F vektortér a K test felett. Tegyük fel, hogy minden $i \in I$ esetén E_i véges dimenziós és $\Big((u_{i,j})_{j\in J_i}\Big)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ indexre $(u_{i,j})_{j\in J_i}$ bázis az E_i^* vektortérben. Legyen továbbá $(z_l)_{l\in L}$ bázis az F vektortében, és alkalmazzuk a $J := \prod\limits_{i\in I} J_i$ definíciót. Ekkor az*

$$\Big(\Big(\mathring{\bigotimes_{i\in I}} u_{i,\sigma(i)}\Big) \dot{\otimes}\, z_l\Big)_{(l,\sigma)\in L\times J} \tag{1}$$

rendszer (ld. **ALG** 19.4.8. példa és 19.1.4.) *bázis a* $\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; F\Big)$ *multilineáris operátortérben, és ha F véges dimenziós, akkor* $\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; F\Big)$ *is véges dimenziós, és fennáll a*

$$\dim\Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)\Big) = (\dim(F)) \cdot \Big(\mathop{\mathrm{P}}_{i\in I} \dim(E_i)\Big) \tag{2}$$

egyenlőség. Speciálisan, ha E és F véges dimenziós vektorterek, akkor minden $n \in \mathbb{N}^*$ esetén

$$\dim(\mathbf{L}_n(E; F)) = (\dim(F)) \cdot (\dim(E))^n. \tag{3}$$

Bizonyítás. Minden $i \in I$ indexre legyen $(e_{i,j})_{j\in J_i}$ az a bázis az E_i vektortérben, amelyre minden $j, j' \in J_i$ esetén $u_{i,j}(e_{i,j'}) = \delta_{j,j'}$ (17.9.11.). Vegyünk tetszőleges $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ rendszert. Ha $i \in I$, akkor egyértelműen létezik olyan $(x_{i,j})_{j\in J_i} \in K^{J_i}$ rendszer, amelyre $x_i = \sum\limits_{j\in J_i} x_{i,j} e_{i,j}$, és ekkor minden $k \in J_i$ esetén

$$u_{i,k}(x_i) = \sum_{j\in J_i} x_{i,j} u_{i,k}(e_{i,j}) = \sum_{j\in J_i} x_{i,j}\delta_{k,j} = x_{i,k},$$

ami azt jelenti, hogy

$$x_i = \sum_{j \in J_i} u_{i,j}(x_i)\, e_{i,j}.$$

Legyen $m \in \mathbf{Mult}\Big(\prod_{i \in I} E_i; F\Big)$. Ekkor a multilineáris operátorok multiadditivitásának és multihomogenitásának tételei szerint

$$m\left((x_i)_{i\in I}\right) = m\Big(\Big(\sum_{j \in J_i} u_{i,j}(x_i)\, e_{i,j}\Big)_{i\in I}\Big) = \sum_{\sigma \in J} m\left(\left(u_{i,\sigma(i)}(x_i)\, e_{i,\sigma(i)}\right)_{i\in I}\right) =$$

$$= \sum_{\sigma\in J}\Big(\mathrm{P}_{i\in I}\, u_{i,\sigma(i)}(x_i)\Big) m\left(\left(e_{i,\sigma(i)}\right)_{i\in I}\right) = \sum_{\sigma\in J}\Big(\Big(\mathop{\mathring{\otimes}}_{i\in I} u_{i,\sigma(i)}\Big)\left((x_i)_{i\in I}\right)\Big) m\left(\left(e_{i,\sigma(i)}\right)_{i\in I}\right) =$$

$$= \Big(\sum_{\sigma\in J}\Big(\mathop{\mathring{\otimes}}_{i\in I} u_{i,\sigma(i)}\Big) \dot{\otimes}\, m\left(\left(e_{i,\sigma(i)}\right)_{i\in I}\right)\Big)\left((x_i)_{i\in I}\right),$$

ami azt jelenti, hogy

$$m = \sum_{\sigma\in J}\Big(\mathop{\mathring{\otimes}}_{i\in I} u_{i,\sigma(i)}\Big) \dot{\otimes}\, m\left(\left(e_{i,\sigma(i)}\right)_{i\in I}\right).$$

Ugyanakkor, minden $\sigma \in J$ esetén létezik olyan $L_\sigma \subseteq L$ véges halmaz és olyan $(\lambda_{\sigma,l})_{l\in L_\sigma} \in K^{L_\sigma}$ rendszer, hogy

$$m\left(\left(e_{i,\sigma(i)}\right)_{i\in I}\right) = \sum_{l\in L_\sigma} \lambda_{\sigma,l}.z_l,$$

következésképpen

$$m = \sum_{\sigma\in J}\sum_{l\in L_\sigma} \lambda_{\sigma,l}\Big(\mathop{\mathring{\otimes}}_{i\in I} u_{i,\sigma(i)}\Big) \dot{\otimes}\, z_l.$$

Ezért az (1) rendszer generátorrendszer a $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ multilineáris operátortérben.

Az (1) rendszer lineáris függetlenségének bizonyításához legyen $L_* \subseteq L$ véges halmaz, és $(\alpha_{\sigma,l})_{(\sigma,l)\in J\times L_*}$ olyan rendszer a K testben, amelyre

$$\sum_{(\sigma,l)\in J\times L_*} \alpha_{\sigma,l}\Big(\mathop{\dot{\otimes}}_{i\in I} u_{i,\sigma(i)}\Big) \dot{\otimes}\, z_l = 0.$$

Ha $\sigma' \in J$, akkor

$$0 = \Big(\sum_{(\sigma,l)\in J\times L_*} \alpha_{\sigma,l}\Big(\mathop{\mathring{\otimes}}_{i\in I} u_{i,\sigma(i)}\Big) \dot{\otimes}\, z_l\Big)\left(\left(e_{i,\sigma'(i)}\right)_{i\in I}\right) =$$

$$= \sum_{(\sigma,l)\in J\times L_*} \alpha_{\sigma,l}\Big(\mathrm{P}_{i\in I}\, u_{i,\sigma(i)}\left(e_{i,\sigma'(i)}\right)\Big).z_l =$$

$$= \sum_{(\sigma,l)\in J\times L_*} \alpha_{\sigma,l}\Big(\mathrm{P}_{i\in I}\, \delta_{\sigma(i),\sigma'(i)}\Big).z_l = \sum_{(\sigma,l)\in J\times L_*} \alpha_{\sigma,l}\delta_{\sigma,\sigma'}.z_l = \sum_{l\in L_*} \alpha_{\sigma',l}.z_l,$$

így az $(z_l)_{l\in L_*}$ rendszer lineáris függetlensége miatt minden $l \in L_*$ esetén $\alpha_{\sigma',l} = 0$. Ezért az (1) rendszer lineárisan független.

Ha F véges dimenziós, akkor ebből a (2) egyenlőség azonnal következik, hiszen ekkor $\mathrm{Card}(L) = \dim(F)$ és minden $i \in I$ esetén $\mathrm{Card}\,(J_i) = \dim\,(E_i)$, ugyanakkor

$$\dim\Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)\Big) = \mathrm{Card}\,(L \times J) =$$
$$= \mathrm{Card}(L) \cdot \mathrm{Card}(J) = \mathrm{Card}(L) \cdot \Big(\underset{i\in I}{\mathrm{P}}\,\mathrm{Card}\,(E_i)\Big).$$

A (3) egyenlőség a (2) egyenlőség speciális esete, amikor $I := n$ és minden $i \in I$ esetén $E_i := E$. ■

19.6. Kanonikus azonosítások multilineáris operátorok között

19.6.1. Állítás. *Legyenek $(E_i)_{i\in I}$ és $(F_j)_{j\in J}$ vektortér-rendszerek. Jelölje F az $(F_j)_{j\in J}$ vektortér-rendszer szorzatát, és minden $j \in J$ esetén legyen pr_j az $F \to F_j$ kanonikus projekció. Ekkor minden $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ és $j \in J$ esetén $\mathrm{pr}_j \circ u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F_j\Big)$, továbbá a*

$$\mathbf{Mult}\Big(\prod_{i\in I} E_i; \prod_{j\in J} F_j\Big) \to \prod_{j\in J}\Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; F_j\Big)\Big); \quad u \mapsto \big(\mathrm{pr}_j \circ u\big)_{j\in J} \tag{1}$$

leképezés izomorfizmus a $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ és $\prod_{j\in J}\Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; F_j\Big)\Big)$ vektorterek között.

Bizonyítás. Jelölje E az $(E_i)_{i\in I}$ vektortér-rendszer szorzatát. Legyen $u \in \mathbf{Mult}\,(E; F)$ és $j \in J$. Ha $i \in I$ és $\mathfrak{a} \in E$, akkor $u \circ \mathrm{in}_{i,\mathfrak{a}} \in \mathbf{L}(E_i; F)$ és $\mathrm{pr}_j \in \mathbf{L}\,(F; F_j)$, tehát $\big(\mathrm{pr}_j \circ u\big) \circ \mathrm{in}_{i,\mathfrak{a}} = \mathrm{pr}_j \circ (u \circ \mathrm{in}_{i,\mathfrak{a}}) \in \mathbf{L}(E_i; F_j)$, ami azt jelenti, hogy $\mathrm{pr}_j \circ u \in \mathbf{Mult}\,(E; F_j)$. Nyilvánvaló, hogy az (1) leképezés lineáris, továbbá, ha $u \in \mathfrak{Mult}\,(E; F)$ olyan, hogy $\big(\mathrm{pr}_j \circ u\big)_{j\in J} = \mathbf{0}$, akkor minden $j \in J$ esetén $\mathrm{pr}_j \circ u = \mathbf{0}$, amiből következik, hogy $u = \mathbf{0}$, ami azt jelenti, hogy az (1) leképezés injektív. E leképezés szürjektivitásának bizonyításához legyen $(v_j)_{j\in J} \in \prod_{j\in J} \mathbf{Mult}(E; F_j)$. Értelmezzük az

$$u : E \to F; \quad x \mapsto (v_j(x))_{j\in J}$$

leképezést. Ha $i \in I$, $\mathfrak{a} \in E$, és $z \in E_i$, akkor $(u \circ \mathrm{in}_{i,\mathfrak{a}})\,(z) = \big((v_j \circ \mathrm{in}_{i,\mathfrak{a}})\,(z)\big)_{j\in J}$, és minden $j \in J$ esetén $v_j \circ \mathrm{in}_{i,\mathfrak{a}} : E_i \to F_j$ lineáris operátor, ezért $u \circ \mathrm{in}_{i,\mathfrak{a}} : E_i \to F$ is lineáris operátor, ami azt jelenti, hogy az $u : E \to F$ leképezés multilineáris operátor. Ugyanakkor világos, hogy $\big(\mathrm{pr}_j \circ u\big)_{j\in J} = (v_j)_{j\in J}$, következésképpen az (1) leképezés szürjektív. ■

19.6.2. Állítás. *Legyen $(E_i)_{i\in I}$ vektortér-rendszer és F vektortér a K test felett.*

a) *Ha J halmaz és $\sigma : J \to I$ bijekció, akkor minden $m \in \mathbf{Mult}\Big(\prod_{j\in J} E_{\sigma(j)}; F\Big)$ esetén a*

$$\widehat{\sigma}(m) : \prod_{i\in I} E_i \to F; \quad (x_i)_{i\in I} \mapsto m\left(\big(x_{\sigma(j)}\big)_{j\in J}\right)$$

leképezés multilineáris operátor, és a

$$\widehat{\sigma} : \mathbf{Mult}\Big(\prod_{j\in J} E_{\sigma(j)}; F\Big) \to \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big); \quad m \mapsto \widehat{\sigma}(m)$$

leképezés izomorfizmus a $\mathbf{Mult}\Big(\prod_{j\in J} E_{\sigma(j)}; F\Big)$ *és* $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ *multilineáris operátorterek között.*

b) *Ha J és K halmazok, valamint $\tau : K \to J$ és $\sigma : J \to I$ bijekciók, akkor*

$$\widehat{\sigma \circ \tau} = \widehat{\sigma} \circ \widehat{\tau}.$$

Bizonyítás. Legyen J halmaz és $\sigma : J \to I$ bijekció. Legyen $m \in \mathbf{Mult}\Big(\prod_{j\in J} E_{\sigma(j)}; F\Big)$, és rögzítsük a $k \in I$ és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ objektumokat. Ha $x \in E_k$, és minden $i \in I$ esetén

$$x'_i := \begin{cases} x_i & , \text{ha } i \neq k, \\ x & , \text{ha } i = k, \end{cases}$$

akkor nyilvánvaló, hogy $(x'_i)_{i\in I} = \mathrm{in}_{k,(x_i)_{i\in I}}(x)$, és minden $j \in J$ indexre

$$x'_{\sigma(j)} := \begin{cases} x_{\sigma(j)} & , \text{ha } j \neq \sigma^{-1}(k), \\ x & , \text{ha } j = \sigma^{-1}(k), \end{cases}$$

következésképpen $\left(x'_{\sigma(j)}\right)_{j\in J} = \mathrm{in}_{\sigma^{-1}(k),\left(x_{\sigma(j)}\right)_{j\in J}}(x)$, ezért

$$\left(\widehat{\sigma}(m) \circ \mathrm{in}_{k,(x_i)_{i\in I}}\right)(x) = \widehat{\sigma}(m)\left((x'_i)_{i\in I}\right) = m\Big(\left(x'_{\sigma(j)}\right)_{j\in J}\Big) = \Big(m \circ \mathrm{in}_{\sigma^{-1}(k),\left(x_{\sigma(j)}\right)_{j\in J}}\Big)(x).$$

Az m leképezés multilinearitása miatt ez azt jelenti, hogy

$$\widehat{\sigma}(m) \circ \mathrm{in}_{k,(x_i)_{i\in I}} = m \circ \mathrm{in}_{\sigma^{-1}(k),\left(x_{\sigma(j)}\right)_{j\in J}} \in \mathbf{L}\left(E_k; F\right),$$

így $\widehat{\sigma}(m) \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$.

Ezért jól értelmezett a

$$\widehat{\sigma} : \mathbf{Mult}\Big(\prod_{j\in J} E_{\sigma(j)}; F\Big) \to \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$$

leképezés, amely lineáris operátor, mert $m, m' \in \mathbf{Mult}\Big(\prod_{j\in J} E_{\sigma(j)}; F\Big)$ és $\lambda \in K$ esetén minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ rendszerre

$$\widehat{\sigma}(m+m')\left((x_i)_{i\in I}\right) = (m+m')\left(\left(x_{\sigma(j)}\right)_{j\in J}\right) = m\left(\left(x_{\sigma(j)}\right)_{j\in J}\right) + m'\left(\left(x_{\sigma(j)}\right)_{j\in J}\right) =$$
$$= \widehat{\sigma}(m)\left((x_i)_{i\in I}\right) + \widehat{\sigma}(m')\left((x_i)_{i\in I}\right) = \left(\widehat{\sigma}(m) + \widehat{\sigma}(m')\right)\left((x_i)_{i\in I}\right),$$

tehát $\widehat{\sigma}(m+m') = \widehat{\sigma}(m) + \widehat{\sigma}(m')$, továbbá

$$\begin{aligned}\widehat{\sigma}(\lambda.m)\left((x_i)_{i\in I}\right) &= (\lambda.m)\left(\left(x_{\sigma(j)}\right)_{j\in J}\right) = \lambda.m\left(\left(x_{\sigma(j)}\right)_{j\in J}\right) = \\ &= \lambda.\widehat{\sigma}(m)\left((x_i)_{i\in I}\right) = (\lambda.\widehat{\sigma}(m))\left((x_i)_{i\in I}\right),\end{aligned}$$

tehát $\widehat{\sigma}(\lambda.m) = \lambda.\widehat{\sigma}(m)$.

Legyenek most J és K halmazok, valamint $\tau : K \to J$ és $\sigma : J \to I$ bijekciók. Ekkor minden $m \in \mathbf{Mult}\Big(\prod_{k\in K} E_{\sigma(\tau(k))}; F\Big)$ és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén

$$\widehat{\sigma\circ\tau}(m)\left((x_i)_{i\in I}\right) = m\left(\left(x_{\sigma(\tau(k))}\right)_{k\in K}\right) = \widehat{\tau}(m)\left(\left(x_{\sigma(j)}\right)_{j\in J}\right) = \widehat{\sigma}\left(\widehat{\tau}(m)\right)\left((x_i)_{i\in I}\right),$$

tehát $\widehat{\sigma\circ\tau} = \widehat{\sigma}\circ\widehat{\tau}$. Ezzel a b) állításban szereplő egyenlőséget igazoltuk, és egyidejűleg az is látható, hogy

$$\widehat{\sigma}\circ\widehat{\sigma^{-1}} = \widehat{\sigma\circ\sigma^{-1}} = \widehat{\mathrm{id}_I} = \widehat{\sigma^{-1}\circ\sigma} = \widehat{\sigma^{-1}}\circ\widehat{\sigma},$$

ezért a $\widehat{\sigma}$ leképezés bijekció és $\widehat{\sigma}^{-1} = \widehat{\sigma^{-1}}$, hiszen $\widehat{\mathrm{id}_I}$ nyilvánvalóan megegyezik a $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ halmaz identikus függvényével. Ezzel az a) állítást is igazoltuk. ■

19.6.3. Következmény. *Legyen I halmaz. Ha E és F vektorterek, akkor az*

$$\mathfrak{S}(I) \to \mathbf{GL}\left(\mathbf{Mult}\left(E^I; F\right)\right); \quad \sigma \mapsto \widehat{\sigma}$$

leképezés lineáris ábrázolása az $\mathfrak{S}(I)$ teljes permutációcsoportnak a $\mathbf{Mult}\left(E^I; F\right)$ multilineáris operátortérben.

Bizonyítás. Elég alkalmazni az előző állítást arra az $(E_i)_{i\in I}$ vektortér-rendszerre, amelyre minden $i \in I$ esetén $E_i := E$. ■

19.6.4. Állítás. *Legyen $(E_i)_{i\in I}$ vektortér-rendszer és F vektortér. Ha A és B olyan diszjunkt halmazok, hogy $I = A\cup B$, akkor minden $u \in \mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$ esetén a*

$$\widehat{u} : \prod_{i\in I} E_i \to F; \quad (x_i)_{i\in I} \mapsto u\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right)$$

leképezés multilineáris operátor, és a

$$\mathrm{p} : \mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big) \to \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big); \quad u \mapsto \widehat{u}$$

leképezés izomorfizmus a $\mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$ és $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ vektorterek között.

Bizonyítás. Legyen $u \in \mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$, és rögzítsük a $k \in I$, $\mathbf{x} := (x_i)_{i\in I} \in \prod_{i\in I} E_i$ és $x \in E_k$ objektumokat. Világos, hogy

$$\left(\widehat{u}\circ \mathrm{in}_{k,\mathbf{x}}\right)(x) = \widehat{u}\left((x'_i)_{i\in I}\right) = u\left((x'_i)_{i\in A}\right)\left((x'_i)_{i\in B}\right),$$

ahol minden $i \in I$ esetén

$$x'_i := \begin{cases} x_i & \text{, ha } i \neq k, \\ x & \text{, ha } i = k. \end{cases}$$

Ha $k \in A$, akkor $(x'_i)_{i\in B} = (x_i)_{i\in B}$ és $(x'_i)_{i\in A} = \mathrm{in}_{k,(x_i)_{i\in A}}(x)$, következésképpen

$$(\widehat{u} \circ \mathrm{in}_{k,\mathbf{x}})(x) = \left(u \circ \mathrm{in}_{k,(x_i)_{i\in A}}\right)(x)\left((x_i)_{i\in B}\right),$$

így $u \circ \mathrm{in}_{k,(x_i)_{i\in A}} \in \mathbf{L}\Big(E_k; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$ miatt az $\widehat{u} \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to F$ leképezés lineáris operátor. Ha $k \in B$, akkor $(x'_i)_{i\in A} = (x_i)_{i\in A}$ és $(x'_i)_{i\in B} = \mathrm{in}_{k,(x_i)_{i\in B}}(x)$, következésképpen

$$(\widehat{u} \circ \mathrm{in}_{k,\mathbf{x}})(x) = \left(u\left((x_i)_{i\in A}\right) \circ \mathrm{in}_{k,(x_i)_{i\in B}}\right)(x),$$

és $u\left((x_i)_{i\in A}\right) \in \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)$ miatt $u\left((x_i)_{i\in A}\right) \circ \mathrm{in}_{k,(x_i)_{i\in B}} \in \mathbf{L}(E_k; F)$, következésképpen az $\widehat{u} \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to F$ leképezés lineáris operátor. Tehát az $\widehat{u} : \prod_{i\in I} E_i \to F$ leképezés multilineáris operátor.

Könnyen látható, hogy a

$$\mathrm{p} : \mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big) \to \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big); \quad u \mapsto \widehat{u}$$

leképezés lineáris operátor, mert ha $u, v \in \mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$ és $\lambda \in K$, akkor minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén

$$\begin{aligned} \widehat{u+v}\left((x_i)_{i\in I}\right) &= (u+v)\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right) = \left(u\left((x_i)_{i\in A}\right) + v\left((x_i)_{i\in A}\right)\right)\left((x_i)_{i\in B}\right) = \\ &= u\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right) + v\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right) = \widehat{u}\left((x_i)_{i\in I}\right) + \widehat{v}\left((x_i)_{i\in I}\right), \end{aligned}$$

tehát $\widehat{u+v} = \widehat{u} + \widehat{v}$; továbbá

$$\begin{aligned} \widehat{\lambda.u}\left((x_i)_{i\in I}\right) &= (\lambda.u)\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right) = \left(\lambda.u\left((x_i)_{i\in A}\right)\right)\left((x_i)_{i\in B}\right) = \\ &= \lambda.\left(u\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right)\right) = \lambda.\widehat{u}\left((x_i)_{i\in I}\right), \end{aligned}$$

tehát $\widehat{\lambda.u} = \lambda.\widehat{u}$.

A p lineáris operátor injektív. Valóban, legyen $u \in \mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$ olyan, hogy $\widehat{u} = 0$, vagyis minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén $u\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right) = 0$. Legyen $(x_i)_{i\in A} \in \prod_{i\in A} E_i$ rögzített. Ekkor $(x_i)_{i\in B} \in \prod_{i\in B} E_i$ esetén $u\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right) = \widehat{u}\left((x_i)_{i\in I}\right) = 0$, tehát $u\left((x_i)_{i\in A}\right) = 0$, így $u = 0$.

A p lineáris operátor szürjektivitásának bizonyításához legyen $v \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ rögzítve. Olyan $u \in \mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$ multilineáris operátort keresünk, amelyre $\widehat{u} = \mathrm{p}(u) = v$.

Legyen minden $\mathbf{x} = (x_i)_{i\in A} \in \prod_{i\in A} E_i$ és $\mathbf{y} = (y_i)_{i\in B} \in \prod_{i\in B} E_i$ esetén $\tau(\mathbf{x},\mathbf{y}) \in \prod_{i\in I} E_i$ az a rendszer, amelyre minden $i \in I$ indexre

$$\tau(\mathbf{x},\mathbf{y})_i := \begin{cases} x_i & \text{, ha } i \in A, \\ y_i & \text{, ha } i \in B. \end{cases}$$

Először megmutatjuk, hogy minden $\mathbf{x} \in \prod_{i\in A} E_i$ esetén az

$$u_{\mathbf{x}} : \prod_{i\in B} E_i \to F; \quad \mathbf{y} \mapsto v(\tau(\mathbf{x},\mathbf{y}))$$

leképezés multilineáris, majd bebizonyítjuk, hogy az

$$u : \prod_{i\in A} E_i \to \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big); \quad \mathbf{x} \mapsto u_{\mathbf{x}}$$

leképezés olyan multilineáris operátor, amelyre $\widehat{u} = v$, tehát $\mathrm{p}(u) = v$.

Legyen $\mathbf{x} = (x_i)_{i\in A} \in \prod_{i\in A} E_i$, és rögzítsük a $k \in B$ és $\mathbf{y} = (y_i)_{i\in B} \in \prod_{i\in B} E_i$ objektumokat. A definíciók szerint nyilvánvaló, hogy ha $y \in E_k$ és $(y'_i)_{i\in B} \in \prod_{i\in B} E_i$ az a rendszer, amelyre minden $i \in B$ esetén

$$y'_i := \begin{cases} y_i & \text{, ha } i \neq k, \\ y & \text{, ha } i = k, \end{cases}$$

továbbá $(z_i)_{i\in I} \in \prod_{i\in I} E_i$ az a rendszer, amelyre minden $i \in I$ esetén

$$z_i := \begin{cases} x_i & \text{, ha } i \in A, \\ y'_i & \text{, ha } i \in B, \end{cases}$$

akkor világos, hogy $(y'_i)_{i\in B} = \mathrm{in}_{k,\mathbf{y}}(y)$ és $(z_i)_{i\in I} = \tau\left(\mathbf{x}, (y'_i)_{i\in B}\right) = \mathrm{in}_{k,\tau(\mathbf{x},\mathbf{y})}(y)$, következésképpen

$$\left(u_{\mathbf{x}} \circ \mathrm{in}_{k,\mathbf{y}}\right)(y) = u_{\mathbf{x}}\left((y'_i)_{i\in B}\right) = v\left(\tau\left(\mathbf{x}, (y'_i)_{i\in B}\right)\right) = v\left((z_i)_{i\in I}\right) = \left(v \circ \mathrm{in}_{k,\tau(\mathbf{x},\mathbf{y})}\right)(y),$$

így v multilinearitása miatt $u_{\mathbf{x}} \circ \mathrm{in}_{k,\mathbf{y}} = v \circ \mathrm{in}_{k,\tau(\mathbf{x},\mathbf{y})} \in \mathbf{L}\left(E_k; F\right)$, ami azt jelenti, hogy $u_{\mathbf{x}}$ multilineáris operátor.

Most az

$$u : \prod_{i\in A} E_i \to \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big); \quad \mathbf{x} \mapsto u_{\mathbf{x}}$$

leképezés multilinearitását fogjuk igazolni. Ehhez legyen $k \in A$ és $\mathbf{x} = (x_i)_{i\in A} \in \prod_{i\in A} E_i$ rögzítve. Ha $x \in E_k$ és $(x'_i)_{i\in A} \in \prod_{i\in A} E_i$ az a rendszer, amelyre minden $i \in A$ esetén

$$x'_i := \begin{cases} x_i & \text{, ha } i \neq k, \\ x & \text{, ha } i = k, \end{cases}$$

akkor világos, hogy $(x'_i)_{i\in A} = \mathrm{in}_{k,\mathbf{x}}(x)$, és minden $\mathbf{y} \in \prod_{i\in B} E_i$ esetén $\tau\left((x'_i)_{i\in A}, \mathbf{y}\right) = \mathrm{in}_{k,\tau(\mathbf{x},\mathbf{y})}(x)$, következésképpen

$$(u \circ \mathrm{in}_{k,\mathbf{x}})(x)(\mathbf{y}) = u_{\left(x'_i\right)_{i\in A}}(\mathbf{y}) = v\left(\tau\left((x'_i)_{i\in A}, \mathbf{y}\right)\right) = \left(v \circ \mathrm{in}_{k,\tau(\mathbf{x},\mathbf{y})}\right)(x),$$

amiből $v \circ \mathrm{in}_{k,\tau(\mathbf{x},\mathbf{y})} \in \mathbf{L}(E_k; F)$ miatt látható, hogy $u \circ \mathrm{in}_{k,\mathbf{x}} \in \mathbf{L}\Big(E_k; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$. Ez azt jelenti, hogy u multilineáris operátor.

Végül, ha $(x_i)_{i\in I} \in \prod_{i\in I} E_i$, akkor nyilvánvaló, hogy $(x_i)_{i\in I} = \tau\left((x_i)_{i\in A}, (x_i)_{i\in B}\right)$, ezért

$$\widehat{u}\left((x_i)_{i\in I}\right) = u\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right) = u_{(x_i)_{i\in A}}\left((x_i)_{i\in B}\right) = v\left(\tau\left((x_i)_{i\in A}, (x_i)_{i\in B}\right)\right) = v\left((x_i)_{i\in I}\right),$$

tehát $\mathrm{p}(u) = \widehat{u} = v$. ■

19.6.5. Definíció. *Ha $(E_i)_{i\in I}$ vektortér-rendszer és F vektortér, valamint A és B olyan diszjunkt halmazok, hogy $I = A \cup B$, akkor a*

$$\mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big) \to \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big);$$

$$u \mapsto \left((x_i)_{i\in I} \mapsto u\left((x_i)_{i\in A}\right)\left((x_i)_{i\in B}\right)\right)$$

leképezést a $\mathbf{Mult}\Big(\prod_{i\in A} E_i; \mathbf{Mult}\Big(\prod_{i\in B} E_i; F\Big)\Big)$ és $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ multilineáris operátorterek közötti **kanonikus azonosításnak** *nevezzük.*

19.6.6. Következmény. *Ha E és F vektorterek, valamint $m, n \in \mathbb{N}$, akkor minden $u \in \mathbf{L}_m(E; \mathbf{L}_n(E; F))$ esetén az*

$$\widehat{u} : E^{m+n} \to F; \quad (x_i)_{i\in m+n} \mapsto u\left((x_i)_{i\in m}\right)\left((x_{m+i})_{i\in n}\right)$$

leképezés eleme $\mathbf{L}_{m+n}(E; F)$-nek, és az

$$\mathbf{L}_m(E; \mathbf{L}_n(E; F)) \to \mathbf{L}_{m+n}(E; F); \quad u \mapsto \widehat{u}$$

leképezés izomorfizmus az $\mathbf{L}_m(E; \mathbf{L}_n(E; F))$ és $\mathbf{L}_{m+n}(E; F)$ vektorterek között.

Bizonyítás. Elegendő az előző állítást alkalmazni a következő szereposztással: $I := m+n$, $A := m$, $B := \{m+i | i \in n\}$ és minden $i \in I$ esetén $E_i := E$. ■

19.7. Vektortér-rendszer tenzorszorzata

19.7.1. Tétel. *Legyen $(E_i)_{i\in I}$ a K test feletti vektortereknek tetszőleges rendszere.*

a) *Létezik olyan (T, m) pár, amelyre rendelkezik a következő tulajdonsággal.*

(ET) *T vektortér a K test felett és $m : \prod_{i\in I} E_i \to T$ olyan multilineáris operátor, hogy minden K feletti F vektortérhez és minden $u : \prod_{i\in I} E_i \to F$ multilineáris operátorhoz* *létezik egyetlen olyan $\widetilde{u} : T \to F$ lineáris operátor, hogy $\widetilde{u} \circ m = u$, vagyis a következő diagram kommutatív*

$$\begin{tikzcd} \prod_{i\in I} E_i \arrow[r, "m"] \arrow[dr, "u"'] & T \arrow[d, "\widetilde{u}"] \\ & F \end{tikzcd}$$

b) *Ha $(\widetilde{T}, \widetilde{m})$ szintén olyan pár, amelyre* (ET) *teljesül, (T, m) helyett $(\widetilde{T}, \widetilde{m})$-t írva, akkor létezik egyetlen olyan $w : T \to \widetilde{T}$ lineáris bijekció, amelyre $w \circ m = \widetilde{m}$.*

Bizonyítás. a) Legyen $E := \prod_{i\in I} E_i$, és jelölje $(\mathbf{e_x})_{\mathbf{x}\in E}$ a $K^{(E)}$ függvénytér kanonikus bázisát, tehát minden $\mathbf{x} \in E$ esetén $\mathbf{e_x} : E \to K$ az a függvény, amelyre minden $\mathbf{x}' \in E$ esetén $\mathbf{e_x}(\mathbf{x}') = 1$, ha $\mathbf{x} = \mathbf{x}'$, és $\mathbf{e_x}(\mathbf{x}') = 0$, ha $\mathbf{x} \neq \mathbf{x}'$. Vezessük be a következő $A, B \subseteq K^{(E)}$ halmazokat:

$$A := \left\{ \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y+z)} - \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)} - \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(z)} \;\middle|\; (k \in I) \wedge (y \in E_k) \wedge (z \in E_k) \wedge (\mathbf{x} \in E) \right\},$$
$$B := \left\{ \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(\lambda.y)} - \lambda.\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)} \;\middle|\; (k \in I) \wedge (y \in E_k) \wedge (\lambda \in K) \wedge (\mathbf{x} \in E) \right\}.$$

Legyen $M := \mathrm{sp}(A \cup B)$, és vezessük be a $T := K^{(E)}/M$ lineáris faktorteret. Jelölje π a $K^{(E)} \to T$ kanonikus szürjekciót, és értelmezzük az

$$m : \prod_{i\in I} E_i \to T; \quad \mathbf{x} \mapsto \pi(\mathbf{e_x})$$

leképezést. Megmutatjuk, hogy a (T, m) párra teljesül (ET).

Az $m : \prod_{i\in I} E_i \to T$ leképezés multilinearitásának bizonyításához legyen $k \in I$ és $\mathbf{x} \in \prod_{i\in I} E_i$ rögzített. Ha $y, z \in E_k$, akkor $\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y+z)} - \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)} - \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(z)} \in A \subseteq \mathrm{Ker}(\pi)$, következésképpen π additivitása folytán

$$m(\mathrm{in}_{k,\mathbf{x}}(y+z)) = \pi\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y+z)}\right) = \pi\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)}\right) + \pi\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(z)}\right) = m(\mathrm{in}_{k,\mathbf{x}}(y)) + m(\mathrm{in}_{k,\mathbf{x}}(z)),$$

tehát az $m \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to T$ leképezés additív. Ha $y \in E_k$ és $\lambda \in K$, akkor $\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(\lambda.y)} - \lambda.\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)} \in B \subseteq \mathrm{Ker}(\pi)$, következésképpen π K-homogenitása folytán

$$m(\mathrm{in}_{k,\mathbf{x}}(\lambda.y)) = \pi\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(\lambda.y)}\right) = \pi\left(\lambda.\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)}\right) = \lambda\pi\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)}\right) = \lambda.m(\mathrm{in}_{k,\mathbf{x}}(y)),$$

tehát az $m \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to T$ leképezés K-homogén. Ezért az $m \circ \mathrm{in}_{k,\mathbf{x}}$ leképezés K-lineáris, vagyis $m \in \mathbf{Mult}\left(\prod_{i\in I} E_i; T\right)$.

Legyen F vektortér K felett és $u \in \mathbf{Mult}\left(\prod_{i\in I} E_i; F\right)$. Mivel $(\mathbf{e_x})_{\mathbf{x}\in E}$ bázisrendszer a $K^{(E)}$ vektortérben, így az $u : E \to F$ függvényhez létezik egyetlen olyan $v : K^{(E)} \to F$ lineáris operátor, amelyre minden $\mathbf{x} \in E$ esetén $v(\mathbf{e_x}) = u(\mathbf{x})$ (17.7.3.). Megmutatjuk, hogy a $v : K^{(E)} \to F$ lineáris operátor faktorizálható az $M \subseteq K^{(E)}$ lineáris altér szerint, vagyis $M \subseteq \mathrm{Ker}(v)$ (17.2.8.).

Ha $k \in I$, $y, z \in E_k$ és $\mathbf{x} \in E$, akkor a v lineáris operátor definíciója és u multilinearitása miatt

$$v\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y+z)} - \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)} - \mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(z)}\right) = v\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y+z)}\right) - v\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)}\right) - v\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(z)}\right) =$$
$$= u\left(\mathrm{in}_{k,\mathbf{x}}(y+z)\right) - u\left(\mathrm{in}_{k,\mathbf{x}}(y)\right) - u\left(\mathrm{in}_{k,\mathbf{x}}(z)\right) = \mathbf{0},$$

hiszen az $u \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to F$ leképezés additív. Tehát $A \subseteq \mathrm{Ker}(v)$.

Ha $k \in I$, $y \in E_k$, $\lambda \in K$ és $\mathbf{x} \in E$, akkor a v lineáris operátor definíciója és u multilinearitása miatt

$$v\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(\lambda.y)} - \lambda.\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)}\right) = v\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(\lambda.y)}\right) - \lambda.v\left(\mathbf{e}_{\mathrm{in}_{k,\mathbf{x}}(y)}\right) = u\left(\mathrm{in}_{k,\mathbf{x}}(\lambda.y)\right) - \lambda.u\left(\mathrm{in}_{k,\mathbf{x}}(y)\right) = \mathbf{0},$$

hiszen az $u \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to F$ leképezés K-homogén. Tehát $B \subseteq \mathrm{Ker}(v)$.

Ez azt jelenti, hogy $A \cup B \subseteq \mathrm{Ker}(u)$, következésképpen $M = \mathrm{sp}(A \cup B) \subseteq \mathrm{Ker}(v)$, így a $v : K^{(E)} \to F$ lineáris operátor faktorizálható az M lineáris altér szerint. Jelölje $\dot{v} : K^{(E)}/M \to F$ a v operátor M szerinti faktorizáltját, tehát $\dot{v}$ az a $T \to F$ lineáris operátor, amelyre $\dot{v} \circ \pi = v$. Ekkor minden $\mathbf{x} \in E$ esetén, a v lineáris operátor és az m multilineáris operátor definíciója miatt

$$\left(\dot{v} \circ m\right)(\mathbf{x}) = \dot{v}\left(m(\mathbf{x})\right) = \dot{v}\left(\pi\left(\mathbf{e}_{\mathbf{x}}\right)\right) = v\left(\mathbf{e}_{\mathbf{x}}\right) = u(\mathbf{x}),$$

tehát $\dot{v} \circ m = u$. Ezért $\tilde{u} := \dot{v} \in \mathbf{L}(T; F)$ olyan, hogy $\tilde{u} \circ m = u$.

Megmutatjuk, hogy ha $\tilde{u}' : T \to F$ szintén olyan lineáris operátor, hogy $\tilde{u}' \circ m = u$, akkor $\tilde{u} = \tilde{u}'$. Valóban, a feltétel szerint $\mathrm{Im}(m) \subseteq \{t \in T | \tilde{u}(t) = \tilde{u}'(t)\}$, és mivel $\{t \in T | \tilde{u}(t) = \tilde{u}'(t)\} = \mathrm{Ker}(\tilde{u} - \tilde{u}')$ lineáris altere T-nek, így $\mathrm{sp}(\mathrm{Im}(m)) \subseteq \{t \in T | \tilde{u}(t) = \tilde{u}'(t)\}$. Ezért a $\tilde{u} = \tilde{u}'$ egyenlőség bizonyításához elég azt belátni, hogy $\mathrm{Im}(m)$ generátorhalmaza a T vektortérnek. Ez viszont nyilvánvaló, mert az $\{\mathbf{e}_{\mathbf{x}} | \mathbf{x} \in E\}$ halmaz generátorhalmaz $K^{(E)}$-ben (valójában bázishalmaz), és $\pi : K^{(E)} \to T$ lineáris szürjekció, így 17.5.4. b) szerint $\pi\langle\{\mathbf{e}_{\mathbf{x}} | \mathbf{x} \in E\}\rangle$ generátorhalmaz T-ben, ugyanakkor m definíciója szerint

$$\mathrm{Im}(m) = \{m(\mathbf{x}) | \mathbf{x} \in E\} = \{\pi\left(\mathbf{e}_{\mathbf{x}}\right) | \mathbf{x} \in E\} = \pi\langle\{\mathbf{e}_{\mathbf{x}} | \mathbf{x} \in E\}\rangle,$$

tehát $\mathrm{Im}(m)$ generátorhalmaza a T vektortérnek.

b) A hipotézis szerint a (T, m) párra teljesül (ET), és $\tilde{m} \in \mathbf{Mult}\left(E; \tilde{T}\right)$, így létezik egyetlen olyan $w : T \to \tilde{T}$ lineáris operátor, amelyre $w \circ m = \tilde{m}$. Ugyanakkor, a $(\tilde{T}, \tilde{m})$ párra teljesül (ET) (ha abban (T, m) helyére $(\tilde{T}, \tilde{m})$-t helyettesítünk), és $m \in \mathbf{Mult}\,(E; T)$, így létezik egyetlen olyan $\tilde{w} : \tilde{T} \to T$ lineáris operátor, amelyre $\tilde{w} \circ \tilde{m} = m$. Ekkor $(\tilde{w} \circ w) \circ m = \tilde{w} \circ \tilde{m} = m$, és $\tilde{w} \circ w \in \mathbf{L}(T; T)$. Világos, hogy $\mathrm{id}_T : T \to T$ szintén olyan lineáris operátor, amelyre $\mathrm{id}_T \circ m = m$, azért az (ET) feltételben szereplő egyértelműségi előírás alapján $\tilde{w} \circ w = \mathrm{id}_T$. Hasonlóan, $(w \circ \tilde{w}) \circ \tilde{m} = w \circ m = \tilde{m}$, és $w \circ \tilde{w} \in \mathbf{L}(\tilde{T}; \tilde{T})$. Világos, hogy $\mathrm{id}_{\tilde{T}} : \tilde{T} \to \tilde{T}$ szintén olyan lineáris operátor, amelyre $\mathrm{id}_{\tilde{T}} \circ \tilde{m} = \tilde{m}$, azért az $(\tilde{T}, \tilde{m})$ párra megfogalmazott (ET) feltételben szereplő egyértelműségi előírás alapján $w \circ \tilde{w} = \mathrm{id}_{\tilde{T}}$. Ez azt jelenti, hogy a $w : T \to \tilde{T}$ leképezés olyan lineáris bijekció, amelyre $w^{-1} = \tilde{w}$ és $w \circ m = \tilde{m}$. A (T, m) párra megfogalmazott (ET) feltételben szereplő egyértelműségi előírás alapján w az egyetlen olyan $T \to \tilde{T}$ lineáris operátor, amelyre $w \circ m = \tilde{m}$ teljesül, tehát ezzel a feltétellel w már $\mathbf{L}(T; \tilde{T})$-ben is egyértelműen van meghatározva. ■

19.7.2. Definíció. *A K test feletti vektorterek $(E_i)_{i \in I}$ rendszere* **tenzorszorzatának** *nevezünk minden olyan (T, m) párt, amelyre teljesül az előző tételben megfogalmazott* (ET) *tulajdonság, amit* **a tenzorszorzat univerzalitási tulajdonságának** *is nevezünk.*

Figyeljük meg, hogy az $(E_i)_{i\in I}$ vektortér-rendszer tenzorszorzatának definíciójában semmilyen előírást nem tettünk az I indexhalmazra és a rendszerben szereplő vektorterek dimenziójára vonatkozóan, tehát végtelen dimenziós vektorterek bármely végtelen rendszerének is vehetjük a tenzorszorzatát.

Vektortér-rendszer tenzorszorzata általában *nem egyértelmű*, mert könnyen látható, hogy ha (T, m) tenzorszorzata az $(E_i)_{i\in I}$ vektortér-rendszernek és E olyan vektortér K felett, amely izomorf T-vel és $v : T \to E$ tetszőleges lineáris bijekció, akkor az $(E, v \circ m)$ pár szintén tenzorszorzata az $(E_i)_{i\in I}$ vektortér-rendszernek, és ez $T \neq E$ esetén különbözik a (T, m) pártól. Az $(E_i)_{i\in I}$ vektortér-rendszer minden tenzorszorzatát a tenzorszorzat *realizációjának* nevezzük. Az előző tétel a) pontjának bizonyításában bevezetett (T, m) realizációt a tenzorszorzat *standard realizációjának* nevezhetjük. Azonban ritkán van szükség a standard realizációra, mert a tétel b) pontja szerint bármely két tenzorszorzat kitüntetett módon azonosítható.

Jelölés. Az $(E_i)_{i\in I}$ vektortér-rendszer tenzorszorzatának bármely realizációját a $\left(\bigotimes_{i\in I} E_i, \otimes\right)$ szimbólummal jelöljük, és minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén az $\otimes((x_i)_{i\in I}) \in \bigotimes_{i\in I} E_i$ elemet $\bigotimes_{i\in I} x_i$ jelöli. Ha E és F vektorterek, és $(G_i)_{i\in\{0,1\}}$ az a rendszer, amelyre $G_0 := E$ és $G_1 := F$, akkor a $\bigotimes_{i\in\{0,1\}} G_i$ vektorteret $E \otimes F$ jelöli, és minden $x \in E$, $y \in F$ esetén $x \otimes y := \bigotimes_{i\in\{0,1\}} z_i$, ahol $z_0 := x$ és $z_1 := y$.

Szokás az $(E_i)_{i\in I}$ vektortér-rendszer tenzorszorzatának nevezni magát a $\bigotimes_{i\in I} E_i$ vektorteret, de lényeges tudni, hogy a tenzorszorzat fogalmához elválaszthatatlanul hozzátartozik a $\otimes : \prod_{i\in I} E_i \to \bigotimes_{i\in I} E_i$ multilineáris operátor is.

A tenzorszorzatok elemeit *tenzoroknak* szokták nevezni, de nyilvánvaló, hogy egy matematikai objektumnak nem belső tulajdonsága az, hogy tenzor, hanem ez attól a körülménytől függ, amelyben a matematikai objektumot értelmeztük. Továbbá, ha $(E_i)_{i\in I}$ vektortér-rendszer, akkor *felbontható tenzoroknak* nevezzük a $\bigotimes_{i\in I} x_i$ alakú tenzorokat, ahol $(x_i)_{i\in I} \in \prod_{i\in I} E_i$.

19.7.3. Állítás. *Ha* $(E_i)_{i\in I}$ *vektortér-rendszer, akkor*

$$\left\{ \bigotimes_{i\in I} x_i \;\middle|\; (x_i)_{i\in I} \in \prod_{i\in I} E_i \right\}$$

(vagyis a felbontható tenzorok $\mathrm{Im}(\otimes)$ *halmaza) generátorhalmaz a* $\bigotimes_{i\in I} E_i$ *vektortérben.*

Bizonyítás. (I. Bizonyítás.) Jelölje (T, m) az $(E_i)_{i\in I}$ vektortér-rendszer tenzorszorzatának standard realizációját, és alkalmazzuk a 19.7.1. tétel a) pontjának bizonyításában bevezetett jelöléseket. A $\pi : K^{(E)} \to T$ kanonikus lineáris szürjekció az $\{\mathbf{e}_\mathbf{x} | \mathbf{x} \in E\}$ bázishalmazt a T vektortér generátorhalmazába viszi át (17.5.4. b) pontja), és mivel $\mathrm{Im}(m) = \{\pi(\mathbf{e}_\mathbf{x}) | \mathbf{x} \in E\}$, így $\mathrm{Im}(m)$ generátorhalmaz T-ben. Tehát az $(E_i)_{i\in I}$ vektortér-rendszer (T, m) standard realizációjára teljesül az, hogy $\mathrm{Im}(m)$ generátorhalmaz T-ben. Mivel $\left(\bigotimes_{i\in I} E_i, \otimes\right)$ szintén realizációja az $(E_i)_{i\in I}$ vektortér-rendszer tenzorszorzatának, így a 19.7.1. tétel b) része alapján vehetünk azt a $v : T \to \bigotimes\limits_{i\in I} E_i$ lineáris bijekciót, amelyre $v \circ m = \otimes$. Ekkor ismét a 17.5.4. állítás b) pontjára hivatkozva kapjuk, hogy $\mathrm{Im}(\otimes) = v\langle \mathrm{Im}(m)\rangle$ generátorhalmaz a $\bigotimes\limits_{i\in I} E_i$ vektortérben.

(II. Bizonyítás.) Mivel $\otimes \in \mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; \bigotimes\limits_{i\in I} E_i\Big)$, így (ET) alapján létezik *egyetlen* olyan $u : \bigotimes\limits_{i\in I} E_i \to \bigotimes\limits_{i\in I} E_i$ lineáris operátor, amelyre $u \circ \otimes = \otimes$, és mivel nyilvánvalóan $\mathrm{id}_{\bigotimes\limits_{i\in I} E_i} \circ \otimes = \otimes$, így $u = \mathrm{id}_{\bigotimes\limits_{i\in I} E_i}$. Legyen N algebrai komplementere az $\mathrm{sp}(\mathrm{Im}(\otimes))$ lineáris altérnek (17.4.4.), és jelölje $s : \mathrm{sp}(\mathrm{Im}(\otimes)) \times N \to \bigotimes\limits_{i\in I} E_i$ a $\bigotimes\limits_{i\in I} E_i$ vektortér összeadásfüggvényének leszűkítését az $\mathrm{sp}(\mathrm{Im}(\otimes)) \times N$ lineáris szorzattérre. Tudjuk, hogy s lineáris bijekció (17.4.2.). Vezessük be a

$$v := \mathrm{pr}_1 \circ s^{-1} : \bigotimes_{i\in I} E_i \to \bigotimes_{i\in I} E_i$$

leképezést, ahol pr_1 az $\mathrm{sp}(\mathrm{Im}(\otimes)) \times N \to \mathrm{sp}(\mathrm{Im}(\otimes))$ első projekció. Ekkor $v : \bigotimes\limits_{i\in I} E_i \to \bigotimes\limits_{i\in I} E_i$ olyan lineáris operátor, amelyre $v \circ \otimes = \otimes$ nyilvánvalóan teljesül, ezért az előzőek szerint $v = \mathrm{id}_{\bigotimes\limits_{i\in I} E_i}$, ugyanakkor $N \subseteq \mathrm{Ker}(v) = \{\mathbf{0}\}$, így $\mathrm{sp}(\mathrm{Im}(\otimes)) = \bigotimes\limits_{i\in I} E_i$. ■

Vigyázzunk arra, hogy ha $(E_i)_{i\in I}$ vektortér-rendszer, akkor általában $\mathrm{Im}(\otimes)$ *nem lineáris altér* a $\bigotimes\limits_{i\in I} E_i$ vektortérben, mert $\otimes$ multilineáris operátor, amely általában nem lineáris.

Figyeljük meg a 19.7.3. állítás kétféle bizonyítása közti lényeges különbséget! Az első kihasználja a tenzorszorzat standard realizációjának speciális tulajdonságait, míg a második csak a tenzorszorzat definíciójára hivatkozik. Világos, hogy mindkét bizonyítás kifogástalan, de a második jobban mutatja a lényeget, mert nem használja ki a standard realizáció esetleges tulajdonságait, hanem pontosan rámutat arra az okra (ti. az (ET) feltételben szereplő egyértelműségre), amely miatt az állítás igaz. Ezért arra törekszünk, hogy a tenzorszorzatokkal kapcsolatos állítások bizonyításában közvetlenül az (ET) tulajdonságot alkalmazzuk, és lehetőség szerint kerülni fogjuk a standard vagy bármiféle realizáció alkalmazását.

19.7.4. Állítás. *Legyen $(E_i)_{i\in I}$ vektortér-rendszer a K test felett. Ekkor minden $t \in \bigotimes\limits_{i\in I} E_i$ elemhez létezik olyan $\big((x_{i,\alpha})_{i\in I}\big)_{\alpha\in A}$ rendszer, hogy A véges halmaz és minden $\alpha \in A$ esetén $(x_{i,\alpha})_{i\in I} \in \prod\limits_{i\in I} E_i$, és*

$$t = \sum_{\alpha\in A} \bigotimes_{i\in I} x_{i,\alpha}.$$

(Vagyis minden tenzor előáll felbontható tenzorok véges összegeként.)

Bizonyítás. Ha $I = \emptyset$, akkor az állítás triviálisan igaz, tehát feltehető, hogy $I \neq \emptyset$, és $k \in I$ rögzített elem. A 19.7.3. állítás szerint a $t \in \bigotimes\limits_{i\in I} E_i$ elemhez van olyan felbontható tenzorokból álló $(t_\alpha)_{\alpha\in A}$ véges rendszer és olyan K-ban haladó $(\lambda_\alpha)_{\alpha\in A}$ rendszer, hogy $t = \sum\limits_{\alpha\in A} \lambda_\alpha . t_\alpha$. Ekkor kiválaszthatunk olyan $(z_{i,\alpha})_{(i,\alpha)\in I\times A}$ rendszert, hogy minden $\alpha \in A$

esetén $\mathbf{z}_\alpha := (z_{i,\alpha})_{i\in I} \in \prod_{i\in I} E_i$ és $t_\alpha = \bigotimes_{i\in I} z_{i,\alpha}$. Ha $\alpha \in A$, akkor

$$\lambda_\alpha . t_\alpha = \lambda_\alpha . \bigotimes_{i\in I} z_{i,\alpha} = \lambda_\alpha . \left(\otimes \circ \mathrm{in}_{k,\mathbf{z}_\alpha}\right)(z_{k,\alpha}) = \left(\otimes \circ \mathrm{in}_{k,\mathbf{z}_\alpha}\right)(\lambda_\alpha . z_{k,\alpha}),$$

ahol felhasználtuk a $\otimes \circ \mathrm{in}_{k,\mathbf{z}_\alpha} : E_k \to \bigotimes_{i\in I} E_i$ lineáris operátor K-homogenitását. Tehát ha minden $\alpha \in A$ esetén bevezetjük az $(x_{i,\alpha})_{i\in I} := \mathrm{in}_{k,\mathbf{z}_\alpha}(\lambda_\alpha . z_{k,\alpha}) \in \prod_{i\in I} E_i$ rendszert, akkor $t = \sum_{\alpha\in A} \bigotimes_{i\in I} x_{i,\alpha}$. ■

19.7.5. Állítás. *Legyen $(E_i)_{i\in I}$ vektortér-rendszer és F vektortér a K test felett. Jelölje*

$$\tau : \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big) \to \mathbf{L}\Big(\bigotimes_{i\in I} E_i; F\Big)$$

azt a leképezést, amelyre teljesül az, hogy minden $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ multilineáris operátorra $\tau(u) \in \mathbf{L}\Big(\bigotimes_{i\in I} E_i; F\Big)$ az a lineáris operátor, amelyre $\tau(u) \circ \otimes = u$, vagyis a következő diagram kommutatív

$$\begin{tikzcd}
\prod_{i\in I} E_i \arrow[r, "\otimes"] \arrow[dr, "u"'] & \bigotimes_{i\in I} E_i \arrow[d, "\tau(u)"] \\
& F
\end{tikzcd}$$

Ekkor τ izomorfizmus a $\mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ és $\mathbf{L}\Big(\bigotimes_{i\in I} E_i; F\Big)$ vektorterek között.

Bizonyítás. Ha $u, u' \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$, akkor $\tau(u)+\tau(u') \in \mathbf{L}\Big(\bigotimes_{i\in I} E_i; F\Big)$ olyan lineáris operátor, amelyre

$$(\tau(u) + \tau(u')) \circ \otimes = (\tau(u) \circ \otimes) + (\tau(u') \circ \otimes) = u + u',$$

ugyanakkor az $u + u' \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ multilineáris operátorra τ definíciója szerint teljesül az, hogy

$$\tau(u + u') \circ \otimes = u + u',$$

így az (ET)-ben szereplő egyértelműségi feltétel alapján $\tau(u) + \tau(u') = \tau(u + u')$. Ezért a τ leképezés additív.

Ha $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ és $\lambda \in K$, akkor $\lambda.\tau(u) \in \mathbf{L}\Big(\bigotimes_{i\in I} E_i; F\Big)$ olyan lineáris operátor, amelyre

$$(\lambda.\tau(u)) \circ \otimes = \lambda.(\tau(u) \circ \otimes) = \lambda.u,$$

ugyanakkor a $\lambda.u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ olyan multilineáris operátorra τ definíciója szerint teljesül az, hogy

$$\tau(\lambda.u) \circ \otimes = \lambda.u,$$

így az (ET)-ben szereplő egyértelműségi feltétel alapján $\tau(\lambda.u) = \lambda.\tau(u)$. Ezért a τ leképezés K-homogén.

Ha $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ olyan, hogy $\tau(u) = 0$, akkor $0 = \tau(u) \circ \otimes = u$, ezért τ injektív lineáris operátor. Ha $v \in \mathbf{L}\Big(\bigotimes_{i\in I} E_i; F\Big)$ tetszőleges, akkor $\otimes \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; \bigotimes_{i\in I} E_i\Big)$ miatt $u := v \circ \otimes \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big)$ (19.1.3.), következésképpen $\tau(u) \circ \otimes = u = v \circ \otimes$, tehát a $\tau(u)$ és v lineáris operátorok megegyeznek az $\mathrm{Im}(\otimes)$ halmazon, amely generátorhalmaz a $\bigotimes_{i\in I} E_i$ vektortérben (19.7.3.), így $\tau(u) = v$. Ez azt jelenti, hogy a $\tau : \mathbf{Mult}\Big(\prod_{i\in I} E_i; F\Big) \to \mathbf{L}\Big(\bigotimes_{i\in I} E_i; F\Big)$ lineáris operátor szürjektív is. ■

19.7.6. Állítás. *Ha $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ (ugyanolyan indexhalmazú) vektortér-rendszerek, és $(u_i)_{i\in I} \in \prod_{i\in I} \mathbf{L}(E_i; F_i)$, akkor létezik egyetlen olyan $u \in \mathbf{L}\Big(\bigotimes_{i\in I} E_i; \bigotimes_{i\in I} F_i\Big)$ lineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén $u\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{i\in I} u_i(x_i)$.*

Bizonyítás. Ha $\otimes$ jelöli a $\prod_{i\in I} F_i \to \bigotimes_{i\in I} F_i$ kanonikus multilineáris operátort, akkor a

$$\prod_{i\in I} E_i \to \bigotimes_{i\in I} F_i; \quad (x_i)_{i\in I} \mapsto \bigotimes_{i\in I} u_i(x_i)$$

leképezés egyenlő a $\otimes \circ \Big(\bigtimes_{i\in I} u_i\Big)$ operátorral, amely 19.1.3. alapján multilineáris, így a tenzorszorzat univerzalitási tulajdonsága szerint létezik egyetlen olyan $u \in \mathbf{L}\Big(\bigotimes_{i\in I} E_i; \bigotimes_{i\in I} F_i\Big)$ lineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén $u\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{i\in I} u_i(x_i)$. ■

19.7.7. Definíció. *Ha $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ (ugyanolyan indexhalmazú) vektortér-rendszerek, és $(u_i)_{i\in I} \in \prod_{i\in I} \mathbf{L}(E_i; F_i)$, akkor $\overset{\circ}{\bigotimes_{i\in I}} u_i$ jelöli azt a $\bigotimes_{i\in I} E_i \to \bigotimes_{i\in I} F_i$ lineáris operátort, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén*

$$\Big(\overset{\circ}{\bigotimes_{i\in I}} u_i\Big)\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{i\in I} u_i(x_i),$$

és ezt az operátort az $(u_i)_{i\in I}$ **operátor-rendszer konkrét tenzorszorzatának** *nevezzük. Ha $I = \{0, 1\}$, akkor a $\overset{\circ}{\bigotimes_{i\in I}} u_i$ operátort az $u_0 \overset{\circ}{\otimes} u_1$ szimbólummal jelöljük, tehát ekkor $u_0 \overset{\circ}{\otimes} u_1$ az az $E_0 \otimes E_1 \to F_0 \otimes F_1$ lineáris operátor, amelyre minden $x_0 \in E_0$ és $x_1 \in E_1$ esetén*

$$\Big(u_0 \overset{\circ}{\otimes} u_1\Big)(x_0 \otimes x_1) = u_0(x_0) \otimes u_1(x_1).$$

Az előző definícióban szereplő $\overset{\circ}{\bigotimes_{i\in I}} u_i$ operátort nem nevezhettük az $(u_i)_{i\in I}$ *operátor-rendszer tenzorszorzatának*, mert $\bigotimes_{i\in I} u_i$ egészen más objektum, ti. a $\bigotimes_{i\in I} \mathbf{L}(E_i;F_i)$ tenzor-szorzat eleme, ugyanakkor $\overset{\circ}{\bigotimes_{i\in I}} u_i \in \mathbf{L}\Big(\bigotimes_{i\in I} E_i; \bigotimes_{i\in I} F_i\Big)$.

19.7.8. Állítás. *Ha $(E_i)_{i\in I}$, $(F_i)_{i\in I}$ és $(G_i)_{i\in I}$ (ugyanolyan indexhalmazú) vektortér-rendszerek, valamint $(u_i)_{i\in I} \in \prod_{i\in I} \mathbf{L}(E_i;F_i)$ és $(v_i)_{i\in I} \in \prod_{i\in I} \mathbf{L}(F_i;G_i)$, akkor*

$$\Big(\overset{\circ}{\bigotimes_{i\in I}} v_i\Big) \circ \Big(\overset{\circ}{\bigotimes_{i\in I}} u_i\Big) = \overset{\circ}{\bigotimes_{i\in I}} (v_i \circ u_i).$$

Bizonyítás. A definíció szerint minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén

$$\Big(\overset{\circ}{\bigotimes_{i\in I}}(v_i\circ u_i)\Big)\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{i\in I}(v_i\circ u_i)(x_i) = \bigotimes_{i\in I} v_i(u_i(x_i)) = \Big(\overset{\circ}{\bigotimes_{i\in I}} v_i\Big)\Big(\bigotimes_{i\in I} u_i(x_i)\Big) =$$
$$= \Big(\overset{\circ}{\bigotimes_{i\in I}} v_i\Big)\Big(\Big(\overset{\circ}{\bigotimes_{i\in I}} u_i\Big)\Big(\bigotimes_{i\in I} x_i\Big)\Big) = \Big(\Big(\overset{\circ}{\bigotimes_{i\in I}} v_i\Big)\circ\Big(\overset{\circ}{\bigotimes_{i\in I}} u_i\Big)\Big)\Big(\bigotimes_{i\in I} x_i\Big),$$

tehát $\overset{\circ}{\bigotimes_{i\in I}}(v_i\circ u_i)$ és $\Big(\overset{\circ}{\bigotimes_{i\in I}} v_i\Big)\circ\Big(\overset{\circ}{\bigotimes_{i\in I}} u_i\Big)$ olyan $\bigotimes_{i\in I} E_i \to \bigotimes_{i\in I} G_i$ lineáris operátorok, amelyek megegyeznek a $\Big\{\bigotimes_{i\in I} x_i \,\Big|\, (x_i)_{i\in I} \in \prod_{i\in I} E_i\Big\}$ halmazon, amely 19.7.3. szerint generátorhalmaz a $\bigotimes_{i\in I} E_i$ vektortérben, ezért ezek a lineáris operátorok egyenlőek. ■

19.7.9. Következmény. *Legyenek $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ (ugyanolyan indexhalmazú) vektortér-rendszerek, valamint $(u_i)_{i\in I} \in \prod_{i\in I} \mathbf{L}(E_i;F_i)$.*

a) *Ha minden $i\in I$ esetén $u_i : E_i \to F_i$ injekció, akkor $\overset{\circ}{\bigotimes_{i\in I}} u_i : \bigotimes_{i\in I} E_i \to \bigotimes_{i\in I} F_i$ is injekció.*

b) *Ha minden $i\in I$ esetén $u_i : E_i \to F_i$ szürjekció, akkor $\overset{\circ}{\bigotimes_{i\in I}} u_i : \bigotimes_{i\in I} E_i \to \bigotimes_{i\in I} F_i$ is szürjekció.*

c) *Ha minden $i\in I$ esetén $u_i : E_i \to F_i$ bijekció, akkor $\overset{\circ}{\bigotimes_{i\in I}} u_i : \bigotimes_{i\in I} E_i \to \bigotimes_{i\in I} F_i$ is bijekció, tehát a $\overset{\circ}{\bigotimes_{i\in I}} u_i$ operátor izomorfizmus a $\bigotimes_{i\in I} E_i$ és $\bigotimes_{i\in I} F_i$ vektorterek között, továbbá ekkor*

$$\Big(\overset{\circ}{\bigotimes_{i\in I}} u_i\Big)^{-1} = \overset{\circ}{\bigotimes_{i\in I}} u_i^{-1}.$$

Bizonyítás. a) A 17.7.5. állítás szerint kiválaszthatunk olyan $(v_i)_{i\in I} \in \prod_{i\in I} \mathbf{L}(F_i;E_i)$ rendszert, hogy minden $i\in I$ esetén $v_i\circ u_i = \mathrm{id}_{E_i}$. Ekkor az előző állítás szerint a $\overset{\circ}{\bigotimes_{i\in I}} v_i \in \mathbf{L}\Big(\bigotimes_{i\in I} F_i; \bigotimes_{i\in I} E_i\Big)$ lineáris operátor a $\overset{\circ}{\bigotimes_{i\in I}} u_i$ operátornak (lineáris) balinverze, tehát $\overset{\circ}{\bigotimes_{i\in I}} u_i : \bigotimes_{i\in I} E_i \to \bigotimes_{i\in I} F_i$ injekció.

b) A 17.4.7. állítás szerint kiválaszthatunk olyan $(v_i)_{i\in I} \in \prod_{i\in I} \mathbf{L}(F_i;E_i)$ rendszert, hogy minden $i \in I$ esetén $u_i \circ v_i = \mathrm{id}_{F_i}$. Ekkor az előző állítás szerint a $\overset{\circ}{\bigotimes\limits_{i\in I}} v_i \in \mathbf{L}\Big(\bigotimes\limits_{i\in I} F_i; \bigotimes\limits_{i\in I} E_i\Big)$ lineáris operátor a $\overset{\circ}{\bigotimes\limits_{i\in I}} u_i$ operátornak (lineáris) jobbinverze, tehát $\overset{\circ}{\bigotimes\limits_{i\in I}} u_i : \bigotimes\limits_{i\in I} E_i \to \bigotimes\limits_{i\in I} F_i$ szürjekció.

c) Az a) és b) állításokból nyilvánvalóan következik. ■

19.7.10. Állítás. *Ha $(E_i)_{i\in I}$ és $(F_i)_{i\in I}$ (ugyanolyan indexhalmazú) vektortér-rendszerek, akkor egyértelműen létezik olyan*

$$\tau : \bigotimes_{i\in I} \mathbf{L}\left(E_i; F_i\right) \to \mathbf{L}\Big(\bigotimes_{i\in I} E_i; \bigotimes_{i\in I} F_i\Big)$$

lineáris operátor, amelyre minden $(u_i)_{i\in I} \in \prod\limits_{i\in I} \mathbf{L}\left(E_i; F_i\right)$ esetén

$$\tau\Big(\bigotimes_{i\in I} u_i\Big) = \overset{\circ}{\bigotimes_{i\in I}} u_i.$$

Bizonyítás. A τ lineáris operátor egyértelmű létezéséhez az (ET) feltétel alapján pontosan azt kell belátni, hogy az

$$m : \prod_{i\in I} \mathbf{L}\left(E_i; F_i\right) \to \mathbf{L}\Big(\bigotimes_{i\in I} E_i; \bigotimes_{i\in I} F_i\Big); \quad (u_i)_{i\in I} \mapsto \overset{\circ}{\bigotimes_{i\in I}} u_i$$

leképezés multilineáris operátor. Ennek bizonyításához legyen $k \in I$ és $\mathbf{u} := (u_i)_{i\in I} \in \prod\limits_{i\in I} \mathbf{L}\left(E_i; F_i\right)$ rögzített.

Ekkor minden $u \in \mathbf{L}(E_k; F_k)$ és $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén

$$\left(\left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u)\right)\Big(\bigotimes_{i\in I} x_i\Big) = \Big(\overset{\circ}{\bigotimes_{i\in I}} \widetilde{u}_i\Big)\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{i\in I} \widetilde{u}_i(x_i) = \left(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\right)(u(x_k)),$$

ahol $(\widetilde{u}_i)_{i\in I} := \mathrm{in}_{k,\mathbf{u}}(u)$, vagyis minden $i \in I \setminus \{k\}$ esetén $\widetilde{u}_i = u_i$ és $\widetilde{u}_k = u$, továbbá $\otimes_F$ a $\prod\limits_{i\in I} F_i \to \bigotimes\limits_{i\in I} F_i$ kanonikus multilineáris operátor.

Ebből látható, hogy ha $u, u' \in \mathbf{L}(E_k; F_k)$, akkor minden $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén a $\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}} : F_k \to \bigotimes\limits_{i\in I} F_i$ leképezés additivitása folytán

$$\begin{aligned}
\left(\left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u + u')\right)\Big(\bigotimes_{i\in I} x_i\Big) &= \left(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\right)((u + u')(x_k)) = \\
&= \left(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\right)(u(x_k) + u'(x_k)) = \\
&= \left(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\right)(u(x_k)) + \left(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\right)(u'(x_k)) = \\
&= \left(\left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u)\right)\Big(\bigotimes_{i\in I} x_i\Big) + \left(\left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u')\right)\Big(\bigotimes_{i\in I} x_i\Big) = \\
&= \left(\left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u) + \left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u')\right)\Big(\bigotimes_{i\in I} x_i\Big),
\end{aligned}$$

ezért $\left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u + u') = \left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u) + \left(m \circ \mathrm{in}_{k,\mathbf{u}}\right)(u')$, vagyis az $m \circ \mathrm{in}_{k,\mathbf{u}} : \mathbf{L}(E_k; F_k) \to \mathbf{L}\Big(\bigotimes\limits_{i\in I} E_i; \bigotimes\limits_{i\in I} F_i\Big)$ leképezés additív.

Továbbá, ha $u \in \mathbf{L}(E_k;F_k)$ és $\lambda \in K$, akkor minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén a $\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}} : F_k \to \bigotimes_{i\in I} F_i$ leképezés K-homogenitása folytán

$$\begin{aligned}((m\circ \mathrm{in}_{k,\mathbf{u}})(\lambda.u))\Big(\bigotimes_{i\in I} x_i\Big) &= \big(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\big)((\lambda.u)(x_k)) = \\ = \big(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\big)(\lambda.u(x_k)) &= \lambda.\big(\otimes_F \circ \mathrm{in}_{k,(u_i(x_i))_{i\in I}}\big)(u(x_k)) = \\ &= \lambda.\Big(((m\circ \mathrm{in}_{k,\mathbf{u}})(u))\Big(\bigotimes_{i\in I} x_i\Big)\Big) = (\lambda.(m\circ \mathrm{in}_{k,\mathbf{u}})(u))\Big(\bigotimes_{i\in I} x_i\Big),\end{aligned}$$

ezért $(m\circ \mathrm{in}_{k,\mathbf{u}})(\lambda.u) = \lambda.(m\circ \mathrm{in}_{k,\mathbf{u}})(u)$, ami azt jelenti, hogy az $m\circ \mathrm{in}_{k,\mathbf{u}} : \mathbf{L}(E_k;F_k) \to \mathbf{L}\Big(\bigotimes_{i\in I} E_i; \bigotimes_{i\in I} F_i\Big)$ leképezés K-homogén. ∎

19.8. Véges vektortér-rendszer tenzorszorzata

19.8.1. Lemma. *Legyen $(E_i)_{i\in I}$ véges vektortér-rendszer a K test felett. Ekkor minden $t \in \bigotimes_{i\in I} E_i$ elemhez létezik olyan $\big((e_{i,j})_{j\in J_i}\big)_{i\in I}$ rendszer, hogy minden $i\in I$ esetén $(e_{i,j})_{j\in J_i}$ véges lineárisan független rendszer E_i-ben, és a $J := \prod_{i\in I} J_i$ halmazhoz létezik olyan K-ban haladó $(\lambda_\sigma)_{\sigma\in J}$ rendszer, hogy*

$$t = \sum_{\sigma\in J} \lambda_\sigma . \bigotimes_{i\in I} e_{i,\sigma(i)}.$$

Bizonyítás. A 19.7.4. állítás szerint vehetünk olyan $\big((x_{i,\alpha})_{i\in I}\big)_{\alpha\in A}$ rendszert, hogy A véges halmaz, és minden $\alpha\in A$ esetén $(x_{i,\alpha})_{i\in I} \in \prod_{i\in I} E_i$, és $t = \sum_{\alpha\in A} \bigotimes_{i\in I} x_{i,\alpha}$. Minden $i\in I$ esetén $\{x_{i,\alpha} | \alpha\in A\} \subseteq E_i$ véges halmaz, így az $\mathrm{sp}(\{x_{i,\alpha}|\alpha\in A\})$ véges dimenziós vektortérben vehetünk egy $(e_{i,j})_{j\in J_i}$ algebrai bázist. Tehát kiválaszthatunk olyan $\big((e_{i,j})_{j\in J_i}\big)_{i\in I}$ rendszert, hogy minden $i\in I$ esetén $(e_{i,j})_{j\in J_i}$ algebrai bázis az $\mathrm{sp}(\{x_{i,\alpha}|\alpha\in A\})$ vektortérben, így egyértelműen létezik olyan $(\lambda_{i,j,\alpha})_{\alpha\in A,\ i\in I,\ j\in J_i}$ rendszer, hogy minden $\alpha\in A$ és $i\in I$ esetén $x_{i,\alpha} = \sum_{j\in J_i} \lambda_{i,j,\alpha}.e_{i,j}$. A multilineáris operátorok multiadditivitása és multihomogenitása (19.3.1. és 19.2.1.) folytán minden $\alpha\in A$ esetén, a $J := \prod_{i\in I} J_i$ definíciót alkalmazva:

$$\bigotimes_{i\in I} x_{i,\alpha} = \bigotimes_{i\in I}\Big(\sum_{j\in J_i} \lambda_{i,j,\alpha}.e_{i,j}\Big) = \sum_{\sigma\in J}\bigotimes_{i\in I}\big(\lambda_{i,\sigma(i),\alpha}.e_{i,\sigma(i)}\big) = \sum_{\sigma\in J}\Big(\prod_{i\in I}\lambda_{i,\sigma(i),\alpha}\Big).\bigotimes_{i\in I} e_{i,\sigma(i)}.$$

Ebből következik, hogy

$$t = \sum_{\alpha\in A}\bigotimes_{i\in I} x_{i,\alpha} = \sum_{\alpha\in A}\Big(\sum_{\sigma\in J}\Big(\prod_{i\in I}\lambda_{i,\sigma(i),\alpha}\Big).\bigotimes_{i\in I} e_{i,\sigma(i)}\Big) = \sum_{\sigma\in J}\Big(\Big(\sum_{\alpha\in A}\Big(\prod_{i\in I}\lambda_{i,\sigma(i),\alpha}\Big)\Big).\bigotimes_{i\in I} e_{i,\sigma(i)}\Big),$$

amiből látható, hogy ha minden $\sigma\in J$ függvényre $\lambda_\sigma := \sum_{\alpha\in A}\Big(\prod_{i\in I}\lambda_{i,\sigma(i),\alpha}\Big)$, akkor a K-ban haladó $(\lambda_\sigma)_{\sigma\in J}$ rendszerre teljesül a $t = \sum_{\sigma\in J}\lambda_\sigma.\bigotimes_{i\in I} e_{i,\sigma(i)}$ egyenlőség. ∎

19.8.2. Állítás. *Legyen $(E_i)_{i\in I}$ nem üres, véges vektortér-rendszer a K test felett. Ekkor egyértelműen létezik olyan*

$$\tau : \bigotimes_{i\in I} E_i \to \mathbf{Mult}\Big(\prod_{i\in I} E_i^*; K\Big)$$

lineáris operátor, amelyre minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ és $(u_i)_{i\in I} \in \prod_{i\in I} E_i^*$ esetén

$$\Big(\tau\Big(\bigotimes_{i\in I} x_i\Big)\Big)\Big((u_i)_{i\in I}\Big) = \mathrm{P}_{i\in I}\, u_i(x_i).$$

Ez a τ lineáris operátor injektív.

Bizonyítás. Az **ALG** 19.4.7. példa szerint jól értelmezett az az

$$m : \prod_{i\in I} E_i \to \mathbf{Mult}\Big(\prod_{i\in I} E_i^*; K\Big)$$

multilineáris operátor, amelyre minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ és $(u_i)_{i\in I} \in \prod_{i\in I} E_i^*$ esetén

$$(m\,((x_i)_{i\in I}))\Big((u_i)_{i\in I}\Big) = \mathrm{P}_{i\in I}\, u_i(x_i),$$

ezért a tenzorszorzatokra vonatkozó (ET) feltétel alapján létezik egyetlen olyan

$$\tau : \bigotimes_{i\in I} E_i \to \mathbf{Mult}\Big(\prod_{i\in I} E_i^*; K\Big)$$

lineáris operátor, amelyre minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ és $(u_i)_{i\in I} \in \prod_{i\in I} E_i^*$ esetén

$$\Big(\tau\Big(\bigotimes_{i\in I} x_i\Big)\Big)\Big((u_i)_{i\in I}\Big) = \mathrm{P}_{i\in I}\, u_i(x_i).$$

A τ operátor injektivitásának bizonyításához legyen $t \in \bigotimes_{i\in I} E_i$ olyan, hogy $\tau(t) = 0$. Ekkor 19.8.1. alapján vehetünk olyan $\Big((e_{i,j})_{j\in J_i}\Big)_{i\in I}$ rendszert, hogy minden $i \in I$ esetén $(e_{i,j})_{j\in J_i}$ véges lineárisan független rendszer E_i-ben, és vehetünk olyan K-ban haladó $(\lambda_\sigma)_{\sigma\in J}$ rendszert, hogy

$$t = \sum_{\sigma\in J} \lambda_\sigma . \bigotimes_{i\in I} e_{i,\sigma(i)},$$

ahol $J := \prod_{i\in I} J_i$. Ekkor $\tau(t) = 0$ és τ definíciója miatt minden $(u_i)_{i\in I} \in \prod_{i\in I} E_i^*$ esetén

$$0 = \Big(\tau\Big(\sum_{\sigma\in J} \lambda_\sigma . \bigotimes_{i\in I} e_{i,\sigma(i)}\Big)\Big)\,((u_i)_{i\in I}) = \sum_{\sigma\in J} \lambda_\sigma . \tau\Big(\bigotimes_{i\in I} e_{i,\sigma(i)}\Big)\,((u_i)_{i\in I}) =$$

$$= \sum_{\sigma\in J} \lambda_\sigma . \mathrm{P}_{i\in I}\, u_i(e_{i,\sigma(i)}) \tag{$*$}$$

Legyen $i \in I$. Ekkor a 17.9.3. állítást alkalmazva az $M_i := \mathrm{sp}\{e_{i,j} | j \in J_i\}$ véges dimenziós vektortérre kapjuk olyan M_i^*-ban haladó $(v_{i,j})_{j \in J_i}$ rendszer létezését, hogy minden $j, j' \in J_i$ indexre $v_{i,j}(e_{i,j'}) = \delta_{j,j'}$. A 17.7.1. tétel alapján kiválaszthatunk olyan E_i^*-ban haladó $(u_{i,j})_{j \in J_i}$ rendszert, hogy minden $j \in J_i$ esetén $v_{i,j} \subseteq u_{i,j}$.

Tehát vehetünk olyan $((u_{i,j})_{j \in J_i})_{i \in I}$ rendszert, hogy minden $i \in I$ indexre $(u_{i,j})_{j \in J_i}$ olyan E_i^*-ban haladó rendszer, hogy minden $j, j' \in J_i$ esetén $u_{i,j}(e_{i,j'}) = \delta_{j,j'}$.

Legyen $\sigma' \in J$. Ekkor a $(*)$ összefüggést alkalmazva az $(u_i)_{i \in I} := (u_{i,\sigma'(i)})_{i \in I}$ rendszerre kapjuk, hogy

$$0 = \sum_{\sigma \in J} \lambda_\sigma \cdot \mathrm{P}_{i \in I} u_{i,\sigma'(i)} \left(e_{i,\sigma(i)}\right) = \sum_{\sigma \in J} \lambda_\sigma \cdot \mathrm{P}_{i \in I} \delta_{\sigma'(i),\sigma(i)} = \lambda_{\sigma'},$$

hiszen minden $\sigma \in J$ esetén nyilvánvalóan $\mathrm{P}_{i \in I} \delta_{\sigma'(i),\sigma(i)} = \delta_{\sigma',\sigma}$. Ebből következik, hogy $t = 0$, tehát a τ lineáris operátor injektív. ■

19.8.3. Következmény. *Legyen $(E_i)_{i \in I}$ nem üres véges vektortér-rendszer a K test felett. Ekkor egyértelműen létezik olyan*

$$\tau : \bigotimes_{i \in I} E_i \to \left(\bigotimes_{i \in I} E_i^* \right)^*$$

lineáris operátor, amelyre minden $(x_i)_{i \in I} \in \prod_{i \in I} E_i$ és $(u_i)_{i \in I} \in \prod_{i \in I} E_i^*$ esetén

$$\left(\tau \left(\bigotimes_{i \in I} x_i \right) \right) \left(\bigotimes_{i \in I} u_i \right) = \mathrm{P}_{i \in I} u_i(x_i).$$

Ez a τ lineáris operátor injektív.

Bizonyítás. A 19.7.5. állítást alkalmazva $(E_i)_{i \in I}$ helyett az $(E_i^*)_{i \in I}$ vektortér-rendszerre és az $F := K$ választással kapjuk, hogy jól értelmezett az az

$$A : \mathbf{Mult}\left(\prod_{i \in I} E_i^*; K \right) \to \mathbf{L}\left(\bigotimes_{i \in I} E_i^*; K \right) = \left(\bigotimes_{i \in I} E_i^* \right)^*$$

lineáris operátor, amelyre minden $m \in \mathbf{Mult}\left(\prod_{i \in I} E_i^*; K \right)$ és $(u_i)_{i \in I} \in \prod_{i \in I} E_i^*$ esetén

$$A(m) \left(\bigotimes_{i \in I} u_i \right) = m\left((u_i)_{i \in I}\right),$$

és ez az A leképezés lineáris bijekció. (Még akkor is, ha az I indexhalmaz végtelen!) Másfelől, véges I esetén az előző állításban láttuk, hogy jól értelmezett az a

$$B : \bigotimes_{i \in I} E_i \to \mathbf{Mult}\left(\prod_{i \in I} E_i^*; K \right)$$

lineáris operátor, amelyre minden $(x_i)_{i \in I} \in \prod_{i \in I} E_i$ és $(u_i)_{i \in I} \in \prod_{i \in I} E_i^*$ esetén

$$\left(B \left(\bigotimes_{i \in I} x_i \right) \right) \left((u_i)_{i \in I}\right) = \mathrm{P}_{i \in I} u_i(x_i),$$

és ez a B leképezés injektív. Ebből következik, hogy az

$$A \circ B : \bigotimes_{i \in I} E_i \to \Big(\bigotimes_{i \in I} E_i^* \Big)^*$$

leképezés lineáris operátor, és a definíciók alapján nyilvánvaló, hogy minden $(x_i)_{i \in I} \in \prod_{i \in I} E_i$ és $(u_i)_{i \in I} \in \prod_{i \in I} E_i^*$ esetén

$$\Big((A \circ B)\Big(\bigotimes_{i \in I} x_i \Big) \Big) ((u_i)_{i \in I}) = \Big(B\Big(\bigotimes_{i \in I} x_i \Big) \Big) ((u_i)_{i \in I}) = \prod_{i \in I} u_i(x_i),$$

tehát $A \circ B$ az az egyértelműen létező lineáris operátor, amelyről az állítás szól, és világos, hogy $A \circ B$ injekció. ■

19.8.4. Következmény. *Legyen $(E_i)_{i \in I}$ nem üres véges vektortér-rendszer a K test felett. Ha $(x_i)_{i \in I} \in \prod_{i \in I} E_i$ olyan rendszer, hogy minden $i \in I$ esetén $x_i \neq 0$, akkor $\bigotimes_{i \in I} x_i \neq 0$.*

Bizonyítás. A 19.8.2. állítás szerint tekinthetjük azt a

$$\tau : \bigotimes_{i \in I} E_i \to \mathbf{Mult}\Big(\prod_{i \in I} E_i^*; K \Big)$$

lineáris operátort, amelyre minden $(x_i)_{i \in I} \in \prod_{i \in I} E_i$ és $(u_i)_{i \in I} \in \prod_{i \in I} E_i^*$ esetén

$$\Big(\tau\Big(\bigotimes_{i \in I} x_i \Big) \Big) ((u_i)_{i \in I}) = \prod_{i \in I} u_i(x_i).$$

Ha $(x_i)_{i \in I} \in \prod_{i \in I} E_i$ olyan rendszer, hogy minden $i \in I$ esetén $x_i \neq 0$, akkor 17.7.4. szerint kiválaszthatunk olyan $(u_i)_{i \in I} \in \prod_{i \in I} E_i^*$ rendszert, hogy minden $i \in I$ indexre $u_i(x_i) \neq 0$, és ekkor

$$\Big(\tau\Big(\bigotimes_{i \in I} x_i \Big) \Big) ((u_i)_{i \in I}) = \prod_{i \in I} u_i(x_i) \neq 0,$$

következésképpen $\tau\Big(\bigotimes_{i \in I} x_i \Big) \neq 0$, így τ linearitása folytán $\bigotimes_{i \in I} x_i \neq 0$. ■

Figyeljük meg, hogy az előző állítás bizonyításában csak a 19.8.2. állításban értelmezett τ lineáris operátor definíciója volt lényeges, a τ leképezés injektivitását nem használtuk ki.

19.8.5. Következmény. *Legyen I nem üres véges halmaz és K test. Ekkor $\bigotimes_{i \in I} 1$ bázis a $\bigotimes_{i \in I} K$ vektortérben, és az*

$$u : K \to \bigotimes_{i \in I} K; \quad \lambda \mapsto \lambda. \bigotimes_{i \in I} 1$$

leképezés lineáris bijekció.

Bizonyítás. Világos, hogy u lineáris operátor. Ha $t \in \bigotimes_{i\in I} K$, akkor 19.7.4. szerint vehetünk olyan $\left((\lambda_{\alpha,i})_{i\in I}\right)_{\alpha\in A}$ rendszert, hogy A véges halmaz és minden $\alpha \in A$ esetén $(\lambda_{\alpha,i})_{i\in I} \in \prod_{i\in I} K$, és $t = \sum_{\alpha\in A} \bigotimes_{i\in I} \lambda_{\alpha,i}$. A $\otimes$ multilineáris operátor multihomogenitásából (19.2.1.) következik, hogy minden $\alpha \in A$ esetén

$$\bigotimes_{i\in I} \lambda_{\alpha,i} = \bigotimes_{i\in I}(\lambda_{\alpha,i}.1) = \Big(\mathrm{P}_{i\in I} \lambda_{\alpha_i}\Big) \bigotimes_{i\in I} 1.$$

Ebből kapjuk, hogy $t = \lambda. \bigotimes_{i\in I} 1 = u(\lambda)$, ahol $\lambda := \sum_{\alpha\in A} \Big(\mathrm{P}_{i\in I} \lambda_{\alpha_i}\Big)$, tehát az u operátor szürjektív. Az u operátor injektivitása azzal ekvivalens, hogy $\bigotimes_{i\in I} 1 \neq 0$, ami az előző állítás szerint igaz. ■

19.8.6. Állítás. *Legyen $(E_i)_{i\in I}$ (nem feltétlenül véges) vektortér-rendszer a K test felett. Ekkor egyértelműen létezik olyan*

$$\tau : \bigotimes_{i\in I} E_i \to \Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)\Big)^*$$

lineáris operátor, amelyre minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ és $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$ esetén

$$\Big(\tau\Big(\bigotimes_{i\in I} x_i\Big)\Big)(u) = u\left((x_i)_{i\in I}\right).$$

Ha I nem üres és véges, akkor ez a τ lineáris operátor injektív.

Bizonyítás. (I) Nyilvánvaló, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén a

$$\mathrm{v}_{(x_i)_{i\in I}} : \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big) \to K; \quad u \mapsto u\left((x_i)_{i\in I}\right)$$

leképezés lineáris funkcionál, vagyis eleme $\Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)\Big)^*$-nak, ezért az állításban szereplő τ lineáris operátor egyértelmű létezéséhez (ET) alapján pontosan azt kell belátni, hogy az

$$m : \prod_{i\in I} E_i \to \Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)\Big)^*; \quad (x_i)_{i\in I} \mapsto \mathrm{v}_{(x_i)_{i\in I}}$$

leképezés multilineáris operátor. Ennek bizonyításához legyen $k \in I$ és $\mathbf{x} := (x_i)_{i\in I}$ rögzített. Ekkor $x \in E_k$ és $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$ esetén

$$\left((m \circ \mathrm{in}_{k,\mathbf{x}})(x)\right)(u) = \mathrm{v}_{\mathrm{in}_{k,\mathbf{x}}(x)}(u) = u\left(\mathrm{in}_{k,\mathbf{x}}(x)\right) = \left(u \circ \mathrm{in}_{k,\mathbf{x}}\right)(x).$$

Ebből látható, hogy ha $x, x' \in E_k$, akkor minden $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$ multilineáris funkcionálra $u \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to K$ additivitása folytán

$$\begin{aligned}\left((m \circ \mathrm{in}_{k,\mathbf{x}})(x + x')\right)(u) &= (u \circ \mathrm{in}_{k,\mathbf{x}})(x + x') = (u \circ \mathrm{in}_{k,\mathbf{x}})(x) + (u \circ \mathrm{in}_{k,\mathbf{x}})(x') = \\ = \left((m \circ \mathrm{in}_{k,\mathbf{x}})(x)\right)(u) &+ \left((m \circ \mathrm{in}_{k,\mathbf{x}})(x')\right)(u) = \Big((m \circ \mathrm{in}_{k,\mathbf{x}})(x) + (m \circ \mathrm{in}_{k,\mathbf{x}})(x')\Big)(u),\end{aligned}$$

tehát $(m \circ \mathrm{in}_{k,\mathbf{x}})(x + x') = (m \circ \mathrm{in}_{k,\mathbf{x}})(x) + (m \circ \mathrm{in}_{k,\mathbf{x}})(x')$, vagyis az $m \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to \left(\mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)\right)^*$ leképezés additív.

Továbbá, ha $x \in E_k$ és $\lambda \in K$, akkor minden $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$ multilineáris funkcionálra $u \circ \mathrm{in}_{k,\mathbf{x}} : E_k \to K$ K-homogenitása folytán

$$\begin{aligned}((m \circ \mathrm{in}_{k,\mathbf{x}})(\lambda.x))(u) = (u \circ \mathrm{in}_{k,\mathbf{x}})(\lambda.x) = \lambda.(u \circ \mathrm{in}_{k,\mathbf{x}})(x) = \\ = \lambda.((m \circ \mathrm{in}_{k,\mathbf{x}})(x))(u) = (\lambda.(m \circ \mathrm{in}_{k,\mathbf{x}})(x))(u),\end{aligned}$$

tehát $(m \circ \mathrm{in}_{k,\mathbf{x}})(\lambda.x) = \lambda.(m \circ \mathrm{in}_{k,\mathbf{x}})(x)$, vagyis az $m\circ\mathrm{in}_{k,\mathbf{x}} : E_k \to \left(\mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)\right)^*$ leképezés K-homogén.

(II) Tegyük fel, hogy I nem üres és véges. A τ operátor injektivitásának bizonyításához legyen $t \in \bigotimes_{i\in I} E_i$ olyan, hogy $\tau(t) = 0$. Ekkor 19.8.1. alapján vehetünk olyan $\left((e_{i,j})_{j\in J_i}\right)_{i\in I}$ rendszert, hogy minden $i \in I$ esetén $(e_{i,j})_{j\in J_i}$ véges lineárisan független rendszer E_i-ben, és vehetünk olyan K-ban haladó $(\lambda_\sigma)_{\sigma\in J}$ rendszert, hogy

$$t = \sum_{\sigma\in J} \lambda_\sigma . \bigotimes_{i\in I} e_{i,\sigma(i)},$$

ahol $J := \prod_{i\in I} J_i$. Ekkor $\tau(t) = 0$ és τ definíciója miatt minden $u \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$ esetén

$$0 = \Big(\tau\Big(\sum_{\sigma\in J} \lambda_\sigma . \bigotimes_{i\in I} e_{i,\sigma(i)}\Big)\Big)(u) = \sum_{\sigma\in J} \lambda_\sigma . \tau\Big(\bigotimes_{i\in I} e_{i,\sigma(i)}\Big)(u) = \sum_{\sigma\in J} \lambda_\sigma u\left((e_{i,\sigma(i)})_{i\in I}\right) \qquad (*)$$

Legyen $i \in I$. Ekkor a 17.9.3. állítást alkalmazva az $M_i := \mathrm{sp}\{e_{i,j} | j \in J_i\}$ véges dimenziós vektortérre kapjuk olyan M_i^*-ban haladó $(v_{i,j})_{j\in J_i}$ rendszer létezését, hogy minden $j, j' \in J_i$ indexre $v_{i,j}(e_{i,j'}) = \delta_{j,j'}$. A 17.7.1. tétel alapján kiválaszthatunk olyan E_i^*-ban haladó $(u_{i,j})_{j\in J_i}$ rendszert, hogy minden $j \in J_i$ esetén $v_{i,j} \subseteq u_{i,j}$.

Tehát vehetünk olyan $((u_{i,j})_{j\in J_i})_{i\in I}$ rendszert, hogy minden $i \in I$ indexre $(u_{i,j})_{j\in J_i}$ olyan E_i^*-ban haladó rendszer, hogy minden $j, j' \in J_i$ esetén $u_{i,j}(e_{j,j'}) = \delta_{j,j'}$.

Legyen $\sigma' \in J$. Ekkor a $(*)$ összefüggést alkalmazva az $u := \dot{\bigotimes_{i\in I}} u_{i,\sigma'(i)} \in \mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)$ multilineáris funkcionálra (**ALG** 19.4.8. példa) kapjuk, hogy

$$0 = \sum_{\sigma\in J} \lambda_\sigma . \Big(\dot{\bigotimes_{i\in I}} u_{i,\sigma'(i)}\Big)\left(\left(e_{i,\sigma(i)}\right)_{i\in I}\right) = \sum_{\sigma\in J} \lambda_\sigma . \mathrm{P}_{i\in I}\, u_{i,\sigma'(i)}\left(e_{i,\sigma(i)}\right) = \sum_{\sigma\in J} \lambda_\sigma . \mathrm{P}_{i\in I}\, \delta_{\sigma'(i),\sigma(i)} = \lambda_{\sigma'},$$

hiszen minden $\sigma \in J$ esetén nyilvánvalóan $\mathrm{P}_{i\in I}\, \delta_{\sigma'(i),\sigma(i)} = \delta_{\sigma',\sigma}$. Ebből következik, hogy $t = 0$, tehát a τ lineáris operátor injektív. ■

19.8.7. Állítás. *Legyen $(E_i)_{i\in I}$ vektorterek olyan nem üres, véges rendszere a K test felett, hogy minden $i \in I$ esetén E_i véges dimenziós. Ha $\left((e_{i,j})_{j\in\dim(E_i)}\right)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(e_{i,j})_{j\in\dim(E_i)}$ bázis az E_i vektortérben, akkor a*

$$\Big(\bigotimes_{i\in I} e_{i,\sigma(i)}\Big)_{\sigma\in\prod_{i\in I}\dim(E_i)}$$

rendszer bázis a $\bigotimes\limits_{i\in I} E_i$ *vektortérben, tehát* $\bigotimes\limits_{i\in I} E_i$ *véges dimenziós vektortér, és*

$$\dim\Big(\bigotimes_{i\in I} E_i\Big) = \mathop{\mathrm{P}}_{i\in I} \dim(E_i).$$

Bizonyítás. Vezessük be a $D := \prod\limits_{i\in I} \dim(E_i)$ rövidítést. Legyen $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$, továbbá minden $i \in I$ esetén legyen $(X_{i,j})_{j\in\dim(E_i)} \in K^{\dim(E_i)}$ az a rendszer, amelyre $x_i = \sum\limits_{j\in\dim(E_i)} X_{i,j}e_{i,j}$. Ekkor a multilineáris operátorok multiadditivitásának és multihomogenitásának tétele (19.3.1. és 19.2.1.) alapján

$$\bigotimes_{i\in I} x_i = \bigotimes_{i\in I}\Big(\sum_{j\in\dim(E_i)} X_{i,j}e_{i,j}\Big) = \sum_{\sigma\in D}\bigotimes_{i\in I}\big(X_{i,\sigma(i)}e_{i,\sigma(i)}\big) = \sum_{\sigma\in D}\Big(\mathop{\mathrm{P}}_{i\in I} X_{i,\sigma(i)}\Big)\Big(\bigotimes_{i\in I} e_{i,\sigma(i)}\Big),$$

következésképpen $\bigotimes\limits_{i\in I} x_i$ eleme a $\Big(\bigotimes\limits_{i\in I} e_{i,\sigma(i)}\Big)_{\sigma\in D}$ rendszer lineáris burkának. Mivel $\mathrm{Im}\,(\otimes)$ generátorhalmaz $\bigotimes\limits_{i\in I} E_i$-ben (19.7.3.), így $\Big(\bigotimes\limits_{i\in I} e_{i,\sigma(i)}\Big)_{\sigma\in D}$ generátorrendszer a $\bigotimes\limits_{i\in I} E_i$ vektortérben.

Az $\Big(\bigotimes\limits_{i\in I} e_{i,\sigma(i)}\Big)_{\sigma\in D}$ rendszer lineáris függetlenségének bizonyításához legyen $(\lambda_\sigma)_{\sigma\in D} \in K^D$ olyan rendszer K-ban, amelyre $\sum\limits_{\sigma\in D}\lambda_\sigma.\bigotimes\limits_{i\in I} e_{i,\sigma(i)} = 0$. Legyen $\Big((u_{i,j})_{j\in\dim(E_i)}\Big)_{i\in I}$ az az egyértelműen meghatározott rendszer, amelyre minden $i \in I$ esetén $(u_{i,j})_{j\in\dim(E_i)} \in (E_i^*)^{\dim(E_i)}$ az $(e_{i,j})_{j\in\dim(E_i)}$ rendszer duálisa (17.9.4.), tehát minden $i \in I$ és $j, j' \in \dim(E_i)$ esetén $u_{i,j} \in E_i^*$ és $u_{i,j}\,(e_{i,j'}) = \delta_{j,j'}$. Ekkor minden $\sigma' \in D$ függvényre

$$0 = \Big(\dot{\bigotimes_{i\in I}} u_{i,\sigma'(i)}\Big)\Big(\sum_{\sigma\in D}\lambda_\sigma.\bigotimes_{i\in I} e_{i,\sigma(i)}\Big) = \sum_{\sigma\in D}\lambda_\sigma\Big(\dot{\bigotimes_{i\in I}} u_{i,\sigma'(i)}\Big)\Big(\bigotimes_{i\in I} e_{i,\sigma(i)}\Big) =$$

$$= \sum_{\sigma\in D}\lambda_\sigma \mathop{\mathrm{P}}_{i\in I} u_{i,\sigma'(i)}\,\big(e_{i,\sigma(i)}\big) = \sum_{\sigma\in D}\lambda_\sigma \mathop{\mathrm{P}}_{i\in I}\delta_{\sigma'(i),\sigma(i)} = \sum_{\sigma\in D}\lambda_\sigma\delta_{\sigma',\sigma} = \lambda_{\sigma'},$$

hiszen nyilvánvaló, hogy $\mathop{\mathrm{P}}\limits_{i\in I}\delta_{\sigma'(i),\sigma(i)} = \delta_{\sigma',\sigma}$. Ezért a $\Big(\bigotimes\limits_{i\in I} e_{i,\sigma(i)}\Big)_{\sigma\in D}$ rendszer lineáris független.

Tehát a $\bigotimes\limits_{i\in I} E_i$ vektortér véges dimenziós, és 9.1.4. alapján

$$\dim\Big(\bigotimes_{i\in I} E_i\Big) = \mathrm{Card}(D) = \mathrm{Card}\Big(\prod_{i\in I}\dim(E_i)\Big) = \mathop{\mathrm{P}}_{i\in I}\dim(E_i). \blacksquare$$

19.8.8. Következmény. *Legyen* $(E_i)_{i\in I}$ *vektorterek olyan nem üres, véges rendszere a* K *test felett, hogy minden* $i \in I$ *esetén* E_i *véges dimenziós. Legyen*

$$\tau : \bigotimes_{i\in I} E_i \to \mathbf{Mult}\Big(\prod_{i\in I} E_i^*; K\Big)$$

az a lineáris operátor, amelyre minden $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ *és* $(u_i)_{i\in I} \in \prod\limits_{i\in I} E_i^*$ *esetén*

$$\Big(\tau\Big(\bigotimes_{i\in I} x_i\Big)\Big)\Big((u_i)_{i\in I}\Big) = \mathop{\mathrm{P}}_{i\in I} u_i(x_i).$$

Ekkor τ izomorfizmus a $\bigotimes\limits_{i\in I} E_i$ és $\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i^*; K\Big)$ vektorterek között.

Bizonyítás. A 19.8.7. állítás szerint $\bigotimes\limits_{i\in I} E_i$ véges dimenziós és $\dim\Big(\bigotimes\limits_{i\in I} E_i\Big) = \sum\limits_{i\in I} \dim(E_i)$. A 19.5.1. állítás szerint $\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i^*; K\Big)$ véges dimenziós és $\dim\Big(\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i^*; K\Big)\Big) = \sum\limits_{i\in I} \dim(E_i)$. A 19.8.2. állítás szerint a τ leképezés lineáris injekció. Ezért 17.6.4. alapján a τ leképezés lineáris bijekció a $\bigotimes\limits_{i\in I} E_i$ és $\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i^*; K\Big)$ vektorterek között. ■

19.8.9. Következmény. *Legyen $(E_i)_{i\in I}$ vektorterek olyan nem üres, véges rendszere a K test felett, hogy minden $i \in I$ esetén E_i véges dimenziós. Legyen*

$$\tau : \bigotimes_{i\in I} E_i \to \Big(\bigotimes_{i\in I} E_i^*\Big)^*$$

az a lineáris operátor, amelyre minden $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ és $(u_i)_{i\in I} \in \prod\limits_{i\in I} E_i^*$ esetén

$$\Big(\tau\Big(\bigotimes_{i\in I} x_i\Big)\Big)\Big(\bigotimes_{i\in I} u_i\Big) = \sum_{i\in I} u_i(x_i).$$

Ekkor τ izomorfizmus a $\bigotimes\limits_{i\in I} E_i$ és $\Big(\bigotimes\limits_{i\in I} E_i^*\Big)^*$ vektorterek között.

Bizonyítás. A 19.8.7. állítás szerint $\bigotimes\limits_{i\in I} E_i$ véges dimenziós és $\dim\Big(\bigotimes\limits_{i\in I} E_i\Big) = \sum\limits_{i\in I} \dim(E_i)$. A 17.9.7. állítás szerint minden $i \in I$ esetén E_i^* is véges dimenziós és $\dim(E_i^*) = \dim(E_i)$, így ismét a 19.8.7. állításra hivatkozva kapjuk, hogy $\bigotimes\limits_{i\in I} E_i^*$ véges dimenziós és $\dim\Big(\bigotimes\limits_{i\in I} E_i^*\Big) = \sum\limits_{i\in I} \dim(E_i^*) = \sum\limits_{i\in I} \dim(E_i)$. Ezért 17.9.7. alapján $\Big(\bigotimes\limits_{i\in I} E_i^*\Big)^*$ véges dimenziós és $\dim\Big(\Big(\bigotimes\limits_{i\in I} E_i^*\Big)^*\Big) = \dim\Big(\bigotimes\limits_{i\in I} E_i^*\Big) = \sum\limits_{i\in I} \dim(E_i)$. A 19.8.3. állítás szerint a τ leképezés lineáris injekció. Ezért 17.6.4. alapján a τ leképezés lineáris bijekció a $\bigotimes\limits_{i\in I} E_i$ és $\Big(\bigotimes\limits_{i\in I} E_i^*\Big)^*$ vektorterek között. ■

19.8.10. Következmény. *Legyen $(E_i)_{i\in I}$ vektorterek olyan nem üres, véges rendszere a K test felett, hogy minden $i \in I$ esetén E_i véges dimenziós. Legyen*

$$\tau : \bigotimes_{i\in I} E_i \to \Big(\mathbf{Mult}\Big(\prod_{i\in I} E_i; K\Big)\Big)^*$$

az a lineáris operátor, amelyre minden $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ és $u \in \mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; K\Big)$ esetén

$$\Big(\tau\Big(\bigotimes_{i\in I} x_i\Big)\Big)(u) = u\left((x_i)_{i\in I}\right).$$

Ekkor τ izomorfizmus a $\bigotimes\limits_{i\in I} E_i$ és $\Big(\mathbf{Mult}\Big(\prod\limits_{i\in I} E_i; K\Big)\Big)^*$ vektorterek között.

Bizonyítás. A 19.8.7. állítás szerint $\bigotimes_{i\in I} E_i$ véges dimenziós és $\dim\left(\bigotimes_{i\in I} E_i\right) = \prod_{i\in I} \dim(E_i)$. A 19.5.1. állítás szerint $\mathbf{Mult}\left(\prod_{i\in I} E_i; K\right)$ véges dimenziós és $\dim\left(\mathbf{Mult}\left(\prod_{i\in I} E_i; K\right)\right) = \prod_{i\in I} \dim(E_i)$. Ezért a 17.9.7. állítás szerint a $\left(\mathbf{Mult}\left(\prod_{i\in I} E_i; K\right)\right)^*$ algebrai duális is véges dimenziós és $\dim\left(\left(\mathbf{Mult}\left(\prod_{i\in I} E_i; K\right)\right)^*\right) = \dim\left(\mathbf{Mult}\left(\prod_{i\in I} E_i; K\right)\right) = \prod_{i\in I} \dim(E_i)$. A 19.8.2. állítás szerint a τ leképezés lineáris injekció. Ezért 17.6.4. alapján a τ leképezés lineáris bijekció a $\bigotimes_{i\in I} E_i$ és $\left(\mathbf{Mult}\left(\prod_{i\in I} E_i; K\right)\right)^*$ vektorterek között. ■

A három előző állítás három teljesen különböző realizációját adja véges sok, véges dimenziós vektortér tenzorszorzatának.

19.9. Két vektortér tenzorszorzata

19.9.1. Lemma. *Legyenek E és F vektorterek a K test felett. Ha $t \in E \otimes F$ és $(e_i)_{i\in I}$ olyan véges E-ben haladó rendszer, és $(f_i)_{i\in I}$ olyan véges F-ben haladó rendszer, hogy $t = \sum_{i\in I}(e_i \otimes f_i)$, valamint $\mathrm{Card}(I)$ minimális, akkor az $(e_i)_{i\in I}$ rendszer lineárisan független E-ben és az $(f_i)_{i\in I}$ rendszer lineárisan független F-ben.*

Bizonyítás. Tegyük fel, hogy, hogy az $(e_i)_{i\in I}$ rendszer lineárisan összefüggő E-ben, tehát vehetünk olyan $i_* \in I$ indexet, hogy az $I_* := I \setminus \{i_*\}$ halmazhoz van olyan $(\lambda_i)_{i\in I_*} \in K^{I_*}$ rendszer, amelyre $e_{i_*} = \sum_{i\in I_*} \lambda_i . e_i$. Ekkor

$$t = \sum_{i\in I}(e_i \otimes f_i) = \sum_{i\in I_*}(e_i \otimes f_i) + e_{i_*} \otimes f_{i_*} = \sum_{i\in I_*}(e_i \otimes f_i) + \left(\sum_{i\in I_*} \lambda_i . e_i\right) \otimes f_{i_*} =$$

$$= \sum_{i\in I_*}(e_i \otimes f_i) + \sum_{i\in I_*} \lambda_i . (e_i \otimes f_{i_*}) = \sum_{i\in I_*}(e_i \otimes f_i) + \sum_{i\in I_*}(e_i \otimes (\lambda_i . f_{i_*})) = \sum_{i\in I_*}(e_i \otimes (f_i + \lambda_i . f_{i_*})),$$

tehát $t = \sum_{i\in I_*}(e_i \otimes \widetilde{f}_i)$, ahol minden $i \in I_*$ esetén $\widetilde{f}_i = f_i + \lambda_i . f_{i_*}$. Mivel $\mathrm{Card}(I_*) = \mathrm{Card}(I) - 1$, így ez ellentmond az I indexhalmaz minimalitásának.

Tegyük fel, hogy az $(f_i)_{i\in I}$ rendszer lineárisan összefüggő F-ben, tehát vehetünk olyan $i_* \in I$ indexet, hogy az $I_* := I \setminus \{i_*\}$ halmazhoz van olyan $(\lambda_i)_{i\in I_*} \in K^{I_*}$ rendszer, amelyre $f_{i_*} = \sum_{i\in I_*} \lambda_i . f_i$. Ekkor

$$t = \sum_{i\in I}(e_i \otimes f_i) = \sum_{i\in I_*}(e_i \otimes f_i) + e_{i_*} \otimes f_{i_*} = \sum_{i\in I_*}(e_i \otimes f_i) + e_{i_*} \otimes \left(\sum_{i\in I_*} \lambda_i . f_i\right) =$$

$$= \sum_{i\in I_*}(e_i \otimes f_i) + \sum_{i\in I_*} \lambda_i . (e_{i_*} \otimes f_i) = \sum_{i\in I_*}(e_i \otimes f_i) + \sum_{i\in I_*}((\lambda_i . e_{i_*}) \otimes f_i) = \sum_{i\in I_*}((e_i + \lambda_i . e_{i_*}) \otimes f_i),$$

tehát $t = \sum_{i\in I_*}(\widetilde{e}_i \otimes f_i)$, ahol minden $i \in I_*$ esetén $\widetilde{e}_i = e_i + \lambda_i . e_{i_*}$. Mivel $\mathrm{Card}(I_*) = \mathrm{Card}(I) - 1$, így ez ellentmond az I indexhalmaz minimalitásának. ■

19.9.2. Állítás. *Legyenek E és F vektorterek a K test felett. Ekkor létezik egyetlen olyan*

$$\tau : E \otimes F \to \mathbf{L}(E^*; F)$$

lineáris operátor, amelyre teljesül az, hogy minden $e \in E$ és $f \in F$ esetén, minden $u \in E^*$ funkcionálra

$$\tau(e \otimes f)(u) = u(e).f.$$

Ez a τ operátor injektív és

$$\mathrm{Im}(\tau) \;\subseteq\; \{v \in \mathbf{L}(E^*; F) | \dim(\mathrm{Im}(v)) < +\infty\}.$$

Bizonyítás. (I) Ha $e \in E$ és $f \in F$, akkor az

$$e \dot{\otimes} f : E^* \to F; \quad u \mapsto u(e).f$$

leképezés lineáris, mert megegyezik az $\mathrm{j}_E(e) : E^* \to K$ lineáris funkcionál (**??**), és az azt követő $K \to F$; $\lambda \mapsto \lambda.f$ lineáris leképezés kompozíciójával. Tehát a τ lineáris operátor egyértelmű létezéséhez a tenzorszorzatok univerzalitási tulajdonsága, vagyis (ET) alapján, pontosan azt kell igazolni, hogy az

$$E \times F \to \mathbf{L}(E^*; F); \quad (e, f) \mapsto e \dot{\otimes} f$$

leképezés bilineáris.

Ha $e, e' \in E$ és $f \in F$, akkor minden $u \in E^*$ funkcionálra

$$\left((e + e') \dot{\otimes} f\right)(u) = u(e + e').f = (u(e) + u(e')).f = u(e).f + u'(e).f =$$
$$= \left(e \dot{\otimes} f\right)(u) + \left(e' \dot{\otimes} f\right)(u) = \left(e \dot{\otimes} f + e' \dot{\otimes} f\right)(u),$$

tehát $(e + e') \dot{\otimes} f = e \dot{\otimes} f + e' \dot{\otimes} f$.

Ha $e \in E$ és $f, f' \in F$, akkor minden $u \in E^*$ funkcionálra

$$\left(e \dot{\otimes} (f + f')\right)(u) = u(e).(f + f') = u(e).f + u(e).f' =$$
$$= \left(e \dot{\otimes} f\right)(u) + \left(e \dot{\otimes} f'\right)(u) = \left(e \dot{\otimes} f + e \dot{\otimes} f'\right)(u),$$

tehát $e \dot{\otimes} (f + f') = e \dot{\otimes} f + e \dot{\otimes} f'$.

Ha $e \in E$, $f \in F$ és $\lambda \in K$, akkor $u \in E^*$ funkcionálra

$$\left((\lambda.e) \dot{\otimes} f\right)(u) = u(\lambda.e).f = (\lambda u(e)).f = \lambda.(u(e).f) =$$
$$= \lambda.\left(e \dot{\otimes} f\right)(u) = \left(\lambda.\left(e \dot{\otimes} f\right)\right)(u) =$$

tehát $(\lambda.e) \dot{\otimes} f = \lambda.\left(e \dot{\otimes} f\right)$.

Ha $e \in E$, $f \in F$ és $\lambda \in K$, akkor $u \in E^*$ funkcionálra

$$\left(e \dot{\otimes} (\lambda.f)\right)(u) = u(e).(\lambda.f) = (u(e)\lambda).f = \lambda.(u(e).f) =$$
$$= \lambda.\left(e \dot{\otimes} f\right)(u) = \left(\lambda.\left(e \dot{\otimes} f\right)\right)(u) =$$

tehát $e \dot{\otimes} (\lambda.f) = \lambda.\left(e \dot{\otimes} f\right)$.

Ez azt jelenti, hogy az $E \times F \to \mathbf{L}(E^*; F)$; $(e, f) \mapsto e \dot{\otimes} f$ leképezés bilineáris.

(II) A τ operátor injektivitásának bizonyításához legyen $t \in E \otimes F$ olyan, hogy $\tau(t) = 0$, vagyis minden $u \in E^*$ funkcionálra $\tau(t)(u) = 0$. Vegyünk olyan E-ben haladó $(e_i)_{i \in I}$ véges rendszert, és olyan F-ben haladó $(f_i)_{i \in I}$ rendszert, hogy $t = \sum_{i \in I}(e_i \otimes f_i)$, és $\mathrm{Card}(I)$ minimális. Az előző lemma szerint az $(f_i)_{i \in I}$ rendszer lineárisan független F-ben. Mivel minden $u \in E^*$ funkcionálra

$$0 = \tau(t)(u) = \sum_{i \in I} \tau(e_i \otimes f_i)(u) = \sum_{i \in I}(u(e_i).f_i),$$

így minden $i \in I$ indexre és minden $u \in E^*$ funkcionálra $u(e_i) = 0$. Ezért **??** alapján minden $i \in I$ esetén $e_i = 0$, tehát $t = 0$.

(III) Ha $t \in E \otimes F$ és $(e_i)_{i \in I}$ olyan véges E-ben haladó rendszer, és $(f_i)_{i \in I}$ olyan F-ben haladó rendszer, hogy $t = \sum_{i \in I}(e_i \otimes f_i)$, akkor minden $u \in E^*$ funkcionálra

$$\tau(t)(u) = \sum_{i \in I} \tau(e_i \otimes f_i)(u) = \sum_{i \in I}(u(e_i).f_i) \in \mathrm{sp}\{f_i | i \in I\},$$

tehát $\mathrm{Im}(\tau(t)) \subseteq \mathrm{sp}\{f_i | i \in I\}$, vagyis $\mathrm{Im}(\tau(t))$ véges dimenziós altere F-nek.

Megfordítva, legyen $v \in \mathbf{L}(E^*; F)$ olyan lineáris operátor, amelyre $\mathrm{Im}(v)$ véges dimenziós altere F-nek. Legyen $(f_i)_{i \in I}$ bázis $\mathrm{Im}(v)$-ben, és jelölje $(w_i)_{i \in I}$ a duális bázist (**??**). Ekkor minden $u \in E^*$ funkcionálra $v(u) = \sum_{i \in I} w_i(v(u)).f_i$, tehát ha minden $i \in I$ indexre $u_i := w_i \circ v$, akkor $(u_i)_{i \in I} \in \prod_{i \in I} E_i^*$ olyan rendszer, hogy minden $u \in E^*$ funkcionálra

$$v(u) = \sum_{i \in I} u_i(e).f_i = \sum_{i \in I}(u_i \dot{\otimes} f_i)(e) = \tau\Big(\sum_{i \in I}(u_i \otimes f_i)\Big)(e),$$

vagyis $t := \sum_{i \in I}(u_i \otimes f_i) \in E \otimes F$ olyan tenzor, hogy $v = \tau(t) \in \mathrm{Im}(\tau)$.

Ezzel igazoltuk, hogy $\mathrm{Im}(\tau) = \{v \in \mathbf{L}(E; F) | \dim(\mathrm{Im}(v)) < +\infty\}$. ■

19.9.3. Állítás. *Legyenek E és F vektorterek a K test felett. Ekkor létezik egyetlen olyan*

$$\tau : E^* \otimes F \to \mathbf{L}(E; F)$$

lineáris operátor, amelyre teljesül az, hogy minden $u \in E^*$ és $f \in F$ esetén, minden $e \in E$ vektorra

$$\tau(u \otimes f)(e) = u(e).f.$$

Ez a τ operátor injektív, és

$$\mathrm{Im}(\tau) = \{v \in \mathbf{L}(E; F) | \dim(\mathrm{Im}(v)) < +\infty\}.$$

Bizonyítás. (I) Ha $u \in E^*$ és $f \in F$, akkor az

$$u \dot{\otimes} f : E \to F; \quad e \mapsto u(e).f$$

leképezés lineáris, mert megegyezik az $u : E \to K$ lineáris funkcionál és az azt követő $K \to F$; $\lambda \mapsto \lambda.f$ lineáris leképezés kompozíciójával.

Ha $u, u' \in E^*$ és $f \in F$, akkor minden $e \in E$ vektorra

$$\left((u+u') \dot{\otimes} f\right)(e) = (u+u')(e).f = (u(e)+u'(e)).f = u(e).f + u'(e).f =$$
$$= \left(u \dot{\otimes} f\right)(e) + \left(u' \dot{\otimes} f\right)(e) = \left(u \dot{\otimes} f + u \dot{\otimes} f\right)(e),$$

tehát $(u+u') \dot{\otimes} f = u \dot{\otimes} f + u' \dot{\otimes} f$.

Ha $u \in E^*$ és $f, f' \in F$, akkor minden $e \in E$ vektorra

$$\left(u \dot{\otimes} (f+f')\right)(e) = u(e).(f+f') = u(e).f + u(e).f' =$$
$$= \left(u \dot{\otimes} f\right)(e) + \left(u \dot{\otimes} f'\right)(e) = \left(u \dot{\otimes} f + u \dot{\otimes} f'\right)(e),$$

tehát $u \dot{\otimes} (f+f') = u \dot{\otimes} f + u \dot{\otimes} f'$.

Ha $u \in E^*$, $f \in F$ és $\lambda \in K$, akkor minden $e \in E$ vektorra

$$\left((\lambda.u) \dot{\otimes} f\right)(e) = (\lambda.u)(e).f = (\lambda u(e)).f = \lambda.(u(e).f) =$$
$$= \lambda.\left(u \dot{\otimes} f\right)(e) = \left(\lambda.\left(u \dot{\otimes} f\right)\right)(e) =$$

tehát $(\lambda.u) \dot{\otimes} f = \lambda.\left(u \dot{\otimes} f\right)$.

Ha $u \in E^*$, $f \in F$ és $\lambda \in K$, akkor minden $e \in E$ vektorra

$$\left(u \dot{\otimes} (\lambda.f)\right)(e) = u(e).(\lambda.f) = (u(e)\lambda).f = \lambda.(u(e).f) =$$
$$= \lambda.\left(u \dot{\otimes} f\right)(e) = \left(\lambda.\left(u \dot{\otimes} f\right)\right)(e) =$$

tehát $u \dot{\otimes} (\lambda.f) = \lambda.\left(u \dot{\otimes} f\right)$.

Ez azt jelenti, hogy az

$$E^* \times F \to \mathbf{L}(E;F); \quad (u,f) \mapsto u \dot{\otimes} f$$

leképezés bilineáris, így a tenzorszorzatok univerzalitási tulajdonsága, vagyis (ET) alapján létezik egyetlen olyan

$$\tau : E^* \otimes F \to \mathbf{L}(E;F)$$

lineáris operátor, amelyre teljesül az, hogy minden $u \in E^*$ és $f \in F$ esetén, $\tau(u \otimes f) = u \dot{\otimes} f$, vagyis minden $e \in E$ vektorra

$$\tau(u \otimes f)(e) = u(e).f.$$

(II) A τ operátor injektivitásának bizonyításához legyen $t \in E^* \otimes F$ olyan, hogy $\tau(t) = 0$, vagyis minden $e \in E$ vektorra $\tau(t)(e) = 0$. Vegyünk olyan E^*-ban haladó $(u_i)_{i \in I}$ véges rendszert, és olyan F-ben haladó $(f_i)_{i \in I}$ rendszert, hogy $t = \sum_{i \in I} (u_i \otimes f_i)$, és $\mathrm{Card}(I)$ minimális. Az előző lemma szerint az $(f_i)_{i \in I}$ rendszer lineárisan független F-ben. Mivel minden $e \in E$ vektorra

$$0 = \tau(t)(e) = \sum_{i \in I} \tau(u_i \otimes f_i)(e) = \sum_{i \in I} (u_i(e).f_i),$$

így minden $i \in I$ indexre $u_i(e) = 0$. Ez azt jelenti, hogy minden $i \in I$ esetén $u_i = 0$, tehát $t = 0$.

(III) Ha $t \in E^* \otimes F$ és $(u_i)_{i \in I}$ olyan véges E^*-ban haladó rendszer, és $(f_i)_{i \in I}$ olyan F-ben haladó rendszer, hogy $t = \sum_{i \in I} (u_i \otimes f_i)$, akkor minden $e \in E$ vektorra

$$\tau(t)(e) = \sum_{i \in I} \tau(u_i \otimes f_i)(e) = \sum_{i \in I} (u_i(e).f_i) \in \mathrm{sp}\{f_i | i \in I\},$$

tehát $\mathrm{Im}(\tau(t)) \subseteq \mathrm{sp}\{f_i | i \in I\}$, vagyis $\mathrm{Im}(\tau(t))$ véges dimenziós altere F-nek.

Megfordítva, legyen $v \in \mathbf{L}(E; F)$ olyan lineáris operátor, amelyre $\mathrm{Im}(v)$ véges dimenziós altere F-nek. Legyen $(f_i)_{i \in I}$ bázis $\mathrm{Im}(v)$-ben, és jelölje $(w_i)_{i \in I}$ a duális bázist (**??**). Ekkor minden $e \in E$ vektorra $v(e) = \sum_{i \in I} w_i(v(e)).f_i$, tehát ha minden $i \in I$ indexre $u_i := w_i \circ v$, akkor $(u_i)_{i \in I}$ olyan E^*-ban haladó rendszer, hogy minden $e \in E$ vektorra

$$v(e) = \sum_{i \in I} u_i(e).f_i = \sum_{i \in I} (u_i \dot{\otimes} f_i)(e) = \tau\Big(\sum_{i \in I} (u_i \otimes f_i)\Big)(e),$$

vagyis $t := \sum_{i \in I} (u_i \otimes f_i) \in E \otimes F$ olyan tenzor, hogy $v = \tau(t) \in \mathrm{Im}(\tau)$.

Ezzel igazoltuk, hogy $\mathrm{Im}(\tau) = \{v \in \mathbf{L}(E; F) | \dim(\mathrm{Im}(v)) < +\infty\}$. ■

19.9.4. Következmény. *Ha E és F vektorterek a K test felett.*

a) *Ha F véges dimenziós, akkor az $E^* \otimes F \to \mathbf{L}(E; F)$ kanonikus lineáris injekció izomorfizmus az $E^* \otimes F$ tenzorszorzat és az $\mathbf{L}(E; F)$ operátortér között.*

Bizonyítás. ■

19.10. Kanonikus azonosítások tenzorszorzatok között

19.10.1. Állítás. (**A tenzorszorzat általános kommutativitása.**) *Legyen $(E_i)_{i \in I}$ vektortér-rendszer, J halmaz és $\sigma : J \to I$ bijekció. Ekkor létezik egyetlen olyan*

$$\widehat{\sigma} : \bigotimes_{i \in I} E_i \to \bigotimes_{j \in J} E_{\sigma(j)}$$

lineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i \in I} \in \prod_{i \in I} E_i$ esetén

$$\widehat{\sigma}\Big(\bigotimes_{i \in I} x_i\Big) = \bigotimes_{j \in J} x_{\sigma(j)}.$$

A $\widehat{\sigma}$ leképezés izomorfizmus a $\bigotimes_{i \in I} E_i$ és $\bigotimes_{j \in J} E_{\sigma(j)}$ vektorterek között.

Bizonyítás. Megmutatjuk, hogy az

$$m : \prod_{i \in I} E_i \to \bigotimes_{j \in J} E_{\sigma(j)}; \quad (x_i)_{i \in I} \mapsto \bigotimes_{j \in J} x_{\sigma(j)}.$$

leképezés multilineáris operátor. Ehhez legyen $k \in I$ és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ rögzített. Nyilvánvaló, hogy minden $x \in E_k$ és $j \in J$ esetén

$$\left(\mathrm{in}_{k,(x_i)_{i\in I}}(x)\right)_{\sigma(j)} = \left(\mathrm{in}_{\sigma^{-1}(k),\left(x_{\sigma(j)}\right)_{j\in J}}(x)\right)_j ,$$

amiből következik, hogy minden $x \in E_k$ vektorra

$$\left(m \circ \mathrm{in}_{k,(x_i)_{i\in I}}\right)(x) = \bigotimes_{j\in J} \left(\mathrm{in}_{k,(x_i)_{i\in I}}(x)\right)_{\sigma(j)} = \left(\otimes \circ \mathrm{in}_{\sigma^{-1}(k),\left(x_{\sigma(j)}\right)_{j\in J}}\right)(x),$$

ahol $\otimes$ a $\prod_{j\in J} E_{\sigma(j)} \to \bigotimes_{j\in J} E_{\sigma(j)}$ multilineáris operátor. Mivel $\otimes \circ \mathrm{in}_{\sigma^{-1}(k),\left(x_{\sigma(j)}\right)_{j\in J}} : E_k \to \bigotimes_{j\in J} E_{\sigma(j)}$ lineáris operátor, így $m \circ \mathrm{in}_{k,(x_i)_{i\in I}}$ is lineáris, tehát m multilineáris. (Itt kihasználtuk, hogy $E_k = E_{\sigma(\sigma^{-1}(k))}$.) Ezért egyértelműen létezik az a

$$\widehat{\sigma} : \bigotimes_{i\in I} E_i \to \bigotimes_{j\in J} E_{\sigma(j)}$$

lineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén

$$\widehat{\sigma}\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{j\in J} x_{\sigma(j)}. \tag{1}$$

Áttérve az $(E_i)_{i\in I}$ vektortér-rendszerről az $\left(E_{\sigma(j)}\right)_{j\in J}$ vektortér-rendszerre, és a $\sigma : J \to I$ bijekcióról a $\sigma^{-1} : I \to J$ bijekcióra, kapjuk, hogy egyértelműen létezik az a

$$\widehat{\sigma^{-1}} : \bigotimes_{j\in J} E_{\sigma(j)} \to \bigotimes_{i\in I} E_i$$

lineáris operátor, amelyre teljesül az, hogy minden $(y_j)_{j\in J} \in \prod_{j\in J} E_{\sigma(j)}$ esetén

$$\widehat{\sigma^{-1}}\Big(\bigotimes_{j\in J} y_j\Big) = \bigotimes_{i\in I} y_{\sigma^{-1}(i)}. \tag{2}$$

Az (1) és (2) egyenlőségek alapján nyilvánvaló, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén

$$\left(\widehat{\sigma^{-1}} \circ \widehat{\sigma}\right)\Big(\bigotimes_{i\in I} x_i\Big) = \widehat{\sigma^{-1}}\Big(\bigotimes_{j\in J} x_{\sigma(j)}\Big) = \bigotimes_{i\in I} x_{\sigma(\sigma^{-1}(i))} = \bigotimes_{i\in I} x_i,$$

így $\widehat{\sigma^{-1}} \circ \widehat{\sigma} = \mathrm{id}_{\bigotimes_{i\in I} E_i}$, hiszen $\left\{ \bigotimes_{i\in I} x_i \,\middle|\, (x_i)_{i\in I} \in \prod_{i\in I} E_i \right\}$ generátorhalmaz $\bigotimes_{i\in I} E_i$-ben.

A (2) és (1) egyenlőségek alapján nyilvánvaló, hogy minden $(y_j)_{j\in J} \in \prod_{j\in J} E_{\sigma(j)}$ esetén

$$\left(\widehat{\sigma} \circ \widehat{\sigma^{-1}}\right)\Big(\bigotimes_{j\in J} y_j\Big) = \widehat{\sigma}\Big(\bigotimes_{i\in I} y_{\sigma^{-1}(i)}\Big) = \bigotimes_{j\in J} y_{\sigma^{-1}(\sigma(j))} = \bigotimes_{j\in J} y_j,$$

így $\widehat{\sigma} \circ \widehat{\sigma^{-1}} = \mathrm{id}_{\bigotimes_{j\in J} E_{\sigma(j)}}$, hiszen $\left\{ \bigotimes_{j\in J} y_j \,\middle|\, (y_j)_{j\in J} \in \prod_{j\in J} E_{\sigma(j)} \right\}$ generátorhalmaz $\bigotimes_{i\in J} E_{\sigma(j)}$-ben.

Ez azt jelenti, hogy $\widehat{\sigma}$ izomorfizmus a $\bigotimes_{i\in I} E_i$ és $\bigotimes_{j\in J} E_{\sigma(j)}$ vektorterek között, és az is látható, hogy $\widehat{\sigma}^{-1} = \widehat{\sigma^{-1}}$. ■

19.10.2. Következmény. *Legyen E vektortér, I halmaz, és jelölje $\mathrm{T}^I(E)$ az $\bigotimes_{i\in I} E_i$ tenzorszorzatot, ahol minden $i \in I$ esetén $E_i := E$. Minden $\sigma \in \mathfrak{S}(I)$ esetén jelölje $\widehat{\sigma}$ azt a $\mathrm{T}^I(E) \to \mathrm{T}^I(E)$ lineáris bijekciót, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in E^I$ esetén*

$$\widehat{\sigma}\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{i\in I} x_{\sigma(i)}.$$

Ekkor az

$$\mathfrak{S}(I) \to \mathbf{GL}\left(\mathrm{T}^I(E)\right); \quad \sigma \mapsto \widehat{\sigma}^{-1}$$

leképezés lineáris ábrázolása az $\mathfrak{S}(I)$ teljes permutációcsoportnak a $\mathrm{T}^I(E)$ vektortérben.

Bizonyítás. Legyenek $\sigma, \tau \in \mathfrak{S}(I)$. A $\widehat{\sigma \circ \tau}$ és $\widehat{\tau} \circ \widehat{\sigma}$ leképezések mindketten olyan $\mathrm{T}^I(E) \to \mathrm{T}^I(E)$ lineáris operátorok, amelyekre minden $(x_i)_{i\in I} \in E^I$ esetén

$$\widehat{\sigma \circ \tau}\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{i\in I} x_{\sigma(\tau(i))} = \widehat{\tau}\Big(\bigotimes_{i\in I} x_{\sigma(i)}\Big) = \widehat{\tau}\Big(\widehat{\sigma}\Big(\bigotimes_{i\in I} x_i\Big)\Big) = (\widehat{\tau} \circ \widehat{\sigma})\Big(\bigotimes_{i\in I} x_i\Big),$$

ezért $\widehat{\sigma \circ \tau} = \widehat{\tau} \circ \widehat{\sigma}$, hiszen $\left\{ \bigotimes_{i\in I} x_i \,\middle|\, (x_i)_{i\in I} \in E^I \right\}$ generátorhalmaz $\mathrm{T}^I(E)$-ben. Mivel nyilvánvalóan $\widehat{\mathrm{id}_I} = \mathrm{id}_{\mathrm{T}^I(E)}$, így ebből következik, hogy a

$$\mathfrak{S}(I) \to \mathbf{GL}\left(\mathrm{T}^I(E)\right); \quad \sigma \mapsto \widehat{\sigma}^{-1}$$

leképezés csoport-morfizmus. ■

19.10.3. Lemma. *Legyenek X, Y, Z vektorterek a K test felett, és $u : X \to \mathbf{L}(Y;Z)$ függvény. A következő állítások ekvivalensek.*

(i) *Minden $y \in Y$ esetén az $u_y : X \to Z;\ x \mapsto u(x)(y)$ leképezés lineáris.*

(ii) *Létezik olyan $G \subseteq Y$ generátorhalmaz, hogy minden $y \in G$ esetén az $u_y : X \to Z;\ x \mapsto u(x)(y)$ leképezés lineáris.*

(iii) *Az u leképezés lineáris, vagyis $u \in \mathbf{L}(X;\mathbf{L}(Y;Z))$.*

(iv) *A $b : X \times Y \to Z;\ (x,y) \mapsto u(x)(y)$ leképezés bilineáris.*

Bizonyítás. (i)⇒(ii) Triviális.

(ii)⇒(iii) Legyenek $x, x' \in X$ és $y \in Y$ tetszőlegesek. Ekkor vehetünk olyan $(\lambda_i)_{i\in I}$ véges rendszert K-ban, és olyan $(y_i)_{i\in I}$ rendszert G-ben, hogy $y = \sum_{i\in I} \lambda_i.y_i$. Ekkor

$$\begin{aligned} u(x+x')(y) &= u(x+x')\Big(\sum_{i\in I}\lambda_i.y_i\Big) \overset{(1)}{=} \sum_{i\in I}\lambda_i.u(x+x')(y_i) \overset{(2)}{=} \\ &\overset{(2)}{=} \sum_{i\in I}\lambda_i.\left(u(x)(y_i)+u(x')(y_i)\right) = \sum_{i\in I}\left(\lambda_i.u(x)(y_i)+\lambda_i.u(x')(y_i)\right) = \\ &= \sum_{i\in I}\lambda_i.u(x)(y_i) + \sum_{i\in I}\lambda_i.u(x')(y_i) \overset{(3)}{=} \\ &\overset{(3)}{=} u(x)\Big(\sum_{i\in I}\lambda_i.y_i\Big) + u(x')\Big(\sum_{i\in I}\lambda_i.y_i\Big) = u(x)(y)+u(x')(y) \overset{(4)}{=} (u(x)+u(x'))(y), \end{aligned}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél az $u(x+x')$, valamint a $\overset{(3)}{=}$ egyenlőségnél az $u(x)$ és $u(x')$

leképezések linearitását alkalmaztuk,

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk azt, hogy a (ii) hipotézis szerint minden $i \in I$ esetén az $u_{y_i} : X \to Z$ leképezés additív;

– a $\overset{(4)}{=}$ egyenlőségnél az $\mathbf{L}(Y; Z)$ operátortér összeadásának definícióját alkalmaztuk.

Ez azt jelenti, hogy minden $x, x' \in X$ esetén $u(x + x') = u(x) + u(x')$, vagyis az $u : X \to \mathbf{L}(Y; Z)$ függvény additív. Legyenek most $x \in X$, $\lambda \in K$ és $y \in Y$ tetszőlegesek. Ismét vehetünk olyan $(\lambda_i)_{i\in I}$ véges rendszert K-ban, és olyan $(y_i)_{i\in I}$ rendszert G-ben, hogy $y = \sum\limits_{i\in I} \lambda_i.y_i$. Ekkor

$$u(\lambda.x)(y) = u(\lambda.x)\Big(\sum_{i\in I} \lambda_i.y_i\Big) \overset{(5)}{=} \sum_{i\in I} \lambda_i.u(\lambda.x)\,(y_i) \overset{(6)}{=} \sum_{i\in I} \lambda_i.\,(\lambda.u(x)\,(y_i)) =$$
$$= \lambda.\sum_{i\in I} \lambda_i.u(x)\,(y_i) \overset{(7)}{=} \lambda.\Big(u(x)\Big(\sum_{i\in I} \lambda_i.y_i\Big)\Big) = \lambda.(u(x)(y)) \overset{(8)}{=} (\lambda.u(x))(y),$$

ahol

– az $\overset{(5)}{=}$ egyenlőségnél az $u(\lambda.x)$, valamint a $\overset{(7)}{=}$ egyenlőségnél az $u(x)$ leképezés linearitását alkalmaztuk,

– a $\overset{(6)}{=}$ egyenlőségnél felhasználtuk azt, hogy a (ii) hipotézis szerint minden $i \in I$ esetén az $u_{y_i} : X \to Z$ leképezés K-homogén;

– a $\overset{(8)}{=}$ egyenlőségnél az $\mathbf{L}(Y; Z)$ operátortérben a K-beli elemekkel való szorzás definícióját alkalmaztuk.

Ez azt jelenti, hogy minden $x \in X$ és $\lambda \in K$ esetán $u(\lambda.x) = \lambda.u(x)$, vagyis az $u : X \to \mathbf{L}(Y; Z)$ függvény K-homogén. Ezzel igazoltuk, hogy az u leképezés K-lineáris.

(iii)⇒(iv) Ha $x \in X$, akkor b és u definíciója szerint $b(x, \cdot) = u(x) \in \mathbf{L}(Y; Z)$. Ha $y \in Y$, akkor minden $x, x' \in X$ és $\lambda \in K$ esetén, u linearitása és az $\mathbf{L}(Y; Z)$ operátortér lineáris műveleteinek definíciója miatt

$$b(x + x', y) = u(x + x')(y) = (u(x) + u(x'))(y) = u(x)(y) + u(x')(y) = b(x, y) + b(x', y),$$
$$b(\lambda.x, y) = u(\lambda.x)(y) = (\lambda.u(x))(y) = \lambda.(u(x)(y)) = \lambda.b(x, y),$$

tehát $b(\cdot, y) \in \mathbf{L}(X; Z)$. Ez azt jelenti, hogy a $b : X \times Y \to Z$ függvény bilineáris.

(iv)⇒(i) Ha $y \in Y$, akkor b bilinearitása miatt $b(\cdot, y) \in \mathbf{L}(X; Z)$, ugyanakkor nyilvánvaló, hogy $u_y = b(\cdot, y)$, tehát (i) teljesül. ■

19.10.4. Állítás. *Legyen $(E_i)_{i\in I}$ vektortér-rendszer, és $(I_j)_{j\in J}$ az I halmaz partíciója. Ekkor létezik egyetlen olyan*

$$u : \bigotimes_{i\in I} E_i \to \bigotimes_{j\in J} \Big(\bigotimes_{i\in I_j} E_i\Big)$$

lineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in \prod\limits_{i\in I} E_i$ esetén

$$u\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{j\in J} \Big(\bigotimes_{i\in I_j} x_i\Big).$$

Bizonyítás. Jelölje $p : I \to J$ azt a függvényt, amely minden $i \in I$ indexhez hozzárendeli azt a $p(i) \in J$ elemet, amelyre $i \in I_{p(i)}$. Ez a függvény jól értelmezett, mert $(I_j)_{j\in J}$ az I halmaz partíciója. Továbbá, legyen $\left(\bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right), \otimes_J\right)$ a $\left(\bigotimes_{i\in I_j} E_i\right)_{j\in J}$ vektortér-rendszer tenzorszorzata, és minden $j \in J$ esetén $\left(\bigotimes_{i\in I_j} E_i, \otimes_j\right)$ az $(E_i)_{i\in I_j}$ vektortér-rendszer tenzorszorzata, tehát az is teljesül, hogy

$$\otimes_J : \prod_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right) \to \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right),$$

$$\otimes_j : \prod_{i\in I_j} E_i \to \bigotimes_{i\in I_j} E_i$$

leképezések multilneáris operátorok.

Tekintsük az

$$m : \prod_{i\in I} E_i \to \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right); \quad (x_i)_{i\in I} \mapsto \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} x_i\right)$$

leképezést. Ez multilineáris operátor, mert ha $k \in I$ és $(x_i)_{i\in I} \in \prod_{i\in I} E_i$, valamint minden $j \in J$ esetén $t_j := \bigotimes_{i\in I_j} x_i$, akkor könnyen ellenőrizhető, hogy

$$m \circ \mathrm{in}_{k,(x_i)_{i\in I}} = \left(\otimes_J \ \circ \ \mathrm{in}_{p(k),(t_j)_{j\in J}}\right) \circ \left(\otimes_{p(k)} \ \circ \ \mathrm{in}_{k,(x_i)_{i\in I_{p(k)}}}\right),$$

és a $\otimes_J$, valamint a $\otimes_{p(k)}$ leképezések multilinearitása miatt a

$$\otimes_{p(k)} \ \circ \ \mathrm{in}_{k,(x_i)_{i\in I_{p(k)}}} : E_k \to \bigotimes_{i\in I_{p(k)}} E_i,$$

$$\otimes_J \ \circ \ \mathrm{in}_{p(k),(t_j)_{j\in J}} : \bigotimes_{i\in I_{p(k)}} E_i \to \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right)$$

leképezések lineárisak. Tehát m multilineáris operátor, így létezik egyetlen olyan

$$u : \bigotimes_{i\in I} E_i \to \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right)$$

lineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén

$$u\Big(\bigotimes_{i\in I} x_i\Big) = m\left((x_i)_{i\in I}\right) = \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} x_i\right). \ \blacksquare$$

19.10.5. Definíció. *Ha $(E_i)_{i\in I}$ vektortér-rendszer, és $(I_j)_{j\in J}$ az I halmaz partíciója, akkor az $\bigotimes_{i\in I} E_i$ és $\bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right)$ vektorterek közötti* **kanonikus lineáris operátornak** *nevezzük azt a*

$$u : \bigotimes_{i\in I} E_i \to \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} E_i\right)$$

lineáris operátort, amelyre teljesül az, hogy minden $(x_i)_{i\in I} \in \prod_{i\in I} E_i$ esetén

$$u\Big(\bigotimes_{i\in I} x_i\Big) = \bigotimes_{j\in J}\left(\bigotimes_{i\in I_j} x_i\right).$$

19.10.6. Lemma. *Legyen $(E_i)_{i\in I}$ vektortér-rendszer, valamint I_0 és I_1 olyan halmazok, hogy $I = I_0 \cup I_1$ és $I_0 \cap I_1 \neq \emptyset$. Ekkor a $\bigotimes_{i\in I} E_i$ és $\Big(\bigotimes_{i\in I_0} E_i\Big) \otimes \Big(\bigotimes_{i\in I_1} E_i\Big)$ vektorterek közötti kanonikus lineáris operátor izomorfizmus.*

Bizonyítás. Jelölje u a $\bigotimes_{i\in I} E_i$ és $\Big(\bigotimes_{i\in I_0} E_i\Big) \otimes \Big(\bigotimes_{i\in I_1} E_i\Big)$ vektorterek közötti kanonikus lineáris operátort, és jelölje $\Big(\bigotimes_{i\in I} E_i, \otimes_I\Big)$ az $(E_i)_{i\in I}$ vektortér-rendszer tenzorszorzatát. Megmutatjuk, hogy egyértelműen létezik olyan

$$v : \Big(\bigotimes_{i\in I_0} E_i\Big) \otimes \Big(\bigotimes_{i\in I_1} E_i\Big) \to \bigotimes_{i\in I} E_i$$

lineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i\in I_0} \in \prod_{i\in I_0} E_i$ és $(y_i)_{i\in I_1} \in \prod_{i\in I_1} E_i$ esetén

$$v\Big(\Big(\bigotimes_{i\in I_0} x_i\Big) \otimes \Big(\bigotimes_{i\in I_1} y_i\Big)\Big) = \bigotimes_{i\in I} z_i,$$

ahol $(z_i)_{i\in I} \in \prod_{i\in I} E_i$ az a rendszer, amelyre minden $i \in I$ indexre

$$z_i := \begin{cases} x_i & \text{, ha } i \in I_0, \\ y_i & \text{, ha } i \in I_1. \end{cases}$$

Világos, hogy egy ilyen v operátor éppen az $\bigotimes_{i\in I} E_i$ és $\Big(\bigotimes_{i\in I_0} E_i\Big) \otimes \Big(\bigotimes_{i\in I_1} E_i\Big)$ vektorterek közötti kanonikus lineáris operátor inverze.
Legyen $\mathbf{x} = (x_i)_{i\in I_0} \in \prod_{i\in I_0} E_i$ rögzített, és értelmezzük az

$$m_{\mathbf{x}} : \prod_{i\in I_1} E_i \to \bigotimes_{i\in I} E_i$$

leképezést, amelyre minden $\mathbf{y} = (y_i)_{i\in I_1} \in \prod_{i\in I_1} E_i$ esetén $m_{\mathbf{x}}(\mathbf{y}) = \bigotimes_{i\in I} z_i$, ahol $(z_i)_{i\in I} \in \prod_{i\in I} E_i$ az a rendszer, amelyre minden $i \in I$ indexre

$$z_i := \begin{cases} x_i & \text{, ha } i \in I_0, \\ y_i & \text{, ha } i \in I_1. \end{cases} \tag{1}$$

Megmutatjuk, hogy az $m_{\mathbf{x}} : \prod_{i\in I_1} E_i \to \bigotimes_{i\in I} E_i$ leképezés multilineáris operátor. Ehhez legyen $k \in I_1$ és $\mathbf{y} = (y_i)_{i\in I_1} \in \prod_{i\in I_1} E_i$. Ha $\mathbf{z} = (z_i)_{i\in I} \in \prod_{i\in I} E_i$ az a rendszer, amelyre minden $i \in I$ esetén (1) teljesül, akkor könnyen ellenőrizhető, hogy

$$m_{\mathbf{x}} \circ \mathrm{in}_{k,\mathbf{y}} = \otimes_I \circ \mathrm{in}_{k,\mathbf{z}} \in \mathbf{L}\Big(E_k; \bigotimes_{i\in I} E_i\Big),$$

tehát $m_{\mathbf{x}}$ multilineáris operátor. Ezért létezik egyetlen olyan $\widetilde{m}_{\mathbf{x}} : \bigotimes_{i\in I_1} E_i \to \bigotimes_{i\in I} E_i$ lineáris operátor, amelyre minden $\mathbf{y} = (y_i)_{i\in I_1} \in \prod_{i\in I_1} E_i$ esetén $\widetilde{m}_{\mathbf{x}}\Big(\bigotimes_{i\in I_1} y_i\Big) = m_{\mathbf{x}}(\mathbf{y})$.

Megmutatjuk, hogy a

$$w : \prod_{i\in I_0} E_i \to \mathbf{L}\Big(\bigotimes_{i\in I_1} E_i; \bigotimes_{i\in I} E_i\Big); \quad \mathbf{x} \mapsto \widetilde{m}_{\mathbf{x}}$$

leképezés multilineáris. Ehhez legyen $k \in I_0$ és $\mathbf{x} = (x_i)_{i\in I_0} \in \prod_{i\in I_0} E_i$. Ha $\mathbf{y} = (y_i)_{i\in I_1} \in \prod_{i\in I_1} E_i$, akkor könnyen ellenőrizhető, hogy minden $x \in E_k$ esetén

$$((w \circ \mathrm{in}_{k,\mathbf{x}})(x))\Big(\bigotimes_{i\in I_1} y_i\Big) = \big(\otimes_I \circ \mathrm{in}_{k,m_{\mathbf{x}}(\mathbf{y})}\big)(x),$$

és mivel $\otimes_I \circ \mathrm{in}_{k,m_{\mathbf{x}}(\mathbf{y})} \in \mathbf{L}\Big(E_k; \bigotimes_{i\in I} E_i\Big)$, így a 19.10.3. lemma szerint $w\circ \mathrm{in}_{k,\mathbf{x}} : E_k \to \bigotimes_{i\in I} E_i$ lineáris operátor. (Itt a 19.10.3. lemmát a következő szereposztásban alkalmaztuk: $X := E_k$, $Y := \bigotimes_{i\in I_1} E_i$, $Z := \bigotimes_{i\in I} E_i$, $G := \Big\{\bigotimes_{i\in I_1} y_i \;\Big|\; (y_i)_{i\in I} \in \prod_{i\in I_1} E_i\Big\}$, valamint $u := w\circ \mathrm{in}_{k,\mathbf{x}}$.) Tehát a w leképezés multilineáris operátor, ezért egyértelműen létezik az a

$$\widetilde{w} : \bigotimes_{i\in I_0} E_i \to \mathbf{L}\Big(\bigotimes_{i\in I_1} E_i; \bigotimes_{i\in I} E_i\Big)$$

lineáris operátor, amelyre minden $\mathbf{x} = (x_i)_{i\in I_0} \in \prod_{i\in I_0} E_i$ esetén $\widetilde{w}\Big(\bigotimes_{i\in I_0} x_i\Big) = m_{\mathbf{x}}$. Ekkor 19.10.3. szerint a

$$\Big(\bigotimes_{i\in I_0} E_i\Big) \times \Big(\bigotimes_{i\in I_1} E_i\Big) \to \bigotimes_{i\in I} E_i; \quad (t,t') \mapsto w(t)(t')$$

leképezés bilineáris operátor, így létezik egyetlen olyan $v : \Big(\bigotimes_{i\in I_0} E_i\Big) \otimes \Big(\bigotimes_{i\in I_1} E_i\Big) \to \bigotimes_{i\in I} E_i$ lineáris operátor, amelyre minden $(t,t') \in \Big(\bigotimes_{i\in I_0} E_i\Big) \times \Big(\bigotimes_{i\in I_1} E_i\Big)$ esetén $v(t\otimes t') = w(t)(t')$. A konstrukció szerint nyilvánvaló, hogy v olyan leképezés, amelynek a létezését kellett igazolni. ■

19.10.7. Állítás. (**A tenzorszorzat általános asszociativitása.**) *Ha $(E_i)_{i\in I}$ vektortér-rendszer, és $(I_j)_{j\in J}$ az I halmaz partíciója, és J véges halmaz, akkor a $\bigotimes_{i\in I} E_i$ és $\bigotimes_{j\in J}\Big(\bigotimes_{i\in I_j} E_i\Big)$ vektorterek közötti kanonikus lineáris operátor izomorfizmus.*

Bizonyítás. Az állítást a J halmaz számossága szerinti teljes indukcióval bizonyítjuk. Ha $\mathrm{Card}(J) = 0$ vagy $\mathrm{Card}(J) = 1$, akkor az állítás triviálisan igaz (és érdektelen). A $\mathrm{Card}(J) = 2$ esetben az előző lemma szerint igaz az állítás. Tegyük fel, hogy $n \in \mathbb{N}$ olyan természetes szám, hogy $n \geq 2$ és az állítás igaz minden olyan J indexhalmaz esetén, amelyre $\mathrm{Card}(J) = n$.

Legyen $(E_i)_{i\in I}$ vektortér-rendszer, és $(I_j)_{j\in J}$ az I halmaznak olyan partíciója, hogy J véges és $\mathrm{Card}(J) = n+1$. Legyen $j_* \in J$ rögzített elem, valamint $J_* := J \setminus \{j_*\}$. Ekkor $\mathrm{Card}(J_*) = n$, tehát ha $I_* := \bigcup_{j\in J_*} I_j$, akkor az indukciós hipotézis szerint az $(E_i)_{i\in I_*}$ vektortér-rendszerre és az I_* indexhalmaz $(I_j)_{j\in J_*}$ partíciójára igaz az állítás, tehát az $u_* : \bigotimes_{i\in I_*} E_i \to \bigotimes_{j\in J_*}\Big(\bigotimes_{i\in I_j} E_i\Big)$ kanonikus lineáris operátor vektortér-izomorfizmus, vagyis lineáris bijekció. Jelölje u_{**} a $\bigotimes_{i\in I} E_i$ és $\Big(\bigotimes_{i\in I_{j_*}} E_i\Big)\otimes\Big(\bigotimes_{i\in I_*} E_i\Big)$ vektorterek közötti kanonikus lineáris operátort, amely 19.10.6. szerint lineáris bijekció. Végül, jelölje v a $\bigotimes_{j\in J}\Big(\bigotimes_{i\in I_j} E_i\Big)$ és $\Big(\bigotimes_{i\in I_{j_*}} E_i\Big)\otimes\Big(\bigotimes_{j\in J_*}\Big(\bigotimes_{i\in I_j} E_i\Big)\Big)$ vektorterek közötti kanonikus lineáris operátort, amely 19.10.6. szerint lineáris bijekció. Ekkor 19.7.9. figyelembe vételével kapjuk, hogy a

$$v^{-1}\circ\Big(\mathrm{id}_{\bigotimes_{i\in I_{j_*}} E_i}\dot{\otimes}\, u_*\Big)\circ u_{**} : \bigotimes_{i\in I} E_i \to \bigotimes_{j\in J}\Big(\bigotimes_{i\in I_j} E_i\Big)$$

lineáris operátor izomorfizmus, és könnyen ellenőrizhető, hogy ez egyenlő a $\bigotimes_{i\in I} E_i$ és $\bigotimes_{j\in J}\Big(\bigotimes_{i\in I_j} E_i\Big)$ vektorterek közötti kanonikus lineáris operátorral. Ezért az állítás $n+1$-re is igaz, amivel a teljes indukciót végrehajtottuk. ■

19.10.8. Állítás. *Tegyük fel, hogy* $\Big((E_{i,j})_{j\in J_i}\Big)_{i\in I}$ *olyan rendszer, hogy minden* $i\in I$ *esetén* $(E_{i,j})_{j\in J_i}$ *vektortér-rendszer, továbbá legyen* $J := \prod_{i\in I} J_i$. *Ekkor létezik egyetlen olyan*

$$\tau : \bigotimes_{i\in I}\Big(\prod_{j\in J_i} E_{i,j}\Big) \to \prod_{\sigma\in J}\Big(\bigotimes_{i\in I} E_{i,\sigma(i)}\Big)$$

lineáris operátor, amelyre teljesül az, hogy minden $\Big((x_{i,j})_{j\in J_i}\Big)_{i\in I}\in\prod_{i\in I}\Big(\prod_{j\in J_i} E_{i,j}\Big)$ *esetén*

$$\tau\Big(\bigotimes_{i\in I}(x_{i,j})_{j\in J_i}\Big) = \Big(\bigotimes_{i\in I} x_{i,\sigma(i)}\Big)_{\sigma\in J}.$$

Bizonyítás. A tenzorszorzat definíciója szerint, az előírt tulajdonságú τ lineáris operátor egyértelmű létezése ekvivalens azzal, hogy az

$$m : \prod_{i\in I}\Big(\prod_{j\in J_i} E_{i,j}\Big) \to \prod_{\sigma\in J}\Big(\bigotimes_{i\in I} E_{i,\sigma(i)}\Big);\quad \Big((x_{i,j})_{j\in J_i}\Big)_{i\in I}\mapsto\Big(\bigotimes_{i\in I} x_{i,\sigma(i)}\Big)_{\sigma\in J}$$

leképezés multilineáris. Tehát azt kell igazolni, hogy minden $k\in I$ és $\mathbf{x} = \Big((x_{i,j})_{j\in J_i}\Big)_{i\in I}\in\prod_{i\in I}\Big(\prod_{j\in J_i} E_{i,j}\Big)$ esetén az $m\circ\mathrm{in}_{k,\mathbf{x}} : \prod_{j\in J_k} E_{k,j}\to\prod_{\sigma\in J}\Big(\bigotimes_{i\in I} E_{i,\sigma(i)}\Big)$ leképezés lineáris, ami a lineáris szorzattérbe vezető leképezések linearitásának kritériuma szerint azzal ekvivalens, hogy minden $\sigma\in J$ függvényre a

$$\mathrm{pr}_\sigma\circ m\circ\mathrm{in}_{k,\mathbf{x}} : \prod_{j\in J_k} E_{k,j}\to\bigotimes_{i\in I} E_{i,\sigma(i)}$$

leképezés lineáris operátor, ahol pr_σ jelöli a $\prod_{\sigma'\in J}\Big(\bigotimes_{i\in I} E_{i,\sigma'(i)}\Big)\to\bigotimes_{i\in I} E_{i,\sigma(i)}$ kanonikus projekciót.

Legyenek tehát $k\in I$, és $\mathbf{x} = \Big((x_{i,j})_{j\in J_i}\Big)_{i\in I}\in\prod_{i\in I}\Big(\prod_{j\in J_i} E_{i,j}\Big)$, valamint $\sigma\in J$ rögzített objektumok. Legyen $(y_j)_{j\in J_k}\in\prod_{j\in J_k} E_{k,j}$ tetszőleges. Ekkor a definíciók szerint

$$(\mathrm{pr}_\sigma\circ m\circ\mathrm{in}_{k,\mathbf{x}})\Big((y_j)_{j\in J_k}\Big) = \bigotimes_{i\in I} x'_{i,\sigma(i)},$$

ahol $\left(\left(x'_{i,j}\right)_{j\in J_i}\right)_{i\in I} := \mathrm{in}_{k,\mathbf{x}}\left((y_j)_{j\in J_k}\right)$, vagyis minden $i \in I \setminus \{k\}$ indexre $\left(x'_{i,j}\right)_{j\in J_i} = \mathbf{x}_i = (x_{i,j})_{j\in J_i}$, és $\left(x'_{k,j}\right)_{j\in J_k} = (y_j)_{j\in J_k}$. Ebből következik, hogy ha $i \in I$ és $i \neq k$, akkor $x'_{i,\sigma(i)} = x_{i,\sigma(i)}$, ugyanakkor $x'_{k,\sigma(k)} = y_{\sigma(k)}$. Tehát, ha $\left(\bigotimes_{i\in I} E_{i,\sigma(i)}, \otimes_{(I,\sigma)}\right)$ jelöli az $\left(E_{i,\sigma(i)}\right)_{i\in I}$ vektortér-rendszer tenzorszorzatát, és $\mathrm{p}_{\sigma(k)}$ jelöli a $\prod_{j\in J_k} E_{k,j} \to E_{k,\sigma(k)}$ kanonikus projekciót, valamint $\mathbf{z} := \left(x_{i,\sigma(i)}\right)_{i\in I} \in \prod_{i\in I} E_{i,\sigma(i)}$, akkor

$$\bigotimes_{i\in I} x'_{i,\sigma(i)} = \left(\otimes_{(I,\sigma)} \circ \mathrm{in}_{k,\mathbf{z}} \circ \mathrm{p}_{\sigma(k)}\right)\left((y_j)_{j\in J_k}\right),$$

ami azt jelenti, hogy

$$\mathrm{pr}_\sigma \circ m \circ \mathrm{in}_{k,\mathbf{x}} = \otimes_{(I,\sigma)} \circ \mathrm{in}_{k,\mathbf{z}} \circ \mathrm{p}_{\sigma(k)}.$$

Itt lényeges, hogy $\mathbf{z}$ a σ függvény és $\mathbf{x}$ által van meghatározva, tehát az $(y_j)_{j\in J_k}$ rendszertől független. Mivel $\otimes_{(I,\sigma)}$ multilineáris operátor, így $\otimes_{(I,\sigma)} \circ \mathrm{in}_{k,\mathbf{z}} : E_{k,\sigma(k)} \to \bigotimes_{i\in I} E_{i,\sigma(i)}$ lineáris operátor, ugyanakkor a $\mathrm{p}_{\sigma(k)} : \prod_{j\in J_k} E_{k,j} \to E_{k,\sigma(k)}$ projekció is lineáris operátor, következésképpen $\mathrm{pr}_\sigma \circ m \circ \mathrm{in}_{k,\mathbf{x}}$ lineáris operátor. ■

19.10.9. Állítás. (**A tenzorszorzat általános disztributivitása.**) *Tegyük fel, hogy $\left((E_{i,j})_{j\in J_i}\right)_{i\in I}$ olyan rendszer, amelyre minden $i \in I$ esetén $(E_{i,j})_{j\in J_i}$ vektortér-rendszer, továbbá legyen $J := \prod_{i\in I} J_i$. Ekkor létezik egyetlen olyan*

$$\tau : \bigotimes_{i\in I}\left(\bigoplus_{j\in J_i} E_{i,j}\right) \to \bigoplus_{\sigma\in J}\left(\bigotimes_{i\in I} E_{i,\sigma(i)}\right)$$

lineáris operátor, amelyre teljesül az, hogy minden $\left((x_{i,j})_{j\in J_i}\right)_{i\in I} \in \prod_{i\in I}\left(\bigoplus_{j\in J_i} E_{i,j}\right)$ esetén

$$\tau\left(\bigotimes_{i\in I} (x_{i,j})_{j\in J_i}\right) = \left(\bigotimes_{i\in I} x_{i,\sigma(i)}\right)_{\sigma\in J}.$$

Bizonyítás. ■

20. fejezet

Antiszimmetrikus multilineáris operátorok

20.1. Alternáló és antiszimmetrikus multilineáris operátorok

Emlékeztetünk arra, hogy ha $p \in \mathbb{N}$, akkor $\mathfrak{S}_p$ jelöli a $p \to p$ bijekciók halmazát a kompozíció művelettel ellátva, tehát $\mathfrak{S}_p$ a p halmaz *teljes permutációcsoportja* (13.2.1.). Továbbá, minden $p \in \mathbb{N}$ esetén ε_p jelöli az $\mathfrak{S}_p$ csoport előjel-függvényét, tehát azt az $\mathfrak{S}_p \to \{-1, 1\}$ csoport-morfizmust, amely a p halmaz minden transzpozíciójához a -1 értéket rendeli (13.3.5.).

20.1.1. Definíció. *Legyenek E és F vektorterek, $p \in \mathbb{N}^*$, valamint $w \in \mathbf{L}_p(E; F)$.*

– *Azt mondjuk, hogy a w multilineáris operátor* **alternáló**, *ha minden olyan $(x_i)_{i \in p} \in E^p$ rendszerre, amelyhez léteznek olyan $j, k \in p$ elemek, hogy $j \neq k$ és $x_j = x_k$, fennáll a*

$$w\left((x_i)_{i \in p}\right) = 0$$

egyenlőség. Az $E^p \to F$ alternáló multilineáris operátorok halmazát $\mathbf{Alt}_p(E; F)$ jelöli, és $\mathbf{Alt}_p(E; F)$ elemeit E **feletti, F-értékű, alternáló p-formáknak** *nevezzük. Ha E vektortér a K test felett, akkor $\mathbf{Alt}_p(E) := \mathbf{Alt}_p(E; K)$, és $\mathbf{Alt}_p(E)$ elemeit E* **feletti alternáló p-formáknak** *nevezzük.*

– *Azt mondjuk, hogy a w multilineáris operátor* **antiszimmetrikus**, *ha minden $(x_i)_{i \in p} \in E^p$ és $\sigma \in \mathfrak{S}_p$ esetén*

$$w\left(\left(x_{\sigma(i)}\right)_{i \in p}\right) = \varepsilon_p(\sigma) w\left((x_i)_{i \in p}\right).$$

Az $E^p \to F$ antiszimmetrikus multilineáris operátorok halmazát $\mathbf{A}_p(E; F)$ jelöli, és $\mathbf{A}_p(E; F)$ elemeit E **feletti, F-értékű, antiszimmetrikus p-formáknak** *nevezzük. Ha E vektortér a K test felett, akkor $\mathbf{A}_p(E) := \mathbf{A}_p(E; K)$, és $\mathbf{A}_p(E)$ elemeit E* **feletti antiszimmetrikus p-formáknak** *nevezzük.*

Megállapodunk abban, hogy ha E és F vektorterek, akkor *definíció szerint*

$$\mathbf{Alt}_0(E; F) := \mathbf{A}_0(E; F) := F.$$

Továbbá, világos, hogy

$$\mathbf{Alt}_1(E; F) := \mathbf{A}_1(E; F) := \mathbf{L}(E; F).$$

A definíció alapján nyilvánvaló, hogy ha E és F vektorterek és $p \in \mathbb{N}^*$, akkor $\mathbf{Alt}_p(E;F)$ és $\mathbf{A}_p(E;F)$ lineáris alterei az $E^p \to F$ multilineáris operátorok $\mathbf{L}_p(E;F)$ terének, ezért a továbbiakban $\mathbf{Alt}_p(E;F)$-et és $\mathbf{A}_p(E;F)$-et vektortereknek fogjuk tekinteni.

20.1.2. Állítás. *Legyenek E és F vektorterek a K test felett, $p \in \mathbb{N}^*$ és $w \in \mathbf{L}_p(E;F)$. Tekintsük a következő kijelentéseket.*

(i) $w \in \mathbf{Alt}_p\,(E;F)$.

(ii) *Minden $\tau \in \mathfrak{S}_p$ transzpozícióra és minden $(x_i)_{i\in p} \in E^p$ rendszerre*

$$w\left(\left(x_{\tau(i)}\right)_{i\in p}\right) = -w\left((x_i)_{i\in p}\right).$$

(iii) $w \in \mathbf{A}_p(E;F)$.

Ekkor (i)⇒(ii)⇔(iii) *teljesül, és ha* $\mathrm{Char}(K) \neq 2$*, akkor* (ii)⇒(i) *is teljesül, tehát akkor a három állítás ekvivalens.*

Bizonyítás. (i)⇒(ii) Legyen $\tau \in \mathfrak{S}_p$ transzpozíció, és legyenek $j,k \in p$ azok az elemek, amelyekre $j \neq k$ és $\tau(j) = k$ és $\tau(k) = j$ (és természetesen minden $i \in p$ esetén, ha $i \neq j$ és $i \neq k$, akkor $\tau(i) = i$). Legyen $\mathbf{x} := (x_i)_{i\in p} \in E^p$ rögzített. Vezessük be a

$$\mathbf{b} : E \times E \to F; \quad (y_0, y_1) \mapsto w\left(\mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(y_1)}(y_0)\right)$$

leképezést. Nyilvánvaló, hogy minden $(y_0,y_1) \in E \times E$ esetén $\mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(y_1)}(y_0) \in E^p$ az a rendszer, amelynek j-edik komponense y_0, és k-adik komponense y_1, és minden $i \in p$ elemre, ha $i \neq j$ és $i \neq k$, akkor az i-edik komponense x_i. Hasonlóan nyilvánvaló, hogy minden $(y_0,y_1) \in E \times E$ esetén $\mathrm{in}_{k,\mathrm{in}_{j,\mathbf{x}}(y_0)}(y_1) \in E^p$ az a rendszer, amelynek k-adik komponense y_1, és j-edik komponense y_0, és minden $i \in p$ elemre, ha $i \neq j$ és $i \neq k$, akkor az i-edik komponense x_i. Ez azt jelenti, hogy minden $(y_0,y_1) \in E \times E$ esetén

$$\mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(y_1)}(y_0) = \mathrm{in}_{k,\mathrm{in}_{j,\mathbf{x}}(y_0)}(y_1).$$

Ebből következik, hogy a $\mathbf{b} : E \times E \to F$ leképezés *bilineáris*, mert w multilinearitása folytán minden $y_1 \in E$ esetén

$$\mathbf{b}\,(\cdot, y_1) = w \circ \mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(y_1)} \in \mathbf{L}(E;F)$$

és minden $y_0 \in E$ esetén

$$\mathbf{b}\,(y_0, \cdot) = w \circ \mathrm{in}_{k,\mathrm{in}_{j,\mathbf{x}}(y_0)} \in \mathbf{L}(E;F).$$

Ha $y \in E$, akkor az $\mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(y)}(y) \in E^p$ rendszer j-edik és k-adik komponense egyenlő y-nal, ezért (i) alapján $\mathbf{b}(y,y) = w\left(\mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(y)}(y)\right) = 0$. Ezért minden $(y_0,y_1) \in E \times E$ esetén

$$0 = \mathbf{b}(y_0+y_1, y_0+y_1) = \mathbf{b}(y_0,y_0) + \mathbf{b}(y_0,y_1) + \mathbf{b}(y_1,y_0) + \mathbf{b}(y_1,y_1) = \mathbf{b}(y_0,y_1) + \mathbf{b}(y_1,y_0),$$

tehát $\mathbf{b}(y_0,y_1) = -\mathbf{b}(y_1,y_0)$. Speciálisan, $\mathbf{b}(x_k,x_j) = -\mathbf{b}(x_j,x_k)$ is teljesül. Nyilvánvaló, hogy $\mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(x_k)}(x_j) = (x_i)_{i\in p}$ és $\mathrm{in}_{k,\mathrm{in}_{j,\mathbf{x}}(x_k)}(x_j) = \left(x_{\tau(i)}\right)_{i\in p}$, ezért a $\mathbf{b} : E \times E \to F$ bilineáris operátor definíciója szerint

$$\mathbf{b}(x_j,x_k) = w\left(\mathrm{in}_{j,\mathrm{in}_{k,\mathbf{x}}(x_k)}(x_j)\right) = w\left((x_i)_{i\in p}\right),$$
$$\mathbf{b}(x_k,x_j) = w\left(\mathrm{in}_{k,\mathrm{in}_{j,\mathbf{x}}(x_k)}(x_j)\right) = w\left(\left(x_{\tau(i)}\right)_{i\in p}\right),$$

tehát $w\left(\left(x_{\tau(i)}\right)_{i\in p}\right) = -w\left((x_i)_{i\in p}\right)$.

(ii)$\Rightarrow$(iii) Legyen S azon $\sigma \in \mathfrak{S}_p$ permutációk halmaza, amelyekre minden $(x_i)_{i\in p} \in E^p$ esetén

$$w\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) = \varepsilon_p(\sigma)w\left((x_i)_{i\in p}\right).$$

Azt kell igazolni, hogy (ii) teljesülése esetén $S = \mathfrak{S}_p$. Mivel a p halmaz minden permutációja előáll transzpozíciók kompozíciójaként (13.3.3.), így elég azt belátni S zárt a kompozíció-képzésre nézve. Ennek bizonyításához legyenek $\sigma, \sigma' \in S$, és rögzítsünk egy $(x_i)_{i\in p} \in E^p$ rendszert. Vezessük be azt az $(x'_i)_{i\in p} \in E^p$ rendszert, amelyre minden $i \in p$ esetén $x'_i := x_{\sigma'(i)}$. Ekkor $\sigma, \sigma' \in S$ és az $(x'_i)_{i\in p} \in E^p$ rendszer definíciója miatt

$$\begin{aligned} w\left(\left(x'_{\sigma(i)}\right)_{i\in p}\right) &= \varepsilon_p(\sigma)w\left((x'_i)_{i\in p}\right) = \varepsilon_p(\sigma)w\left(\left(x_{\sigma'(i)}\right)_{i\in p}\right) = \\ &= \varepsilon_p(\sigma)\varepsilon_p(\sigma')w\left((x_i)_{i\in p}\right) = \varepsilon_p(\sigma'\circ\sigma)w\left((x_i)_{i\in p}\right). \end{aligned}$$

Ugyanakkor $\left(x'_{\sigma(i)}\right)_{i\in p} = \left(x_{\sigma'(\sigma(i))}\right)_{i\in p} = \left(x_{(\sigma'\circ\,\sigma)(i)}\right)_{i\in p}$, tehát

$$w\left(\left(x_{(\sigma'\circ\,\sigma)(i)}\right)_{i\in p}\right) = \varepsilon_p(\sigma'\circ\sigma)w\left((x_i)_{i\in p}\right),$$

vagyis $\sigma'\circ\sigma \in S$.

(iii)$\Rightarrow$(ii) Nyilvánvaló, mert ha $\tau \in \mathfrak{S}_p$ transzpozíció, akkor ε_p definíciója szerint $\varepsilon_p(\tau) = -1$.

Tegyük fel, hogy a K test nem 2 karakterisztikájú, és (ii) teljesül. Legyen $(x_i)_{i\in p} \in E^p$ olyan rendszer, és legyenek $j, k \in p$ olyan elemek, hogy $j \neq k$ és $x_j = x_k$. Legyen $\tau \in \mathfrak{S}_p$ az a transzpozíció, amelyre $j \neq k$ és $\tau(j) = k$ és $\tau(k) = j$ (és természetesen minden $i \in p$ esetén, ha $i \neq j$ és $i \neq k$, akkor $\tau(i) = i$). Világos, hogy ekkor $\left(x_{\tau(i)}\right)_{i\in p} = (x_i)_{i\in p}$, következésképpen (ii) alapján

$$w\left((x_i)_{i\in p}\right) = w\left(\left(x_{\tau(i)}\right)_{i\in p}\right) = -w\left((x_i)_{i\in p}\right),$$

ezért $2w\left((x_i)_{i\in p}\right) = 0$, amiből a $2 \in K$ elem invertálhatósága miatt $w\left((x_i)_{i\in p}\right) = 0$ következik, tehát (i) teljesül. ■

Az előző állításban láttuk, hogy ha E és F vektorterek a K test felett, és $p \in \mathbb{N}^*$, akkor

$$\mathbf{Alt}_p(E;F) \subseteq \mathbf{A}_p(E;F),$$

és itt egyenlőség áll, ha $\mathrm{Char}(K) \neq 2$. Azonban a fordított tartalmazás nem szükségképpen igaz, ha a K test 2 karakterisztikájú. Például, ha $\mathrm{Char}(K) = 2$ (konkrét példa: $K = \mathbb{F}_2$), és $n \in \mathbb{N}^*$, akkor az

$$u : K^n \times K^n \to K; \quad \left((x_i)_{i\in n}, (y_i)_{i\in n}\right) \mapsto \sum_{i\in n} x_i y_i$$

leképezés antiszimmetrikus bilineáris operátor, mert szimmetrikus és minden $\lambda \in K$ esetén $-\lambda = \lambda$, de u nem alternáló, mert ha $e \in K^n$ a K^n kanonikus bázisának bármelyik tagja, akkor $u(e,e) = 1 \neq 0$. Általánosabban: minden K testre $\mathbf{A}_2(K^n;K)$ lineárisan azonosítható az $n \times n$-es antiszimmetrikus mátrixok vektorterével, és $\mathbf{Alt}_2(K^n;K)$ lineárisan azonosítható azon $n \times n$-es antiszimmetrikus mátrixok vektorterével, amelyek főátlójában mindenütt 0 áll. Pontosabban: ha $\mathrm{Char}(K) = 2$, akkor minden $u \in$

$\mathbf{A}_2(K^n;K)$ antiszimmetrikus bilineáris formához egyértelműen létezik olyan $\mathbf{a} \in \mathrm{M}_n(K)$ antiszimmetrikus mátrix, amelyre minden $i \in n$ esetén $\mathbf{a}_{i,i} = 0$, és egyértelműen létezik olyan $\mathbf{b} \in K^n$, hogy minden $((x_i)_{i\in n}, (y_i)_{i\in n} \in K^n$ esetén

$$u\left(((x_i)_{i\in n}, (y_i)_{i\in n}\right) = \sum_{i\in n} \mathbf{b}_i x_i y_i + \sum_{\substack{(i,j)\in n\times n\\ i<j}} \mathbf{a}_{i,j}(x_i y_j - x_j y_i),$$

és az u antiszimmetrikus bilineáris forma pontosan akkor alternáló, ha $\mathbf{b} = \mathbf{0}$. Ebből következik, hogy $\mathrm{Char}(K) = 2$ esetén $\dim_K\left(\mathbf{A}_2(K^n;K)\right) = \dfrac{n(n-1)}{2} + n = \dfrac{n(n+1)}{2}$, és $\dim_K\left(\mathbf{Alt}_2(K^n;K)\right) = \dfrac{n(n-1)}{2}$.

20.2. Antiszimmetrizáció

20.2.1. Definíció. *Legyenek E és F vektorterek 0 karakterisztikájú test felett. Ha $p \in \mathbb{N}^*$, akkor az $u \in \mathbf{L}_p(E;F)$ multilineáris operátor* **antiszimmetrizáltjának** *nevezzük és $\mathbb{A}_p(u)$-val jelöljük azt az $E^p \to F$ függvényt, amelyre minden $(x_i)_{i\in p} \in E^p$ esetén*

$$\mathbb{A}_p(u)\left((x_i)_{i\in p}\right) := \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right).$$

20.2.2. Állítás. *Legyenek E és F vektorterek a 0 karakterisztikájú K test felett, és legyen $p \in \mathbb{N}^*$.*

a) *Ha $u \in \mathbf{L}_p(E;F)$, akkor $\mathbb{A}_p(u) \in \mathbf{A}_p(E;F)$, és $u \in \mathbf{A}_p(E;F)$ pontosan akkor teljesül, ha $u = \mathbb{A}_p(u)$.*

b) *Az $\mathbf{L}_p(E;F) \to \mathbf{A}_p(E;F)$; $u \mapsto \mathbb{A}_p(u)$ leképezés lineáris operátor.*

Bizonyítás. a) Legyen $\mathfrak{a} = (\mathfrak{a}_i)_{i\in p} \in E^p$ és $k \in p$. Megmutatjuk, hogy $\mathbb{A}_p(u) \circ \mathrm{in}_{k,\mathfrak{a}} \in \mathbf{L}(E;F)$. Valóban, ha $x \in E$, akkor minden $\sigma \in \mathfrak{S}_p$ és $i \in p$ esetén

$$(\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(i)} = \begin{cases} x & \text{, ha } \sigma(i) = k, \text{ azaz } i = \sigma^{-1}(k), \\ \mathfrak{a}_{\sigma(i)} & \text{, ha } \sigma(i) \neq k, \text{ azaz } i \neq \sigma^{-1}(k), \end{cases}$$

ami azt jelenti, hogy $\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(i)}\right)_{i\in p} = \mathrm{in}_{\sigma^{-1}(k),\sigma_*(\mathfrak{a})}(x)$, ahol $\sigma_*(\mathfrak{a}) := \left(\mathfrak{a}_{\sigma(i)}\right)_{i\in p}$. Ebből következik, hogy minden $x \in E$ vektorra:

$$\left(\mathbb{A}_p(u) \circ \mathrm{in}_{k,\mathfrak{a}}\right)(x) = \mathbb{A}_p(u)\left(\mathrm{in}_{k,\mathfrak{a}}(x)\right) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) u\left(\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(i)}\right)_{i\in p}\right) =$$

$$= \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) u\left(\mathrm{in}_{\sigma^{-1}(k),\sigma_*(\mathfrak{a})}(x)\right),$$

vagyis

$$\mathbb{A}_p(u) \circ \mathrm{in}_{k,\mathfrak{a}} = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\left(u \circ \mathrm{in}_{\sigma^{-1}(k),\sigma_*(\mathfrak{a})}\right) \in \mathbf{L}(E;F),$$

hiszen u multilinearitása folytán minden $\sigma \in \mathfrak{S}_p$ permutációra $u \circ \mathrm{in}_{\sigma^{-1}(k),\sigma_*(\mathfrak{a})} \in \mathbf{L}(E;F)$. Ezért $\mathbb{A}_p(u) \in \mathbf{A}_p(E;F)$ teljesül.

Az $\mathbb{A}_p(u)$ multilineáris operátor antiszimmetrikusságának bizonyításához legyen $(x_i)_{i\in p} \in E^p$ és $\sigma' \in \mathfrak{S}_p$. Ekkor

$$\mathbb{A}_p(u)\left(\left(x_{\sigma'(i)}\right)_{i\in p}\right) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)u\left(\left(x_{\sigma'(\sigma(i))}\right)_{i\in p}\right) =$$

$$= \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma')\varepsilon_p(\sigma'\circ\sigma)u\left(\left(x_{(\sigma'\circ\sigma)(i)}\right)_{i\in p}\right) = \varepsilon_p(\sigma')\frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma'\circ\sigma)u\left(\left(x_{(\sigma'\circ\sigma)(i)}\right)_{i\in p}\right) =$$

$$= \varepsilon_p(\sigma')\frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) = \varepsilon_p(\sigma')\mathbb{A}_p(u)\left((x_i)_{i\in p}\right),$$

mert minden $\sigma \in \mathfrak{S}_p$ esetén $\varepsilon_p(\sigma) = \varepsilon_p(\sigma')\varepsilon_p(\sigma')\varepsilon_p(\sigma) = \varepsilon_p(\sigma')\varepsilon_p(\sigma'\circ\sigma)$, és az $\mathfrak{S}_p \to \mathfrak{S}_p;\ \sigma \mapsto \sigma'\circ\sigma$ leképezés bijekció. Ezzel igazoltuk, hogy az $\mathbb{A}_p(u)$ multilineáris operátor antiszimmetrikus.

Ebből látható, hogy $u = \mathbb{A}_p(u)$ esetén u antiszimmetrikus. Megfordítva, ha u antiszimmetrikus, akkor minden $(x_i)_{i\in p} \in E^p$ esetén

$$\mathbb{A}_p(u)\left((x_i)_{i\in p}\right) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\varepsilon_p(\sigma)u\left((x_i)_{i\in p}\right) = u\left((x_i)_{i\in p}\right),$$

vagyis $\mathbb{A}_p(u) = u$.

b) Ha $u, v \in \mathbf{L}_p(E;F)$, akkor minden $(x_i)_{i\in p} \in E^p$ esetén

$$\mathbb{A}_p(u+v)\left((x_i)_{i\in p}\right) := \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)(u+v)\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) =$$

$$= \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\left(u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) + v\left(\left(x_{\sigma(i)}\right)_{i\in p}\right)\right) =$$

$$= \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) + \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) =$$

$$= \mathbb{A}_p(u)\left((x_i)_{i\in p}\right) + \mathbb{A}_p(v)\left((x_i)_{i\in p}\right) = \left(\mathbb{A}_p(u) + \mathbb{A}_p(v)\right)\left((x_i)_{i\in p}\right),$$

tehát $\mathbb{A}_p(u+v) = \mathbb{A}_p(u) + \mathbb{A}_p(v)$.

Ha $u \in \mathbf{L}_p(E;F)$ és $c \in K$, akkor minden $(x_i)_{i\in p} \in E^p$ esetén

$$\mathbb{A}_p(c.u)\left((x_i)_{i\in p}\right) := \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)(c.u)\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)c.u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) =$$

$$= c.\frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) = c.\mathbb{A}_p(u)\left((x_i)_{i\in p}\right) = \left(c.\mathbb{A}_p(u)\right)\left((x_i)_{i\in p}\right),$$

tehát $\mathbb{A}_p(c.u) = c.\mathbb{A}_p(u)$. ■

20.3. Antiszimmetrikus multilineáris operátorok külső szorzata

20.3.1. Definíció. *Legyen* $n \in \mathbb{N}^*$ *és* $\mathbf{p} = (p_i)_{i \in n} \in (\mathbb{N}^*)^n$. *Ekkor* $|\mathbf{p}| := \sum_{i=0}^{n-1} p_i$, *és minden* $i \leq n$ *természetes számra*

$$\mathrm{s}_{\mathbf{p}}(i) := \begin{cases} 0 & , \text{ ha } i = 0, \\ \sum_{j=0}^{i-1} p_j & , \text{ ha } i > 0. \end{cases}$$

Továbbá, $\mathfrak{S}_{\mathbf{p}}$ *jelöli azon* $\sigma \in \mathfrak{S}_{|\mathbf{p}|}$ *permutációk halmazát, amelyekre minden* $i \in n$ *esetén a* $\sigma|_{[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![} : [\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![\to |\mathbf{p}|$ *függvény monoton növő.*

Tehát ha $n \in \mathbb{N}^*$ és $\mathbf{p} = (p_i)_{i \in n} \in (\mathbb{N}^*)^n$, akkor minden $i < n$ természetes számra $\mathrm{s}_{\mathbf{p}}(i+1) = \mathrm{s}_{\mathbf{p}}(i) + p_i$, és $\mathrm{s}_{\mathbf{p}}(n) = |\mathbf{p}|$, és az $([\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![)_{i \in n}$ halmazrendszer diszjunkt és

$$|\mathbf{p}| = \bigcup_{i \in n} [\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![.$$

Gyakran előforduló speciális eset az, amikor $\mathbf{p} := (p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ (és itt a (p, q) párt az ismert módon $(\mathbb{N}^*)^2$ elemének tekintjük). Ekkor $|\mathbf{p}| = p + q$ és $\mathrm{s}_{\mathbf{p}}(0) = 0$, $\mathrm{s}_{\mathbf{p}}(1) = p$, $\mathrm{s}_{\mathbf{p}}(2) = p + q$, valamint $\mathfrak{S}_{(p,q)}$ azon $\sigma : p + q \to p + q$ bijekciók halmaza, amelyek a $[\![0, p[\![$ és $[\![p, p + q[\![$ halmazokon növekvőek.

Ugyancsak gyakran előfordul az, hogy $\mathbf{p} := (p, q, r) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^*$ (és itt a (p, q, r) hármast az ismert módon $(\mathbb{N}^*)^3$ elemének tekintjük). Ekkor $|\mathbf{p}| = p + q + r$ és $\mathrm{s}_{\mathbf{p}}(0) = 0$, $\mathrm{s}_{\mathbf{p}}(1) = p$, $\mathrm{s}_{\mathbf{p}}(2) = p + q$, $\mathrm{s}_{\mathbf{p}}(3) = p + q + r$, valamint $\mathfrak{S}_{(p,q,r)}$ azon $\sigma : p + q + r \to p + q + r$ bijekciók halmaza, amelyek a $[\![0, p[\![$ és $[\![p, p+q[\![$ és $[\![p+q, p+q+r[\![$ halmazokon növekvőek.

20.3.2. Állítás. *Legyen* $n \in \mathbb{N}^*$ *és* $\mathbf{p} = (p_i)_{i \in n} \in (\mathbb{N}^*)^n$. *Ekkor*

$$\mathrm{Card}\,(\mathfrak{S}_{\mathbf{p}}) = \frac{\left(\sum_{i=0}^{n-1} p_i\right)!}{\prod_{i=0}^{n-1} p_i!}.$$

Bizonyítás. Jelölje $\mathfrak{M}_{\mathbf{p}}$ azon $(X_i)_{i \in n} \in (\mathscr{P}(|\mathbf{p}|))^n$ diszjunkt halmazrendszerek halmazát, amelyekre minden $i \in n$ esetén $\mathrm{Card}(X_i) = p_i$. Nyilvánvaló, hogy minden $\sigma \in \mathfrak{S}_{\mathbf{p}}$ esetén $(\sigma\langle[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![\rangle)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$. Az

$$\mathfrak{S}_{\mathbf{p}} \to \mathfrak{M}_{\mathbf{p}}; \quad \sigma \mapsto (\sigma\langle[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![\rangle)_{i \in n} \tag{$*$}$$

leképezés injektív, mert ha $\sigma, \tau \in \mathfrak{S}_{\mathbf{p}}$ és minden $i \in n$ esetén $\sigma\langle[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![\rangle = \tau\langle[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![\rangle$, akkor a $(\tau^{-1} \circ \sigma)\,|_{[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![}$ függvény monoton növő permutációja az $[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![$ halmaznak, ezért 8.2.5. szerint egyenlő az identikus függvénnyel, így $\tau = \sigma$ a $[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![$ halmazon, következésképpen $\tau = \sigma$, hiszen $|\mathbf{p}| = \bigcup_{i \in n} [\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![$. Ugyanakkor a $(*)$ leképezés szürjektív is, mert ha $(X_i)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$, akkor minden $i \in n$ számra az X_i halmaz p_i elemű, így ismét 8.2.5. alapján létezik egyetlen monton növő $\sigma_i : [\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![\to X_i$ bijekció, és ekkor $\sigma := \bigcup_{i \in n} \sigma_i \in \mathfrak{S}_{\mathbf{p}}$ olyan permutáció, hogy minden $i \in n$ esetén $\sigma\langle[\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![\rangle = \mathrm{Im}(\sigma_i) = X_i$.

A $(*)$ függvény bijektivitásából következik, hogy $\mathrm{Card}\,(\mathfrak{S}_{\mathbf{p}}) = \mathrm{Card}\,(\mathfrak{M}_{\mathbf{p}})$. Az $\mathfrak{M}_{\mathbf{p}}$ halmaz számosságának meghatározásához rögzítsünk egy $(Z_i)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$ rendszert. Világos, hogy $\sigma \in \mathfrak{S}_{|\mathbf{p}|}$ esetén $(\sigma\langle Z_i\rangle)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$, és az

$$f : \mathfrak{S}_{|\mathbf{p}|} \to \mathfrak{M}_{\mathbf{p}}; \quad \sigma \mapsto (\sigma\langle Z_i\rangle)_{i \in n}$$

leképezés *szürjektív*, mert ha $(X_i)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$, akkor minden $i \in n$ esetén $\mathrm{Card}(X_i) = p_i = \mathrm{Card}(Z_i)$, így létezik olyan $(\sigma_i)_{i \in n}$ rendszer, hgy minden $i \in n$ számra $\sigma_i : Z_i \to X_i$ bijekció, így $\sigma := \bigcup_{i \in n} \sigma_i \in \mathfrak{S}_{|\mathbf{p}|}$ olyan permutáció, hogy $(\sigma\langle Z_i\rangle)_{i \in n} = (X_i)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$.

Ha $y := (Y_i)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$ és minden $i \in n$ esetén $\mathbb{B}(Z_i; Y_i)$ jelöli a $Z_i \to Y_i$ bijekciók halmazát, akkor a

$$\overset{-1}{f}\langle\{y\}\rangle \to \prod_{i \in n} \mathbb{B}(Z_i; Y_i); \quad \sigma \mapsto (\sigma|_{Z_i})_{i \in n}$$

leképezés bijekció, amelynek az inverze a

$$\prod_{i \in n} \mathbb{B}(Z_i; Y_i) \to \overset{-1}{f}\langle\{y\}\rangle; \quad (\sigma_i)_{i \in n} \mapsto \bigcup_{i \in n} \sigma_i$$

leképezés. Tehát minden $y := (Y_i)_{i \in n} \in \mathfrak{M}_{\mathbf{p}}$ esetén

$$\mathrm{Card}\left(\overset{-1}{f}\langle\{y\}\rangle\right) = \mathrm{Card}\left(\prod_{i \in n} \mathbb{B}(Z_i; Y_i)\right) = \prod_{i=0}^{n-1} \mathrm{Card}(\mathbb{B}(Z_i; Y_i)) = \prod_{i=0}^{n-1} p_i!,$$

hiszen minden $i \in n$ indexre $\mathrm{Card}(Z_i) = p_i = \mathrm{Card}(Y_i)$ miatt $\mathrm{Card}(\mathbb{B}(Z_i; Y_i)) = p_i!$ teljesül. Ezért alkalmazva a 6.8.2. tételt az $E := \mathfrak{S}_{|\mathbf{p}|}$, $F := \mathfrak{M}_{\mathbf{p}}$ és $G := \prod_{i=0}^{n-1} p_i!$ választással kapjuk, hogy $\mathfrak{S}_{|\mathbf{p}|}$ ekvipotens a $\mathfrak{M}_{\mathbf{p}} \times \prod_{i=0}^{n-1} p_i!$ szorzathalmazzal, így

$$\left(\sum_{i=0}^{n-1} p_i\right)! = |\mathbf{p}|! = \mathrm{Card}\left(\mathfrak{S}_{|\mathbf{p}|}\right) = \mathrm{Card}\left(\mathfrak{M}_{\mathbf{p}} \times \prod_{i=0}^{n-1} p_i!\right) = \mathrm{Card}(\mathfrak{M}_{\mathbf{p}}) \cdot \prod_{i=0}^{n-1} p_i!. \blacksquare$$

20.3.3. Állítás. *Legyen $n \in \mathbb{N}^*$ és $\mathbf{p} = (p_i)_{i \in n} \in (\mathbb{N}^*)^n$. Legyenek E és G vektorterek, $(F_i)_{i \in n}$ vektortér rendszer, és $\mathbf{m} \in \mathbf{Mult}\left(\prod_{i \in n} F_i; G\right)$. Ha $(u_i)_{i \in n} \in \prod_{i \in n} \mathbf{A}_{p_i}(E; F_i)$, akkor az*

$$(\mathbf{m}) \bigwedge_{i=0}^{n-1} u_i : E^{|\mathbf{p}|} \to G;$$
$$(x_i)_{i \in |\mathbf{p}|} \mapsto \sum_{\sigma \in \mathfrak{S}_{\mathbf{p}}} \varepsilon_{|\mathbf{p}|}(\sigma) \mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j \in p_i}\right)\right)_{i \in n}\right)$$

leképezés eleme $\mathbf{A}_{|\mathbf{p}|}(E; G)$-nek, és a

$$\prod_{i \in n} \mathbf{A}_{p_i}(E; F_i) \to \mathbf{A}_{|\mathbf{p}|}(E; G); \quad (u_i)_{i \in n} \mapsto (\mathbf{m}) \bigwedge_{i=0}^{n-1} u_i$$

leképezés multilineáris.

Bizonyítás. Legyen $(u_i)_{i\in n} \in \prod_{i\in n} \mathbf{A}_{p_i}(E;F_i)$, és jelölje u az állításban értelmezett $(\mathbf{m})\bigwedge_{i=0}^{n-1} u_i$ leképezést.

(I) Először megmutatjuk, hogy az $u : E^{|\mathbf{p}|} \to G$ leképezés multilineáris. Ehhez legyen $k \in |\mathbf{p}|$ és $\mathfrak{a} \in E^{|\mathbf{p}|}$ rögzített. Azt kell igazolni, hogy az $u \circ \mathrm{in}_{k,\mathfrak{a}} : E \to G$ leképezés lineáris. A definíció szerint minden $x \in E$ esetén

$$(u \circ \mathrm{in}_{k,\mathfrak{a}})(x) = \sum_{\sigma\in\mathfrak{S}_{\mathbf{p}}} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right).$$

Ebből látható, hogy az $u \circ \mathrm{in}_{k,\mathfrak{a}}$ leképezés linearitásának bizonyításához elegendő azt megmutatni, hogy minden $\sigma \in \mathfrak{S}_{\mathbf{p}}$ esetén az

$$E \to G; \quad x \mapsto \mathbf{m}\left(\left(u_i\left(\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right)$$

leképezés lineáris. Legyen tehát $\sigma \in \mathfrak{S}_{\mathbf{p}}$ rögzítve. Ekkor $\sigma^{-1}(k) \in |\mathbf{p}|$ miatt egyértelműen létezik olyan $i_* \in n$, amelyre $\sigma^{-1}(k) \in [\![\mathrm{s}_{\mathbf{p}}(i_*), \mathrm{s}_{\mathbf{p}}(i_*+1)[\![$, tehát egyértelműen létezik olyan $j_* \in p_{i_*}$, amelyre $k = \sigma(\mathrm{s}_{\mathbf{p}}(i_*) + j_*)$.

Ha $i \in n$ és $i \neq i_*$, akkor minden $j \in p_i$ esetén $\mathrm{s}_{\mathbf{p}}(i) + j \notin [\![\mathrm{s}_{\mathbf{p}}(i_*), \mathrm{s}_{\mathbf{p}}(i_* + 1)[\![$, tehát $\mathrm{s}_{\mathbf{p}}(i) + j \neq \sigma^{-1}(k)$, így minden $x \in E$ esetén

$$\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i} = \left(\mathfrak{a}_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}.$$

Ez azt jelenti, hogy a vizsgált $E \to G$ leképezésben az $\mathbf{m}$ multilineáris operátornak csak az i_*-adik változója függhet az $x \in E$ vektortól. Legyen $x \in E$ és minden $i \in n$ indexre vezessük be az

$$y_i := u_i\left(\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right) \in F_i$$

vektort. Az előzőek szerint $i \in n$ és $i \neq i_*$ esetén

$$y_i = u_i\left(\left(\mathfrak{a}_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right).$$

Ugyanakkor, minden $j \in p_{i_*}$ esetén

$$(\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j)} = \begin{cases} \mathfrak{a}_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j)} & \text{, ha } j \neq j_*, \\ x & \text{, ha } j = j_*, \end{cases}$$

hiszen $k = \sigma(\mathrm{s}_{\mathbf{p}}(i_*) + j_*)$. Ebből látható, hogy ha $\mathfrak{a}_* := \left(\left(\mathfrak{a}_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j)}\right)_{j\in p_{i_*}}\right) \in E^{p_{i_*}}$, akkor $\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j)}\right)_{j\in p_{i_*}} = \mathrm{in}_{j_*,\mathfrak{a}_*}(x)$, következésképpen

$$y_{i_*} = u_{i_*}\left(\mathrm{in}_{j_*,\mathfrak{a}_*}(x)\right).$$

Bevezetve a $\mathfrak{b}_* := \left(u_i\left(\left(\mathfrak{a}_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n} \in \prod_{i\in n} F_i$ elemet, ebből kapjuk, hogy minden $x \in E$ vektorra

$$\mathbf{m}\left(\left(u_i\left(\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = \left((\mathbf{m} \circ \mathrm{in}_{i_*,\mathfrak{b}_*}) \circ (u_{i_*} \circ \mathrm{in}_{j_*,\mathfrak{a}_*})\right)(x).$$

Itt az i_* és j_* indexek, valamint az $\mathfrak{a}_*$ és $\mathfrak{b}_*$ rendszerek x-től függetlenek (csak σ-tól, k-tól és $\mathfrak{a}$-tól függenek), továbbá $\mathbf{m}$ és u_{i_*} multilinearitása miatt $\mathbf{m} \circ \mathrm{in}_{i_*,\mathfrak{b}_*} \in \mathbf{L}(F_{i_*}; G)$ és $u_{i_*} \circ \mathrm{in}_{j_*,\mathfrak{a}_*} \in \mathbf{L}(E; F_{i_*})$, ezért az

$$E \to G; \quad x \mapsto \mathbf{m}\left(\left(u_i\left(\left((\mathrm{in}_{k,\mathfrak{a}}(x))_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right)$$

leképezés lineáris. Ezzel az u operátor multilinearitását igazoltuk. (Vegyük észre, hogy ehhez nem lényeges az u_i multilineáris operátorok antiszimmetrikussága, és az sem számít, hogy u előállításában csak az $\mathfrak{S}_{\mathbf{p}}$ permutáció-halmazon összegeztünk a teljes $\mathfrak{S}_{|\mathbf{p}|}$ helyett.)

(II) Az u multilineáris operátor antiszimmetrikusságának bizonyításához legyen $\tau \in \mathfrak{S}_{|\mathbf{p}|}$ rögzített transzpozíció, és $k, l \in |\mathbf{p}|$ azok az elemek, amelyekre $k \neq l$ és $\tau(k) = l$ és $\tau(l) = k$. Legyen

$$\mathfrak{S}_{\mathbf{p}}(k,l) := \left\{\sigma \in \mathfrak{S}_{\mathbf{p}} \,\middle|\, (\exists i \in n)\left(\left(\sigma^{-1}(k) \in [\![\mathrm{s}(i), \mathrm{s}(i+1)[\![\right) \wedge \left(\sigma^{-1}(l) \in [\![\mathrm{s}(i), \mathrm{s}(i+1)[\![\right)\right)\right\}.$$

Legyen $(x_i)_{i\in|\mathbf{p}|} \in E^{|\mathbf{p}|}$ rögzített. Bevezetve a

$$z := \sum_{\sigma\in\mathfrak{S}_{\mathbf{p}}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right),$$
$$z' := \sum_{\sigma\in\mathfrak{S}_{\mathbf{p}}\setminus\mathfrak{S}_{\mathbf{p}}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right)$$

vektorokat, a definíció szerint világos, hogy

$$u\left(\left(x_{\tau(i)}\right)_{i\in|\mathbf{p}|}\right) = \sum_{\sigma\in\mathfrak{S}_{\mathbf{p}}} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = z + z'.$$

Először azt fogjuk igazolni, hogy minden $\sigma \in \mathfrak{S}_{\mathbf{p}}(k,l)$ esetén

$$\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = -\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right), \tag{1}$$

amiből következik, hogy

$$z = -\sum_{\sigma\in\mathfrak{S}_{\mathbf{p}}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right). \tag{2}$$

Legyen $\sigma \in \mathfrak{S}_{\mathbf{p}}(k,l)$ rögzített, és $i_* \in n$ olyan, hogy $\sigma^{-1}(k) \in [\![\mathrm{s}(i_*), \mathrm{s}(i_*+1)[\![$. Ekkor az i_* index egyértelműen van meghatározva, mert az $([\![\mathrm{s}_{\mathbf{p}}(i), \mathrm{s}_{\mathbf{p}}(i+1)[\![)_{i\in n}$ halmazrendszer diszjunkt. Legyenek $k_*, l_* \in p_{i_*}$ azok az egyértelműen meghatározott számok, amelyekre $\sigma^{-1}(k) = \mathrm{s}_{\mathbf{p}}(i_*) + k_*$ és $\sigma^{-1}(l) = \mathrm{s}_{\mathbf{p}}(i_*) + l_*$, vagy ami ugyanaz: $k = \sigma(\mathrm{s}_{\mathbf{p}}(i_*) + k_*)$ és $l = \sigma(\mathrm{s}_{\mathbf{p}}(i_*) + l_*)$. Vezessük be az

$$\mathfrak{a} := \left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n} \in \prod_{i\in n} F_i$$

vektort, amelynek alkalmazásával nyilvánvalóan írható, hogy

$$\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = (\mathbf{m} \circ \mathrm{in}_{i_*,\mathfrak{a}})\left(u_{i_*}\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j))}\right)_{j\in p_{i_*}}\right)\right). \tag{3}$$

Ha $i \in n$ és $i \neq i_*$, akkor minden $j \in p_i$ esetén $\mathrm{s}_{\mathbf{p}}(i) + j \notin [\![\mathrm{s}(i_*), \mathrm{s}(i_*+1)[\![$, ezért $\mathrm{s}_{\mathbf{p}}(i) + j \neq \sigma^{-1}(k)$ és $\mathrm{s}_{\mathbf{p}}(i) + j \neq \sigma^{-1}(l)$, vagyis $\sigma\left(\mathrm{s}_{\mathbf{p}}(i) + j\right) \neq k$ és $\sigma\left(\mathrm{s}_{\mathbf{p}}(i) + j\right) \neq l$, amiből következik, hogy $\tau\left(\sigma\left(\mathrm{s}_{\mathbf{p}}(i) + j\right)\right) = \sigma\left(\mathrm{s}_{\mathbf{p}}(i) + j\right)$, tehát

$$u_i\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right) = \mathfrak{a}_i.$$

Ugyanakkor, minden $j \in p_{i_*}$ esetén

$$\tau\left(\sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + j\right)\right) = \begin{cases} \sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + j\right) & \text{, ha } j \neq k_* \text{ és } j \neq l_*, \\ l & \text{, ha } j = k_*, \\ k & \text{, ha } j = l_* \end{cases}$$

hiszen ha $j \neq k_*$ és $j \neq l_*$, akkor $\sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + j\right) \neq k$ és $\sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + j\right) \neq l$, amiből következik, hogy $\tau\left(\sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + j\right)\right) = \sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + j\right)$, továbbá $\tau\left(\sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + k_*\right)\right) = \tau(k) = l$ és $\tau\left(\sigma\left(\mathrm{s}_{\mathbf{p}}(i_*) + l_*\right)\right) = \tau(k) = k$. Ez azt jelenti, hogy ha $\tau_* \in \mathfrak{S}_{p_{i_*}}$ jelöli azt a transzpozíciót, amelyre $\tau_*(k_*) = l_*$ és $\tau_*(l_*) = k_*$, akkor

$$\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j))}\right)_{j\in p_{i_*}} = \left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+\tau_*(j))}\right)_{j\in p_{i_*}}.$$

Ebből (3) alapján következik, hogy

$$\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_{\mathbf{p}}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = \left(\mathbf{m}\circ \mathrm{in}_{i_*,\mathfrak{a}}\right)\left(u_{i_*}\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+\tau_*(j))}\right)_{j\in p_{i_*}}\right)\right) \stackrel{(1)}{=}$$
$$\stackrel{(1)}{=} \left(\mathbf{m}\circ \mathrm{in}_{i_*,\mathfrak{a}}\right)\left(-u_{i_*}\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j)}\right)_{j\in p_{i_*}}\right)\right) \stackrel{(2)}{=} -\left(\mathbf{m}\circ \mathrm{in}_{i_*,\mathfrak{a}}\right)\left(u_{i_*}\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i_*)+j)}\right)_{j\in p_{i_*}}\right)\right) =$$
$$= -\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right),$$

ahol

– az $\stackrel{(1)}{=}$ egyenlőségnél felhasználtuk, hogy $u_{i_*} : E^{p_{i_*}} \to F_{i_*}$ antiszimmetrikus multilineáris operátor és $\tau_* \in \mathfrak{S}_{p_{i_*}}$ transzpozíció;

– a $\stackrel{(2)}{=}$ egyenlőségnél arra hivatkozhatunk, hogy $\mathbf{m} : \prod_{i\in n} F_i \to G$ multilineáris operátor, így $\mathbf{m}\circ \mathrm{in}_{i_*,\mathfrak{a}} : F_{i_*} \to G$ lineáris operátor, tehát minden $x \in F_{i_*}$ esetén $\left(\mathbf{m}\circ \mathrm{in}_{i_*,\mathfrak{a}}\right)(-x) = -\left(\mathbf{m}\circ \mathrm{in}_{i_*,\mathfrak{a}}\right)(x)$;

Tehát ekkor fennáll az (1) egyenlőség, amivel igazoltuk a (2) összefüggést.

Ha $\sigma \in \mathfrak{S}_{\mathbf{p}}$, akkor $\sigma \in \mathfrak{S}_{\mathbf{p}} \setminus \mathfrak{S}_{\mathbf{p}}(k, l)$ azzal ekvivalens, hogy minden $i \in n$ esetén $\sigma^{-1}(k) \notin [\![\mathrm{s}(i), \mathrm{s}(i+1)[\![$ vagy $\sigma^{-1}(l) \notin [\![\mathrm{s}(i), \mathrm{s}(i+1)[\![$. Tehát $\sigma \in \mathfrak{S}_{\mathbf{p}} \setminus \mathfrak{S}_{\mathbf{p}}(k, l)$ esetén egyértelműen léteznek olyan $i, i' \in n$ elemek, amelyekre $i \neq i'$, és $\sigma^{-1}(k) \in [\![\mathrm{s}(i), \mathrm{s}(i+1)[\![$ és $\sigma^{-1}(l) \in [\![\mathrm{s}(i'), \mathrm{s}(i'+1)[\![$, így egyértelműen léteznek olyan $j \in i$ és $j' \in i'$ számok, amelyekre $\sigma^{-1}(k) = \mathrm{s}_{\mathbf{p}}(i) + j$ és $\sigma^{-1}(l) = \mathrm{s}_{\mathbf{p}}(i') + j'$, vagy ami ugyanaz: $k = \sigma\left(\mathrm{s}_{\mathbf{p}}(i) + j\right)$ és $l = \sigma\left(\mathrm{s}_{\mathbf{p}}(i') + j'\right)$. Ez azt jelenti, hogy ha

$$A := \{(i, i', j, j') | (i \in n) \wedge (i' \in n) \wedge (j \in i) \wedge (j' \in i')\},$$

valamint minden $(i, i', j, j') \in A$ esetén

$$\mathfrak{S}_{\mathbf{p}}(i, i', j, j') := \left\{\sigma \in \mathfrak{S}_{\mathbf{p}} \;\middle|\; \left(\sigma\left(\mathrm{s}_{\mathbf{p}}(i) + j\right) = k\right) \wedge \left(\sigma\left(\mathrm{s}_{\mathbf{p}}(i') + j'\right) = l\right)\right\},$$

akkor

$$\mathfrak{S}_{\mathbf{p}} \setminus \mathfrak{S}_{\mathbf{p}}(k, l) = \bigcup_{(i,i',j,j')\in A} \mathfrak{S}_{\mathbf{p}}(i, i', j, j'),$$

és az $([\![\mathrm{s}_\mathbf{p}(i), \mathrm{s}_\mathbf{p}(i+1)[\![)_{i\in n}$ halmazrendszer diszjunktságából azonnal következik, hogy az $(\mathfrak{S}_\mathbf{p}(i,i',j,j'))_{(i,i',j,j')\in A}$ halmazrendszer diszjunkt. Ekkor írható, hogy

$$\begin{aligned}
z' &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}\setminus\mathfrak{S}_\mathbf{p}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_\mathbf{p}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right) \overset{(1)}{=} \\
&\overset{(1)}{=} \sum_{(i,i',j,j')\in A}\left(\sum_{\sigma\in\mathfrak{S}_\mathbf{p}(i,i',j,j')} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_\mathbf{p}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right)\right) \overset{(2)}{=} \\
&\overset{(2)}{=} -\sum_{(i,i',j,j')\in A}\left(\sum_{\sigma\in\mathfrak{S}_\mathbf{p}(i,i',j,j')} \varepsilon_{|\mathbf{p}|}(\tau\circ\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{(\tau\circ\sigma)(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right)\right) \overset{(3)}{=} \\
&\overset{(3)}{=} -\sum_{(i,i',j,j')\in A}\left(\sum_{\sigma'\in\mathfrak{S}_\mathbf{p}(i',i,j',j)} \varepsilon_{|\mathbf{p}|}(\sigma')\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma'(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right)\right) \overset{(4)}{=} \\
&\overset{(4)}{=} -\sum_{(i',i,j',j)\in A}\left(\sum_{\sigma'\in\mathfrak{S}_\mathbf{p}(i',i,j',j)} \varepsilon_{|\mathbf{p}|}(\sigma')\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma'(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right)\right) = \\
&= -\sum_{\sigma\in\mathfrak{S}_\mathbf{p}\setminus\mathfrak{S}_\mathbf{p}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right),
\end{aligned}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk a K-beli összeadás általános asszociativitását;

– a $\overset{(2)}{=}$ egyenlőségnél az $\varepsilon_{|\mathbf{p}|}(\sigma) = -\varepsilon_{|\mathbf{p}|}(\tau\circ\sigma)$ összefüggést alkalmaztuk;

– a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk azt, hogy minden $(i,i',j,j')\in A$ esetén $(i',i,j',j)\in A$, és az

$$\mathfrak{S}_\mathbf{p}(i,i',j,j') \to \mathfrak{S}_\mathbf{p}(i',i,j',j); \quad \sigma\mapsto\tau\circ\sigma$$

leképezés bijekció, így alkalmazható a K-beli összeadás általános kommutativitása;

– a $\overset{(4)}{=}$ egyenlőségnél azt a nyilvánvaló tényt használtuk ki, hogy minden $(i,i',j,j')\in\mathbb{N}^4$ esetén $((i,i',j,j')\in A)\Leftrightarrow((i',i,j',j)\in A)$.

Ez azt jelenti, hogy

$$z' = -\sum_{\sigma\in\mathfrak{S}_\mathbf{p}\setminus\mathfrak{S}_\mathbf{p}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right). \tag{4}$$

A (2) és (4) egyenlőségekből következik, hogy

$$\begin{aligned}
u\left(\left(x_{\tau(i)}\right)_{i\in|\mathbf{p}|}\right) &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\tau(\sigma(\mathrm{s}_\mathbf{p}(i)+j))}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = z+z' = \\
&= -\sum_{\sigma\in\mathfrak{S}_\mathbf{p}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right) - \\
&\quad -\sum_{\sigma\in\mathfrak{S}_\mathbf{p}\setminus\mathfrak{S}_\mathbf{p}(k,l)} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = \\
&= -\sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right) = -u\left((x_i)_{i\in|\mathbf{p}|}\right),
\end{aligned}$$

így 20.1.2. alapján az $u : E^{|\mathbf{p}|}\to G$ multilineáris operátor antiszimmetrikus.

(III) Vezessük be az

$$f : \prod_{i\in n} \mathbf{A}_{p_i}(E;F_i) \to \mathbf{A}_{|\mathbf{p}|}(E;G); \quad (u_i)_{i\in n} \mapsto (\mathbf{m}) \bigwedge_{i=0}^{n-1} u_i$$

függvényt. Az f leképezés multilinearitásának bizonyításához legyen $k \in n$ és $\mathbf{w} := (w_i)_{i\in n} \in \prod_{i\in n} \mathbf{A}_{p_i}(E;F_i)$ rögzített. Azt kell igazolni, hogy $f \circ \mathrm{in}_{k,\mathbf{w}} : \mathbf{A}_{p_k}(E;F_k) \to \mathbf{A}_{|\mathbf{p}|}(E;G)$ lineáris operátor.

Legyen $\mathbf{x} := (x_i)_{i\in|\mathbf{p}|} \in E^{|\mathbf{p}|}$ és $u \in \mathbf{A}_{p_k}(E;F_k)$. Minden $\sigma \in \mathfrak{S}_\mathbf{p}$ permutációra legyen $\mathbf{x}(\mathbf{w},\sigma) := \left(w_i\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n} \in \prod_{i\in n} F_i$. Ekkor a definíciók szerint

$$\begin{aligned}((f\circ \mathrm{in}_{k,\mathbf{w}})(u))\left((x_i)_{i\in|\mathbf{p}|}\right) &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(((\mathrm{in}_{k,\mathbf{w}}(u))_i\left(x_{\sigma(\mathrm{s}_\mathbf{p}(i)+j)}\right)\right)_{j\in p_i}\right)_{i\in n}\right) = \\ &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)\left(u\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right).\end{aligned}$$

Mivel $\mathbf{m} \in \mathbf{Mult}\left(\prod_{i\in n} F_i;G\right)$, így minden $\sigma \in \mathfrak{S}_\mathbf{p}$ esetén $\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\sigma)} : F_k \to G$ lineáris operátor. Tehát ha $u,v \in \mathbf{A}_{p_k}(E;F_k)$, akkor minden $\mathbf{x} := (x_i)_{i\in|\mathbf{p}|} \in E^{|\mathbf{p}|}$ esetén

$$\begin{aligned}((f\circ \mathrm{in}_{k,\mathbf{w}})(u+v))\left((x_i)_{i\in|\mathbf{p}|}\right) &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)\left((u+v)\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right) = \\ &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)\left(u\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)+v\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right) = \\ &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)\left(u\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right) + \\ &\quad + \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)\left(v\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right) = \\ &= ((f\circ \mathrm{in}_{k,\mathbf{w}})(u))\left((x_i)_{i\in|\mathbf{p}|}\right) + ((f\circ \mathrm{in}_{k,\mathbf{w}})(v))\left((x_i)_{i\in|\mathbf{p}|}\right),\end{aligned}$$

következésképpen $(f\circ \mathrm{in}_{k,\mathbf{w}})(u+v) = (f\circ \mathrm{in}_{k,\mathbf{w}})(u) + (f\circ \mathrm{in}_{k,\mathbf{w}})(v)$, vagyis az $f\circ \mathrm{in}_{k,\mathbf{w}}$ operátor additív. Hasonlóan, ha K az a test, amely felett E vektortér, akkor $\lambda \in K$ és $u \in \mathbf{A}_{p_k}(E;F_k)$ esetén minden $\mathbf{x} := (x_i)_{i\in|\mathbf{p}|} \in E^{|\mathbf{p}|}$ rendszerre

$$\begin{aligned}((f\circ \mathrm{in}_{k,\mathbf{w}})(\lambda.u))\left((x_i)_{i\in|\mathbf{p}|}\right) &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)\left((\lambda.u)\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right) = \\ &= \sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)\left(\lambda.u\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right) = \\ = \lambda.\sum_{\sigma\in\mathfrak{S}_\mathbf{p}} \varepsilon_{|\mathbf{p}|}(\sigma)\left(\mathbf{m}\circ \mathrm{in}_{k,\mathbf{x}(\mathbf{w},\sigma)}\right)&\left(u\left(\left(x_{\sigma(\mathrm{s}_\mathbf{p}(k)+j)}\right)_{j\in p_k}\right)\right) = \lambda.((f\circ \mathrm{in}_{k,\mathbf{w}})(u))\left((x_i)_{i\in|\mathbf{p}|}\right),\end{aligned}$$

következésképpen $(f\circ \mathrm{in}_{k,\mathbf{w}})(\lambda.u) = \lambda.(f\circ \mathrm{in}_{k,\mathbf{w}})(u)$, vagyis az $f\circ \mathrm{in}_{k,\mathbf{w}}$ operátor K-homogén. ■

20.3.4. Definíció. *Legyen $n \in \mathbb{N}^*$ és $\mathbf{p} = (p_i)_{i\in n} \in (\mathbb{N}^*)^n$. Legyenek E és G vektorterek, $(F_i)_{i\in n}$ vektortér rendszer a K test felett, és $\mathbf{m} \in \mathbf{Mult}\left(\prod_{i\in n} F_i;G\right)$. Ekkor minden*

$(u_i)_{i\in n} \in \prod_{i\in n} \mathbf{A}_{p_i}(E;F_i)$ *esetén az*

$$(\mathbf{m})\bigwedge_{i=0}^{n-1} u_i : E^{|\mathbf{p}|} \to G;$$
$$(x_i)_{i\in|\mathbf{p}|} \mapsto \sum_{\sigma\in\mathfrak{S}_{\mathbf{p}}} \varepsilon_{|\mathbf{p}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathbf{s}_{\mathbf{p}}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in n}\right)$$

antiszimmetrikus multilineáris operátort az $(u_i)_{i\in n}$ *multilineáris operátor rendszer* **külső szorzatának** *nevezzük (tehát ekkor* $(\mathbf{m})\bigwedge_{i=0}^{n-1} u_i \in \mathbf{A}_{|\mathbf{p}|}(E;G)$*). Ha minden* $i\in n$ *esetén* $p_i := 1$, $F_i := K$, $G := K$, *és* $\mathbf{m}$ *egyenlő a*

$$K^n \to K; \quad (\lambda_i)_{i\in n} \mapsto \mathrm{P}_{i\in n} \lambda_i$$

multilineáris funkcionállal, akkor az E^**-ban haladó* $(u_i)_{i\in n}$ *lineáris funkcionál rendszer külső szorzatát a* $\bigwedge_{i=0}^{n-1} u_i$ *szimbólummal jelöljük (tehát ekkor* $\bigwedge_{i=0}^{n-1} u_i \in \mathbf{A}_n(E)$*).*

20.3.5. Állítás. *Legyen* E *vektortér a* K *test felett és* $p\in\mathbb{N}^*$*.*

a) *Ha* $(u_i)_{i\in p} \in (E^*)^p$*, akkor* $\bigwedge_{i=0}^{p-1} u_i \in \mathbf{Alt}_p(E)$*, és minden* $(x_i)_{i\in p}\in E^p$ *esetén*

$$\left(\bigwedge_{i=0}^{p-1} u_i\right)((x_i)_{i\in p}) = \det\left((u_i(x_j))_{(i,j)\in p\times p}\right).$$

b) *Az* $(E^*)^p \to \mathbf{Alt}_p(E)$; $(u_i)_{i\in p} \mapsto \bigwedge_{i=0}^{p-1} u_i$ *leképezés multilineáris és alternáló, tehát eleme* $\mathbf{Alt}_p\left(E^*;\mathbf{Alt}_p(E)\right)$*-nek.*

Bizonyítás. a) Legyen $\mathbf{1}\in(\mathbb{N}^*)^p$ az a szám p-es, amelynek mindegyik komponense 1. Világos, hogy $|\mathbf{1}| = p$, és minden $i\le p$ természetes számra $\mathbf{s_1}(i) = i$, és $\mathfrak{S}_{\mathbf{1}} = \mathfrak{S}_p$. Jelölje továbbá $\mathbf{m}$ a

$$K^p \to K; \quad (\lambda_i)_{i\in p} \mapsto \mathrm{P}_{i\in p} \lambda_i$$

multilineáris funkcionált. Ekkor minden $(u_i)_{i\in p}\in(E^*)^p$ és $(x_i)_{i\in p}\in E^p$ esetén

$$\left(\bigwedge_{i=0}^{p-1} u_i\right)((x_i)_{i\in p}) = \sum_{\sigma\in\mathfrak{S}_{\mathbf{1}}} \varepsilon_{|\mathbf{1}|}(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(\mathbf{s_1}(i)+j)}\right)_{j\in p_i}\right)\right)_{i\in p}\right) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\mathbf{m}\left(\left(u_i\left(\left(x_{\sigma(i+j)}\right)_{j\in 1}\right)\right)_{i\in p}\right) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\mathbf{m}\left(\left(u_i\left(x_{\sigma(i)}\right)\right)_{i\in p}\right) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) \mathrm{P}_{i\in p} u_i\left(x_{\sigma(i)}\right) = \det\left((u_i(x_j))_{(i,j)\in p\times p}\right).$$

Ebből látható, hogy a $\bigwedge_{i=0}^{p-1} u_i$ antiszimmetrikus forma alternáló, mert ha $(x_i)_{i\in p}\in E^p$ és $k,l\in p$ olyanok, hogy $k\ne l$ és $x_k = x_l$, akkor az $(u_i(x_j))_{(i,j)\in p\times p} \in \mathrm{M}_p(K)$ mátrix k-adik és l-edik oszlopa egyenlő, amiből 15.2.10. alapján következik, hogy $\det\left((u_i(x_j))_{(i,j)\in p\times p}\right) = 0$, vagyis $\left(\bigwedge_{i=0}^{p-1} u_i\right)\left((x_i)_{i\in p}\right) = 0$.

b) Megmutatjuk, hogy a

$$w : (E^*)^p \to \mathbf{Alt}_p(E); \quad (u_i)_{i\in p} \mapsto \bigwedge_{i=0}^{p-1} u_i$$

leképezés multilineáris, vagyis eleme $\mathbf{L}_p\left(E^*; \mathbf{Alt}_p(E)\right)$-nek. Ehhez legyenek $\mathbf{u} = (u_i)_{i\in p} \in (E^*)^p$ és $k \in p$ rögzítve. Ha $v \in E^*$, akkor minden $(x_i)_{i\in p} \in E^p$ esetén a) alapján

$$((w \circ \mathrm{in}_{k,\mathbf{u}})(v))((x_i)_{i\in p}) = \left(\bigwedge_{i=0}^{p-1} (\mathrm{in}_{k,\mathbf{u}}(v))_i\right)((x_i)_{i\in p}) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) \prod_{i\in p} (\mathrm{in}_{k,\mathbf{u}}(v))_i \left(x_{\sigma(i)}\right) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) v\left(x_{\sigma(k)}\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right).$$

Ebből látszik, hogy ha $v, v' \in E^*$, akkor minden $(x_i)_{i\in p} \in E^p$ esetén

$$((w \circ \mathrm{in}_{k,\mathbf{u}})(v+v'))((x_i)_{i\in p}) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)(v+v')\left(x_{\sigma(k)}\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\left(v\left(x_{\sigma(k)}\right) + v'\left(x_{\sigma(k)}\right)\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)v\left(x_{\sigma(k)}\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right) + \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)v'\left(x_{\sigma(k)}\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right) =$$
$$= ((w \circ \mathrm{in}_{k,\mathbf{u}})(v))((x_i)_{i\in p}) + ((w \circ \mathrm{in}_{k,\mathbf{u}})(v'))((x_i)_{i\in p}) =$$
$$= ((w \circ \mathrm{in}_{k,\mathbf{u}})(v) + (w \circ \mathrm{in}_{k,\mathbf{u}})(v'))((x_i)_{i\in p}),$$

tehát az $\mathrm{in}_{k,\mathbf{u}} : E^* \to \mathbf{Alt}_p(E)$ leképezés additív, továbbá, ha $v \in E^*$ és $\lambda \in K$, akkor minden $(x_i)_{i\in p} \in E^p$ esetén

$$((w \circ \mathrm{in}_{k,\mathbf{u}})(\lambda.v))((x_i)_{i\in p}) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)(\lambda.v)\left(x_{\sigma(k)}\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\left(\lambda\, v\left(x_{\sigma(k)}\right)\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right) = \lambda \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)v\left(x_{\sigma(k)}\right) \prod_{\substack{i\in p\\ i\neq k}} u_i\left(x_{\sigma(i)}\right) =$$
$$= \lambda\, ((w \circ \mathrm{in}_{k,\mathbf{u}})(v))((x_i)_{i\in p}) = (\lambda.(w \circ \mathrm{in}_{k,\mathbf{u}})(v))((x_i)_{i\in p}),$$

tehát az $\mathrm{in}_{k,\mathbf{u}} : E^* \to \mathbf{Alt}_p(E)$ leképezés K-homogén. Ezért a w leképezés multilineáris (pontosabban p-lineáris).

Végül, az $(E^*)^p \to \mathbf{Alt}_p(E)$; $(u_i)_{i\in p} \mapsto \bigwedge_{i=0}^{p-1} u_i$ multilineáris operátor alternáló, mert ha $(u_i)_{i\in p} \in (E^*)^p$ és $k, l \in p$ olyan indexek, hogy $k \neq l$ és $u_k = u_l$, akkor minden $(x_i)_{i\in p} \in E^p$ esetén az $(u_i(x_j))_{(i,j)\in p\times p} \in \mathrm{M}_p(K)$ mátrix k-adik és l-edik sora egyenlő, amiből 15.2.10. alapján következik, hogy $\det\left((u_i(x_j))_{(i,j)\in p\times p}\right) = 0$, vagyis $\bigwedge_{i=0}^{p-1} u_i = \mathbf{0}$. ■

A 20.3.3. állításnak különösen fontos speciális esete az, amikor $n = 2$, ezért ezt külön állításban megfogalmazzuk.

20.3.6. Állítás. *Legyenek E, F, G és H vektorterek, $p, q \in \mathbb{N}^*$, valamint $\mathbf{b} : F\times G \to H$ bilineáris operátor. Ha $u \in \mathbf{A}_p(E;F)$ és $v \in \mathbf{A}_q(E;G)$, akkor az*

$$u \bigwedge_{(\mathbf{b})} v : E^{p+q} \to H;$$

$$(x_i)_{i\in p+q} \mapsto \sum_{\sigma\in\mathfrak{S}_{(p,q)}} \varepsilon_{p+q}(\sigma)\mathbf{b}\left(u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right), v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right)\right)$$

leképezés eleme $\mathbf{A}_{p+q}(E;H)$*-nak.* ■

20.3.7. Lemma. *Legyenek* $p,q\in\mathbb{N}^*$, *és minden* $(\mu,\nu,\sigma)\in\mathfrak{S}_p\times\mathfrak{S}_q\times\mathfrak{S}_{(p,q)}$ *esetén legyen*

$$\varrho_{\mu,\nu,\sigma}: p+q\to p+q;\quad i\mapsto \varrho_{\mu,\nu,\sigma}(i) := \begin{cases} \sigma(\mu(i)) & , \text{ha } i<p,\\ \sigma(p+\nu(i-p)) & , \text{ha } p\le i<p+q.\end{cases}$$

Ekkor minden $(\mu,\nu,\sigma)\in\mathfrak{S}_p\times\mathfrak{S}_q\times\mathfrak{S}_{(p,q)}$ *esetén* $\varrho_{\mu,\nu,\sigma}\in\mathfrak{S}_{p+q}$, *és*

$$\varepsilon_{p+q}\left(\varrho_{\mu,\nu,\sigma}\right) = \varepsilon_p(\mu)\varepsilon_q(\nu)\varepsilon_{p+q}(\sigma).$$

Továbbá, az

$$\mathfrak{S}_p\times\mathfrak{S}_q\times\mathfrak{S}_{(p,q)}\to\mathfrak{S}_{p+q};\quad (\mu,\nu,\sigma)\mapsto\varrho_{\mu,\nu,\sigma}$$

leképezés bijekció.

Bizonyítás. Legyenek $p,q\in\mathbb{N}^*$ és $(\mu,\nu,\sigma)\in\mathfrak{S}_p\times\mathfrak{S}_q\times\mathfrak{S}_{(p,q)}$. A definíció alapján világos, hogy a $\varrho_{\mu,\nu,\sigma}$ függvény injektív a $[\![0,p[\![$ és $[\![p,p+q[\![$ halmazokon, és ha $i\in[\![0,p[\![$, valamint $j\in[\![p,p+q[\![$, akkor $\varrho_{\mu,\nu,\sigma}(i)\neq\varrho_{\mu,\nu,\sigma}(j)$ lehetetlen, különben $\sigma(\mu(i))=\sigma(p+\nu(j-p))$ teljesülne, így σ injektivitása folytán $p>\mu(i)=p+\nu(j-p)\ge p$ igaz lenne. Tehát a $\varrho_{\mu,\nu,\sigma}: p+q\to p+q$ függvény injekció, így a $p+q$ halmaz végessége miatt bijekció, azaz $\varrho_{\mu,\nu,\sigma}\in\mathfrak{S}_{p+q}$.

Legyen ismét $p,q\in\mathbb{N}^*$ és $(\mu,\nu,\sigma)\in\mathfrak{S}_p\times\mathfrak{S}_q\times\mathfrak{S}_{(p,q)}$, továbbá vezessük be a következő halmazokat:

$$\begin{aligned}
\mathrm{T}\left(\varrho_{\mu,\nu,\sigma}\right) &:= \{(i,j)\in(p+q)\times(p+q)|(i<j)\wedge(\varrho_{\mu,\nu,\sigma}(i)>\varrho_{\mu,\nu,\sigma}(j))\},\\
\mathrm{T}(\mu) &:= \{(i,j)\in p\times p|(i<j)\wedge(\mu(i)>\mu(j))\},\\
\mathrm{T}(\nu) &:= \{(i,j)\in q\times q|(i<j)\wedge(\nu(i)>\nu(j))\},\\
\mathrm{T}(\sigma) &= \{(i,j)\in(p+q)\times(p+q)|(i<j)\wedge(\sigma(i)>\sigma(j))\}.
\end{aligned}$$

Legyenek továbbá

$$\begin{aligned}
\mathrm{T}'(\nu) &:= \{(p+i,p+j)|(i,j)\in\mathrm{T}(\nu)\},\\
\mathrm{T}'(\sigma) &:= \{(i,j)\in p\times(p+q)|(i<p\le j)\wedge((\mu(i),p+\nu(j-p))\in\mathrm{T}(\sigma))\}.
\end{aligned}$$

Megmutatjuk, hogy

$$\mathrm{T}\left(\varrho_{\mu,\nu,\sigma}\right) = \mathrm{T}(\mu)\cup\mathrm{T}'(\nu)\cup\mathrm{T}'(\sigma). \tag{1}$$

Ha $(i,j)\in\mathrm{T}(\mu)$, akkor $i<j$ és $\mu(i)>\mu(j)$, amiből következik, hogy $\varrho_{\mu,\nu,\sigma}(i)=\sigma(\mu(i))>\sigma(\mu(j))=\varrho_{\mu,\nu,\sigma}(j)$, mert $\mu(i),\mu(j)\in[\![0,p[\![$ és $\sigma\in\mathfrak{S}_{(p,q)}$ miatt σ növő a $[\![0,p[\![$ halmazon. Ezért $\mathrm{T}(\mu)\subseteq\mathrm{T}\left(\varrho_{\mu,\nu,\sigma}\right)$. Hasonlóan, ha $(i,j)\in\mathrm{T}(\nu)$, akkor $p+\nu(i)>p+\nu(j)$, amiből következik, hogy $\varrho_{\mu,\nu,\sigma}(p+i)=\sigma(p+\nu(i))>\sigma(p+\nu(j))=\varrho_{\mu,\nu,\sigma}(p+j)$, mert $p+\nu(i),p+\nu(j)\in[\![p,p+q[\![$ és $\sigma\in\mathfrak{S}_{(p,q)}$ miatt σ növő a $[\![p,p+q[\![$ halmazon. Ezért $\mathrm{T}'(\nu)\subseteq\mathrm{T}\left(\varrho_{\mu,\nu,\sigma}\right)$. Végül, ha $(i,j)\in\mathrm{T}'(\sigma)$, azaz $0\le i<p\le j$ és $(\mu(i),p+\nu(j-p))\in\mathrm{T}(\sigma)$, akkor $\varrho_{\mu,\nu,\sigma}(i)=\sigma(\mu(i)>\sigma(p+\nu(j-p))=\varrho_{\mu,\nu,\sigma}(j)$. Ezért $\mathrm{T}'(\sigma)\subseteq\mathrm{T}\left(\varrho_{\mu,\nu,\sigma}\right)$ Ezzel megmutattuk, hogy

$$\mathrm{T}(\mu)\cup\mathrm{T}'(\nu)\cup\mathrm{T}'(\sigma)\subseteq\mathrm{T}\left(\varrho_{\mu,\nu,\sigma}\right).$$

Megfordítva, tegyük fel, hogy $(i,j) \in \mathrm{T}(\varrho_{\mu,\nu,\sigma})$. Ekkor három, páronként kizáró eset lehetséges.

– Ha $j < p$, akkor $\sigma(\mu(i)) = \varrho_{\mu,\nu,\sigma}(i) > \varrho_{\mu,\nu,\sigma}(j) = \sigma(\mu(j))$, ezért $\mu(i) > \mu(j)$, hiszen $\mu(i), \mu(j) \in [\![0,p[\![$ és $\sigma \in \mathfrak{S}_{(p,q)}$ miatt σ növő a $[\![0,p[\![$ halmazon. Tehát ekkor $(i,j) \in \mathrm{T}(\mu)$.
– Ha $i < p \leq j$, akkor $\sigma(\mu(i)) = \varrho_{\mu,\nu,\sigma}(i) > \varrho_{\mu,\nu,\sigma}(j) = \sigma(p + \nu(j-p))$, ezért $(\mu(i), p+\nu(j-p)) \in \mathrm{T}(\sigma)$. Tehát ekkor $(i,j) \in \mathrm{T}'(\sigma)$.

– Ha $p \leq i$, akkor $\sigma(p+\nu(i-p)) = \varrho_{\mu,\nu,\sigma}(i) > \varrho_{\mu,\nu,\sigma}(j) = \sigma(p+\nu(j-p))$, így $\nu(i-p) > \nu(j-p)$, hiszen $p+\nu(i-p), p+\nu(j-p) \in [\![p,p+q[\![$ és $\sigma \in \mathfrak{S}_{(p,q)}$ miatt σ növő a $[\![p,p+q[\![$ halmazon. Tehát ekkor $(i-p, j-p) \in \mathrm{T}(\nu)$, így $(i,j) = (p+(i-p), p+(j-p)) \in \mathrm{T}'(\mu)$. Ezzel megmutattuk, hogy

$$\mathrm{T}(\varrho_{\mu,\nu,\sigma}) \subseteq \mathrm{T}(\mu) \cup \mathrm{T}'(\nu) \cup \mathrm{T}'(\sigma),$$

így fennáll az (1) egyenlőség. Továbbá,

– ha $(i,j) \in \mathrm{T}(\mu)$, akkor $i < j < p$,

– ha $(i,j) \in \mathrm{T}'(\nu)$, akkor $p \leq i < j$,

– ha $(i,j) \in \mathrm{T}'(\sigma)$, akkor $i < p \leq j$,

amiből azonnal következik, hogy a $\mathrm{T}(\mu)$, $\mathrm{T}'(\nu)$ és $\mathrm{T}'(\sigma)$ halmazok páronként diszjunktak. Ezért az (1) egyenlőségből következik, hogy

$$\mathrm{Card}\,(\mathrm{T}(\varrho_{\mu,\nu,\sigma})) = \mathrm{Card}\,(\mathrm{T}(\mu)) + \mathrm{Card}\,(\mathrm{T}'(\nu)) + \mathrm{Card}\,(\mathrm{T}'(\sigma)). \tag{2}$$

Nyilvánvaló, hogy a

$$\mathrm{T}(\nu) \to \mathrm{T}'(\nu); \quad (i,j) \mapsto (p+i, p+j)$$

leképezés bijekció, ezért $\mathrm{Card}\,(\mathrm{T}'(\nu)) = \mathrm{Card}\,(\mathrm{T}(\nu))$. Megmutatjuk, hogy az

$$f : \mathrm{T}'(\sigma) \to \mathrm{T}(\sigma); \quad (i,j) \mapsto (\mu(i), p+\nu(j-p))$$

leképezés bijekció. A μ és ν függvények injektivitásából azonnal következik f injektivitása. Az f függvény szürjektivitásának bizonyításához legyen $(i',j') \in \mathrm{T}(\sigma)$ rögzített. Ekkor $0 \leq i' < j' < p+q$ és $\sigma(i') > \sigma(j')$. Ha $j' \leq p$ teljesülne, akkor $i', j' \in [\![0,p[\![$ és $\sigma \in \mathfrak{S}_{(p,q)}$ miatt σ növő a $[\![0,p[\![$ halmazon, így $\sigma(i') < \sigma(j')$, ami lehetetlen. Ha $p \leq i'$ teljesülne, akkor $i', j' \in [\![p,p+q[\![$ és $\sigma \in \mathfrak{S}_{(p,q)}$ miatt σ növő a $[\![p,p+q[\![$ halmazon, így $\sigma(i') < \sigma(j')$, ami lehetetlen. Ezért szükségképpen $i' < p \leq j' < p+q$, így $\mu \in \mathfrak{S}_p$ és $\nu \in \mathfrak{S}_q$ alapján léteznek olyan $i \in p$ és $j \in q$ számok, amelyekre $\mu(i) = i'$ és $\nu(j) = j'-p$. Ez azt jelenti, hogy $(i, p+j) \in p \times (p+q)$ olyan pár, hogy $i < p \leq p+j$ és az $(i',j') \in \mathrm{T}(\sigma)$ feltétel alapján $\sigma(\mu(i)) = \sigma(i') > \sigma(j') = \sigma(p+\nu((p+j)-p))$, vagyis $(i, p+j) \in \mathrm{T}'(\sigma)$, ugyanakkor $f(i,p+j) = (\mu(i), p+\nu(j)) = (i',j')$. Ezért az f függvény szürjektív is, így bijekció $\mathrm{T}'(\sigma)$ és $\mathrm{T}(\sigma)$ között. Ezért fennáll a $\mathrm{Card}(\mathrm{T}'(\sigma)) = \mathrm{Card}(\mathrm{T}(\sigma)$ egyenlőség is, tehát (2)-ből kapjuk, hogy

$$\mathrm{Card}\,(\mathrm{T}(\varrho_{\mu,\nu,\sigma})) = \mathrm{Card}\,(\mathrm{T}(\mu)) + \mathrm{Card}\,(\mathrm{T}(\nu)) + \mathrm{Card}\,(\mathrm{T}(\sigma)).$$

Ebből 13.3.4. alapján következik, hogy

$$\begin{aligned} \varepsilon_{p+q}(\varrho_{\mu,\nu,\sigma}) &= (-1)^{\mathrm{Card}(\mathrm{T}(\varrho_{\mu,\nu,\sigma}))} = \\ &= (-1)^{\mathrm{Card}(\mathrm{T}(\mu))}(-1)^{\mathrm{Card}(\mathrm{T}(\nu))}(-1)^{\mathrm{Card}(\mathrm{T}(\sigma))} = \varepsilon_p(\mu)\varepsilon_q(\nu)\varepsilon_{p+q}(\sigma). \end{aligned}$$

Végül megmutatjuk, hogy a

$$\mathfrak{S}_p \times \mathfrak{S}_q \times \mathfrak{S}_{p+q} \to \mathfrak{S}_{p+q}; \quad (\mu,\nu,\sigma) \mapsto \varrho_{\mu,\nu,\sigma} \tag{3}$$

leképezés bijekció.

A (3) függvény szürjektivitásának bizonyításához legyen $\tilde{\sigma} \in \mathfrak{S}_{p+q}$ rögzített. A 8.2.5. állítás szerint egyértelműen léteznek $\sigma_p : p \to \tilde{\sigma}\langle [\![0, p[\![\rangle$ és $\sigma_{p+q} : q \to \tilde{\sigma}\langle [\![p, p+q[\![\rangle$ szigorúan monoton növő bijekciók. Ekkor $\tilde{\sigma}|_{[\![0,p[\![} : [\![0, p[\![\to \tilde{\sigma}\langle [\![0, p[\![\rangle$ és $\sigma_p^{-1} : \tilde{\sigma}\langle [\![0, p[\![\rangle \to p$ bijekciók, így

$$\mu := \sigma_p^{-1} \circ \left(\tilde{\sigma}|_{[\![0,p[\![}\right) \in \mathfrak{S}_p.$$

Ugyanakkor a $\tau : q \to [\![p, p+q[\![;\ i \mapsto p+i$ függvény, és a $\tilde{\sigma}|_{[\![p,p+q[\![} : [\![p, p+q[\![\to \tilde{\sigma}\langle [\![p, p+q[\![\rangle$, valamint $\sigma_{p+q}^{-1} : \tilde{\sigma}\langle [\![p, p+q[\![\rangle \to q$ függvények bijekciók, így

$$\nu := \sigma_{p+q}^{-1} \circ \tilde{\sigma}|_{[\![p,p+q[\![} \circ \tau \in \mathfrak{S}_q.$$

Végül bevezetjük a

$$\sigma : p+q \to p+q; \quad i \mapsto \begin{cases} \sigma_p(i) & \text{, ha } i < p, \\ \left(\sigma_{p+q} \circ \tau^{-1}\right)(i) & \text{, ha } p \leq i < p+q \end{cases}$$

leképezést. Nyilvánvaló, hogy σ injektív, mert a definíció szerint injektív a $[\![0, p[\![$ és $[\![p, p+q[\![$ halmazokon, valamint $\sigma\langle [\![0, p[\![\rangle = \operatorname{Im}(\sigma_p) = \tilde{\sigma}\langle [\![0, p[\![\rangle$ és $\sigma\langle [\![p, p+q[\![\rangle = \operatorname{Im}(\sigma_{p+q}) = \tilde{\sigma}\langle [\![p, p+q[\![\rangle$ diszjunkt halmazok. Ezért $\sigma \in \mathfrak{S}_{p+q}$, és a definíció alapján világos, hogy σ növő a $[\![0, p[\![$ és $[\![p, p+q[\![$ halmazokon, tehát $\sigma \in \mathfrak{S}_{(p,q)}$, következésképpen $(\mu, \nu, \sigma) \in \mathfrak{S}_p \times \mathfrak{S}_q \times \mathfrak{S}_{(p,q)}$.

Ha $i \in p$, akkor $\varrho_{\mu,\nu,\sigma}(i) = \sigma(\mu(i)) = \sigma_p(\mu(i)) = \tilde{\sigma}(i)$, hiszen $\mu(i) < p$. Ha $i \in [\![p, p+q[\![$, akkor $\varrho_{\mu,\nu,\sigma}(i) = \sigma(p + \nu(i-p)) = \left(\sigma_{p+q} \circ \tau^{-1}\right)(\tau(\nu(i-p))) = \sigma_{p+q}(\nu(i-p)) = \tilde{\sigma}(i)$, hiszen a definíciók szerint $\sigma_{p+q} \circ \nu \circ \tau^{-1} = \tilde{\sigma}|_{[\![p,p+q[\![}$. Ez azt jelenti, hogy $\varrho_{\mu,\nu,\sigma} = \tilde{\sigma}$, tehát a (3) függvény szürjektív.

A (3) függvény injektivitásának bizonyításához legyenek $(\mu, \nu, \sigma), (\mu', \nu', \sigma') \in \mathfrak{S}_p \times \mathfrak{S}_q \times \mathfrak{S}_{(p,q)}$ olyan hármasok, amelyekre $\varrho_{\mu,\nu,\sigma} = \tilde{\sigma} = \varrho_{\mu',\nu',\sigma'}$. Ekkor $\mu, \mu' \in \mathfrak{S}_p$ miatt

$$\begin{gathered} \sigma\langle [\![0, p[\![\rangle = \sigma\langle \mu\langle [\![0, p[\![\rangle \rangle = \\ = \varrho_{\mu,\nu,\sigma}\langle [\![0, p[\![\rangle = \tilde{\sigma}\langle [\![0, p[\![\rangle = \varrho_{\mu',\nu',\sigma'}\langle [\![p, p+q[\![\rangle = \\ = \sigma'\langle \mu'\langle [\![0, p[\![\rangle \rangle = \sigma'\langle [\![0, p[\![\rangle, \end{gathered}$$

tehát mind $\sigma|_{[\![0,p[\![}$, mind $\sigma'|_{[\![0,p[\![}$ olyan $p \to \tilde{\sigma}\langle [\![0, p[\![\rangle$ függvények, amelyek szigorúan monoton növekvőek, hiszen $\sigma, \sigma' \in \mathfrak{S}_p$. Ezért a 8.2.5. állításban szereplő egyértelműség miatt $\sigma|_{[\![0,p[\![} = \sigma'|_{[\![0,p[\![}$. Ebből következik, hogy

$$\sigma|_{[\![0,p[\![} \circ \mu = \tilde{\sigma}|_{[\![0,p[\![} = \sigma'|_{[\![0,p[\![} \circ \mu',$$

következésképpen $\mu = \mu'$. Továbbá, ismét τ-val jelölve a $q \to [\![p, p+q[\![;\ i \mapsto p+i$ függvényt, fennállnak a

$$\begin{gathered} \left(\left(\sigma|_{[\![p,p+q[\![}\right) \circ \tau\right) \langle [\![0, q[\![\rangle = \sigma\langle \{p + j | j \in q\} \rangle = \sigma\langle \{p + \nu(i-p) | i \in [\![p, p+q[\![\} \rangle = \\ = \varrho_{\mu,\nu,\sigma}\langle [\![p, p+q[\![\rangle = \tilde{\sigma}\langle [\![p, p+q[\![\rangle = \varrho_{\mu',\nu',\sigma'}\langle [\![p, p+q[\![\rangle = \\ = \sigma'\langle \{p + \nu'(i-p) | i \in [\![p, p+q[\![\} \rangle = \sigma'\langle \{p + j | j \in q\} \rangle = \left(\left(\sigma'|_{[\![p,p+q[\![}\right) \circ \tau\right) \langle [\![0, q[\![\rangle \end{gathered}$$

egyenlőségek, tehát mind $\left(\sigma|_{[\![p,p+q[\![}\right) \circ \tau$, mind $\left(\sigma'|_{[\![p,p+q[\![}\right) \circ \tau$ olyan $q \to \tilde{\sigma}\langle [\![p, p+q[\![\rangle$ függvények, amelyek szigorúan monoton növekvőek, hiszen $\sigma, \sigma' \in \mathfrak{S}_p$. Ezért a 8.2.5. állításban szereplő egyértelműség miatt $\sigma|_{[\![p,p+q[\![} \circ \tau = \sigma'|_{[\![0,p[\![} \circ \tau$, tehát $\sigma|_{[\![p,p+q[\![} = \sigma'|_{[\![p,p+q[\![}$. Ebből következik, hogy $\sigma = \sigma'$, és minden $j \in q$ esetén

$$(\sigma \circ \tau)(\nu(j)) = \sigma(p + \nu(j)) = \varrho_{\mu,\nu,\sigma}(p+j) = \varrho_{\mu',\nu',\sigma'}(p+j) = \sigma'(p + \nu(j)) = (\sigma' \circ \tau)(\nu(j)),$$

tehát $\sigma \circ \tau = \sigma' \circ \tau$ miatt $\nu(j) = \nu'(j)$, tehát $\nu = \nu'$. Ezzel bebizonyítottuk, hogy $(\mu, \nu, \sigma) = (\mu', \nu', \sigma')$, tehát a (3) leképezés injektív. ■

20.3.8. Állítás. *Legyenek E, F, G és H vektorterek a 0 karakterisztikájú K test felett, és $\mathbf{b} : F \times G \to H$ bilineáris operátor. Ha $p, q \in \mathbb{N}^*$ és $u \in \mathbf{A}_p(E; F)$ és $v \in \mathbf{A}_q(E; G)$, akkor az*

$$u \underset{(\mathbf{b})}{\otimes} v : E^{p+q} \to H; \quad (x_i)_{i \in p+q} \mapsto \mathbf{b}\left(u\left((x_i)_{i \in p}\right), v\left((x_{p+i})_{i \in q}\right)\right)$$

leképezés multilineáris operátor (tehát eleme $\mathbf{L}_{p+q}(E; H)$-nak), és

$$u \underset{(\mathbf{b})}{\bigwedge} v = \frac{(p+q)!}{p!q!} \mathbb{A}_{p+q}\left(u \underset{(\mathbf{b})}{\otimes} v\right).$$

Bizonyítás. Először megmutatjuk, hogy az $u \underset{(\mathbf{b})}{\otimes} v : E^{p+q} \to H$ leképezés $(p+q)$-lineáris operátor. Ehhez legyenek $k \in p+q$ és $\mathbf{x} = (x_i)_{i \in p+q} \in E^{p+q}$ rögzítettek. Ekkor minden $x \in E$ esetén

$$\left(\left(u \underset{(\mathbf{b})}{\otimes} v\right) \circ \mathrm{in}_{k,\mathbf{x}}\right)(x) = \left(u \underset{(\mathbf{b})}{\otimes} v\right)(\mathrm{in}_{k,\mathbf{x}}(x)) = \mathbf{b}\left(\left((\mathrm{in}_{k,\mathbf{x}}(x))_i\right)_{i \in p}, \left((\mathrm{in}_{k,\mathbf{x}}(x))_{p+i}\right)_{i \in q}\right) =$$
$$= \begin{cases} \mathbf{b}\left(\left(u \circ \mathrm{in}_{k,(x_i)_{i \in p}}\right)(x), v\left((x_{p+i})_{i \in q}\right)\right) & \text{, ha } k < p, \\ \mathbf{b}\left(u\left((x_i)_{i \in p}\right), \left(v \circ \mathrm{in}_{k,(x_{p+i})_{i \in q}}\right)(x)\right) & \text{, ha } p \le k < p+q, \end{cases}$$

tehát $k < p$ esetén

$$\left(u \underset{(\mathbf{b})}{\otimes} v\right) \circ \mathrm{in}_{k,\mathbf{x}} = \mathbf{b}\left(\cdot, v\left((x_{p+i})_{i \in q}\right)\right) \circ \left(u \circ \mathrm{in}_{k,(x_i)_{i \in p}}\right)$$

lineáris operátor, és $p \le k < p+q$ esetén

$$\left(u \underset{(\mathbf{b})}{\otimes} v\right) \circ \mathrm{in}_{k,\mathbf{x}} = \mathbf{b}\left(u\left((x_i)_{i \in p}\right), \cdot\right) \circ \left(v \circ \mathrm{in}_{k,(x_{p+i})_{i \in q}}\right)$$

lineáris operátor. Ezért az $u \underset{(\mathbf{b})}{\otimes} v : E^{p+q} \to H$ leképezés $(p+q)$-lineáris operátor.

Ha $(x_i)_{i \in p+q} \in E^{p+q}$, akkor

$$\left(\mathbb{A}_{p+q}\left(u \underset{(\mathbf{b})}{\otimes} v\right)\right)((x_i)_{i \in p+q}) \overset{(1)}{=} \frac{1}{(p+q)!} \sum_{\tilde\sigma \in \mathfrak{S}_{p+q}} \varepsilon_{p+q}(\tilde\sigma) \left(u \underset{(\mathbf{b})}{\otimes} v\right)\left(\left(x_{\tilde\sigma(i)}\right)_{i \in p+q}\right) \overset{(2)}{=}$$
$$\overset{(2)}{=} \frac{1}{(p+q)!} \sum_{\tilde\sigma \in \mathfrak{S}_{p+q}} \varepsilon_{p+q}(\tilde\sigma) \mathbf{b}\left(u\left(\left(x_{\tilde\sigma(i)}\right)_{i \in p}\right), v\left(\left(x_{\tilde\sigma(p+i)}\right)_{i \in q}\right)\right) \overset{(3)}{=}$$
$$\overset{(3)}{=} \frac{1}{(p+q)!} \sum_{\substack{(\mu,\nu,\sigma) \in \\ \in \mathfrak{S}_p \times \mathfrak{S}_q \times \mathfrak{S}_{(p,q)}}} \varepsilon_{p+q}(\varrho_{\mu,\nu,\sigma}) \mathbf{b}\left(u\left(\left(x_{\varrho_{\mu,\nu,\sigma}(i)}\right)_{i \in p}\right), v\left(\left(x_{\varrho_{\mu,\nu,\sigma}(p+i)}\right)_{i \in q}\right)\right) \overset{(4)}{=}$$
$$\overset{(4)}{=} \frac{1}{(p+q)!} \sum_{\sigma \in \mathfrak{S}_{(p,q)}} \sum_{\substack{\mu \in \mathfrak{S}_p \\ \nu \in \mathfrak{S}_q}} \varepsilon_p(\mu)\varepsilon_q(\nu)\varepsilon_{p+q}(\sigma) \mathbf{b}\left(u\left(\left(x_{\sigma(\mu(i))}\right)_{i \in p}\right), v\left(\left(x_{\sigma(p+\nu(i))}\right)_{i \in q}\right)\right) \overset{(5)}{=}$$

$$\overset{(5)}{=} \frac{1}{(p+q)!} \sum_{\sigma \in \mathfrak{S}_{(p,q)}} \sum_{\substack{\mu \in \mathfrak{S}_p \\ \nu \in \mathfrak{S}_q}} \varepsilon_p(\mu)\varepsilon_q(\nu)\varepsilon_{p+q}(\sigma)\mathbf{b}\left(\varepsilon_p(\mu)u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right), \varepsilon_q(\nu)v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right)\right) \overset{(6)}{=}$$

$$\overset{(6)}{=} \frac{1}{(p+q)!} \sum_{\sigma \in \mathfrak{S}_{(p,q)}} \varepsilon_{p+q}(\sigma) \sum_{\substack{\mu \in \mathfrak{S}_p \\ \nu \in \mathfrak{S}_q}} \varepsilon_p(\mu)^2\varepsilon_q(\nu)^2\mathbf{b}\left(u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right), v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right)\right) \overset{(7)}{=}$$

$$\overset{(7)}{=} \frac{p!q!}{(p+q)!} \sum_{\sigma \in \mathfrak{S}_{(p,q)}} \varepsilon_{p+q}(\sigma)\mathbf{b}\left(u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right), v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right)\right) \overset{(8)}{=}$$

$$\overset{(8)}{=} \frac{p!q!}{(p+q)!} \left(u \underset{(\mathbf{b})}{\bigwedge} v\right) \left((x_i)_{i\in p+q}\right),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél az antiszimetrizáció definícióját, és a $\overset{(2)}{=}$ egyenlőségnél az $u \underset{(\mathbf{b})}{\bigotimes} v$ multilineáris operátor definícióját alkalmaztuk;

– a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk az előző lemmában bevezetett

$$\mathfrak{S}_p \times \mathfrak{S}_q \times \mathfrak{S}_{p+q} \to \mathfrak{S}_{p+q}; \quad (\mu, \nu, \sigma) \mapsto \varrho_{\mu,\nu,\sigma}$$

bijekciót ahhoz, hogy alkalmazhassuk a H vektortér összeadás-függvényének általános kommutativitását;

– a $\overset{(4)}{=}$ egyenlőségnél az előző lemmában igazolt, előjel-függvényekre vonatkozó egyenlőséget alkalmaztuk;

– az $\overset{(5)}{=}$ egyenlőségnél kihasználtuk az u és v multilineáris operátorok antiszimmetrikusságát;

– a $\overset{(6)}{=}$ egyenlőség a $\mathbf{b}$ leképezés biadditivitása miatt teljesül;

– a $\overset{(7)}{=}$ egyenlőségnél felhasználtuk a

$$\sum_{\substack{\mu \in \mathfrak{S}_p \\ \nu \in \mathfrak{S}_q}} \varepsilon_p(\mu)^2\varepsilon_q(\nu)^2 = \left(\sum_{\mu \in \mathfrak{S}_p} 1\right)\left(\sum_{\nu \in \mathfrak{S}_q} 1\right) = \mathrm{Card}\,(\mathfrak{S}_p)\,\mathrm{Card}\,(\mathfrak{S}_q) = p!q!$$

egyenlőséget;

– a $\overset{(8)}{=}$ egyenlőségnél a multilineáris operátorok külső szorzatának definícióját alkalmaztuk. ■

20.4. A külső szorzás antikommutativitása

20.4.1. Definíció. *Ha $p, q \in \mathbb{N}^*$, akkor*

$$\sigma_{p,q} : p+q \to q+p; \quad i \mapsto \begin{cases} p+i & , \text{ha } 0 \le i < q, \\ i-q & , \text{ha } q \le i < q+p. \end{cases}$$

20.4.2. Lemma. a) *Ha $p, q \in \mathbb{N}^*$, akkor $\sigma_{p,q} \in \mathfrak{S}_{(q,p)}$, és*

$$\varepsilon_{p+q}(\sigma_{p,q}) = (-1)^{pq},$$
$$\sigma_{p,q}^{-1} = \sigma_{q,p},$$

továbbá, minden $\sigma \in \mathfrak{S}_{(p,q)}$ *esetén* $\sigma \circ \sigma_{p,q} \in \mathfrak{S}_{(q,p)}$*, és az*

$$\mathfrak{S}_{(p,q)} \to \mathfrak{S}_{(q,p)}; \quad \sigma \mapsto \sigma \circ \sigma_{p,q}$$

leképezés bijekció.

b) *Ha* $p, q, r \in \mathbb{N}^*$*, akkor minden* $\sigma \in \mathfrak{S}_{(p,q,r)}$ *esetén* $\sigma \circ \sigma_{p,q+r} \in \mathfrak{S}_{(q,r,p)}$*, és az*

$$\mathfrak{S}_{(p,q,r)} \to \mathfrak{S}_{(q,r,p)}; \quad \sigma \mapsto \sigma \circ \sigma_{p,q+r}$$

leképezés bijekció.

Bizonyítás. a) A $\sigma_{p,q}$ függvény nyilvánvalóan injektív a $[\![0,q[\![$ és $[\![q,p+q[\![$ halmazokon, továbbá $i \in [\![0,q[\![$ és $j \in [\![q,p+q[\![$ esetén $\sigma_{p,q}(j) = j - q < p \leq p + i = \sigma_{p,q}(i)$, ezért $\sigma_{p,q}$ injekció. A definíció szerint világos, hogy $\sigma_{p,q}$ növő a $[\![0,q[\![$ és $[\![q,p+q[\![$ halmazokon, ezért $\sigma_{p,q} \in \mathfrak{S}_{(q,p)}$.

Vezessük be a

$$\mathrm{T}\left(\sigma_{p,q}\right) := \{(i,j) \in (p+q) \times (p+q) | (i < j) \wedge (\sigma_{p,q}(i) > \sigma_{p,q}(j))\}$$

halmazt, amelyre 13.3.4. alapján $\varepsilon_{p+q}\left(\sigma_{p,q}\right) = (-1)^{\mathrm{Card}(\mathrm{T}(\sigma_{p,q}))}$ teljesül. Ha $(i,j) \in \mathrm{T}\left(\sigma_{p,q}\right)$, akkor $j < q$ vagy $q \leq i$ lehetetlen, mert $\sigma_{p,q}$ a $[\![0,q[\![$ és $[\![q,p+q[\![$ halmazokon növő, ezért $i < q \leq j < p + q$. Megfordítva, $i, j \in \mathbb{N}$ olyanok, hogy $i < q \leq j < p + q$, akkor $\sigma_{p,q}(i) = p + i \geq p > j - q = \sigma_{p,q}(j)$, tehát $(i,j) \in \mathrm{T}\left(\sigma_{p,q}\right)$. Ebből következik, hogy

$$\mathrm{T}\left(\sigma_{p,q}\right) = \{(i,j) \in \mathbb{N} \times \mathbb{N}\} | i < q \leq j < p + q\} = \bigcup_{i \in q} \{(i,j) \in \mathbb{N} \times \mathbb{N}\} | q \leq j < p + q\},$$

ezért $\mathrm{Card}\left(\mathrm{T}\left(\sigma_{p,q}\right)\right) = \sum_{i \in q} \mathrm{Card}\{(i,j) | q \leq j < q + p\} = pq$, hiszen minden $i \in q$ esetén $\mathrm{Card}\{(i, q+j) | q \leq j < q + p\} = p$. Tehát $\varepsilon_{p+q}\left(\sigma_{p,q}\right) = (-1)^{pq}$.

Legyen $\sigma \in \mathfrak{S}_{(p,q)}$. Mivel $\sigma_{p,q}$ növő a $[\![0,q[\![$ halmazon és $\sigma_{p,q}\langle[\![0,q[\![\rangle = [\![p,p+q[\![$, valamint σ növő a $[\![p,p+q[\![$ halmazon, így $\sigma \circ \sigma_{p,q}$ növő a $[\![0,q[\![$ halmazon. Mivel $\sigma_{p,q}$ növő a $[\![q,p+q[\![$ halmazon és $\sigma_{p,q}\langle[\![q,p+q[\![\rangle = [\![0,p[\![$, valamint σ növő a $[\![0,p[\![$ halmazon, így $\sigma \circ \sigma_{p,q}$ növő a $[\![q,,p+q[\![$ halmazon. Ezért $\sigma \circ \sigma_{p,q} \in \mathfrak{S}_{(q,p)}$.

Ha $i \in [\![0,q[\![$, akkor $\left(\sigma_{q,p} \circ \sigma_{p,q}\right)(i) = \sigma_{q,p}(p+i) = (p+i) - p = i$, és ha $i \in [\![q,p+q[\![$, akkor $\left(\sigma_{q,p} \circ \sigma_{p,q}\right)(i) = \sigma_{q,p}(i-q) = q + (i-q) = i$, tehát $\sigma_{q,p} \circ \sigma_{p,q} = \mathrm{id}_{p+q}$, vagyis $\sigma_{p,q}^{-1} = \sigma_{q,p}$. Ebből következik, hogy az

$$\mathfrak{S}_{(p,q)} \to \mathfrak{S}_{(q,p)}; \quad \sigma \mapsto \sigma \circ \sigma_{p,q}$$

leképezésnek inverze az

$$\mathfrak{S}_{(q,p)} \to \mathfrak{S}_{(p,q)}; \quad \sigma \mapsto \sigma \circ \sigma_{q,p}$$

leképezés.

b) Legyen $\sigma \in \mathfrak{S}_{(p,q,r)}$. A $\sigma_{p,q+r}$ függvény növő a $[\![0,q[\![$ halmazon és $\sigma_{p,q+r}\langle[\![0,q[\![\rangle = [\![p,p+q[\![$, és σ növő a $[\![p,p+q[\![$ halmazon, ezért $\sigma \circ \sigma_{p,q+r}$ növő a $[\![0,q[\![$ halmazon. A $\sigma_{p,q+r}$ függvény növő a $[\![q,q+r[\![$ halmazon és $\sigma_{p,q+r}\langle[\![q,q+r[\![\rangle = [\![p+q,p+q+r[\![$, és σ növő a $[\![p+q,p+q+r[\![$ halmazon, ezért $\sigma \circ \sigma_{p,q+r}$ növő a $[\![q,q+r[\![$ halmazon. A $\sigma_{p,q+r}$ függvény növő a $[\![q+r,q+r+p[\![$ halmazon és $\sigma_{p,q+r}\langle[\![q+r,q+r+p[\![\rangle = [\![0,p[\![$, és σ növő a $[\![0,p[\![$ halmazon, ezért $\sigma \circ \sigma_{p,q+r}$ növő a $[\![q+r,q+r+p[\![$ halmazon. Ez azt jelenti, hogy $\sigma \circ \sigma_{p,q+r} \in \mathfrak{S}_{(q,r,p)}$.

Legyen $\sigma' \in \mathfrak{S}_{(q,r,p)}$. A $\sigma_{q+r,p}$ függvény növő a $[\![0,p[\![$ halmazon és $\sigma_{q+r,p}\langle[\![0,p[\![\rangle = [\![q+r, q+r+p[\![$, és σ' növő a $[\![q+r, q+r+p[\![$ halmazon, ezért $\sigma' \circ \sigma_{q+r,p}$ növő a $[\![0,p[\![$ halmazon. A $\sigma_{q+r,p}$ függvény növő a $[\![p, p+q[\![$ halmazon és $\sigma_{q+r,p}\langle[\![p,p+q[\![\rangle = [\![0,q[\![$, és σ' növő a $[\![0,q[\![$ halmazon, ezért $\sigma' \circ \sigma_{q+r,p}$ növő a $[\![p,p+q[\![$ halmazon. A $\sigma_{q+r,p}$ függvény növő a $[\![p+q, p+q+r[\![$ halmazon és $\sigma_{q+r,p}\langle[\![p+q, p+q+r[\![\rangle = [\![q, q+r[\![$, és σ' növő a $[\![q, q+r[\![$ halmazon, ezért $\sigma' \circ \sigma_{q+r,p}$ növő a $[\![p+q, p+q+r[\![$ halmazon. Ez azt jelenti, hogy $\sigma' \circ \sigma_{q+r,p} \in \mathfrak{S}_{(p,q,r)}$.

Az a) állítás szerint $\sigma_{q+r,p} = \sigma_{p,q+r}^{-1}$, ezért az előzek alapján az

$$\mathfrak{S}_{(p,q,r)} \to \mathfrak{S}_{(q,r,p)}; \quad \sigma \mapsto \sigma \circ \sigma_{p,q+r}$$

leképezésnek inverze az

$$\mathfrak{S}_{(q,r,p)} \to \mathfrak{S}_{(p,q,r)}; \quad \sigma' \mapsto \sigma' \circ \sigma_{q+r,p}$$

leképezés. ■

20.4.3. Állítás. *Legyenek E, F, G és H vektorterek, valamint $\mathbf{b} : F \times G \to H$ bilineáris operátor. Vezessük be a*

$$\check{\mathbf{b}} : G \times F \to H; \quad (z, y) \mapsto (y, z)$$

bilineáris operátort. Ha $p, q \in \mathbb{N}^*$, valamint $u \in \mathbf{A}_p(E; F)$ és $v \in \mathbf{A}_q(E; G)$, akkor

$$v \underset{(\check{\mathbf{b}})}{\bigwedge} u = (-1)^{pq}\, u \underset{(\mathbf{b})}{\bigwedge} v.$$

Bizonyítás. Minden $(x_i)_{i \in p+q} \in E^{p+q}$ esetén

$$\begin{aligned}
&(v \underset{(\check{\mathbf{b}})}{\bigwedge} u)\left((x_i)_{i\in q+p}\right) = \sum_{\sigma' \in \mathfrak{S}_{(q,p)}} \varepsilon_{q+p}(\sigma')\check{\mathbf{b}}\left(v\left(\left(x_{\sigma'(i)}\right)_{i\in q}\right), u\left(\left(x_{\sigma'(q+i)}\right)_{i\in p}\right)\right) \overset{(1)}{=} \\
&\overset{(1)}{=} \sum_{\sigma \in \mathfrak{S}_{(p,q)}} \varepsilon_{q+p}(\sigma \circ \sigma_{p,q})\check{\mathbf{b}}\left(v\left(\left(x_{\sigma(\sigma_{p,q}(i))}\right)_{i\in q}\right), u\left(\left(x_{\sigma(\sigma_{p,q}(q+i))}\right)_{i\in p}\right)\right) = \\
&= \varepsilon_{q+p}\left(\sigma_{p,q}\right) \sum_{\sigma \in \mathfrak{S}_{(p,q)}} \varepsilon_{q+p}(\sigma)\check{\mathbf{b}}\left(v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right), u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right)\right) \overset{(2)}{=} \\
&\overset{(2)}{=} (-1)^{pq} \sum_{\sigma \in \mathfrak{S}_{(p,q)}} \varepsilon_{q+p}(\sigma)\mathbf{b}\left(u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right), v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right)\right) = (-1)^{pq}\, (u \underset{(\mathbf{b})}{\bigwedge} v)\left((x_i)_{i\in p+q}\right),
\end{aligned} \tag{20.1}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk azt, hogy az előző lemma szerint a

$$\mathfrak{S}_{(p,q)} \to \mathfrak{S}_{(q,p)}; \quad \sigma \mapsto \sigma \circ \sigma_{p,q}$$

leképezés bijekció és a G-beli összeadásra alkalmaztuk az általános kommutativitás tételét;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk az előző lemma a) pontjában igazolt $\varepsilon_{p+q}\left(\sigma_{p,q}\right) = (-1)^{pq}$ összefüggést és a $\check{\mathbf{b}}$ bilineáris operátor definícióját. ■

20.4.4. Következmény. (**A külső szorzás antikommutativitása.**) *Legyenek E, F és H vektorterek, $p, q \in \mathbb{N}^*$, valamint $\mathbf{b} : F \times F \to H$ szimmetrikus bilineáris operátor. Ha $u \in \mathbf{A}_p(E; F)$ és $v \in \mathbf{A}_q(E; F)$, akkor*

$$v \bigwedge_{(\mathbf{b})} u = (-1)^{pq}\, u \bigwedge_{(\mathbf{b})} v.$$

Bizonyítás. Nyilvánvalóan következik az előző állításból, mert $\mathbf{b}$ szimmetrikussága pontosan azt jelenti, hogy $\check{\mathbf{b}} = \mathbf{b}$. ■

Figyeljük meg, hogy az antikommutativitás formula érvényességéhez egészen lényeges a $\mathbf{b}$ bilineáris operátor *szimmetrikussága.*

20.5. A külső szorzás asszociativitása

20.5.1. Lemma. *Legyenek $p, q, r \in \mathbb{N}^*$.*
Minden $(\sigma, \sigma') \in \mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)}$ esetén a

$$\pi_{\sigma,\sigma'} : p+q+r \to p+q+r; \quad i \mapsto \begin{cases} \sigma(\sigma'(i)) & , \text{ha } i < p+q, \\ \sigma(i) & , \text{ha } p+q \le i < p+q+r \end{cases}$$

függvényre $\pi_{\sigma,\sigma'} \in \mathfrak{S}_{(p,q,r)}$ teljesül, és

$$\varepsilon_{p+q+r}\left(\pi_{\sigma,\sigma'}\right) = \varepsilon_{p+q+r}(\sigma)\varepsilon_{p+q}(\sigma'),$$

továbbá, a

$$\mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)} \to \mathfrak{S}_{(p,q,r)}; \quad (\sigma, \sigma') \mapsto \pi_{\sigma,\sigma'}$$

függvény bijekció.

Bizonyítás. Legyen $(\sigma, \sigma') \in \mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)}$ rögzített.
Megmutatjuk, hogy $\pi_{\sigma,\sigma'} \in \mathfrak{S}_{(p,q,r)}$. Valóban, $\mathrm{Im}(\sigma') = [\![0, p+q[\![$, és σ növő ezen a halmazon (mert $\sigma \in \mathfrak{S}_{p+q,r}$), továbbá σ' növő a $[\![0, p[\![$ és $[\![p, p+q[\![$ halmazokon (mert $\sigma' \in \mathfrak{S}_{p,q}$), ezért $\sigma \circ \sigma'$ növő a $[\![0, p[\![$ és a $[\![p, p+q[\![$ halmazon. Továbbá, σ növő a $[\![p+q, p+q+r[\![$ halmazon (mert $\sigma \in \mathfrak{S}_{p+q,r}$). Ezért a definíció szerint a $\pi_{\sigma,\sigma'}$ függvény növő a $[\![0, p[\![$, a $[\![p, p+q[\![$ és $[\![p+q, p+q+r[\![$ halmazok mindegyikén. Világos, hogy $\pi_{\sigma,\sigma'}$ injekció, mert a $[\![0, p+q[\![$ halmazon egyenlő $\sigma \circ \sigma'$-vel, vagyis két injekció kompozíciójával, továbbá a $[\![p+q, p+q+r[\![$ halmazon egyenlő σ-val, ami szintén injekció, és végül $i \in [\![0, p+q[\![$ és $j \in [\![p+q, p+q+r[\![$ esetén $\pi_{\sigma,\sigma'}(i) = \sigma(\sigma'(i)) \neq \sigma(j) = \pi_{\sigma,\sigma'}(j)$, hiszen $\sigma'(i) < p+q \le j$ és σ injekció. Ezért $\pi_{\sigma,\sigma'} \in \mathfrak{S}_{p+q+r}$, és az imént igazolt monotonitási tulajdonságok alapján $\pi_{\sigma,\sigma'} \in \mathfrak{S}_{(p,q,r)}$.
Most igazoljuk az $\varepsilon_{p+q+r}(\pi_{\sigma,\sigma'}) = \varepsilon_{p+q+r}(\sigma)\varepsilon_{p+q}(\sigma')$ formulát. Ehhez legyen $n := p+q+r$ és vezessük be a következő halmazokat:

$$\begin{gathered} \mathrm{T}\left(\pi_{\sigma,\sigma'}\right) := \{(i,j) \in n \times n | (i < j) \wedge (\pi_{\sigma,\sigma'}(i) > \pi_{\sigma,\sigma'}(j))\}, \\ \mathrm{T}(\sigma) := \{(i,j) \in n \times n | (i < j) \wedge (\sigma(i) > \sigma(j)\}, \\ \mathrm{T}(\sigma') := \{(i,j) \in (p+q) \times (p+q) | (i < j) \wedge (\sigma'(i) > \sigma'(j)\}. \end{gathered}$$

A 13.3.4. tétel alapján ezekkel a halmazokkal a bizonyítandó egyenlőség így fejezhető ki:

$$(-1)^{\mathrm{Card}\left(\mathrm{T}\left(\pi_{\sigma,\sigma'}\right)\right)} = (-1)^{\mathrm{Card}(\mathrm{T}(\sigma))}(-1)^{\mathrm{Card}(\mathrm{T}(\sigma'))}. \tag{1}$$

A $\pi_{\sigma,\sigma'}$ permutáció (szigorúan monoton) növő a $[\![0,p[\![$, a $[\![p,p+q[\![$ és $[\![p+q,p+q+r[\![$ halmazok mindegyikén, ezért $(i,j) \in \mathrm{T}\,(\pi_{\sigma,\sigma'})$ esetén a következő három, páronként kizáró eset lehetséges:

1) $i < p \leq j < p+q$ és $\pi_{\sigma,\sigma'}(i) > \pi_{\sigma,\sigma'}(j)$;

2) $i < p < p+q \leq j$ és $\pi_{\sigma,\sigma'}(i) > \pi_{\sigma,\sigma'}(j)$;

3) $p \leq i < p+q \leq j$ és $\pi_{\sigma,\sigma'}(i) > \pi_{\sigma,\sigma'}(j)$.

Ezeknek megfelelően bevezetjük a következő halmazokat

$$\begin{aligned}
\mathrm{T}_1\,(\pi_{\sigma,\sigma'}) &:= \{(i,j) \in n \times n | (i < p \leq j < p+q) \wedge (\pi_{\sigma,\sigma'}(i) > \pi_{\sigma,\sigma'}(j))\},\\
\mathrm{T}_2\,(\pi_{\sigma,\sigma'}) &:= \{(i,j) \in n \times n | (i < p < p+q \leq j) \wedge (\pi_{\sigma,\sigma'}(i) > \pi_{\sigma,\sigma'}(j))\},\\
\mathrm{T}_3\,(\pi_{\sigma,\sigma'}) &:= \{(i,j) \in n \times n | (p \leq i < p+q \leq j) \wedge (\pi_{\sigma,\sigma'}(i) > \pi_{\sigma,\sigma'}(j))\},
\end{aligned}$$

tehát teljesül az, hogy

$$\mathrm{T}\,(\pi_{\sigma,\sigma'}) = \mathrm{T}_1\,(\pi_{\sigma,\sigma'}) \cup \mathrm{T}_2\,(\pi_{\sigma,\sigma'}) \cup \mathrm{T}_3\,(\pi_{\sigma,\sigma'})\,, \tag{2}$$

$$\mathrm{T}_1\,(\pi_{\sigma,\sigma'}) \cap \mathrm{T}_2\,(\pi_{\sigma,\sigma'}) = \mathrm{T}_1\,(\pi_{\sigma,\sigma'}) \cap \mathrm{T}_3\,(\pi_{\sigma,\sigma'}) = \mathrm{T}_2\,(\pi_{\sigma,\sigma'}) \cap \mathrm{T}_3\,(\pi_{\sigma,\sigma'}) = \emptyset. \tag{3}$$

A $\pi_{\sigma,\sigma'}$ permutáció definíciója szerint nyilvánvaló, hogy

$$\begin{aligned}
\mathrm{T}_1\,(\pi_{\sigma,\sigma'}) &:= \{(i,j) \in n \times n | (i < p \leq j < p+q) \wedge (\sigma(\sigma'(i)) > \sigma(\sigma'(j)))\},\\
\mathrm{T}_2\,(\pi_{\sigma,\sigma'}) &:= \{(i,j) \in n \times n | (i < p < p+q \leq j) \wedge (\sigma(\sigma'(i)) > \sigma(j))\},\\
\mathrm{T}_3\,(\pi_{\sigma,\sigma'}) &:= \{(i,j) \in n \times n | (p \leq i < p+q \leq j) \wedge (\sigma(\sigma'(i)) > \sigma(j))\}.
\end{aligned}$$

Ha $(i,j) \in \mathrm{T}_1\,(\pi_{\sigma,\sigma'})$, akkor $(i,j) \in (p+q) \times (p+q)$ és $i < j$ és mivel a σ függvény növő a $[\![0,p+q[\![$ halmazon és $\sigma'(i), \sigma'(j) \in [\![0,p+q[\![$, így $\sigma'(i) > \sigma'(j)$ teljesül, vagyis $(i,j) \in \mathrm{T}(\sigma')$. Megfordítva, legyen $(i,j) \in \mathrm{T}(\sigma')$. Ekkor $i < j < p+q$ és $\sigma'(i) > \sigma'(j)$. Továbbá, a σ' függvény növő a $[\![0,p[\![$ és $[\![p,p+q[\![$ halmazokon (hiszen $\sigma' \in \mathfrak{S}_{p,q}$), ezért szükségképpen $i < p \leq j$, mert

– ha $p \leq i$, akkor $i,j \in [\![p,p+q[\![$, így $\sigma'(i) < \sigma'(j)$ teljesülne, ami lehetetlen;

– ha $j < p$, akkor $i,j \in [\![0,p[\![$, így ismét $\sigma'(i) < \sigma'(j)$ teljesülne, ami lehetetlen.

Tehát ekkor $i < p \leq j < p+q$ és $\sigma'(i) > \sigma'(j)$, így $\sigma(\sigma'(i)) > \sigma(\sigma'(j))$ (hiszen $\sigma \in \mathfrak{S}_{p+q,r}$, tehát σ növő a $[\![0,p+q[\![$ halmazon), vagyis $(i,j) \in \mathrm{T}_1\,(\pi_{\sigma,\sigma'})$. Tehát

$$\mathrm{T}_1\,(\pi_{\sigma,\sigma'}) = \mathrm{T}(\sigma'). \tag{4}$$

Ha $(i,j) \in \mathrm{T}_2\,(\pi_{\sigma,\sigma'})$, akkor $i < p < p+q \leq j$ és $\sigma(\sigma'(i)) > \sigma(j)$, és mivel $\sigma'(i) < p+q \leq j$, így $(\sigma'(i),j) \in \mathrm{T}(\sigma)$. Ha $(i,j) \in \mathrm{T}_3\,(\pi_{\sigma,\sigma'})$, akkor $p \leq i < p+q \leq j$ és $\sigma(\sigma'(i)) > \sigma(j)$, és mivel $\sigma'(i) < p+q \leq j$, így ismét $(\sigma'(i),j) \in \mathrm{T}(\sigma)$. Tehát jól értelmezett az

$$\mathrm{T}_2\,(\pi_{\sigma,\sigma'}) \cup \mathrm{T}_3\,(\pi_{\sigma,\sigma'}) \to \mathrm{T}(\sigma); \quad (i,j) \mapsto (\sigma'(i),j) \tag{5}$$

leképezés. Ez a függvény injektív, mert ha $(i,j),(i',j') \in \mathrm{T}_2\,(\pi_{\sigma,\sigma'}) \cup \mathrm{T}_3\,(\pi_{\sigma,\sigma'})$ olyanok, hogy $(\sigma'(i),j) = (\sigma'(i'),j')$, akkor $j = j'$ és $\sigma'(i) = \sigma'(i')$, így σ' injektivitása miatt $i = i'$, tehát $(i,j) = (i',j')$. Ez a függvény szürjektív is. Valóban, legyen $(k,j) \in \mathrm{T}(\sigma)$ tetszőleges. Ekkor $k < j$ és $\sigma(k) > \sigma(j)$. Ebből következik, hogy $k < p+q \leq j$ teljesül, mert

– ha $p+q \leq k$, akkor $k \leq j$ miatt $k,j \in [\![p+q,p+q+r[\![$, így $\sigma(k) < \sigma(j)$ teljesülne, mert $\sigma \in \mathfrak{S}_{(p+q,r)}$ miatt σ növő a $[\![p+q,p+q+r[\![$ halmazon;

– ha $j < p+q$, akkor $k, j \in [\![0, p+q[\![$, így ismét $\sigma(k) < \sigma(k)$ teljesülne, mert $\sigma \in \mathfrak{S}_{(p+q,r)}$ miatt σ növő a $[\![0, p+q[\![$ halmazon;

így ellentmondásba kerülnénk a $\sigma(k) > \sigma(j)$ egyenlőtlenséggel. Tehát $k < p+q$, így $\sigma' \in \mathfrak{S}_{(p,q)} \subseteq \mathfrak{S}_{p+q}$ miatt egyértelműen létezik olyan $i \in p+q$, amelyre $\sigma'(i) = k$. Világos, hogy ekkor $i < p+q \leq j$ és $\sigma(\sigma'(i)) = \sigma(k) > \sigma(j)$, tehát $i \leq p$ esetén $(i,j) \in \mathrm{T}_2(\pi_{\sigma,\sigma'})$, míg $p \leq i$ esetén $(i,j) \in \mathrm{T}_3(\pi_{\sigma,\sigma'})$, vagyis $(i,j) \in \mathrm{T}_2(\pi_{\sigma,\sigma'}) \cup \mathrm{T}_3(\pi_{\sigma,\sigma'})$ olyan pár, amelyre $(\sigma'(i), j) = (k, j)$. Ez azt jelenti, hogy az (5)-ben értelmezett függvény bijekció, így (3) alapján kapjuk, hogy

$$\mathrm{Card}\,(\mathrm{T}_2(\pi_{\sigma,\sigma'})) + \mathrm{Card}\,(\mathrm{T}_3(\pi_{\sigma,\sigma'})) = \mathrm{Card}\,(\mathrm{T}(\sigma)).$$

Ebből, (2)-ből, (3)-ból és (4)-ből következik, hogy

$$\begin{aligned}\mathrm{Card}\,(\mathrm{T}(\pi_{\sigma,\sigma'})) = \mathrm{Card}\,(\mathrm{T}_1(\pi_{\sigma,\sigma'})) + \mathrm{Card}\,(\mathrm{T}_2(\pi_{\sigma,\sigma'})) + \mathrm{Card}\,(\mathrm{T}_3(\pi_{\sigma,\sigma'})) = \\ = \mathrm{Card}\,(\mathrm{T}(\sigma')) + \mathrm{Card}\,(\mathrm{T}(\sigma)),\end{aligned}$$

amiből kapjuk a bizonyítandó (1) egyenlőséget, tehát az

$$\varepsilon_{p+q+r}(\pi_{\sigma,\sigma'}) = \varepsilon_{p+q+r}(\sigma)\varepsilon_{p+q}(\sigma')$$

formulát.

Hátravan még a

$$\mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)} \to \mathfrak{S}_{(p,q,r)}; \quad (\sigma, \sigma') \mapsto \pi_{\sigma,\sigma'} \tag{6}$$

leképezés bijektivitásának bizonyítása. Ehhez legyenek $(\sigma, \sigma'), (\tau, \tau') \in \mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)}$ olyanok, hogy $\pi_{\sigma,\sigma'} = \pi_{\tau,\tau'}$. Ekkor

$$\sigma \circ \sigma' = \pi_{\sigma,\sigma'}|_{[\![0,p+q[\![} = \pi_{\tau,\tau'}|_{[\![0,p+q[\![} = \tau \circ \tau',$$

amiből, figyelembe véve az $\mathrm{Im}(\sigma') = [\![0, p+q[\![= \mathrm{Im}(\tau')$ egyenlőségeket következik, hogy $\sigma\langle[\![0, p+q[\![\rangle = \tau\langle[\![0, p+q[\![\rangle$. Ezért $(\tau^{-1} \circ \sigma)\langle[\![0, p+q[\![\rangle = [\![0, p+q[\![$, és σ szigorúan monoton növő a $[\![0, p+q[\![$ halmazon, és τ^{-1} szigorúan monoton növő a $tau\langle[\![0, p+q[\![\rangle$ halmazon, így $(\tau^{-1} \circ \sigma)|_{[\![0,p+q[\![} : [\![0, p+q[\![\to [\![0, p+q[\![$ szigorúan monoton növő bijekció. Ezért 6.13.11. szerint $(\tau^{-1} \circ \sigma)|_{[\![0,p+q[\![} = \mathrm{id}_{[\![0,p+q[\![}$, vagyis $\sigma|_{[\![0,p+q[\![} = \tau|_{[\![0,p+q[\![}$. Ugyanakkor a deiníció szerint nyilvánvaló, hogy $\sigma|_{[\![p+q,p+q+r[\![} = \pi_{\sigma,\sigma'}|_{[\![p+q,p+q+r[\![} = \pi_{\tau,\tau'}|_{[\![p+q,p+q+r[\![} = \tau|_{[\![p+q,p+q+r[\![}$. Ezért $\sigma = \tau$, amiből $\sigma \circ \sigma' = \tau \circ \tau'$ alapján következik, hogy $\sigma' = \tau'$. Ez azt jelenti, hogy a (6) leképezés injektív.

Végül, a (6) függvény szürjektivitásának bizonyításához legyen $\pi \in \mathfrak{S}_{(p,q,r)}$ rögzített: olyan $(\sigma, \sigma') \in \mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)}$ párt keresünk, amelyre $\pi_{\sigma,\sigma'} = \pi$. Világos, hogy $\mathrm{Card}\,(\pi\langle[\![0, p+q[\![\rangle) = p+q$, tehát 8.2.4. szerint létezik egyetlen olyan $\varrho : [\![0, p+q[\![\to \pi\langle[\![0, p+q[\![\rangle$ bijekció, amely szigorúan monoton növő. Legyen $\sigma' := \varrho^{-1} \circ \left(\pi|_{[\![0,p+q[\![}\right)$ és $\sigma : p+q+r \to p+q+r$ az a függvény, amelyre minden $i \in p+q+r$ esetén

$$\sigma(i) := \begin{cases} \varrho(i) & \text{, ha } 0 \leq i < p+q, \\ \pi(i) & \text{, ha } p+q \leq i < p+q+r. \end{cases}$$

Nyilvánvaló, hogy $\sigma' \in \mathfrak{S}_{p+q}$, továbbá π monoton növő a $[\![0, p[\![$ és $[\![p, p+q[\![$ halmazokon és ϱ^{-1} monoton növő a $\pi\langle[\![0, p+q[\![\rangle$ halmazon, így $\sigma' \in \mathfrak{S}_{p,q}$. Világos, hogy σ injektív a $[\![0, p+q[\![$ és $[\![p+q, p+q+r[\![$ halmazokon, és $\mathrm{Im}(\varrho) \cap \pi\langle[\![p+q, p+q+r[\![\rangle = \emptyset$, ezért σ injekció, tehát $\sigma \in \mathfrak{S}_{p+q+r}$. Ugyanakkor σ növő a $[\![0, p+q[\![$ halmazon, mert itt egyenlő ϱ-val, és σ növő a $[\![p+q, p+q+r[\![$ halmazon, mert itt egyenlő π-vel és $\pi \in \mathfrak{S}_{(p,q,r}$, ezért $\sigma \in \mathfrak{S}_{p+q,r}$. Ugyanakkor $\sigma \circ \sigma' = \pi|_{[\![0,p+q[\![}$ és $\sigma|_{[\![p+q,p+q+r[\![} = \pi|_{[\![p+q,p+q+r[\![}$, tehát $\pi_{\sigma,\sigma'} = \pi$. Ez azt jelenti, hogy a (6) leképezés szürjektív. ■

20.5.2. Állítás. (**A külső szorzás asszociativitása.**) *Legyen E vektortér a K test felett, $p, q, r \in \mathbb{N}^*$, és $u \in \mathbf{A}_p(E)$, $v \in \mathbf{A}_q(E)$, $w \in \mathbf{A}_r(E)$. Ekkor*

$$(u \bigwedge v) \bigwedge w = u \bigwedge v \bigwedge w = u \bigwedge (v \bigwedge w),$$

ahol $u \wedge v \wedge w := \bigwedge\limits_{i=0}^{2} u_i$, *az* $u_0 := u$, $u_1 := v$ *és* $u_2 := w$ *definíciókkal.*

Bizonyítás. (I) Először megmutatjuk, hogy

$$u \bigwedge v \bigwedge w = (u \bigwedge v) \bigwedge w.$$

Legyen $(x_i)_{i \in p+q+r} \in E^{p+q+r}$ rögzített elem. Ekkor

$$(u \bigwedge v \bigwedge w)\left((x_i)_{i\in p+q+r}\right) = \\ = \sum_{\pi \in \mathfrak{S}_{(p,q,r)}} \varepsilon_{p+q+r}(\pi) u\left(\left(x_{\pi(i)}\right)_{i\in p}\right) v\left(\left(x_{\pi(p+i)}\right)_{i\in q}\right) w\left(\left(x_{\pi(p+q+i)}\right)_{i\in r}\right).$$

Ezért az előző lemma a) pontjában értelmezett $\mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)} \to \mathfrak{S}_{(p,q,r)}$; $(\sigma, \sigma') \mapsto \pi_{\sigma,\sigma'}$ bijekciót alkalmazva, a K-beli összeadás általános kommutativitása alapján

$$(u \bigwedge v \bigwedge w)\left((x_i)_{i\in p+q+r}\right) = \\ \sum_{(\sigma,\sigma') \in \mathfrak{S}_{(p+q,r)} \times \mathfrak{S}_{(p,q)}} \varepsilon_{p+q+r}(\pi_{\sigma,\sigma'}) u\left(\left(x_{\pi_{\sigma,\sigma'}(i)}\right)_{i\in p}\right) v\left(\left(x_{\pi_{\sigma,\sigma'}(p+i)}\right)_{i\in q}\right) w\left(\left(x_{\pi_{\sigma,\sigma'}(p+q+i)}\right)_{i\in r}\right) \\ \overset{(1)}{=} \sum_{\sigma \in \mathfrak{S}_{(p+q,r)}} \sum_{\sigma' \in \mathfrak{S}_{(p,q)}} \varepsilon_{p+q+r}(\sigma)\varepsilon_{p+q}(\sigma') u\left(\left(x_{\sigma(\sigma'(i))}\right)_{i\in p}\right) v\left(\left(x_{\sigma(\sigma'(p+i))}\right)_{i\in q}\right) w\left(\left(x_{\sigma(p+q+i)}\right)_{i\in r}\right),$$

ahol a $\overset{(1)}{=}$ egyenlőségnél felhasználtuk az előző lemma a) pontjában szereplő definíciót és szignatúrákra vonatkozó egyenlőséget.

Ugyanakkor, $u \wedge v$ és $(u \wedge v) \wedge w$ definíciója szerint:

$$((u \bigwedge v) \bigwedge w)\left((x_i)_{i\in p+q+r}\right) = \\ \sum_{\sigma \in \mathfrak{S}_{(p+q,r)}} \varepsilon_{p+q+r}(\sigma)\,(u \bigwedge v)\left(\left(x_{\sigma(i)}\right)_{i\in p+q}\right) w\left(\left(x_{\sigma(p+q+i)}\right)_{i\in r}\right) = \\ \sum_{\sigma \in \mathfrak{S}_{(p+q,r)}} \varepsilon_{p+q+r}(\sigma)\Bigg(\sum_{\sigma' \in \mathfrak{S}_{(p,q)}} \varepsilon_{p+q}(\sigma') u\left(\left(x_{\sigma(\sigma'(i))}\right)_{i\in p}\right) v\left(\left(x_{\sigma(\sigma'(p+i))}\right)_{i\in q}\right)\Bigg) w\left(\left(x_{\sigma(p+q+i)}\right)_{i\in r}\right) \\ = \sum_{\sigma \in \mathfrak{S}_{(p+q,r)}} \sum_{\sigma' \in \mathfrak{S}_{(p,q)}} \varepsilon_{p+q+r}(\sigma)\varepsilon_{p+q}(\sigma') u\left(\left(x_{\sigma(\sigma'(i))}\right)_{i\in p}\right) v\left(\left(x_{\sigma(\sigma'(p+i))}\right)_{i\in q}\right) w\left(\left(x_{\sigma(p+q+i)}\right)_{i\in r}\right).$$

Ebből látható, hogy $(u \wedge v \wedge w)\left((x_i)_{i\in p+q+r}\right) = ((u \wedge v) \wedge w)\left((x_i)_{i\in p+q+r}\right)$, és mivel ez minden $(x_i)_{i\in p+q+r} \in E^{p+q+r}$ esetén igaz, így $u \wedge v \wedge w = (u \wedge v) \wedge w$.

(II) Bebizonyítjuk, hogy

$$v \bigwedge w \bigwedge u = (-1)^{p(q+r)}\,(u \bigwedge v \bigwedge w).$$

Legyen $(x_i)_{i\in q+r+p} \in E^{q+r+p}$ rögzített elem. Ekkor

$$(v \wedge w \wedge u)\left((x_i)_{i\in q+r+p}\right) =$$
$$= \sum_{\sigma\in\mathfrak{S}_{(q,r,p)}} \varepsilon_{q+r+p}(\sigma) v\left(\left(x_{\sigma(i)}\right)_{i\in q}\right) w\left(\left(x_{\sigma(q+i)}\right)_{i\in r}\right) u\left(\left(x_{\sigma(q+r+i)}\right)_{i\in p}\right) \overset{(1)}{=}$$
$$\sum_{\sigma\in\mathfrak{S}_{(p,q,r)}} \varepsilon_{q+r+p}(\sigma\circ\sigma_{p,q+r}) v\left(\left(x_{\sigma(\sigma_{p,q+r}(i))}\right)_{i\in q}\right) w\left(\left(x_{\sigma(\sigma_{p,q+r}(q+i))}\right)_{i\in r}\right) u\left(\left(x_{\sigma(\sigma_{p,q+r}(q+r+i))}\right)_{i\in p}\right)$$
$$\overset{(2)}{=} \varepsilon_{p+q+r}(\sigma_{p,q+r}) \sum_{\sigma\in\mathfrak{S}_{(p,q,r)}} \varepsilon_{p+q+r}(\sigma) v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right) w\left(\left(x_{\sigma(p+q+i)}\right)_{i\in r}\right) u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) \overset{(3)}{=}$$
$$\overset{(3)}{=} (-1)^{p(q+r)} \sum_{\sigma\in\mathfrak{S}_{(p,q,r)}} \varepsilon_{p+q+r}(\sigma) u\left(\left(x_{\sigma(i)}\right)_{i\in p}\right) v\left(\left(x_{\sigma(p+i)}\right)_{i\in q}\right) w\left(\left(x_{\sigma(p+q+i)}\right)_{i\in r}\right) =$$
$$= (-1)^{p(q+r)} (u \wedge v \wedge w)\left((x_i)_{i\in p+q+r}\right),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk a 20.4.2. lemma b) pontját, amely szerint az

$$\mathfrak{S}_{(p,q,r)} \to \mathfrak{S}_{(q,r,p)}; \quad \sigma \mapsto \sigma\circ\sigma_{p,q+r}$$

leképezés bijekció, valamint alkalmaztuk az általános asszociativitás tételét a K test $+$ műveletére;

– a $\overset{(2)}{=}$ egyenlőségnél az ε_{p+q+r} előjel-függvény multiplikativitását és a $\sigma_{p,q+r}$ permutáció definícióját alkalmaztuk;

– a $\overset{(3)}{=}$ egyenlőségnél hivatkozunk a 20.4.2. lemma a) pontjában bizonyított összefüggésre. Ebből látható, hogy

$$(v \wedge w \wedge u)\left((x_i)_{i\in p+q+r}\right) = (-1)^{p(q+r)} (u \wedge v \wedge w)\left((x_i)_{i\in p+q+r}\right),$$

és mivel ez minden $(x_i)_{i\in p+q+r} \in E^{p+q+r}$ esetén igaz, ebből következik, hogy $v \wedge w \wedge u = (-1)^{p(q+r)} (u \wedge v \wedge w)$.

(III) Végül igazoljuk azt, hogy

$$u \wedge (v \wedge w) = u \wedge v \wedge w.$$

Valóban, írható, hogy

$$u \wedge (v \wedge w) \overset{(4)}{=} (-1)^{p(q+r)} ((v \wedge w) \wedge u) \overset{(5)}{=} (-1)^{p(q+r)} (v \wedge w \wedge u) \overset{(6)}{=}$$
$$\overset{(6)}{=} (-1)^{p(q+r)}(-1)^{p(q+r)} (u \wedge v \wedge w) = u \wedge v \wedge w,$$

ahol

– a $\overset{(4)}{=}$ egyenlőségnél a külső szorzás antikommutativitásának tételét (20.4.3.) alkalmaztuk az $u \in \mathbf{A}_p(E)$ és $v \wedge w \in \mathbf{A}_{q+r}(E)$ multilineáris formákra;

– az $\overset{(5)}{=}$ egyenlőségnél felhasználtuk a bizonyítás (I) részében nyert eredményt;

– a $\overset{(6)}{=}$ egyenlőségnél felhasználtuk a bizonyítás (II) részében nyert eredményt. ■

20.5.3. Állítás. (**Poincaré-tétel.**) *Ha E véges dimenziós vektortér a K test felett és $p \in \mathbb{N}^*$, akkor az E^*-ban haladó $(u_i)_{i\in p}$ rendszer pontosan akkor lineárisan független, ha* $\bigwedge_{i=0}^{p-1} u_i \neq \mathbf{0}$.

Bizonyítás. Tegyük fel, hogy az $(u_i)_{i\in p}$ rendszer lineárisan független E^*-ban. A 17.5.8. állítás szerint az $(u_i)_{i\in p}$ rendszer kiterjeszthető egy $(u_i)_{i\in \dim_K(E)}$ algebrai bázissá E^*-ban, így a 17.9.11. állítás szerint létezik olyan $(e_i)_{i\in\dim_K(E)}$ rendszer E-ben, hogy minden $i,j \in \dim_K(E)$ indexre $u_i(e_j) = \delta_{i,j}$. Ekkor $p \leq \dim_K(E)$ és az $(u_i(e_j))_{(i,j)\in p\times p}$ mátrix egyenlő a $p \times p$-es egységmátrixszal, következésképpen $\left(\bigwedge_{i=0}^{p-1} u_i\right)\left((e_i)_{i\in p}\right) = \det\left((u_i(e_j))_{(i,j)\in p\times p}\right) = 1$, tehát $\bigwedge_{i=0}^{p-1} u_i \neq \mathbf{0}$.

Tegyük fel, hogy az $(u_i)_{i\in p}$ rendszer lineárisan függő E^*-ban, és legyen $k \in p$ olyan szám, valamint $(\lambda_i)_{i\in p\setminus\{k\}}$ olyan rendszer K-ban, amelyre $u_k = \sum_{\substack{i=0\\ i\neq k}}^{p-1} \lambda_i.u_i$. Jelölje Φ az

$$(E^*)^p \to \mathbf{Alt}_p(E); \quad (v_i)_{i\in n} \mapsto \bigwedge_{i=0}^{p-1} v_i$$

leképezést, amelyről tudjuk, hogy multilineáris és alternáló (20.3.5.). Vezessük be az $\mathbf{u} := (u_i)_{i\in p} \in (E^*)^p$ elemet. Ekkor a $\Phi \circ \mathrm{in}_{k,\mathbf{u}} : E^* \to \mathbf{Alt}_p(E)$ leképezés lineáris operátor, ezért

$$\bigwedge_{i=0}^{p-1} u_i = \Phi\left((u_i)_{i\in p}\right) = \left(\Phi \circ \mathrm{in}_{k,\mathbf{u}}\right)(u_k) = \sum_{\substack{i=0\\ i\neq k}}^{p-1} \lambda_i.\left(\Phi \circ \mathrm{in}_{k,\mathbf{u}}\right)(u_i).$$

Ha $i \in p$ és $i \neq k$, akkor $\left(\mathrm{in}_{k,\mathbf{u}}(u_i)\right)_i = u_i = \left(\mathrm{in}_{k,\mathbf{u}}(u_i)\right)_k$, ezért $\left(\Phi \circ \mathrm{in}_{k,\mathbf{u}}\right)(u_i) = \bigwedge_{j=0}^{p-1} \left(\mathrm{in}_{k,\mathbf{u}}(u_i)\right)_j = \mathbf{0}$, következésképpen $\bigwedge_{i=0}^{p-1} u_i = \mathbf{0}$. ■

Emlékeztetünk arra, hogy ha $n, p \in \mathbb{N}$, akkor $\mathscr{M}(p;n)$ jelöli a $p \to n$ szigorúan monoton növő függvények halmazát (9.4.7.).

20.5.4. Állítás. *Legyen E vektortér a K test felett és $n := \dim_K(E) < +\infty$.*

a) *Ha $(e_k)_{k\in n}$ algebrai bázis E-ben, és $(e_k^*)_{k\in n}$ a duális algebrai bázis E^*-ban, akkor minden $1 \leq p \leq n$ természetes számra és $u \in \mathbf{Alt}_p(E)$ alternáló multilineáris formára*

$$u = \sum_{\varrho\in\mathscr{M}(p;n)} u\left(\left(e_{\varrho(i)}\right)_{i\in p}\right).\left(\bigwedge_{i=0}^{p-1} e^*_{\varrho(i)}\right),$$

és minden $p > n$ természetes számra $\mathbf{Alt}_p(E) = \{0\}$.

b) *Ha $(u_i)_{i\in n}$ algebrai bázis E^*-ban, akkor minden $1 \leq p \leq n$ természetes számra az*

$$\left(\bigwedge_{i=0}^{p-1} u_{\varrho(i)}\right)_{\varrho\in\mathscr{M}(p;n)}$$

rendszer algebrai bázis az $\mathbf{Alt}_p(E)$ vektortérben.

c) *Minden $1 \leq p \leq \dim_K(E)$ természetes számra*

$$\dim_K\left(\mathbf{Alt}_p(E)\right) = \binom{\dim_K(E)}{p}.$$

Bizonyítás. a) Legyen $1 \leq p \leq n$ természetes szám, $u \in \mathbf{Alt}_p(E)$, és $(x_i)_{i \in p} \in E^p$. Minden $i \in p$ esetén jelölje $(X_{i,k})_{k \in n} \in K^n$ azt a rendszert, amelyre $x_i = \sum_{k \in n} X_{i,k} e_k$. A multilineáris operátorok multiadditivitásának és multihomogenitásának tétele (19.3.1. és 19.2.1.) szerint

$$u\left((x_i)_{i \in p}\right) = u\left(\left(\sum_{k \in n} X_{i,k} e_k\right)_{i \in p}\right) = \sum_{\sigma \in \mathscr{F}(p;n)} u\left(\left(X_{i,\sigma(i)} e_{\sigma(i)}\right)_{i \in p}\right) =$$

$$= \sum_{\sigma \in \mathscr{F}(p;n)} u\left(\left(e_{\sigma(i)}\right)_{i \in p}\right) \prod_{i \in p} X_{i,\sigma(i)} = \sum_{\sigma \in \mathscr{I}(p;n)} u\left(\left(e_{\sigma(i)}\right)_{i \in p}\right) \prod_{i \in p} X_{i,\sigma(i)},$$

ahol $\mathscr{F}(p;n)$ az összes $p \to n$ függvények halmaza, és $\mathscr{I}(p;n)$ az injektív $p \to n$ függvények halmaza. Itt az utolsó egyenlőségnél használtuk ki, hogy az u antiszimmetrikus multilineáris operátor *alternáló*, tehát minden $\sigma : p \to n$ nem injektív függvényre $u\left(\left(e_{\sigma(i)}\right)_{i \in p}\right) = 0$. Ebből már következik, hogy minden $p > n$ természetes számra $\mathbf{Alt}_p(E;K) = \{0\}$, hiszen ekkor $\mathscr{I}(p;n) = \emptyset$.

A 9.4.7. állítás b) pontja szerint $\mathscr{I}(p;n) = \bigcup_{\varrho \in \mathscr{M}(p;n)} \{\varrho \circ \sigma' | \sigma' \in \mathfrak{S}_p\}$, és itt diszjunkt unió áll, ezért

$$\sum_{\sigma \in \mathscr{I}(p;n)} u\left(\left(e_{\sigma(i)}\right)_{i \in p}\right) \prod_{i \in p} X_{i,\sigma(i)} \overset{(1)}{=} \sum_{\varrho \in \mathscr{M}(p;n)} \left(\sum_{\sigma' \in \mathfrak{S}_p} u\left(\left(e_{\varrho(\sigma'(i))}\right)_{i \in p}\right) \prod_{i \in p} X_{i,\varrho(\sigma'(i))}\right) \overset{(2)}{=}$$

$$\overset{(2)}{=} \sum_{\varrho \in \mathscr{M}(p;n)} \left(\sum_{\sigma' \in \mathfrak{S}_p} \varepsilon_p(\sigma') u\left(\left(e_{\varrho(i)}\right)_{i \in p}\right) \prod_{i \in p} X_{i,\varrho(\sigma'(i))}\right) =$$

$$= \sum_{\varrho \in \mathscr{M}(p;n)} u\left(\left(e_{\varrho(i)}\right)_{i \in p}\right) \left(\sum_{\sigma' \in \mathfrak{S}_p} \varepsilon_p(\sigma') \prod_{i \in p} X_{i,\varrho(\sigma'(i))}\right) \overset{(3)}{=}$$

$$\overset{(3)}{=} \sum_{\varrho \in \mathscr{M}(p;n)} u\left(\left(e_{\varrho(i)}\right)_{i \in p}\right) \det\left(\left(X_{i,\varrho(j)}\right)_{(i,j) \in p \times p}\right) \overset{(4)}{=}$$

$$\overset{(4)}{=} \sum_{\varrho \in \mathscr{M}(p;n)} u\left(\left(e_{\varrho(i)}\right)_{i \in p}\right) \det\left(\left(X_{j,\varrho(i)}\right)_{(i,j) \in p \times p}\right) \overset{(5)}{=}$$

$$\overset{(5)}{=} \sum_{\varrho \in \mathscr{M}(p;n)} u\left(\left(e_{\varrho(i)}\right)_{i \in p}\right) \left(\bigwedge_{i=0}^{p-1} e^*_{\varrho(i)}\right) \left((x_i)_{i \in p}\right),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél az összeadás általános asszociativitását (8.7.1.) alkalmaztuk;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk azt, hogy u antiszimmetrikus, ezért minden $\varrho \in \mathscr{M}(p;n)$ és $\sigma' \in \mathfrak{S}_p$ esetén

$$u\left(\left(e_{\varrho(\sigma'(i))}\right)_{i \in p}\right) = \varepsilon_p(\sigma') u\left(\left(e_{\varrho(i)}\right)_{i \in p}\right);$$

– a $\overset{(3)}{=}$ egyenlőségnél a determináns definícióját alkalmaztuk;

– a $\overset{(4)}{=}$ egyenlőségnél felhasználtuk azt, hogy négyzetes mátrix determinánsa egyenlő a transzponált mátrix determinánsával (15.2.6.);

– az $\overset{(5)}{=}$ egyenlőségnél a 20.3.5. állítás a) pontjára hivatkozhatunk, figyelembe véve, hogy minden $i, j \in p$ esetén

$$e^*_{\varrho(i)}(x_j) = e^*_{\varrho(i)}\Big(\sum_{k\in n} X_{j,k}e_k\Big) = \sum_{k\in n} X_{j,k}e^*_{\varrho(i)}(e_k) = \sum_{k\in n} X_{j,k}\delta_{\varrho(i),k} = X_{j,\varrho(i)},$$

ezért

$$\left(\bigwedge_{i=0}^{p-1} e^*_{\varrho(i)}\right)((x_i)_{i\in p}) = \det\left(\left(X_{j,\varrho(i)}\right)_{(i,j)\in p\times p}\right).$$

b) Legyen $(u_i)_{i\in n}$ algebrai bázis E^*-ban, és vegyünk olyan $(e_i)_{i\in n}$ rendszert E-ben, amelyre minden $i, j \in n$ esetén $u_i(e_j) = \delta_{i,j}$ (17.9.11.). Legyen $(c_\varrho)_{\varrho\in\mathscr{M}(p;n)}$ olyan K-ban haladó rendszer, hogy $\sum\limits_{\varrho\in\mathscr{M}(p;n)} c_\varrho\cdot\left(\bigwedge\limits_{i=0}^{p-1} u_{\varrho(i)}\right) = 0$. Megmutatjuk, hogy ekkor minden $\varrho \in \mathscr{M}(p;n)$ esetén $c_\varrho = 0$, tehát a $\left(\bigwedge\limits_{i=0}^{p-1} u_{\varrho(i)}\right)_{\varrho\in\mathscr{M}(p;n)}$ rendszer lineárisan független az $\mathbf{Alt}_p(E)$ vektortérben.

Legyen $\varrho' \in \mathscr{M}(p;n)$. Ekkor a 20.3.5. állítás a) pontja szerint

$$0 = \left(\sum_{\varrho\in\mathscr{M}(p;n)} c_\varrho\cdot\left(\bigwedge_{i=0}^{p-1} u_{\varrho(i)}\right)\right)((e_{\varrho'(i)})_{i\in p}) = \sum_{\varrho\in\mathscr{M}(p;n)} c_\varrho\cdot\left(\bigwedge_{i=0}^{p-1} u_{\varrho(i)}\right)((e_{\varrho'(i)})_{i\in p}) =$$
$$= \sum_{\varrho\in\mathscr{M}(p;n)} c_\varrho\cdot\det\left(\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}\right).$$

Ha igazolnánk azt, hogy minden $\varrho \in \mathscr{M}(p;n)$ esetén $\det\left(\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}\right) = \delta_{\varrho,\varrho'}$, akkor az előző egyenlőségből következne, hogy $c_{\varrho'} = 0$, amit bizonyítani kell. Legyen tehát $\varrho \in \mathscr{M}(p;n)$ is rögzített. Ha $\varrho' = \varrho$, akkor ϱ injektivitásából következik, hogy az $\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}$ mátrix egyenlő a $p\times p$-es egységmátrixszal, következésképpen $\det\left(\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}\right) = 1$. Tegyük fel, hogy $\varrho' \neq \varrho$. A 9.4.7. állítás a) pontja szerint ekkor $\mathrm{Im}(\varrho') \neq \mathrm{Im}(\varrho)$, tehát $\mathrm{Im}(\varrho') \setminus \mathrm{Im}(\varrho) \neq \emptyset$, vagy $\mathrm{Im}(\varrho) \setminus \mathrm{Im}(\varrho') \neq \emptyset$. Ha $\mathrm{Im}(\varrho') \setminus \mathrm{Im}(\varrho) \neq \emptyset$, és rögzítünk olyan $j_* \in p$ elemet, amelyre $\varrho'(j_*) \notin \mathrm{Im}(\varrho)$, akkor minden $i \in p$ esetén $\varrho'(j_*) \neq \varrho(i)$, tehát $u_{\varrho(i)}\left(e_{\varrho'(j_*)}\right) = 0$, vagyis az $\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}$ mátrix j_*-adik oszlopának minden tagja 0, így 15.2.10. alapján $\det\left(\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}\right) = 0$. Ha $\mathrm{Im}(\varrho) \setminus \mathrm{Im}(\varrho') \neq \emptyset$, és rögzítünk olyan $i_* \in p$ elemet, amelyre $\varrho(i_*) \notin \mathrm{Im}(\varrho')$, akkor minden $j \in p$ esetén $\varrho(i_*) \neq \varrho'(j)$, tehát $u_{\varrho(i_*)}\left(e_{\varrho'(j)}\right) = 0$, vagyis az $\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}$ mátrix i_*-adik sorának minden tagja 0, így 15.2.10. és a 9.4.7. állítás a) pontja szerint $\det\left(\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}\right) = 0$. Ez azt jelenti, hogy $\varrho' \neq \varrho$ esetén $\det\left(\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}\right) = 0$. Tehát minden $\varrho \in \mathscr{M}(p;n)$ esetén $\det\left(\left(u_{\varrho(i)}\left(e_{\varrho'(j)}\right)\right)_{(i,j)\in p\times p}\right) = \delta_{\varrho,\varrho'}$.

Ha $(u_i)_{i\in n}$ algebrai bázis E^*-ban, és $(e_i)_{i\in n}$ olyan rendszer E-ben, amelyre minden $i, j \in n$ esetén $u_i(e_j) = \delta_{i,j}$, akkor $(e_i)_{i\in n}$ olyan algebrai bázis E-ben, amelynek $(u_i)_{i\in n}$ a duális bázisa (17.9.11.), így az a) állítás szerint $\left(\bigwedge\limits_{i=0}^{p-1} u_{\varrho(i)}\right)_{\varrho\in\mathscr{M}(p;n)}$ generátorrendszer az $\mathbf{Alt}_p(E)$ vektortérben, és az előzőek szerint ez a rendszer lineárisan független, ezért $\left(\bigwedge\limits_{i=0}^{p-1} u_{\varrho(i)}\right)_{\varrho\in\mathscr{M}(p;n)}$ algebrai bázis az $\mathbf{Alt}_p(E)$ vektortérben.

c) A b) állításból következik, hogy $\dim_K(\mathbf{Alt}_p(E)) = \mathrm{Card}(\mathscr{M}(p;n))$, ugyanakkor a 9.4.7. állítás a) pontja szerint $\mathrm{Card}(\mathscr{M}(p;n)) = \binom{n}{p} = \binom{\dim_K(E)}{p}$. ∎

20.5.5. Következmény. *Legyen E vektortér a K test felett,* $\mathrm{Char}(K) \neq 2$ *és* $\dim_K(E) < +\infty$. *Ekkor minden $1 \leq p \leq \dim_K(E)$ számra, és minden $(u_i)_{i \in \dim_K(E)}$ algebrai bázisra E^*-ban teljesül az, hogy az*

$$\left(\bigwedge_{i=0}^{p-1} u_{\varrho(i)}\right)_{\varrho \in \mathscr{M}(p;\dim_K(E))}$$

rendszer algebrai bázis az $\mathbf{A}_p(E)$ vektortérben. Továbbá, minden $p \in \mathbb{N}$ esetén

$$\dim_K\left(\mathbf{A}_p(E)\right) = \binom{\dim_K(E)}{p},$$

Bizonyítás. A $\mathrm{Char}(K) \neq 2$ feltétel alapján a 20.1.2. állításból következik, hogy $\mathbf{A}_p(E) = \mathbf{Alt}_p(E)$, így a 20.5.4. állítás c) pontja szerint minden $1 \leq p \leq \dim_K(E)$ esetén

$$\dim_K\left(\mathbf{A}_p(E)\right) = \binom{\dim_K(E)}{p},$$

továbbá a 20.5.4. állítás a) pontja és a binomiális együtthatók értelmezése (9.4.4.) szerint $p > \dim_K(E)$ esetén

$$\dim_K\left(\mathbf{A}_p(E)\right) = 0 = \binom{\dim_K(E)}{p}.$$

Végül, a definíció szerint nyilvánvaló, hogy

$$\dim_K\left(\mathbf{A}_0(E)\right) = \dim_K(K) = 1 = \binom{\dim_K(E)}{0}. \blacksquare$$

A 20.5.5. állításban lényeges az, hogy a K test nem 2 karakterisztikájú.

21. fejezet

Algebrák

21.1. Algebrák és algebra-morfizmusok értelmezése

Bizonyos függvényterek esetében a lineáris műveletek mellett még egy szorzás-művelet is bevezethető, amint az a következő állításból látható.

21.1.1. Állítás. *Legyen T halmaz, K test és $A := \mathscr{F}(T;K)$. Minden $x, y \in A$ esetén legyen $x \cdot y$ az a $T \to K$ függvény, amelyre minden $t \in T$ esetén*

$$(x \cdot y)(t) := x(t) \cdot y(t).$$

Jelölje $+$ és $.$ az A függvénytér lineáris műveleteit. Ekkor az

$$A \times A \to E; \quad (x, y) \mapsto x \cdot y$$

művelet rendelkezik a következő tulajdonsággal:

(ALG) *Minden $x, y, z \in A$ és $\alpha \in K$ elemre*

$$\begin{gathered}(x \cdot y) \cdot z = x \cdot (y \cdot z);\\ x \cdot (y + z) = x \cdot y + x \cdot z;\\ (y + z) \cdot x = y \cdot x + z \cdot x;\\ \alpha.(x \cdot y) = (\alpha.x) \cdot y = x \cdot (\alpha.y).\end{gathered}$$

(ALG) *Minden $x, y, z \in A$ és $\alpha \in K$ elemre*

Bizonyítás. Nyilvánvalóan következik a testaxiómákból. ■

21.1.2. Definíció. *Az $(A, +, ., \cdot)$ négyest* **algebrának** *nevezzük K test felett, ha az $(A, +, .)$ hármas vektortér a K test felett, és $\cdot : A \times A \to A$ olyan művelet, amelyre az előző állítás* (ALG) *feltétele teljesül.*

Tehát ha T halmaz és K test, akkor az $\mathscr{F}(T;K)$ függvényhalmaz a korábban bevezetett $+$ és $.$ vektortér-műveletekkel, valamint az előző állításban értelmezett $\cdot$ művelettel ellátva algebra a K test felett; a továbbiakban $\mathscr{F}(T;K)$-t ezekkel a műveletekkel ellátva algebrának fogjuk tekinteni. Az ilyen alakú algebrákat *teljes függvényalgebráknak* nevezzük. A teljes függvényalgebrák műveleteit *pontonként értelmezett* műveleteknek szoktuk nevezni.

Megjegyezzük, hogy a K test feletti $(A, +, ., \cdot)$ algebrát akkor nevezzük *kommutatívnak* (illetve *egységelemesnek*), ha a $\cdot$ művelet kommutatív (illetve A-nak létezik neutrális eleme a $\cdot$ művelet szerint). Világos, hogy a teljes függvényalgebrák kommutatívak és egységelemesek.

A legelemibb algebra-konstrukciók a következők.

– Algebra minden *részalgebrája* szintén algebra a műveletek leszűkítésével ellátva. Most bemutatunk két nevezetes részalgebra-konstrukciót.

a) Legyen A algebra és $e \in A$ *idempotens* elem, vagyis $e^2 = e$. Ekkor az

$$eAe := \{eae \mid a \in A\}$$

halmaz olyan részalgebrája A-nak, amelynek e egységeleme; ezt nevezzük az e idempotens elem által *redukált részalgebrának* A-ban. Könnyen látható, hogy

$$eAe = \{a \in A \mid ea = ae = a\}.$$

b) Legyen A algebra és $S \subseteq A$. Ekkor a

$$\mathrm{C}(S) := \{a \in A \mid (\forall s \in S): \ as = sa\}$$

halmaz részalgebrája A-nak; ezt nevezzük az S halmaz *kommutánsának*. A $\mathrm{C}(\mathrm{C}(S))$ halmaz S-t tartalmazó részalgebra A-ban; $\mathrm{C}(\mathrm{C}(S))$-t az S halmaz *bikommutánsának* nevezzük. Ha S kommutatív halmaz (vagyis bármely két eleme felcserélhető), akkor az S bikommutánsa is kommutatív részalgebra A-ban. Megjegyezzük, hogy ha A kommutatív algebra, akkor minden $S \subseteq A$ halmazra $\mathrm{C}(S) = A$, tehát a kommutáns-képzés csak nemkommutatív algebrában nem triviális részalgebra-konstrukció.

– Adott test feletti algebrák tetszőleges rendszerének a *szorzata*, a komponensenként értelmezett műveletekkel ellátva algebra.

– Ha A algebra és $\mathfrak{m}$ *ideál* A-ban, akkor az $A/\mathfrak{m}$ lineáris faktortér felett egyértelműen létezik olyan szorzás, amellyel az $A/\mathfrak{m}$ algebra, és amely szerint a $\pi_{A/\mathfrak{m}} : A \to A/\mathfrak{m}$ kanonikus leképezés algebra-morfizmus; ezt az $A/\mathfrak{m}$ algebrát nevezzük az A algebra $\mathfrak{m}$ ideál szerinti *faktoralgebrájának*. Algebra ideálját *valódinak* nevezzük, ha különbözik az alaphalmaztól. Algebra valódi ideáljainak halmazán a tartalmazás-reláció rendezés; ennek a rendezett halmaznak a maximális elemeit nevezzük *maximális ideáloknak*.

Példák (algebrákra).

(I) Legyen T halmaz, K test, és tekintsük a $T \to K$ függvények $\mathscr{F}(T;K)$ halmazát. Ez a függvényhalmaz a pontonként értelmezett lineáris műveletekkel és a pontonként értelmezett szorzással ellátva kommutatív egységelemes algebra. Az ilyen alakú algebrák részalgebráit *függvényalgebráknak* nevezzük.

Függvényalgebrák kijelölésére szokásos módszer az, hogy a T halmazon és a K testen megadunk egy hasonló típusú struktúrát, és az adott struktúrákat megtartó $T \to K$ függvények algebráját vesszük. Ennek nevezetes speciális esetei a következők.

– Legyen T halmaz; ekkor a

$$K^{(T)} := \{f \in \mathscr{F}(T;K) | \text{ "a } \{t \in T | f(t) \neq 0\} \text{ halmaz véges"}\}$$

halmaz részalgebrája $\mathscr{F}(T;K)$-nak. Továbbá az

$$\mathscr{F}^b(T;\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K}) | \text{ "az } f \text{ függvény korlátos"}\}$$

halmaz részalgebrája az $\mathscr{F}(T;\mathbb{K})$ algebrának.

– Legyen T topologikus tér; ekkor a

$$\mathscr{C}(T;\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K})| \text{ "az } f \text{ függvény folytonos"}\}$$

halmaz, valamint a

$$\mathscr{C}^b(T;\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K})| \text{ "az } f \text{ függvény folytonos és korlátos"}\}$$

halmazok részalgebrái az $\mathscr{F}(T;\mathbb{K})$ algebrának.

– Legyen T lokálisan kompakt tér; ekkor a

$$\mathscr{K}(T;\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K})| \text{ "az } f \text{ függvény folytonos és kompakt tartójú"}\}$$

halmaz, valamint a

$$\overline{\mathscr{K}}(T;\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K})| \text{"az } f \text{ függvény folytonos és végtelenben eltűnő"}\}$$

halmazok részalgebrái az $\mathscr{F}(T;\mathbb{K})$ algebrának.

– Legyen $\mathscr{R}$ halmazgyűrű a T halmaz felett; ekkor a $T \to \mathbb{K}$ $\mathscr{R}$-lépcsősfüggvények $\mathscr{E}_{\mathbb{K}}(T,\mathscr{R})$ halmaza, valamint a $T \to \mathbb{K}$ $\mathscr{R}$-egyszerű függvények $\widehat{\mathscr{E}}_{\mathbb{K}}(T,\mathscr{R})$ halmaza részalgebrája az $\mathscr{F}(T;\mathbb{K})$ algebrának.

– Legyen $\mathscr{A}$ σ-algebra a T halmaz felett; ekkor

$$\mathscr{F}(T,\mathscr{A};\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K})| \text{ "az } f \text{ függvény } \mathscr{A} - \mathscr{B}(\mathbb{K}) \text{ mérhető"}\},$$

halmaz részalgebrája az $\mathscr{F}(T;\mathbb{K})$ algebrának, ahol $\mathscr{B}(\mathbb{K})$ a $\mathbb{K}$ Borel-féle σ-algebrája. Továbbá, a

$$\mathscr{F}^b(T,\mathscr{A};\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K})| \text{"az } f \text{ függvény } \mathscr{A} - \mathscr{B}(\mathbb{K}) \text{ mérhető és korlátos"}\}$$

halmaz szintén részalgebrája az $\mathscr{F}(T;\mathbb{K})$ algebrának.

– Legyen T metrikus tér; ekkor az

$$\mathfrak{A}(T,\mathbb{K}) := \{f \in \mathscr{F}(T;\mathbb{K})| \text{ "az } f \text{ függvény egyenletesen folytonos"}\}$$

halmaz részalgebrája az $\mathscr{F}(T;\mathbb{K})$ algebrának.

– Legyen Ω nyílt részhalmaza a $\mathbb{K}$ test feletti E normált térnek és $r \in \mathbb{N}$ vagy $r = \infty$. Ekkor a

$$C^r(\Omega;\mathbb{K}) := \{f \in \mathscr{F}(\Omega;\mathbb{K})| \text{ "az } f \text{ függvény } r\text{-szer folytonosan differenciálható"}\}$$

halmaz részalgebrája az $\mathscr{F}(\Omega;\mathbb{K})$ algebrának. Továbbá, a

$$\begin{aligned} C^{r,b}(\Omega;\mathbb{K}) := \{f \in \mathscr{F}(\Omega;\mathbb{K})| &\text{ "az } f \text{ függvény } r\text{-szer folytonosan differenciálható,} \\ &\text{és minden } 0 \le k \le r \text{ természetes számra } \mathrm{D}^k f \text{ korlátos függvény"}\} \end{aligned}$$

halmaz szintén részalgebrája az $\mathscr{F}(\Omega;\mathbb{K})$ algebrának.

– Legyen $\Omega \subseteq \mathbb{C}$ nyílt halmaz; ekkor a

$$\mathscr{H}(\Omega;\mathbb{C}) := \{f \in \mathscr{F}(\Omega;\mathbb{C})| \text{ "az } f \text{ függvény holomorf"}\}$$

halmaz részalgebrája az $\mathscr{F}(\Omega;\mathbb{C})$ algebrának. Speciálisan, az

$$\mathscr{E}(\mathbb{C}) := \mathscr{H}(\mathbb{C};\mathbb{C})$$

halmaz, vagyis a $\mathbb{C} \to \mathbb{C}$ *egészfüggvények* halmaza részalgebrája az $\mathscr{F}(\mathbb{C};\mathbb{C})$ algebrának.

(II) Legyen E vektortér a K test felett, és $\mathbf{L}(E)$ az $E \to E$ K-lineáris operátorok halmaza. Ekkor $\mathbf{L}(E)$ a lineáris operátorműveletekkel és a függvénykompozícióval ellátva egységelemes algebra, amely nem kommutatív, ha E legalább két dimenziós. Az ilyen alakú algebrák részalgebráit nevezzük *operátoralgebráknak.* Ha $n \in \mathbb{N}$, akkor az $\mathbf{L}(K^n)$ operátoralgebrát $M_n(K)$ jelöli; az ilyen alakú operátoralgebrák részalgebrái a *mátrixalgebrák.*

Operátoralgebrák kijelölésére szokásos módszer az, hogy az E vektortéren megadunk valamilyen struktúrát és az azt megtartó lineáris operátorok halmazát vesszük. Ennek legfontosabb speciális esetei a következők.

– Ha E vektortér K felett, akkor az $E \to E$ *véges dimenziós értékkészletű* lineáris operátorok halmaza részalgebrája az $\mathbf{L}(E)$ algebrának.

– Ha E topologikus vektortér, akkor az

$$\mathscr{L}(E) := \{u \in \mathbf{L}(E) | \text{"}u \text{ folytonos operátor"}\},$$

valamint a

$$\mathscr{B}(E) := \{u \in \mathbf{L}(E) | \text{"}u \text{ korlátos operátor"}\},$$

halmazok részalgebrái az $\mathbf{L}(E)$ algebrának.

– Ha E normált tér, akkor a

$$\mathscr{C}(E) := \{u \in \mathbf{L}(E) | \text{"}u \text{ kompakt operátor"}\}$$

részalgebrája (sőt ideálja) az $\mathbf{L}(E)$ algebrának.

(III) Legyen S egységelemes félcsoport (azaz *monoid*), K test, és ismét tekintsük a

$$K^{(S)} := \{a \in \mathscr{F}(S;K) | \text{ "az } \{s \in S | a(s) \neq 0\} \text{ halmaz véges"}\}$$

halmazt. Ez lineáris altere az $\mathscr{F}(S;K)$ függvénytérnek, amit az S halmaz által generált *szabad vektortérnek* nevezünk K felett. Most a $K^{(S)}$ felett értelmezzük a $*$ műveletet úgy, hogy minden $a, b \in K^{(S)}$ és $s \in S$ esetén

$$(a * b)(s) = \sum_{(s',s'') \in S \times S,\ s's''=s} a(s')b(s'').$$

Könnyen látható, hogy $a, b \in K^{(S)}$ esetén $a * b \in K^{(S)}$, és a $K^{(S)}$ vektortér a $*$ szorzással ellátva egységelemes algebra; ezt nevezzük az S monoid K feletti *konvolúciós algebrájának*, és $A_K(S)$-sel jelöljük. Legyen minden $s \in S$ esetén $\varepsilon_s \in K^{(S)}$ az az elem, amelyre minden $S \ni s'$-re, ha $s' \neq s$, akkor $\varepsilon_s(s') = 0$, és $\varepsilon_s(s) = 1$. Ekkor az $\{\varepsilon_s | s \in S\}$ halmaz bázisa $K^{(S)}$ vektortérnek, és a $j : S \to A_K(S)$ leképezés injektív egységelem-tartó félcsoport-morfizmus S és az $A_K(S)$ multiplikatív félcsoport között. Az $A_K(S)$ algebra pontosan akkor kommutatív, ha S kommutatív. Ha A egységelemes algebra K felett, akkor minden $f : S \to A$ egységelem-tartó félcsoport-morfizmushoz létezik egyetlen olyan $\tilde{f} : A_K(S) \to A$ egységelem-tartó algebra-morfizmus, amelyre $\tilde{f} \circ j = f$. Fontos speciális esetek a következők.

– $S := \mathbb{N}$ és S művelete az összeadás. Az így értelmezett $\mathbb{N}$ kommutatív monoid K test feletti konvolúciós algebráját a $K[X]$ szimbólummal is jelöljük, és X jelöli azt az elemet ebben az algebrában, amelyre $n \in \mathbb{N}$ esetén $\mathrm{X}(n) = 0$, ha $n \neq 1$, és $\mathrm{X}(1) = 1$ (vagyis $X := \varepsilon_1$). A $K[X]$ algebrát a K feletti *egyváltozós polinomok algebrájának* nevezzük. Nyilvánvaló, hogy az X elem generálja a $K[X]$ algebrát, és minden $P \in K[X]$ esetén fennáll a

$$P = \sum_{k=0}^{\infty} P(k)X^k$$

egyenlőség, ahol természetesen véges összegzés áll.

– $S := \mathbb{N}^n$, ahol $n \in \mathbb{N}^*$, és S művelete az összeadás. Az így értelmezett $\mathbb{N}^n$ kommutatív monoid K test feletti konvolúciós algebráját a $K[X_1, ..., X_n]$ szimbólummal is jelöljük, és minden $1 \leq k \leq n$ természetes számra X_k jelöli azt az elemet ebben az algebrában, amelyre $\alpha \in \mathbb{N}^n$ esetén $X_k(\alpha) = 0$, ha $\alpha \neq e_k$, és $X_k(e_k) = 1$, ahol e_k a k-adik kanonikus báziselem $\mathbb{N}^n$-ben (vagyis $X_k := \varepsilon_{e_k}$). A $K[X_1, ..., X_n]$ algebrát a K feletti *n-változós polinomok algebrájának* nevezzük. Nyilvánvaló, hogy az $X_1, ..., X_n$ elemek generálják a $K[X_1, ..., X_n]$ algebrát, és minden $P \in K[X_1, ..., X_n]$ esetén fennáll a

$$P = \sum_{\alpha \in \mathbb{N}^n}^{\infty} P(\alpha) \left(\prod_{k=1}^{n} X_k^{\alpha(k)} \right)$$

egyenlőség, ahol természetesen véges összegzés áll.

Megjegyezzük még, hogy ha G csoport, akkor az $A_K(G)$ algebrát a G csoport K feletti *csoport-algebrájának* nevezzük.

(IV) Legyen A vektortér a K test felett, és értelmezzük A felett a szorzást úgy, hogy minden $a, b \in A$ esetén $ab := 0$; ekkor A kommutatív algebra. Az ilyen alakú algebrákat *nulla-szorzású algebráknak* nevezzük.

21.2. Algebra feletti véges műveletek

Ha $(A, +, ., \cdot)$ algebra, akkor a definíció szerint $(A, +, \cdot)$ gyűrű, ezért a gyűrűkben végehajtható rendezett véges műveletekre vonatkozó állítások (14.2) algebrákban is érvényesek. Azonban, ha $(A, +, ., \cdot)$ algebra a K test felett, akkor $(A, +, .)$ vektortér is a K test felett, ezért alkalmazhatóak rá a vektorterekre megfogalmazott fogalmak és állítások (17. fejezet).

21.2.1. Állítás. *Ha A algebra a K test felett, akkor minden $a, b \in A$ esetén az*

$$\begin{aligned} A \to A; &\quad x \mapsto a \cdot x, \\ A \to A; &\quad x \mapsto x \cdot b, \\ A \to A; &\quad x \mapsto a \cdot x \cdot b \end{aligned}$$

leképezések lineáris operátorok.

Bizonyítás. Legyen $a \in A$. Ha $x, y \in A$ és $\lambda \in K$, akkor (ALG) szerint $a \cdot (x+y) = a \cdot x + a \cdot y$ és $a \cdot (\lambda.x) = \lambda.(a \cdot x)$, ezért az $A \to A;\ x \mapsto a \cdot x$ leképezés lineáris.

Legyen $b \in A$. Ha $x, y \in A$ és $\lambda \in K$, akkor (ALG) szerint $(x + y) \cdot b = x \cdot b + y \cdot b$ és

$(\lambda.x)\cdot b = \lambda.(x\cdot b)$, ezért az $A \to A;\ x \mapsto x\cdot b$ leképezés lineáris.

Ha $a, b \in A$, akkor az $A \to A;\ x \mapsto a\cdot x\cdot b$ leképezés egyenlő a $A \to A;\ x \mapsto a\cdot x$ és $A \to A;\ x \mapsto x\cdot b$ lineáris operátorok (tetszőleges sorrendű) kompozíciójával, ezért lineáris operátor. ■

Ettől kezdve áttérünk algebrák műveleteinek egyszerűsített jelölésére, tehát ha $(A, +, ., \cdot)$ algebra a K test felett, akkor az $a, b \in A$ elemek $a\cdot b$ szorzatát ab-vel jelöljük, továbbá $a \in A$ és $\lambda \in K$ esetén $\lambda.a$ helyett λa-t írunk, ha ez nem vezet félreértésre.

Továbbá, ha $(A, +, ., \cdot)$ algebra, akkor $(A, +)$ kommutatív csoport, ezért minden olyan A-ban haladó $(a_i)_{i\in I}$ rendszerre, amelyre $\{i \in I | a_i \neq 0\}$ véges halmaz, értelmes a $\mathop{+}\limits_{i\in I} a_i \in A$ objektum (12.5.3.), amit a továbbiakban a

$$\sum_{i\in I} a_i$$

szimbólummal fogunk jelölni, és az $(a_i)_{i\in I}$ rendszer *véges összegének nevezünk* az A algebrában. Ha $(a_n)_{n\in\mathbb{N}}$ olyan A-ban haladó sorozat, hogy $\{n \in \mathbb{N} | a_n \neq 0\}$ véges halmaz, akkor gyakran a

$$\sum_{n=0}^{\infty} a_n := \sum_{n\in\mathbb{N}} a_n$$

jelölést alkalmazzuk. Továbbá, ha $(A, +, ., \cdot)$ algebra, akkor $(A, \cdot)$ (nem szükségképpen neutrális elemes) félcsoport, így minden $m, n \in \mathbb{N}$, $m \leq n$ természetes számra és minden A-ban haladó $(a_i)_{i\in[\![m,n]\!]}$ rendszerre értelmes a $\mathop{\cdot}\limits_{i=m}^{n} a_i$ objektum (8.5.3.), amit a

$$\mathop{\mathrm{P}}\limits_{i=m}^{n} a_i$$

szimbólummal fogunk jelölni, és az $(a_i)_{i\in[\![m,n]\!]}$ rendszer *rendezett véges szorzatának* nevezünk az A algebrában.

21.2.2. Állítás. *Ha A algebra a K test felett, akkor minden $n \in \mathbb{N}^*$ esetén az*

$$A^n \to A; \quad (x_i)_{i\in n} \mapsto \mathop{\mathrm{P}}\limits_{i=0}^{n-1} x_i$$

leképezés multilineáris operátor.

Bizonyítás. Természetesen feltehető, hogy $n > 1$, mert $n = 1$ esetén az $A \to A$ identikus leképezésről van szó, amely lineáris operátor. Jelölje $\mathbf{m}$ a vizsgálandó leképezést, és legyenek $\mathbf{a} := (a_i)_{i\in n} \in A^n$ és $k \in n$ rögzítettek: azt kell igazolni, hogy az $\mathbf{m} \circ \mathrm{in}_{k,\mathbf{a}} : A \to A$ leképezés lineáris. Ehhez legyen $x \in A$ tetszőleges, tehát ekkor

$$(\mathbf{m} \circ \mathrm{in}_{k,\mathbf{a}})(x) = \mathbf{m}\left((x_i)_{i\in n}\right) = \mathop{\mathrm{P}}\limits_{i=0}^{n-1} x_i,$$

ahol $x_k = x$, és minden $i \in n \setminus \{k\}$ esetén $x_i = a_i$. A $k \in n$ szám elhelyezkedése szerint három eset lehetséges.

1) $k=0$, tehát $x_0=x$ és minden $1\le i<n-1$ természetes számra $x_i=a_i$. Ekkor 8.3.5. a) és e) alapján

$$\prod_{i=0}^{n-1} x_i = \left(\prod_{i=0}^{0} x_i\right)\left(\prod_{i=0+1}^{n-1} x_i\right) = x_0\left(\prod_{i=1}^{n-1} a_i\right) = x\left(\prod_{i=1}^{n-1} a_i\right).$$

2) $0<k<n-1$, tehát $x_k=x$ és minden $i\in n\setminus\{k\}$ esetén $x_i=a_i$. Ekkor 8.3.5. e) alapján

$$\prod_{i=0}^{n-1} x_i = \left(\prod_{i=0}^{k-1} x_i\right) x_k \left(\prod_{i=k+1}^{n-1} x_i\right) = \left(\prod_{i=0}^{k-1} a_i\right) x \left(\prod_{i=k+1}^{n-1} a_i\right).$$

3) $k=n-1$, tehát $x_{n-1}=x$ és minden $i<n-1$ természetes számra $x_i=a_i$. Ekkor 8.3.5. b) alapján

$$\prod_{i=0}^{n-1} x_i = \left(\prod_{i=0}^{n-2} x_i\right) x_{n-1} = \left(\prod_{i=0}^{n-2} a_i\right) x.$$

Természetesen az első két esetben kihasználtuk A szorzásának asszociativitását.

Ezzel beláttuk, hogy minden $x\in A$ esetén

– ha $k=0$, akkor $\mathbf{m}\circ \mathrm{in}_{k,\mathbf{a}}$ egyenlő az

$$A\to A;\quad x\mapsto x\left(\prod_{i=1}^{n-1} a_i\right)$$

leképezéssel, és

– ha $0<k<n-1$, akkor $\mathbf{m}\circ \mathrm{in}_{k,\mathbf{a}}$ egyenlő az

$$A\to A;\quad x\mapsto \left(\prod_{i=0}^{k-1} a_i\right) x \left(\prod_{i=k+1}^{n-1} a_i\right)$$

leképezéssel, és

– ha $k=n-1$, akkor $\mathbf{m}\circ \mathrm{in}_{k,\mathbf{a}}$ egyenlő az

$$A\to A;\quad x\mapsto \left(\prod_{i=0}^{n-2} a_i\right) x$$

leképezéssel, tehát 21.2.1. alapján $\mathbf{m}\circ \mathrm{in}_{k,\mathbf{a}}: A\to A$ lineáris operátor. ■

21.2.3. Állítás. *Legyen A algebra a K test felett, $n\in\mathbb{N}^*$ és $(a_i)_{i\in n+1}\in A^{n+1}$.*

a) *Minden $(x_i)_{i\in n}\in A^n$ esetén*

$$\left(\prod_{i=0}^{n-1} a_i x_i\right) a_n = a_0\left(\prod_{i=0}^{n-1} x_i a_{i+1}\right).$$

b) *A következő leképezés multilineáris:*

$$A^n\to A;\quad (x_i)_{i\in n}\mapsto \left(\prod_{i=0}^{n-1} a_i x_i\right) a_n.$$

Bizonyítás. a) Az 1 számtól indított n szerinti teljes indukcióval bizonyítunk. Az $n=1$ esetben minden $x_0\in A$ elemre teljesül a következő:

$$\left(\prod_{i=0}^{0} a_i x_i\right) a_1 \overset{(1)}{=} (a_0x_0)a_1 \overset{(2)}{=} a_0(x_0a_1) \overset{(3)}{=} a_0\left(\prod_{i=0}^{0} x_i a_{i+1}\right),$$

ahol az $\stackrel{(1)}{=}$ és $\stackrel{(3)}{=}$ egyenlőségeknél a 8.3.5. a) állítást alkalmaztuk, és a $\stackrel{(2)}{=}$ egyenlőségnél felhasználtuk A szorzásának asszociativitását. Tehát az állítás $n = 1$ esetén igaz.

Legyen $n \in \mathbb{N}^*$ olyan, amelyre igaz az állítás, és legyen $(a_i)_{i\in n+2} \in A^{n+2}$ rögzített. Ekkor minden $(x_i)_{i\in n} \in A^n$ esetén

$$\left(\sum_{i=0}^{n} a_i x_i\right) a_{n+1} \stackrel{(4)}{=} \left(\left(\sum_{i=0}^{n-1} a_i x_i\right)(a_n x_n)\right) a_{n+1} \stackrel{(5)}{=} \left(\sum_{i=0}^{n-1} a_i x_i\right)((a_n x_n) a_{n+1}) \stackrel{(6)}{=}$$

$$\stackrel{(6)}{=} \left(\left(\sum_{i=0}^{n-1} a_i x_i\right) a_n\right)(x_n a_{n+1}) \stackrel{(7)}{=} \left(a_0 \left(\sum_{i=0}^{n-1} x_i a_{i+1}\right)\right)(x_n a_{n+1}) \stackrel{(8)}{=}$$

$$\stackrel{(8)}{=} a_0 \left(\left(\sum_{i=0}^{n-1} x_i a_{i+1}\right)(x_n a_{n+1})\right) \stackrel{(9)}{=} a_0 \left(\sum_{i=0}^{n} x_i a_{i+1}\right),$$

ahol a $\stackrel{(4)}{=}$ és $\stackrel{(9)}{=}$ egyenlőségnél a 8.3.5. b) állítást alkalmaztuk, és a $\stackrel{(7)}{=}$ egyenlőségnél felhasználtuk az indukciós hipotézist, továbbá az $\stackrel{(5)}{=}$, $\stackrel{(6)}{=}$ és $\stackrel{(8)}{=}$ egyenlőségnél A szorzásának asszociativitását alkalmaztuk. Tehát az állítás $n + 1$ esetén is igaz.

b) Jelölje $\mathbf{m}$ a vizsgálandó leképezést, és legyen

$$u : A^n \to A; \quad (x_i)_{i\in n} \mapsto \sum_{i=0}^{n-1} x_i$$

ami az előző állítás szerint multilineáris operátor. Minden $i \in n$ esetén legyen

$$v_i : A \to A; \quad x \mapsto a_i x,$$

ami 21.2.1. szerint lineáris operátor, továbbá legyen

$$w : A \to A; \quad x \mapsto x a_n,$$

ami 21.2.1. szerint lineáris operátor. Nyilvánvaló, hogy minden $(x_i)_{i\in n} \in A^n$ esetén

$$\left(w \circ u \circ \bigtimes_{i\in n} v_i\right)((x_i)_{i\in n}) = w\left(u\left((v_i(x_i))_{i\in n}\right)\right) = \left(\sum_{i=0}^{n-1} a_i x_i\right) a_n = \mathbf{m}\left((x_i)_{i\in n}\right),$$

tehát fennáll az

$$\mathbf{m} = w \circ u \circ \left(\bigtimes_{i\in n} v_i\right).$$

egyenlőség, és a jobb oldalon álló leképezés 19.1.3. szerint multilineáris operátor. ■

21.3. Algebra egységelemesítése

A következő állítás megmutatja, hogy minden algebra természetes módon kibővíthető egységelemmel. Ezáltal az algebrákkal kapcsolatos problémák megoldásának jó része visszavezethető az egységelemes algebrák esetére.

21.3.1. Állítás. *Legyen A algebra a K test felett.*

a) *Létezik olyan B egységelemes algebra K felett, és olyan $j : A \to B$ algebra-morfizmus, amelyre teljesül az, hogy minden C egységelemes algebrához, és minden $\pi : A \to C$*

algebra-morfizmushoz egyértelműen létezik olyan $\tilde{\pi} : B \to C$ egységelem-tartó algebra-morfizmus, hogy $\tilde{\pi} \circ j = \pi$.

b) *Legyenek (B_1, j_1) és (B_2, j_2) olyan párok, hogy B_1 és B_2 egységelemes algebrák a K test felett, $j_1 : A \to B_1$ és $j_2 : A \to B_2$ algebra-morfizmusok, és minden C egységelemes algebrához, valamint minden $\pi_1 : A \to C$ és $\pi_2 : A \to C$ algebra-morfizmushoz egyértelműen létezik olyan $\tilde{\pi}_1 : B_1 \to C$ és $\tilde{\pi}_2 : B_2 \to C$ egységelem-tartó algebra-morfizmusok, hogy $\tilde{\pi}_1 \circ j_1 = \pi_1$ és $\tilde{\pi}_2 \circ j_2 = \pi_2$. Ekkor létezik egyetlen olyan $\pi : B_1 \to B_2$ algebra-morfizmus, amelyre $\pi \circ j_1 = j_2$, és ez a leképezés algebra-izomorfizmus.*

Bizonyítás. a) Legyen $\tilde{A} := K \times A$, és értelmezzük a

$$+ : \tilde{A} \times \tilde{A} \to \tilde{A}, \quad \cdot : \tilde{A} \times \tilde{A} \to \tilde{A}, \quad . : K \times \tilde{A} \to \tilde{A}$$

leképezéseket úgy, hogy minden $(\lambda, a), (\lambda', a') \in \tilde{A}$ és $\alpha \in K$ esetén

$$\begin{aligned}(\lambda, a) + (\lambda', a') &:= (\lambda + \lambda', a + a'),\\ (\lambda, a) \cdot (\lambda', a') &:= (\lambda\lambda', \lambda.a' + \lambda'.a + aa'),\\ \alpha.(\lambda, a) &:= (\alpha\lambda, \alpha.a).\end{aligned}$$

Ekkor az $\tilde{A}$ halmaz a $+$, $\cdot$ és . leképezésekkel ellátva egységelemes algebra K felett, amelyben $\mathbf{1} := (1, 0)$ az egységelem, továbbá a

$$j : A \to \tilde{A}; \quad a \mapsto (0, a)$$

leképezés injektív algebra-morfizmus, és $\mathrm{Im}(j)$ olyan 1-kodimenziós ideál $\tilde{A}$-ban, amelyre $\tilde{A} = (K.\mathbf{1}) \oplus \mathrm{Im}(j)$.

Legyen C egységelemes algebra K felett, és $\pi : A \to C$ algebra-morfizmus. Jelölje $\mathbf{1}_C$ a C egységelemét, és értelmezzük a

$$\tilde{\pi} : \tilde{A} \to C; \quad (\lambda, a) \mapsto \lambda.\mathbf{1}_C + \pi(a)$$

leképezést. Könnyen ellenőrizhető, hogy $\tilde{\pi}$ egységelem-tartó algebra-morfizmus, és nyilvánvalóan $\tilde{\pi} \circ j = \pi$. Ha $\tilde{\pi}' : \tilde{A} \to C$ szintén olyan egységelem-tartó algebra-morfizmus, amelyre $\tilde{\pi}' \circ j = \pi$, akkor $\tilde{\pi} = \tilde{\pi}'$ az $\mathrm{Im}(j)$ és $K.\mathbf{1}$ lineáris altereken, így $\tilde{\pi} = \tilde{\pi}'$, mert $\tilde{A} = (K.\mathbf{1}) \oplus \mathrm{Im}(j)$.

b) A feltevés szerint B_2 egységelemes algebra, és $j_2 : A \to B_2$ algebra-morfizmus, így egyértelműen létezik olyan $\pi : B_1 \to B_2$ egységelem-tartó algebra-morfizmus, amelyre $\pi \circ j_1 = j_2$. Ugyanakkor B_1 egységelemes algebra, és $j_1 : A \to B_1$ algebra-morfizmus, így egyértelműen létezik olyan $\pi' : B_2 \to B_1$ egységelem-tartó algebra-morfizmus, amelyre $\pi' \circ j_2 = j_1$. Ekkor $\pi' \circ \pi : B_1 \to B_1$ olyan egységelem-tartó algebra-morfizmus, amelyre $(\pi' \circ \pi) \circ j_1 = j_1$, és a feltevések alapján egyetlen ilyen létezhet. Mivel pedig az id_{B_1} függvény nyilvánvalóan ilyen tulajdonságú, így $\pi' \circ \pi = \mathrm{id}_{B_1}$. Teljesen hasonló érveléssel kapható, hogy $\pi \circ \pi' = \mathrm{id}_{B_2}$, ami azt jelenti, hogy $\pi : B_1 \to B_2$ algebra-izomorfizmus. ■

21.3.2. Definíció. *Ha A algebra a K test felett, akkor az A* **egységelemesítésének** *nevezünk minden olyan (B, j) párt, amelyre B egységelemes algebra K felett, $j : A \to B$ algebra-morfizmus, és minden C egységelemes algebrához, és minden $\pi : A \to C$ algebra-morfizmushoz egyértelműen létezik olyan $\tilde{\pi} : B \to C$ egységelem-tartó algebra-morfizmus, hogy $\tilde{\pi} \circ j = \pi$. Az előző állítás bizonyításának a) pontjában bevezetett $(\tilde{A}, j)$ párt az A* **standard egységelemesítésének** *nevezzük.*

Az előző állítás szerint minden algebrának létezik egységelemesítése, és bármely két egységelemesítése kitüntetett módon azonosítható, tehát lényegében egyetlen egységelemesítés létezik. Természetesen egységelemes algebrának is vehető az egységelemesítése. Tetszőleges algebrának mindig tekinthetjük a standard egységelemesítését, de nem mindig célszerű ez a választás. A következő példa megmutatja, hogy vannak olyan algebrák, amelyeknek természetes módon megadható nem standard egységelemesítése.

Példa. Legyen T lokálisan kompakt tér, és tekintsük a $T \to \mathbb{K}$ folytonos, végtelenben eltűnő függvények $\overline{\mathscr{K}}(T;\mathbb{K})$ algebráját. Könnyen látható, hogy a $\overline{\mathscr{K}}(T;\mathbb{K})$ algebra egységelemessége ekvivalens a T kompaktságával. Jelölje T' a T egypontú kompaktifikációját, és legyen ω a végtelen távoli pont T'-ben. Minden $f \in \overline{\mathscr{K}}(T;\mathbb{K})$ esetén jelölje f^0 az f függvény 0-val vett kiterjesztését T'-re. Értelmezzük a

$$j' : \overline{\mathscr{K}}(T;\mathbb{K}) \to \mathscr{C}(T';\mathbb{K}); \quad f \mapsto f^0$$

leképezést. Ekkor a $(\overline{\mathscr{K}}(T;\mathbb{K}), j')$ pár – nem standard – egységelemesítése a $\overline{\mathscr{K}}(T;\mathbb{K})$ algebrának, ugyanis a

$$\pi : \mathscr{C}(T';\mathbb{K}) \to \mathbb{K} \times \overline{\mathscr{K}}(T;\mathbb{K}); \quad g \mapsto (g(\omega), g|_T - g(\omega).1_T)$$

leképezés olyan algebra-izomorfizmus, amelyre $\pi \circ j' = j$.

21.4. Algebra karakterei és a reguláris ideálok

21.4.1. Definíció. *A K test feletti A algebra* **karakterének** *nevezünk minden $A \to K$ algebra-morfizmust, és az A karaktereinek halmazát $\mathrm{X}'(A)$, valamint az A nem nulla karaktereinek halmazát $\mathrm{X}(A)$ jelöli.*

21.4.2. Definíció. *Az A algebra $\mathfrak{m}$ ideálját* **regulárisnak** *nevezzük, ha $\mathfrak{m}$ valódi ideál A-ban (vagyis $\mathfrak{m} \neq A$), és létezik olyan $e \in A$, amelyre minden $a \in A$ esetén $ae - a \in \mathfrak{m}$ és $ea - a \in \mathfrak{m}$.*

Természetesen egységelemes algebra *minden* valódi ideálja reguláris. Nyilvánvaló, hogy nulla-szorzású algebrának nincs reguláris ideálja.

21.4.3. Állítás. *Az A algebra $\mathfrak{m}$ ideálja pontosan akkor reguláris, ha az $A/\mathfrak{m}$ faktoralgebra nem nulla és egységelemes.*

Bizonyítás. Ha $\mathfrak{m}$ reguláris ideál, és $e \in A$ olyan elem, amelyre minden $a \in A$ esetén $ae - a \in \mathfrak{m}$ és $ea - a \in \mathfrak{m}$, akkor $\pi_{A/\mathfrak{m}}(e)$ multiplikatív neutrális elem az $A/\mathfrak{m}$ faktoralgebrában, továbbá a faktoralgebra nem nulla, mert $\mathfrak{m}$ valódi ideál. Megfordítva, ha $\mathfrak{m}$ olyan ideál A-ban, hogy az $A/\mathfrak{m}$ faktoralgebra nem nulla és egységelemes, akkor $\mathfrak{m}$ valódi ideál, és van olyan $e \in A$, amelyre $\pi_{A/\mathfrak{m}}(e)$ multiplikatív neutrális elem $A/\mathfrak{m}$-ben; természetesen ekkor minden $a \in A$ esetén

$$\pi_{A/\mathfrak{m}}(ae) = \pi_{A/\mathfrak{m}}(a)\pi_{A/\mathfrak{m}}(e) = \pi_{A/\mathfrak{m}}(a) = \pi_{A/\mathfrak{m}}(e)\pi_{A/\mathfrak{m}}(a) = \pi_{A/\mathfrak{m}}(ea),$$

tehát $ae - a, ea - a \in \mathrm{Ker}(\pi_{A/\mathfrak{m}}) = \mathfrak{m}$, vagyis $\mathfrak{m}$ reguláris ideál. ■

21.4.4. Állítás. *Legyen A algebra. Ha $\chi \in \mathrm{X}(A)$, akkor* $\mathrm{Ker}(\chi)$ 1*-kodimenziós reguláris ideál A-ban, és az A minden $\mathfrak{m}$* 1*-kodimenziós reguláris ideáljához egyértelműen létezik olyan $\chi \in \mathrm{X}(A)$, amelyre* $\mathrm{Ker}(\chi) = \mathfrak{m}$.

Bizonyítás. Legyen $\chi \in \mathrm{X}(A)$. Az nyilvánvaló, hogy $\mathrm{Ker}(\chi)$ 1-kodimenziós ideál A-ban. A $\chi \neq 0$ feltétel miatt van olyan $e \in A$, hogy $\chi(e) = 1$; ekkor minden $a \in A$ esetén $\chi(ae) = \chi(a) = \chi(ea)$, vagyis $ae - a, ea - a \in \mathrm{Ker}(\chi)$, így $\mathrm{Ker}(\chi)$ reguláris ideál.

Legyen $\mathfrak{m}$ tetszőleges 1-kodimenziós reguláris ideál A-ban. Az előző állítás szerint $A/\mathfrak{m}$ nem nulla és egységelemes algebra K felett. Legyen $e \in A$ olyan, hogy minden $a \in A$ esetén $ae - a, ea - a \in \mathfrak{m}$; ekkor $\pi_{A/\mathfrak{m}}(e)$ az $A/\mathfrak{m}$-nek egységeleme. Ebből következik, hogy a

$$\sigma : K \to A/\mathfrak{m}; \quad \lambda \mapsto \lambda.\pi_{A/\mathfrak{m}}(e)$$

leképezés algebra-morfizmus, és ez *bijekció*, mert $A/\mathfrak{m}$ a K felett 1 dimenziós vektortér. Tehát σ algebra-izomorfizmus, így $\chi := \sigma^{-1} \circ \pi_{A/\mathfrak{m}} : A \to K$ algebra-morfizmus, és $\mathrm{Ker}(\chi) = \mathrm{Ker}(\pi_{A/\mathfrak{m}}) = \mathfrak{m}$, vagyis $\chi \in \mathrm{X}(A)$ és $\mathrm{Ker}(\chi) = \mathfrak{m}$. Ha $\chi' \in \mathrm{X}(A)$ szintén olyan, hogy $\mathrm{Ker}(\chi') = \mathfrak{m}$, akkor van olyan $\lambda \in K$, hogy $\chi' = \lambda.\chi$. Véve olyan $a \in A$ elemet, amelyre $\chi'(a) \neq 0$; ebből kapjuk, hogy $\chi(a) \neq 0$, valamint $\lambda \neq 0$, továbbá

$$\lambda^2\chi(a)^2 = (\chi'(a))^2 = \chi'(a^2) = \lambda\chi(a^2) = \lambda\chi(a)^2,$$

így $\lambda = 1$, vagyis $\chi' = \chi$. ■

Természetesen minden 1-kodimenziós ideál maximális ideál. Azonban maximális ideál nem szükségképpen 1-kodimenziós. Például az $\mathbb{R}[X]$ polinomalgebrában az $X^2 + 1$ polinom által generált főideál maximális, de 2-kodimenziós. A nulla-szorzású algebrák példája mutatja, hogy maximális, sőt még 1-kodimenziós ideál sem szükségképpen reguláris.

Nyilvánvaló, hogy ha A nulla szorzású algebra, akkor $\mathrm{X}(A) = \emptyset$, mert ha χ karaktere A-nak, akkor minden $a \in A$ esetén $(\chi(a))^2 = \chi(a^2) = \chi(0) = 0$, tehát $\chi(a) = 0$. Azonban az előző állítás alkalmazható annak bizonyítására, hogy létezik nem nulla dimenziós egységelemes algebra, amelynek nincs nem triviális karaktere.

Példa. Ha K test és $n \in \mathbb{N}$, akkor $n \geq 2$ esetén $\mathrm{X}(\mathrm{M}_n(K)) = \emptyset$, ahol $\mathrm{M}_n(K)$ a K-beli együtthatós $n \times n$-es mátrixok n^2-dimenziós algebrája. Ennek bizonyításához legyen minden $i, j < n$ természetes számra $\mathbf{e}_{i,j} \in \mathrm{M}_n(K)$ az a mátrix, amelyre minden $k, l < n$ természetes számra $(\mathbf{e}_{i,j})_{k,l} := \delta_{i,k}\delta_{j,l}$, vagyis $\mathbf{e}_{i,j}$ az az $n \times n$-es mátrix, amelynek i-edik sorában és j-edik oszlopában 1 áll, és a többi mátrixeleme 0. Világos, hogy az $(\mathbf{e}_{i,j})_{0 \leq i,j < n}$ rendszer bázis az $\mathrm{M}_n(K)$ vektortérben. Könnyen kiszámítható, hogy ha $i, j, k, l < n$ tetszőleges természetes számok, akkor $\mathbf{e}_{i,j}\mathbf{e}_{k,l} = \delta_{j,k}\mathbf{e}_{i,l}$. Speciálian, ha $a \in \mathrm{M}_n(K)$, akkor $a = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_{i,j}\mathbf{e}_{i,j}$, amiből egyszerűen kiszámítható, hogy ha $i, j, k, l < n$ tetszőleges természetes számok, akkor $\mathbf{e}_{i,j}a\mathbf{e}_{k,l} = a_{j,k}\mathbf{e}_{i,l}$. Ha $\mathfrak{m} \subseteq \mathrm{M}_n(K)$ ideál, és $a \in \mathfrak{m}$ olyan elem, amelynek (j,k)-adik mátrixeleme nem 0, akkor *minden* $i, l < n$ természetes számra $\mathbf{e}_{i,l} = a_{j,k}^{-1}\mathbf{e}_{i,j}a\mathbf{e}_{k,l} \in \mathfrak{m}$, tehát $\mathfrak{m} = \mathrm{M}_n(K)$. Ez azt jelenti, hogy az $\mathrm{M}_n(K)$ algebrában minden nem nulla dimenziós ideál egyenlő $\mathrm{M}_n(K)$-val, ezért az előző állítás alapján $\mathrm{M}_n(K)$ felett nem létezik nem nulla karakter.

21.4.5. Állítás. *Egységelemes algebra minden valódi ideálja részhalmaza egy maximális ideálnak.*

Bizonyítás. Legyen $\mathfrak{m}$ valódi ideál az A egységelemes algebrában, és jelölje $S_{\mathfrak{m}}$ az A $\mathfrak{m}$-t tartalmazó valódi ideáljainak halmazát. Az $S_{\mathfrak{m}}$ halmazt a tartalmazás relációval rendezve, könnyen látható, hogy $S_{\mathfrak{m}}$ induktívan rendezett halmaz. Valóban, ha $(\mathfrak{n}_i)_{i \in I}$

olyan $S_{\mathfrak{m}}$-ben haladó rendszer, amelyre minden $i, j \in I$ esetén $\mathfrak{n}_i \subseteq \mathfrak{n}_j$ vagy $\mathfrak{n}_j \subseteq \mathfrak{n}_i$, akkor az $\mathfrak{n} := \bigcup_{i \in I} \mathfrak{n}_i$ halmaz olyan ideál A-ban, amely $\mathfrak{m}$-et tartalmazza, és valódi is, mert minden $I \ni i$-re $\mathbf{1} \notin \mathfrak{n}_i$, így $\mathbf{1} \notin \mathfrak{n}$; ezért $\mathfrak{n} \in S_{\mathfrak{m}}$, és $\mathfrak{n}$ felső korlátja (sőt szuprémuma) az $(\mathfrak{n}_i)_{i \in I}$ rendszernek. A Zorn-lemma alapján létezik $S_{\mathfrak{m}}$-nek maximális eleme; ez maximális ideál A-ban, amely $\mathfrak{m}$-et tartalmazza. ■

21.4.6. Állítás. *Ha A algebra K felett, és $\mathfrak{m}$ reguláris maximális ideál A-ban, akkor létezik olyan $\tilde{\mathfrak{m}}$ maximális ideál $\tilde{A}$-ban, amelyre $\mathfrak{m} = \tilde{\mathfrak{m}} \cap A$.*

Bizonyítás. Legyen $e \in A$ olyan elem, amelyre hogy minden $a \in A$ esetén $ae - a, ea - a \in \mathfrak{m}$, és vezessük be a

$$\mathfrak{n} := K.(\mathbf{1} - e) + \mathfrak{m}$$

lineáris alteret $\tilde{A}$-ban, ahol $\mathbf{1}$ az egységelemet jelöli $\tilde{A}$-ban. Ekkor a definíció alapján $\mathfrak{n} = \{(\lambda, a - \lambda.e) | (\lambda \in K) \wedge (a \in \mathfrak{m})\}$, amiből közvetlenül látható, hogy $\mathfrak{n}$ ideál $\tilde{A}$-ban, hiszen ha $(\lambda, a - \lambda.e) \in \mathfrak{n}$ és $(\lambda', a') \in \tilde{A}$, akkor

$$(\lambda, a - \lambda.e)(\lambda', a') = (\lambda\lambda', (\lambda.(a' - ea') + \lambda'.a + aa') - (\lambda'\lambda).e) \in \mathfrak{n},$$
$$(\lambda', a')(\lambda, a - \lambda.e) = (\lambda'\lambda, (\lambda.(a' - a'e) + \lambda'.a + a'a) - (\lambda'\lambda).e) \in \mathfrak{n},$$

hiszen $a' - ea', a' - a'e \in \mathfrak{m}$ és $aa', a'a \in \mathfrak{m}$.

Az $\mathfrak{n}$ ideál valódi, mert ha $\mathfrak{n} = \tilde{A}$ teljesülne, akkor $(0, e) \in \mathfrak{n}$ miatt létezne $\lambda \in K$ és $a \in \mathfrak{m}$ úgy, hogy $(\lambda, a - \lambda.e) = (0, e)$, tehát $\lambda = 0$ és $e = a \in \mathfrak{m}$, amiből (az e definíciója alapján) $\mathfrak{m} = A$ következne. Az előző állítás szerint vehetünk egy $\tilde{\mathfrak{m}}$ maximális ideált $\tilde{A}$-ban, amelyre $\mathfrak{n} \subseteq \tilde{\mathfrak{m}}$. Világos, hogy $\mathfrak{m} \subseteq \tilde{\mathfrak{m}} \cap A$. Ha itt nem állna egyenlőség, akkor $\tilde{\mathfrak{m}} \cap A = A$ teljesülne, mert $\tilde{\mathfrak{m}} \cap A$ ideál A-ban és $\mathfrak{m}$ maximális ideál A-ban; ekkor $e \in A \subseteq \tilde{\mathfrak{m}}$, ugyanakkor $\mathbf{1} - e \in \mathfrak{n} \subseteq \tilde{\mathfrak{m}}$, tehát $\mathbf{1} = e + (\mathbf{1} - e) \in \tilde{\mathfrak{m}}$, ami ellentmond annak, hogy $\tilde{\mathfrak{m}}$ valódi ideál $\tilde{A}$-ban. ■

21.4.7. Következmény. *Ha A kommutatív algebra a K test felett és $\mathfrak{m}$ reguláris maximális ideál A-ban, akkor $A/\mathfrak{m}$ testbővítése K-nak.*

Bizonyítás. Legyen $e \in A$ olyan elem, amelyre minden $a \in A$ esetén $ae - a, ea - a \in \mathfrak{m}$. Ekkor $\pi_{A/\mathfrak{m}}(e)$ egységeleme az $A/\mathfrak{m}$ kommutatív algebrának. Legyen $a \in A$ olyan, hogy $\pi_{A/\mathfrak{m}}(a) \neq 0$. Ekkor $a \notin \mathfrak{m}$, és az $Aa + \mathfrak{m}$ halmaz olyan ideál A-ban, amely $\mathfrak{m}$-t tartalmazza, így $\mathfrak{m} = Aa + \mathfrak{m}$ vagy $A = Aa + \mathfrak{m}$. De $\mathfrak{m} = Aa + \mathfrak{m}$ lehetetlen, különben $ea \in Aa \subseteq \mathfrak{m}$, így $a = ea + (a - ea) \in \mathfrak{m} + \mathfrak{m} \subseteq \mathfrak{m}$, holott $a \notin \mathfrak{m}$. Ezért $e \in A = Aa + \mathfrak{m}$, így létezik olyan $b \in A$, amelyre $e - ba \in \mathfrak{m}$, következésképpen $\pi_{A/\mathfrak{m}}(e) = \pi_{A/\mathfrak{m}}(b)\pi_{A/\mathfrak{m}}(a)$. Ez azt jelenti, hogy a $\pi_{A/\mathfrak{m}}(a)$ elem invertálható $A/\mathfrak{m}$-ben, vagyis az $A/\mathfrak{m}$ gyűrű test. Továbbá, a

$$K \to A/\mathfrak{m}; \quad \lambda \mapsto \lambda.\pi_{A/\mathfrak{m}}(e)$$

leképezés injektív algebra-morfizmus, így $A/\mathfrak{m}$ testbővítése K-nak. ■

Az előző állítás bizonyításában lényegesen kihasználtuk A kommutativitását. Ugyanis, ha A nem kommutatív, akkor az Aa halmaz nem feltétlenül ideál (hanem csak baloldali ideál) A-ban, ezért Aa helyett az AaA halmazt kell venni. Ekkor $\mathfrak{m} = AaA + \mathfrak{m}$ lehetetlen, különben $a = (a - ea) + (ea - eae) + eae \in \mathfrak{m} + \mathfrak{m} + \mathfrak{m} \subseteq \mathfrak{m}$ teljesülne. Ezért $A = AaA + \mathfrak{m}$, amiből következik olyan $b, c \in A$ létezése, hogy $\pi_{A/\mathfrak{m}}(e) = \pi_{A/\mathfrak{m}}(b)\pi_{A/\mathfrak{m}}(a)\pi_{A/\mathfrak{m}}(c)$, és itt $\pi_{A/\mathfrak{m}}(e)$ az $A/\mathfrak{m}$ faktoralgebra egységeleme. Ebből viszont nem következik a $\pi_{A/\mathfrak{m}}(a)$ elem invertálhatósága $A/\mathfrak{m}$-ben. (Például, legyen A a $K^{(\mathbb{N})}$ vektortér lineáris operátorainak egységelemes, nem kommutatív algebrája, és

– legyen $c \in A$ az az operátor, amelyre $x \in K^{(\mathbb{N})}$ esetén minden $\mathbb{N} \ni k$-ra $c(x)(k) = x(k-2)$, ha $k \geq 2$ és $c(x)(1) := c(x)(0) := 0$, továbbá

– legyen $b := a \in A$ az az operátor, amelyre $x \in K^{(\mathbb{N})}$ esetén minden $\mathbb{N} \ni k$-ra $a(x)(k) = x(k+1)$.

Ekkor $b \circ a \circ c = \mathbf{1}$, de az $a, b, c \in A$ elemek egyike sem invertálható A-ban, hiszen c nem szürjektív operátor és a, b nem injektív operátorok.)

21.5. Részalgebrák

– Algebra minden *részalgebrája* szintén algebra a műveletek leszűkítésével ellátva. Most bemutatunk két nevezetes részalgebra-konstrukciót.

a) Legyen A algebra és $e \in A$ *idempotens* elem, vagyis $e^2 = e$. Ekkor az

$$eAe := \{eae \mid a \in A\}$$

halmaz olyan részalgebrája A-nak, amelynek e egységeleme; ezt nevezzük az e idempotens elem által *redukált részalgebrának* A-ban. Könnyen látható, hogy

$$eAe = \{a \in A \mid ea = ae = a\}.$$

b) Legyen A algebra és $S \subseteq A$. Ekkor a

$$\mathrm{C}(S) := \{a \in A \mid (\forall s \in S): \ as = sa\}$$

halmaz részalgebrája A-nak; ezt nevezzük az S halmaz *kommutánsának*. A $\mathrm{C}(\mathrm{C}(S))$ halmaz S-t tartalmazó részalgebra A-ban; $\mathrm{C}(\mathrm{C}(S))$-t az S halmaz *bikommutánsának* nevezzük. Ha S kommutatív halmaz (vagyis bármely két eleme felcserélhető), akkor az S bikommutánsa is kommutatív részalgebra A-ban. Megjegyezzük, hogy ha A kommutatív algebra, akkor minden $S \subseteq A$ halmazra $\mathrm{C}(S) = A$, tehát a kommutáns-képzés csak nemkommutatív algebrában nem triviális részalgebra-konstrukció.

21.6. Ideálok és faktoralgebrák

21.7. Félcsoport-algebrák és csoportalgebrák

Legyen S egységelemes félcsoport (azaz *monoid*), K test, és ismét tekintsük a

$$K^{(S)} := \{a \in \mathscr{F}(S;K) | \text{"az } \{s \in S | a(s) \neq 0\} \text{ halmaz véges"}\}$$

halmazt. Ez lineáris altere az $\mathscr{F}(S;K)$ függvénytérnek, amit az S halmaz által generált *szabad vektortérnek* nevezünk K felett. Most a $K^{(S)}$ felett értelmezzük a $*$ műveletet úgy, hogy minden $a, b \in K^{(S)}$ és $s \in S$ esetén

$$(a * b)(s) = \sum_{(s',s'') \in S \times S, \ s's''=s} a(s')b(s'').$$

Könnyen látható, hogy $a, b \in K^{(S)}$ esetén $a * b \in K^{(S)}$, és a $K^{(S)}$ vektortér a $*$ szorzással ellátva egységelemes algebra; ezt nevezzük az S monoid K feletti *konvolúciós* *algebrájának*, és $A_K(S)$-sel jelöljük. Legyen minden $s \in S$ esetén $\varepsilon_s \in K^{(S)}$ az az elem, amelyre minden $S \ni s'$-re, ha $s' \neq s$, akkor $\varepsilon_s(s') = 0$, és $\varepsilon_s(s) = 1$. Ekkor az $\{\varepsilon_s | s \in S\}$ halmaz bázisa $K^{(S)}$ vektortérnek, és a $j : S \to A_K(S)$ leképezés injektív egységelem-tartó félcsoport-morfizmus S és az $A_K(S)$ multiplikatív félcsoport között. Az $A_K(S)$ algebra pontosan akkor kommutatív, ha S kommutatív. Ha A egységelemes algebra K felett, akkor minden $f : S \to A$ egységelem-tartó félcsoport-morfizmushoz létezik egyetlen olyan $\tilde{f} : A_K(S) \to A$ egységelem-tartó algebra-morfizmus, amelyre $\tilde{f} \circ j = f$. Fontos speciális esetek a következők.

– $S := \mathbb{N}$ és S művelete az összeadás. Az így értelmezett $\mathbb{N}$ kommutatív monoid K test feletti konvolúciós algebráját a $K[X]$ szimbólummal is jelöljük, és X jelöli azt az elemet ebben az algebrában, amelyre $n \in \mathbb{N}$ esetén $\mathrm{X}(n) = 0$, ha $n \neq 1$, és $\mathrm{X}(1) = 1$ (vagyis $X := \varepsilon_1$). A $K[X]$ algebrát a K feletti *egyváltozós polinomok algebrájának* nevezzük. Nyilvánvaló, hogy az X elem generálja a $K[X]$ algebrát, és minden $P \in K[X]$ esetén fennáll a

$$P = \sum_{k=0}^{\infty} P(k) X^k$$

egyenlőség, ahol természetesen véges összegzés áll.

– $S := \mathbb{N}^n$, ahol $n \in \mathbb{N}^*$, és S művelete az összeadás. Az így értelmezett $\mathbb{N}^n$ kommutatív monoid K test feletti konvolúciós algebráját a $K[X_1, ..., X_n]$ szimbólummal is jelöljük, és minden $1 \leq k \leq n$ természetes számra X_k jelöli azt az elemet ebben az algebrában, amelyre $\alpha \in \mathbb{N}^n$ esetén $X_k(\alpha) = 0$, ha $\alpha \neq e_k$, és $X_k(e_k) = 1$, ahol e_k a k-adik kanonikus báziselem $\mathbb{N}^n$-ben (vagyis $X_k := \varepsilon_{e_k}$). A $K[X_1, ..., X_n]$ algebrát a K feletti *n-változós polinomok algebrájának* nevezzük. Nyilvánvaló, hogy az $X_1, ..., X_n$ elemek generálják a $K[X_1, ..., X_n]$ algebrát, és minden $P \in K[X_1, ..., X_n]$ esetén fennáll a

$$P = \sum_{\alpha \in \mathbb{N}^n}^{\infty} P(\alpha) \left(\prod_{k=1}^{n} X_k^{\alpha(k)} \right)$$

egyenlőség, ahol természetesen véges összegzés áll.

Megjegyezzük még, hogy ha G csoport, akkor az $A_K(G)$ algebrát a G csoport K feletti *csoport-algebrájának* nevezzük.

21.8. Polinomiális vektorfüggvények

1. (*Többváltozós polinomiális függvények.*) Legyen $n \in \mathbb{N}^*$ rögzített, és az $\mathbb{N}^n$ halmaz elemeit nevezzük *n-dimenziós multiindexeknek*. Ha $\alpha \in \mathbb{N}^n$, akkor $|\alpha| := \sum_{i \in n} \alpha_i$, továbbá minden K testre és $t \in K^n$ elemre $t^\alpha := \underset{i \in n}{\mathrm{P}}\, t_i^{\alpha_i}$.

a) Legyen F vektortér a K test felett. Egy $f : K^n \to F$ leképezést F-be ható, n-változós *polinomiális függvénynek* nevezünk, ha létezik olyan $(z_\alpha)_{\alpha \in \mathbb{N}^n} \in F^{(\mathbb{N}^n)}$ rendszer, hogy minden $K^n \ni t$-re

$$f(t) = \sum_{\alpha \in \mathbb{N}^n} t^\alpha . z_\alpha$$

teljesül. (Itt véges összegzés áll, hiszen $F^{(\mathbb{N}^n)}$ azon $\mathbb{N}^n \to F$ függvények halmaza, amelyek csak véges sok helyen vesznek fel nem nulla értéket.) Jelölje $\mathrm{P}(K^n; F)$ az F-be érkező n-változós polinomiális függvények halmazát. Ekkor $\mathrm{P}(K^n; F)$ lineáris altere az $\mathscr{F}(K^n; F)$

függvénytérnek, továbbá az

$$F^{(\mathbb{N}^n)} \to \mathrm{P}(K^n; F); \quad (z_\alpha)_{\alpha \in \mathbb{N}^n} \mapsto \left(t \mapsto \sum_{\alpha \in \mathbb{N}^n} t^\alpha . z_\alpha \right)$$

leképzés *szürjekció.*

b) Ha K *végtelen* test és F vektortér K felett, akkor az előző leképzés *injekció* (tehát az a) alapján *bijekció is*). Ekkor minden $f : K^n \to F$ polinomiális függvényhez *egyértelműen* létezik olyan $(z_\alpha)_{\alpha \in \mathbb{N}^n} \in F^{(\mathbb{N}^n)}$ rendszer, hogy minden $K^n \ni t$-re $f(t) = \sum_{\alpha \in \mathbb{N}^n} t^\alpha . z_\alpha$. (Ez a *polinomiális függvények együtthatói egyértelműségének* tétele.)

(*Útmutatás.* A b) bizonyításához azt kell igazolni, hogy ha K végtelen test és F vektortér K felett, akkor minden $n \in \mathbb{N}^*$ számra és minden $(z_\alpha)_{\alpha \in \mathbb{N}^n} \in F^{(\mathbb{N}^n)}$ rendszerre; ha minden $K^n \ni t$-re $\sum_{\alpha \in \mathbb{N}^n} t^\alpha . z_\alpha = 0$, akkor minden $\alpha \in \mathbb{N}^n$ multiindexre $z_\alpha = 0$. Ezt n szerinti teljes indukcióval bizonyítjuk.

Az $n = 1$ esetben legyen $(z_\alpha)_{\alpha \in \mathbb{N}} \in F^{(\mathbb{N})}$ olyan rendszer, amelyre minden $t \in K$ esetén $\sum_{\alpha \in \mathbb{N}} t^\alpha . z_\alpha = 0$. Ekkor minden $F^* \ni u$-ra és $K \ni t$-re $\sum_{\alpha \in \mathbb{N}} t^\alpha u(z_\alpha) = 0$ teljesül. Tehát ha az állítás igaz az $F := K$ esetben, akkor minden $F^* \ni u$-ra és minden $\mathbb{N} \ni \alpha$-ra $u(z_\alpha) = 0$, így a VI. fejezet, 2. pont, **19**. gyakorlat szerint minden $\mathbb{N} \ni \alpha$-ra $z_\alpha = 0$. Ezzel az $n = 1$ esetben a problémát visszavezettük az $F := K$ speciális esetre. Ekkor az $f : K \to K;\ t \mapsto \sum_{\alpha \in \mathbb{N}} t^\alpha . z_\alpha$ polinomiális függvénynek legfeljebb N darab nullhelye létezhet, ha a $(z_\alpha)_{\alpha \in \mathbb{N}} \in K[X]$ polinom N-ed fokú és $N > 0$ (II. fejezet, 1. pont, **12**. gyakorlat). Ezért a K végtelensége miatt minden $\mathbb{N} \ni \alpha$-ra $z_\alpha = 0$.

Tegyük fel, hogy az állítás igaz az $n \in \mathbb{N}^*$ számra, és legyen $(z_\alpha)_{\alpha \in \mathbb{N}^{n+1}} \in F^{(\mathbb{N}^{n+1})}$ olyan rendszer, hogy az

$$f : K^{n+1} \to F; \quad t \mapsto \sum_{\alpha \in \mathbb{N}^n} t^\alpha . z_\alpha$$

függvény azonosan 0. Rögzítsünk olyan $N \in \mathbb{N}$ számot, amelyre minden $\alpha \in \mathbb{N}^{n+1}$ esetén, ha $|\alpha| > N$, akkor $z_\alpha = 0$. Minden $s \in K$ elemre értelmezzük a következő függvényt

$$f_s : K^n \to F; \quad (t_i)_{i \in n} \mapsto f(t_0, ..., t_{n-1}, s).$$

Ha $s \in K$, akkor minden $(t_i)_{i \in n} \in K^n$ elemre

$$f_s((t_i)_{i \in n}) := f(t_0, ..., t_{n-1}, s) =$$

$$= \sum_{\beta \in \mathbb{N}^n,\ |\beta| \leq N} t^\beta z_{\beta_0, ..., \beta_{n-1}, 0} + \sum_{\beta \in \mathbb{N}^{n+1},\ |\beta| \leq N,\ \beta_n > 0} \left(\mathrm{P}_{i \in n} t_i^{\beta_i} \right) s^{\beta_n} z_\beta =$$

$$= \sum_{\beta \in \mathbb{N}^n,\ |\beta| \leq N} t^\beta z_{\beta_0, ..., \beta_{n-1}, 0} + \sum_{\beta \in \mathbb{N}^n,\ |\beta| < N} t^\beta \left(\sum_{k=1}^{N - |\beta|} s^k . z_{\beta_0, ..., \beta_{n-1}, k} \right) =$$

$$= \sum_{\beta \in \mathbb{N}^n,\ |\beta| = N} t^\beta z_{\beta_0, ..., \beta_{n-1}, 0} + \sum_{\beta \in \mathbb{N}^n,\ |\beta| < N} t^\beta \left(z_{\beta_0, ..., \beta_{n-1}, 0} + \sum_{k=1}^{N - |\beta|} s^k z_{\beta_0, ..., \beta_{n-1}, k} \right)$$

tehát $f_s \in \mathrm{P}(K^n; F)$, és a feltevés szerint f_s az azonosan 0 függvény. Az indukciós hipotézis alapján ebből következik, hogy minden $K \ni s$-re és minden $N^n \ni \beta$-ra; ha

$|\beta| = N$, akkor $z_{\beta_0,\ldots,\beta_{n-1},0} = 0$, és ha $|\beta| < N$, akkor

$$z_{\beta_0,\ldots,\beta_{n-1},0} + \sum_{k=1}^{N-|\beta|} s^k z_{\beta_0,\ldots,\beta_{n-1},k} = 0.$$

Alkalmazva az állítást $n = 1$ esetén; ebből kapjuk, hogy minden $N^n \ni \beta$-ra; ha $|\beta| = N$, akkor $z_{\beta_0,\ldots,\beta_{n-1},0} = 0$, és ha $|\beta| < N$, akkor $z_{\beta_0,\ldots,\beta_{n-1},0} = 0$ és minden $1 \leq k \leq N - |\beta|$ természetes számra $z_{\beta_0,\ldots,\beta_{n-1},k} = 0$. Könnyen látható, hogy ez azt jelenti, hogy minden $\beta \in \mathbb{N}^{n+1}$ multiindexre $z_\beta = 0$.)

13. Minden $p, n \in \mathbb{N}$ esetén jelölje $\mathscr{M}(p; n)$ a $p \to n$ szigorúan monoton növő függvények halmazát. Legyenek E és F vektorterek a K test felett, és minden $f : E \to F$ függvényre, $\mathbb{N}^* \ni n$-re és $\mathbf{x} := (x_i)_{i\in n} \in E^n$ rendszerre értelmezzük a

$$\Delta_{\mathbf{x}} f : E \to F; \quad z \mapsto \sum_{p=0}^{n} (-1)^{n-p} \sum_{\sigma\in\mathscr{M}(p;n)} f\left(z + \sum_{k\in p} x_{\sigma(k)}\right)$$

függvényt (azzal a megállapodással, hogy üres indexhalmaz esetén az összeg egyenlő 0-val).

a) Ha $f : E \to F$ függvény, $x_0, x_1, x_2 \in E$ és $z \in E$, akkor

$$(\Delta_{(x_0)} f)(z) = f(z + x_0) - f(z),$$

$$(\Delta_{(x_0,x_1)} f)(z) = f(z + x_0 + x_1) - f(z + x_0) - f(z + x_1) + f(z),$$

$$(\Delta_{(x_0,x_1,x_2)} f)(z) = f(z + x_0 + x_1 + x_1) - f(z + x_0 + x_1) - f(z + x_0 + x_2) -$$

$$-f(z + x_1 + x_2) + f(z + x_0) + f(z + x_1) + f(z + x_2) - f(z).$$

Ennek alapján sejthető, hogy ha $f : E \to F$ függvény, $n \in \mathbb{N}^*$, és $(x_i)_{i\in n+1} \in E^{n+1}$, akkor

$$\Delta_{(x_i)_{i\in n+1}} f = \Delta_{(x_n)}(\Delta_{(x_i)_{i\in n}} f).$$

Ez n szerinti teljes indukcióval könnyen igazolható.

b) Legyen $n \in \mathbb{N}^*$, $u \in \mathbf{L}^s_n(E; F)$, és jelölje $u \circ \mathrm{id}_E^{[n]}$ az $E \to F;\ x \mapsto u(x^{[n]})$ függvényt. Ekkor minden $\mathbf{x} \in E^n$ és $z \in E$ esetén

$$n!u(\mathbf{x}) = (\Delta_{\mathbf{x}}(u \circ \mathrm{id}_E^{[n]}))(z),$$

tehát a $\Delta_{\mathbf{x}}(u \circ \mathrm{id}_E^{[n]})$ függvény *állandó*, és az értéke egyenlő $n!u(\mathbf{x})$-szel. Ha tehát a K test nulla karakterisztikájú, akkor minden $\mathbf{x} \in E^n$ elemre

$$u(\mathbf{x}) = \frac{1}{n!}(\Delta_{\mathbf{x}}(u \circ \mathrm{id}_E^{[n]}))(0)$$

teljesül. Ebből új bizonyítást nyerhetünk a szimmetrikus multilineáris operátorok meghatározottsági tételére.

21.9. Vektortér tenzoralgebrája

21.9.1. Definíció. *Legyen E vektortér a K test felett. Ekkor*

$$\mathbf{T}^0(E) := K,$$
$$\mathbf{T}^1(E) := E,$$

és minden $n \in \mathbb{N}$, $n \geq 2$ számra

$$\mathbf{T}^n(E) := \bigotimes_{i \in n} E_i,$$

ahol minden $i \in n$ esetén $E_i := E$. Továbbá:

$$\mathbf{T}(E) := \bigoplus_{n \in \mathbb{N}} \mathbf{T}^n(E),$$

és minden $n \in \mathbb{N}$ esetén $\mathrm{in}_{\mathbf{T}^n(E),\mathbf{T}(E)} : \mathbf{T}^n(E) \to \mathbf{T}(E)$ jelöli az n-edik kanonikus injekciót, tehát minden $t \in \mathbf{T}^n(E)$ esetén $\mathrm{in}_{\mathbf{T}^n(E),\mathbf{T}(E)}(t)$ az a sorozat, amelynek n-edik komponense egyenlő t-vel, és minden $m \in \mathbb{N}$, $m \neq n$ számra az m-edik komponense egyenlő a $\mathbf{T}^m(E)$ vektortér additív neutrális elemével.

Tehát ha E vektortér a K test felett, akkor $\mathbf{T}(E)$ az a vektortér, amelynek elemei azok a $(t_n)_{n\in\mathbb{N}}$ (tenzor)sorozatok, amelyekre minden $n \in \mathbb{N}$ esetén $t_n \in \mathbf{T}^n(E)$, és $\{n \in \mathbb{N} | t_n \neq 0\}$ véges halmaz, továbbá minden $(t_n)_{n\in\mathbb{N}}, (t'_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$ és $\lambda \in K$ esetén

$$(t_n)_{n\in\mathbb{N}} + (t'_n)_{n\in\mathbb{N}} := (t_n + t'_n)_{n\in\mathbb{N}},$$
$$\lambda.(t_n)_{n\in\mathbb{N}} = (\lambda.t_n)_{n\in\mathbb{N}}.$$

Megjegyezzük, hogy ha K test, akkor $\mathbf{T}(K)$ kanonikusan lineárisan izomorf a $K^{(\mathbb{N})}$ (végtelen dimenziós) sorozattérrel.

21.9.2. Állítás. *Legyen E vektortér a K test felett. Minden $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$ párhoz létezik egyetlen olyan*

$$\mathrm{p}_{m,n} : \mathbf{T}^m(E) \times \mathbf{T}^n(E) \to \mathbf{T}^{m+n}(E)$$

bilineáris leképezés, amelyre teljesül az, hogy minden $(x_i)_{i\in m} \in E^m$ és $(y_j)_{j\in n} \in E^n$ esetén

$$\mathrm{p}_{m,n}\left(\bigotimes_{i\in m} x_i, \bigotimes_{j\in n} y_j\right) = \bigotimes_{k\in m+n} z_k,$$

ahol minden $k \in m+n$ számra

$$z_k := \begin{cases} x_k & , \text{ha } k < m, \\ y_{k-m} & , \text{ha } m \leq k < m+n. \end{cases} \tag{1}$$

Bizonyítás. (*Egzisztencia.*) Legyen $\mathbf{y} := (y_j)_{j\in n} \in E^n$ rögzítve, és értelmezzük azt a

$$\tau_{\mathbf{y}} : E^m \to \mathbf{T}^{m+n}(E)$$

leképezést, amelyre minden $(x_i)_{i\in m} \in E^m$ esetén

$$\tau_{\mathbf{y}}\left((x_i)_{i\in m}\right) := \bigotimes_{k\in m+n} z_k,$$

ahol $(z_k)_{k\in m+n} \in E^{m+n}$ az a rendszer, amelyet az (1) egyenlőség értelmez. Ekkor $\tau_{\mathbf{y}}$ m-lineáris operátor, vagyis $\tau_{\mathbf{y}} \in \mathbf{L}_m(E; \mathbf{T}^{m+n}(E))$. Valóban, legyen $l \in m$ és

$\mathbf{x} = (x_i)_{i \in m} \in E^m$ rögzített. Vezessük be a $\mathbf{z} = (z_k)_{k \in m+n} \in E^{m+n}$ rendszert úgy, hogy minden $k \in m+n$ esetén

$$z_k := \begin{cases} x_k & \text{, ha } k < m, , \\ y_{k-m} & \text{, ha } m \leq k < m+n. \end{cases}$$

Könnyen látható, hogy

$$\tau_{\mathbf{y}} \circ \mathrm{in}_{l,\mathbf{x}} = u \circ \mathrm{in}_{l,\mathbf{z}}, \tag{2}$$

ahol $u : E^{m+n} \to \mathbf{T}^{m+n}(E)$ a kanonikus $m+n$-lineáris operátor, hiszen minden $x \in E$ esetén

$$(\tau_{\mathbf{y}} \circ \mathrm{in}_{l,\mathbf{x}})(x) = \tau_{\mathbf{y}}(\mathrm{in}_{l,\mathbf{x}}(x)) = \bigotimes_{k \in m+n} z'_k,$$

ahol minden $k \in m+n$ számra

$$z'_k := \begin{cases} x_k & \text{, ha } k < m \text{ és } k \neq l, \\ x & \text{, ha } k = l, \\ y_{k-m} & \text{, ha } m \leq k < m+n, \end{cases}$$

ugyanakkor

$$(u \circ \mathrm{in}_{l,\mathbf{z}})(x) = u(\mathrm{in}_{l,\mathbf{z}}(x)) = \bigotimes_{k \in m+n} z''_k,$$

ahol minden $k \in m+n$ esetén $z''_k = (\mathrm{in}_{l,\mathbf{z}}(x))_k$, vagyis $z''_l = x$ és $k \neq l$ esetén $z''_k = z_k$, ezért $\mathbf{z}$ definíciója szerint

$$z''_k = \begin{cases} x_k & \text{, ha } k < m \text{ és } k \neq l, \\ x & \text{, ha } k = l, \\ y_{k-m} & \text{, ha } m \leq k < m+n, \end{cases}$$

azaz $(z'_k)_{k \in m+n} = (z''_k)_{k \in m+n}$. Tehát fennáll az (2) egyenlőség, így u multilinearitása folytán a $\tau_{\mathbf{y}} \circ \mathrm{in}_{l,\mathbf{x}} : E \to \mathbf{T}^{m+n}(E)$ leképezés lineáris operátor. A tenzorszorzat univerzalitási tulajdonsága alapján ebből következik, hogy létezik egyetlen olyan

$$\tilde{\tau_{\mathbf{y}}} : \mathbf{T}^m(E) \to \mathbf{T}^{m+n}(E)$$

lineáris operátor, hogy minden $(x_i)_{i \in m} \in E^m$ esetén

$$\tilde{\tau_{\mathbf{y}}}\left(\bigotimes_{i \in m} x_i\right) = \tau_{\mathbf{y}}\left((x_i)_{i \in m}\right).$$

Megmutatjuk, hogy a

$$\tau : E^n \to \mathbf{L}\left(\mathbf{T}^m(E); \mathbf{T}^{m+n}(E)\right); \quad \mathbf{y} \mapsto \tilde{\tau_{\mathbf{y}}}$$

leképezés n-lineáris operátor. Ennek bizonyításához legyen $l \in n$ és $\mathbf{y} = (y_j)_{j \in n} \in E^n$ rögzített. Rögzítsünk egy $\mathbf{x} = (x_i)_{i \in m} \in E^m$ rendszert is, és vezessük be a $\mathbf{z} = (z_k)_{k \in m+n} \in E^{m+n}$ rendszert úgy, hogy minden $k \in m+n$ esetén

$$z_k := \begin{cases} x_k & \text{, ha } k < m, , \\ y_{k-m} & \text{, ha } m \leq k < m+n. \end{cases}$$

Könnyen látható, hogy minden $y \in E$ esetén

$$((\tau \circ \mathrm{in}_{l,\mathbf{y}})(y))\left(\bigotimes_{i\in m} x_i\right) = (u \circ \mathrm{in}_{m+l,\mathbf{z}})(y), \tag{3}$$

ahol $u : E^{m+n} \to \mathbf{T}^{m+n}(E)$ a kanonikus $m+n$-lineáris operátor, hiszen minden $y \in E$ esetén

$$((\tau \circ \mathrm{in}_{l,\mathbf{y}})(y))\left(\bigotimes_{i\in m} x_i\right) = \tilde{\tau}_{\mathrm{in}_{l,\mathbf{y}}(y)}\left(\bigotimes_{i\in m} x_i\right) = \tau_{\mathrm{in}_{l,\mathbf{y}}(y)}\left((x_i)_{i\in m}\right) = \bigotimes_{k\in m+n} z'_k,$$

ahol minden $k \in m+n$ esetén

$$z'_k := \begin{cases} x_k & \text{, ha } k < m, \\ y & \text{, ha } k = m+l, \\ y_{k-m} & \text{, ha } m \le k < m+n \text{ és } k \ne m+l, \end{cases}$$

ugyanakkor

$$(u \circ \mathrm{in}_{m+l,\mathbf{z}})(y) = u\left(\mathrm{in}_{m+l,\mathbf{z}}(y)\right) = \bigotimes_{k\in m+n} z''_k,$$

ahol minden $k \in m+n$ esetén $z''_k = \left(\mathrm{in}_{m+l,\mathbf{z}}(y)\right)_k$, vagyis $z''_{m+l} = y$ és $k \ne m+l$ esetén $z''_k = z_k$, ezért $\mathbf{z}$ definíciója szerint

$$z''_k = \begin{cases} x_k & \text{, ha } k < m, \\ y & \text{, ha } k = m+l, \\ y_{k-m} & \text{, ha } m \le k < m+n \text{ és } k \ne m+l, \end{cases}$$

azaz $(z'_k)_{k\in m+n} = (z''_k)_{k\in m+n}$. Tehát minden $y \in E$ esetén fennáll a (3) egyenlőség. Ezért minden $y, y' \in E$ vektorra és $\lambda \in K$ elemre kihasználva az $u \circ \mathrm{in}_{m+l,\mathbf{z}} : E \to \mathbf{T}^{m+n}(E)$ leképezés linearitását kapjuk, hogy

$$\begin{aligned}((\tau \circ \mathrm{in}_{l,\mathbf{y}})(y+y'))\left(\bigotimes_{i\in m} x_i\right) &= (u \circ \mathrm{in}_{m+l,\mathbf{z}})(y+y') = (u \circ \mathrm{in}_{m+l,\mathbf{z}})(y) + (u \circ \mathrm{in}_{m+l,\mathbf{z}})(y') = \\ &= ((\tau \circ \mathrm{in}_{l,\mathbf{y}})(y))\left(\bigotimes_{i\in m} x_i\right) + ((\tau \circ \mathrm{in}_{l,\mathbf{y}})(y'))\left(\bigotimes_{i\in m} x_i\right) = \\ &= ((\tau \circ \mathrm{in}_{l,\mathbf{y}})(y) + (\tau \circ \mathrm{in}_{l,\mathbf{y}})(y'))\left(\bigotimes_{i\in m} x_i\right),\end{aligned}$$

valamint

$$\begin{aligned}((\tau \circ \mathrm{in}_{l,\mathbf{y}})(\lambda.y))\left(\bigotimes_{i\in m} x_i\right) &= (u \circ \mathrm{in}_{m+l,\mathbf{z}})(\lambda.y) = \lambda.(u \circ \mathrm{in}_{m+l,\mathbf{z}})(y) = \\ &= \lambda.((\tau \circ \mathrm{in}_{l,\mathbf{y}})(y))\left(\bigotimes_{i\in m} x_i\right) = (\lambda.(\tau \circ \mathrm{in}_{l,\mathbf{y}})(y))\left(\bigotimes_{i\in m} x_i\right).\end{aligned}$$

Mivel a felbontható tenzorok generálják a $\mathbf{T}^n(E)$ vektorteret, ebből következik, hogy minden $y, y' \in E$ vektorra és $\lambda \in K$ elemre

$$\begin{aligned}(\tau \circ \mathrm{in}_{l,\mathbf{y}})(y+y') &= (\tau \circ \mathrm{in}_{l,\mathbf{y}})(y) + (\tau \circ \mathrm{in}_{l,\mathbf{y}})(y'), \\ (\tau \circ \mathrm{in}_{l,\mathbf{y}})(\lambda.y) &= \lambda.(\tau \circ \mathrm{in}_{l,\mathbf{y}})(y),\end{aligned}$$

tehát a $\tau \circ \mathrm{in}_{l,\mathbf{y}} : E \to \mathbf{T}^{m+n}(E)$ leképezés lineáris operátor.

A tenzorszorzat univerzalitási tulajdonsága alapján ebből következik, hogy létezik egyetlen olyan

$$\tilde{\tau} : \mathbf{T}^n(E) \to \mathbf{L}\left(\mathbf{T}^m(E); \mathbf{T}^{m+n}(E)\right)$$

lineáris operátor, hogy minden $(y_j)_{j\in n} \in E^n$ esetén

$$\tilde{\tau}\left(\bigotimes_{j\in n} y_j\right) = \tau\left((y_j)_{j\in n}\right),$$

következésképpen minden $(x_i)_{i\in m} \in E^m$ esetén

$$\left(\tilde{\tau}\left(\bigotimes_{j\in n} y_j\right)\right)\left(\bigotimes_{i\in m} x_i\right) = \left(\tau\left((y_j)_{j\in n}\right)\right)\left(\bigotimes_{i\in m} x_i\right) =$$
$$= \tilde{\tau}_{(y_j)_{j\in n}}\left(\bigotimes_{i\in m} x_i\right) = \tau_{(y_j)_{j\in n}}\left((x_i)_{i\in m}\right) = \bigotimes_{k\in m+n} z_k,$$

ahol minden $k \in m+n$ számra

$$z_k := \begin{cases} x_i & , \text{ha } k < m, \\ y_{k-m} & , \text{ha } m \le k < m+n. \end{cases}$$

Ez azt jelenti, hogy a

$$\mathrm{p}_{m,n} : \mathbf{T}^m(E) \times \mathbf{T}^n(E) \to \mathbf{T}^{m+n}(E); \quad (t,t') \mapsto (\tilde{\tau}(t'))\,(t)$$

leképezés olyan bilineáris operátor, amely eleget tesz a követelménynek.

(*Unicitás.*) Legyen $\mathrm{p} : \mathrm{T^m(E)} \times \mathrm{T^n(E)} \to \mathrm{T^{m+n}(E)}$ olyan bilineáris operátor, amelyre teljesül az, hogy minden $(x_i)_{i\in m} \in E^m$ és $(y_j)_{j\in n} \in E^n$ esetén

$$\mathrm{p}\left(\bigotimes_{i\in m} x_i, \bigotimes_{j\in n} y_j\right) = \bigotimes_{k\in m+n} z_k,$$

ahol minden $k \in m+n$ esetén z_k-t (1) határozza meg. Ez azt jelenti, hogy a

$$\mathbf{T}^n(E) \to \mathbf{L}\left(\mathbf{T}^m(E); \mathbf{T}^{m+n}(E)\right); \quad t' \mapsto (t \mapsto \mathrm{p}(t,t'))$$

lineáris operátor *egyenlő* az egzisztencia bizonyításában értelmezett $\tilde{\tau}$ operátorral, amiből következik, hogy $\mathrm{p} = \mathrm{p}_{m,n}$. ■

21.9.3. Definíció. *Legyen E vektortér a K test felett. Ekkor minden $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$ párra*

$$\mathrm{p}_{m,n} : \mathbf{T}^m(E) \times \mathbf{T}^n(E) \to \mathbf{T}^{m+n}(E)$$

jelöli azt a bilineáris leképezést, amelyre teljesül az, hogy minden $(x_i)_{i\in m} \in E^m$ és $(y_j)_{j\in n} \in E^n$ esetén

$$\mathrm{p}_{m,n}\left(\bigotimes_{i\in m} x_i, \bigotimes_{j\in n} y_j\right) = \bigotimes_{k\in m+n} z_k,$$

ahol minden $k \in m+n$ számra

$$z_k := \begin{cases} x_k & , \textit{ha } k < m, \\ y_{k-m} & , \textit{ha } m \le k < m+n. \end{cases}$$

Továbbá, minden $n \in \mathbb{N}$ esetén a

$$\mathrm{p}_{0,n} : K \times \mathbf{T}^n(E) \to \mathbf{T}^n(E); \quad (\lambda, t) \mapsto \lambda.t,$$
$$\mathrm{p}_{n,0} : \mathbf{T}^n(E) \times K \to \mathbf{T}^n(E); \quad (t, \lambda) \mapsto \lambda.t$$

jelöléseket alkalmazzuk.

Tehát ha E vektortér, akkor *minden* $(m,n) \in \mathbb{N} \times \mathbb{N}$ párra értelmezve van a

$$\mathrm{p}_{m,n} : \mathbf{T}^m(E) \times \mathbf{T}^n(E) \to \mathbf{T}^{m+n}(E)$$

bilineáris operátor.

21.9.4. Definíció. *Legyen E vektortér. Minden $\left((t_n)_{n\in\mathbb{N}}, (t'_n)_{n\in\mathbb{N}}\right) \in \mathbf{T}(E)\times\mathbf{T}(E)$ párra*

$$(t_n)_{n\in\mathbb{N}} \cdot (t'_n)_{n\in\mathbb{N}} := \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k}\left(t_k, t'_{n-k}\right) \right)_{n\in\mathbb{N}}.$$

21.9.5. Lemma. *Ha E vektortér és $q,r,s \in \mathbb{N}$, akkor minden $a \in \mathbf{T}^q(E)$, $b \in \mathbf{T}^r(E)$ és $c \in \mathbf{T}^s(E)$ esetén*

$$\mathrm{p}_{q+r,s}\left(\mathrm{p}_{q,r}(a,b), c\right) = \mathrm{p}_{q,r+s}\left(a, \mathrm{p}_{r,s}(b,c)\right).$$

Bizonyítás. A $\mathrm{p}_{q+r,s}$, $\mathrm{p}_{q,r}$, $\mathrm{p}_{q,r+s}$ és $\mathrm{p}_{r,s}$ leképezések bilinearitása miatt elég azt igazolni, hogy minden $(a_i)_{i\in q} \in E^q$, $(b_i)_{i\in r} \in E^r$ és $(c_i)_{i\in s} \in E^s$ esetén

$$\mathrm{p}_{q+r,s}\left(\mathrm{p}_{q,r}\left(\bigotimes_{i\in q} a_i, \bigotimes_{i\in r} b_i\right), \bigotimes_{i\in s} c_i\right) = \mathrm{p}_{q,r+s}\left(\bigotimes_{i\in q} a_i, \mathrm{p}_{r,s}\left(\bigotimes_{i\in r} b_i, \bigotimes_{i\in s} c_i\right)\right),$$

hiszen a felbontható tenzorok generátorhalmazt alkotnak a tenzortérben.

Legyenek $(a_i)_{i\in q} \in E^q$, $(b_i)_{i\in r} \in E^r$ és $(c_i)_{i\in s} \in E^s$ rögzítve. Vezessük be a $(d_i)_{i\in q+r} \in E^{q+r}$ rendszert úgy, hogy minden $i \in q+r$ esetén

$$d_i := \begin{cases} a_i & \text{, ha } i < q, \\ b_{i-q} & \text{, ha } q \le i < q+r. \end{cases}$$

Legyen továbbá $(e_i)_{i\in q+r+s} \in E^{q+r+s}$ az a rendszer, amelyre minden $i \in q+r+s$ esetén

$$e_i := \begin{cases} d_i & \text{, ha } i < q+r, \\ c_{i-q-r} & \text{, ha } q+r \le i < q+r+s. \end{cases}$$

Ekkor a definíció szerint

$$\mathrm{p}_{q,r}\left(\bigotimes_{i\in q} a_i, \bigotimes_{i\in r} b_i\right) = \bigotimes_{i\in q+r} d_i, \mathrm{p}_{q+r,s}\left(\mathrm{p}_{q,r}\left(\bigotimes_{i\in q} a_i, \bigotimes_{i\in r} b_i\right), \bigotimes_{i\in s} c_i\right) = \bigotimes_{i\in q+r+s} e_i. \quad (1)$$

Nyilvánvaló, hogy minden $i \in q+r+s$ esetén

$$e_i = \begin{cases} a_i & \text{, ha } i < q, \\ b_{i-q} & \text{, ha } q \le i < q+r, \\ c_{i-q-r} & \text{, ha } q+r \le i < q+r+s, \end{cases}$$

tehát ha bevezetjük azt az $(f_i)_{i\in r+s} \in E^{r+s}$ rendszert, amelyre minden $i \in r+s$ esetén

$$f_i := \begin{cases} b_i & \text{, ha } i < r, \\ c_{i-r} & \text{, ha } r \le i < r+q, \end{cases}$$

akkor teljesül az, hogy minden $i \in q+r+s$ esetén

$$e_i = \begin{cases} a_i & \text{, ha } i < q, \\ f_{i-q} & \text{, ha } q \le i < q+r+s. \end{cases}$$

Ugyanakkor világos, hogy

$$\mathrm{p}_{r,s}\left(\bigotimes_{i\in r} b_i, \bigotimes_{i\in s} c_i\right) = \bigotimes_{i\in r+s} f_i,$$

$$\mathrm{p}_{q,r+s}\left(\bigotimes_{i\in q} a_i, \mathrm{p}_{r,s}\left(\bigotimes_{i\in r} b_i, \bigotimes_{i\in s} c_i\right)\right) = \bigotimes_{i\in q+r+s} e_i. \tag{2}$$

Az (1) és (2) egyenlőségek alapján az állítást igazoltuk. ■

21.9.6. Állítás. *Ha E vektortér a K test felett, akkor minden $t, t' \in \mathbf{T}(E)$ esetén $t \cdot t' \in \mathbf{T}(E)$, és a $\mathbf{T}(E)$ vektortér, a $\cdot$ művelettel ellátva egységelemes algebra a K test felett.*

Bizonyítás. Legyenek $t = (t_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$ és $t' = (t'_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$. Vegyünk olyan $N, N' \in \mathbb{N}$ számokat, amelyekre teljesül az, hogy minden $n > N$ természetes számra $t_n = \mathbf{0}$, és minden $n > N'$ természetes számra $t'_n = \mathbf{0}$. Ekkor minden $n > N + N'$ természetes számra teljesül az, hogy minden $k \leq n$ természetes számra $k > N$ vagy $n - k > N'$, különben $n = k + (n-k) \leq N + N'$ teljesülne. Ezért minden $n > N + N'$ természetes számra $(t \cdot t')_n = \sum_{k=0}^{n} \mathrm{p}_{k,n-k}\left(t_k, t'_{n-k}\right) = \mathbf{0}$, hiszen minden $k \leq n$ természetes számra $t_k = \mathbf{0}$ (ha $k > N$), vagy $t'_{n-k} = \mathbf{0}$ (ha $n - k > N'$), így $\mathrm{p}_{k,n-k}$ bilinearitása miatt $\mathrm{p}_{k,n-k}\left(t_k, t'_{n-k}\right) = \mathbf{0}$. Ezért $t \cdot t' \in \mathbf{T}(E)$, vagyis $\cdot$ művelet a $\mathbf{T}(E)$ halmaz felett.

A $\cdot$ művelet asszociativitásának bizonyításához legyenek $t = (t_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$, $t' = (t'_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$, és $t'' = (t''_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$. Ekkor

$$\begin{aligned}
t \cdot (t' \cdot t'') &= (t_n)_{n\in\mathbb{N}} \cdot \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k}\left(t'_k, t''_{n-k}\right)\right)_{n\in\mathbb{N}} = \\
&= \left(\sum_{m=0}^{n} \mathrm{p}_{m,n-m}\left(t_m, \sum_{k=0}^{n-m} \mathrm{p}_{k,n-m-k}\left(t'_k, t''_{n-m-k}\right)\right)\right)_{n\in\mathbb{N}} \overset{(1)}{=} \\
&\overset{(1)}{=} \left(\sum_{m=0}^{n}\sum_{k=0}^{n-m} \mathrm{p}_{m,n-m}\left(t_m, \mathrm{p}_{k,n-m-k}\left(t'_k, t''_{n-m-k}\right)\right)\right)_{n\in\mathbb{N}} \overset{(2)}{=} \\
&\overset{(2)}{=} \left(\sum_{m=0}^{n}\sum_{k=0}^{n-m} \mathrm{p}_{m+k,n-(m+k)}\left(\mathrm{p}_{m,k}\left(t_m, t'_k\right), t''_{n-(m+k)}\right)\right)_{n\in\mathbb{N}} \overset{(3)}{=} \\
&\overset{(3)}{=} \left(\sum_{m=0}^{n}\sum_{j=m}^{n} \mathrm{p}_{j,n-j}\left(\mathrm{p}_{m,j-m}\left(t_m, t'_{j-m}\right), t''_{n-j}\right)\right)_{n\in\mathbb{N}} \overset{(4)}{=} \\
&\overset{(4)}{=} \left(\sum_{j=0}^{n}\sum_{m=0}^{j} \mathrm{p}_{j,n-j}\left(\mathrm{p}_{m,j-m}\left(t_m, t'_{j-m}\right), t''_{n-j}\right)\right)_{n\in\mathbb{N}} \overset{(5)}{=} \\
&\overset{(5)}{=} \left(\sum_{j=0}^{n} \mathrm{p}_{j,n-j}\left(\sum_{m=0}^{j} \mathrm{p}_{m,j-m}\left(t_m, t'_{j-m}\right), t''_{n-j}\right)\right)_{n\in\mathbb{N}} = \\
&= \left(\sum_{m=0}^{n} \mathrm{p}_{m,n-m}\left(t_m, t'_{n-m}\right)\right)_{n\in\mathbb{N}} \cdot (t''_n)_{n\in\mathbb{N}} = (t \cdot t') \cdot t'',
\end{aligned}$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél azt használtuk fel, hogy minden $m, n \in \mathbb{N}$, $m \leq n$ esetén a $\mathrm{p}_{m,n-m}$ leképezés a második változójában additív;

– a $\overset{(2)}{=}$ egyenlőségnél az előző lemmát alkalmaztuk minden $k, m, n \in \mathbb{N}$, $m \leq n$, $k \leq n-m$ esetén a $q := m$, $r := k$ és $s := n - (m + k)$ választással;

– a $\overset{(3)}{=}$ egyenlőségnél minden $m, n \in \mathbb{N}$, $m \leq n$ esetén a belső szummában a k összegzőindexről áttértünk a $j := m + k$ összegzőindexre, azaz minden $n \in \mathbb{N}$ számra a $\mathbf{T}^n(E)$ vektortér additív csoportműveletének általános kommutativitására hivatkoztunk (8.6.1.);

– a $\overset{(4)}{=}$ egyenlőségnél a felcserélési formulát (8.4.2.) alkalmaztuk minden $n \in \mathbb{N}$ esetén a $\mathbf{T}^n(E)$ vektortér additív csoportműveletére;

– az $\overset{(5)}{=}$ egyenlőségnél azt használtuk fel, hogy minden $j, n \in \mathbb{N}$, $j \leq n$ esetén a $\mathrm{p}_{j,n-j}$ leképezés az első változójában additív.

Tehát a $\mathbf{T}(E)$ halmazon értelmezett $\cdot$ művelet asszociatív. Továbbá, ha $\mathbf{1}$ jelöli azt az elemet $\mathbf{T}(E)$-ben, amelyre minden $n \in \mathbb{N}$ esetén

$$\mathbf{1}_n := \begin{cases} 1_K & , \text{ha } n = 0, \\ \mathbf{0}_n & , \text{ha } n > 0, \end{cases}$$

ahol 1_K a K test multiplikatív neutrális eleme, és minden $n \in \mathbb{N}^*$ esetén $\mathbf{0}_n$ a $\mathbf{T}^n(E)$ vektortér additív neutrális eleme, akkor könnyen látható, hogy $\mathbf{1} \in \mathbf{T}(E)$ a $\cdot$ művelet szerinti neutrális elem, hiszen minden $t = (t_n)_{n \in N} \in \mathbf{T}(E)$ rendszerre

$$\mathbf{1} \cdot t = \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(\mathbf{1}_k, t_{n-k} \right) \right)_{n \in \mathbb{N}} = \left(\mathrm{p}_{0,n} \left(1_K, t_n \right) \right)_{n \in \mathbb{N}} = (t_n)_{n \in N} = t,$$

$$t \cdot \mathbf{1} = \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, \mathbf{1}_{n-k} \right) \right)_{n \in \mathbb{N}} = \left(\mathrm{p}_{n,0} \left(t_n, 1_K \right) \right)_{n \in \mathbb{N}} = (t_n)_{n \in N} = t.$$

Minden $k, n \in \mathbb{N}$, $k \leq n$ számra a $\mathrm{p}_{k,n-k} : \mathbf{T}^k(E) \times \mathbf{T}^{n-k}(E) \to \mathbf{T}^n(E)$ leképezés biadditív, ezért minden $t = (t_n)_{n \in \mathbb{N}} \in \mathbf{T}(E)$, $t' = (t'_n)_{n \in \mathbb{N}} \in \mathbf{T}(E)$, és $t'' = (t''_n)_{n \in \mathbb{N}} \in \mathbf{T}(E)$ esetén

$$t \cdot (t' + t'') = (t_n)_{n \in \mathbb{N}} \cdot (t'_n + t''_n)_{n \in \mathbb{N}} = \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, t'_{n-k} + t''_{n-k} \right) \right)_{n \in \mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \left(\mathrm{p}_{k,n-k} \left(t_k, t'_{n-k} \right) + \mathrm{p}_{n-k} \left(t_k, t''_{n-k} \right) \right) \right)_{n \in \mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, t'_{n-k} \right) + \sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, t''_{n-k} \right) \right)_{n \in \mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, t'_{n-k} \right) \right)_{n \in \mathbb{N}} + \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, t''_{n-k} \right) \right)_{n \in \mathbb{N}} = t \cdot t' + t \cdot t'',$$

és hasonlóan

$$(t' + t'') \cdot t = (t'_n + t''_n)_{n\in\mathbb{N}} \cdot (t_n)_{n\in\mathbb{N}} = \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t'_k + t''_k, t_{n-k}\right) \right)_{n\in\mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \left(\mathrm{p}_{k,n-k} \left(t'_k, t_{n-k}\right) + \mathrm{p}_{n-k} \left(t''_k, t_{n-k}\right)\right) \right)_{n\in\mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t'_k, t_{n-k}\right) + \sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t''_k, t_{n-k}\right) \right)_{n\in\mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t'_k, t_{n-k}\right) \right)_{n\in\mathbb{N}} + \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t''_k, t_{n-k}\right) \right)_{n\in\mathbb{N}} = t' \cdot t + t'' \cdot t.$$

Ez azt jelenti, hogy a $\cdot$ művelet disztributív a $\mathbf{T}(E)$ vektortér $+$ műveletére nézve. Minden $k, n \in \mathbb{N}$, $k \leq n$ számra a $\mathrm{p}_{k,n-k} : \mathbf{T}^k(E) \times \mathbf{T}^{n-k}(E) \to \mathbf{T}^n(E)$ leképezés bihomogén, ezért minden $t = (t_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$ és $t' = (t'_n)_{n\in\mathbb{N}} \in \mathbf{T}(E)$ esetén

$$(\lambda.t) \cdot t'' = (\lambda.t_n)_{n\in\mathbb{N}} \cdot (t'_n)_{n\in\mathbb{N}} = \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(\lambda.t_k, t'_{n-k}\right) \right)_{n\in\mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \lambda.\mathrm{p}_{k,n-k} \left(t_k, t'_{n-k}\right) \right)_{n\in\mathbb{N}} = \left(\lambda. \sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, t'_{n-k}\right) \right)_{n\in\mathbb{N}} = \lambda.(t \cdot t'),$$

és hasonlóan

$$t \cdot (\lambda.t'') = (t_n)_{n\in\mathbb{N}} \cdot (\lambda.t'_n)_{n\in\mathbb{N}} = \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, \lambda.t'_{n-k}\right) \right)_{n\in\mathbb{N}} =$$

$$= \left(\sum_{k=0}^{n} \lambda.\mathrm{p}_{k,n-k} \left(t_k, t'_{n-k}\right) \right)_{n\in\mathbb{N}} = \left(\lambda. \sum_{k=0}^{n} \mathrm{p}_{k,n-k} \left(t_k, t'_{n-k}\right) \right)_{n\in\mathbb{N}} = \lambda.(t \cdot t').$$

Végül, triviális, hogy minden $t \in \mathbf{T}(E)$ sorozatra $1_K.t = t$. Tehát a $\mathbf{T}(E)$ vektortér a $\cdot$ művelettel ellátva egységelemes algebra a K test felett. ∎

21.9.7. Definíció. *Ha E vektortér, akkor a $\mathbf{T}(E)$ vektorteret a $\cdot$ művelettel ellátva az E* **vektortér tenzoralgebrájának** *nevezzük, és az $\mathrm{in}_{E,\mathbf{T}(E)} : E \to \mathbf{T}(E)$ lineáris injekciót az E vektortér és a $\mathbf{T}(E)$ tenzoralgebra közötti* **kanonikus injekciónak** *bevezzük.*

A következő tétel teljes jellemzést ad vektortér tenzoralgebrájára. Előtte szükségünk lesz egy lemmára.

21.9.8. Lemma. *Legyen E vektortér. Minden $n \in \mathbb{N}^*$ és $(x_i)_{i\in n} \in E^n$ esetén*

$$\prod_{i=0}^{n-1} \mathrm{in}_{E,\mathbf{T}(E)}(x_i) = \mathrm{in}_{\mathbf{T}^n(E),\mathbf{T}(E)} \left(\bigotimes_{i\in n} x_i \right).$$

Bizonyítás. A lemmát n szerinti teljes indukcióval igazoljuk. Az állítás triviálisan igaz $n = 1$ esetén. Tegyük fel, hogy $n \in \mathbb{N}^*$ olyan szám, amelyre minden és $(x_i)_{i\in n} \in E^n$ esetén

$$\prod_{i=0}^{n-1} \mathrm{in}_{E,\mathbf{T}(E)}(x_i) = \mathrm{in}_{\mathbf{T}^n(E),\mathbf{T}(E)} \left(\bigotimes_{i\in n} x_i \right),$$

és legyen $(x_i)_{i\in n+1} \in E^{n+1}$ rögzítve. Legyen

$$(t_m)_{m\in\mathbb{N}} := \mathrm{in}_{\mathbf{T}^n(E),\mathbf{T}(E)}\left(\bigotimes_{i\in n} x_i\right),$$
$$(t'_m)_{m\in\mathbb{N}} := \mathrm{in}_{E,\mathbf{T}(E)}(x_n),$$

tehát minden $m \in \mathbb{N}$ esetén

$$t_m = \begin{cases} \mathbf{0}_m & \text{, ha } m \neq n, \\ \bigotimes\limits_{i\in n} x_i & \text{, ha } m = n, \end{cases}$$

valamint

$$t'_m = \begin{cases} \mathbf{0}_m & \text{, ha } m \neq 1, \\ x_n & \text{, ha } m = 1, \end{cases}$$

ahol $\mathbf{0}_m$ a $\mathbf{T}^m(E)$ vektortér additív neutrális eleme. Ekkor 8.3.5. b) és az indukciós hipotézis alapján

$$\prod_{i=0}^{n} \mathrm{in}_{E,\mathbf{T}(E)}(x_i) = \left(\prod_{i=0}^{n-1} \mathrm{in}_{E,\mathbf{T}(E)}(x_i)\right) \cdot \mathrm{in}_{E,\mathbf{T}(E)}(x_n) =$$
$$= \left(\mathrm{in}_{\mathbf{T}^n(E),\mathbf{T}(E)}\left(\bigotimes_{i\in n} x_i\right)\right) \cdot \mathrm{in}_{E,\mathbf{T}(E)}(x_n) = (t_m)_{m\in\mathbb{N}} \cdot (t'_m)_{m\in\mathbb{N}} =$$
$$= \left(\sum_{k=0}^{m} \mathrm{p}_{k,m-k}\left(t_k, t'_{m-k}\right)\right)_{m\in\mathbb{N}}.$$

Nyilvánvaló, hogy minden $k, m \in \mathbb{N}$, $k \leq m$ esetén, ha $k \neq n$ vagy $m - k \neq 1$, akkor $\mathrm{p}_{k,m-k}\left(t_k, t'_{m-k}\right) = \mathbf{0}_m$. Ebből következik, hogy minden $m \in \mathbb{N}$ számra

$$\sum_{k=0}^{m} \mathrm{p}_{k,m-k}\left(t_k, t'_{m-k}\right) = \begin{cases} \mathrm{p}_{n,1}(t_n, t'_1) & \text{, ha } m = n+1, \\ \mathbf{0}_m & \text{, ha } m \neq n+1, \end{cases}$$

ugyanakkor

$$\mathrm{p}_{n,1}(t_n, t'_1) = \mathrm{p}_{n,1}\left(\bigotimes_{i\in n} x_i, x_n\right) = \bigotimes_{i\in n+1} x_i,$$

ami azt jelenti, hogy

$$\prod_{i=0}^{(n+1)-1} \mathrm{in}_{E,\mathbf{T}(E)}(x_i) = \left(\sum_{k=0}^{m} \mathrm{p}_{k,m-k}\left(t_k, t'_{m-k}\right)\right)_{m\in\mathbb{N}} = \mathrm{in}_{\mathbf{T}^{n+1}(E),\mathbf{T}(E)}\left(\bigotimes_{i\in n+1} x_i\right).$$

Ezért az állítás az $n + 1$ számra is igaz. ■

21.9.9. Következmény. *Ha E vektortér, akkor az $\mathrm{Im}\left(\mathrm{in}_{E,\mathbf{T}(E)}\right)$ halmaz által generált egységelemes részalgebra a $\mathbf{T}(E)$ tenzoralgebrában egyenlő $\mathbf{T}(E)$-vel.*

Bizonyítás. Az előző lemmából következik, hogy ha B olyan egységelemes részalgebra a $\mathbf{T}(E)$ tenzoralgebrában, hogy $\mathrm{Im}\left(\mathrm{in}_{E,\mathbf{T}(E)}\right) \subseteq B$, akkor minden $n \in \mathbb{N}^*$ esetén $\mathrm{Im}\left(\mathrm{in}_{\mathbf{T}^n(E),\mathbf{T}(E)}\right) \subseteq B$, és mivel $\mathbf{T}(E)$ multiplikatív neutrális eleme benne van B-ben, így $\mathrm{Im}\left(\mathrm{in}_{\mathbf{T}^0(E),\mathbf{T}(E)}\right) \subseteq B$ is teljesül, tehát $B = \mathbf{T}(E)$. ■

21.9.10. Tétel. *Legyen E vektortér a K test felett.*

a) *A $\left(\mathbf{T}(E), \mathrm{in}_{E,\mathbf{T}(E)}\right)$ pár rendelkezik azzal a tulajdonsággal, hogy ha B egységelemes algebra a K test felett, és $u : E \to B$ lineáris operátor, akkor létezik egyetlen olyan $\tilde{u} : \mathbf{T}(E) \to B$ egységelem-tartó algebra-morfizmus, amelyre $\tilde{u} \circ \mathrm{in}_{E,\mathbf{T}(E)} = u$, vagyis a következő diagram kommutatív.*

$$\begin{tikzcd} E \arrow[r, "\mathrm{in}_{E,\mathbf{T}(E)}"] \arrow[dr, "u"'] & \mathbf{T}(E) \arrow[d, "\tilde{u}"] \\ & B \end{tikzcd}$$

b) *Tegyük fel, hogy (A, i) olyan pár, amelyre A egységelemes algebra K felett, és $i : E \to A$ lineáris operátor, és teljesül a következő állítás.*

(TEN) *Minden K feletti B egységelemes algebrához, és minden $u : E \to B$ lineáris operátorhoz, létezik egyetlen olyan $\tilde{u} : A \to B$ egységelem-tartó algebra-morfizmus, hogy $\tilde{u} \circ i = u$, vagyis a következő diagram kommutatív.*

$$\begin{tikzcd} E \arrow[r, "i"] \arrow[dr, "u"'] & A \arrow[d, "\tilde{u}"] \\ & B \end{tikzcd}$$

Ekkor létezik egyetlen olyan $\pi : \mathbf{T}(E) \to A$ egységelem-tartó algebra-morfizmus, amelyre $\pi \circ \mathrm{in}_{E,\mathbf{T}(E)} = i$, továbbá ekkor π izomorfizmus a $\mathbf{T}(E)$ tenzoralgebra ás az A algebra között, és $i : E \to A$ szükségképpen injekció, és A egyenlő az $\mathrm{Im}(i)$ *halmaz által generált egységelemes részalgebrával.*

Bizonyítás. a) Legyen B egységelemes algebra a K test felett, és jelölje $\mathbf{1}_B$ a multiplikatív neutrális elemet B-ben. Rögzítsünk egy $u : E \to B$ lineáris operátort.

Megmutatjuk, hogy minden $n \in \mathbb{N}^*$ esetén a

$$\mu_n : E^n \to B; \quad (x_i)_{i\in n} \mapsto \prod_{i=0}^{n-1} u(x_i)$$

leképezés multilineáris. Valóban, ha $k \in n$ és $\mathbf{x} = (x_i)_{i\in n} \in E^n$, akkor minden $x \in E$ vektorra, B szorzásának általános asszociativitása miatt

$$(\mu_n \circ \mathrm{in}_{k,\mathbf{x}})(x) = \prod_{i=0}^{n-1} u\left((\mathrm{in}_{k,\mathbf{x}}(x))_i\right) = \left(\prod_{i=0}^{k-1} u(x_i)\right) u(x) \left(\prod_{i=k+1}^{n-1} u(x_i)\right),$$

azzal a konvencióval, hogy $k = 0$ esetén $\prod_{i=0}^{k-1} u(x_i) := \mathbf{1}_B$, valamint $k = n-1$ esetén $\prod_{i=k+1}^{n-1} u(x_i) := \mathbf{1}_B$. Nyilvánvaló, hogy minden $b, b' \in B$ esetén az $E \to B;\ x \mapsto bu(x)b'$ leképezés lineáris, így a $\mu_n \circ \mathrm{in}_{k,\mathbf{x}} : E \to B$ leképezés is lineáris. Ezért a μ_n leképezés multilineáris.

Minden $n \in \mathbb{N}^*$ esetén jelölje $u_n : \mathbf{T}^n(E) \to B$ azt a lineáris operátort, amelyre minden $(x_i)_{i\in n} \in E^n$ esetén

$$u_n\left(\bigotimes_{i\in n} x_i\right) = \mu_n\left((x_i)_{i\in n}\right) = \prod_{i=0}^{n-1} u(x_i),$$

továbbá vezessük be az

$$u_0 : K \to B; \quad \lambda \mapsto \lambda.\mathbf{1}_B$$

leképezést. Ekkor $(u_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbf{L}(\mathbf{T}^n(E); B)$, így jól értelmezett a

$$\tilde{u} : \mathbf{T}(E) \to B; \quad (t_n)_{n\in\mathbb{N}} \mapsto \sum_{n=0}^{\infty} u_n(t_n)$$

lineáris operátor, amelyre $\tilde{u} \circ \mathrm{in}_{E,\mathbf{T}(E)} = u$ triviálisan teljesül, valamint $\tilde{u}(\mathbf{1}) = \mathbf{1}_B$ is nyilvánvaló. Megmutatjuk, hogy $\tilde{u}$ multiplikatív is. Ehhez először igazoljuk azt, hogy minden $k, n \in \mathbb{N}$ esetén, ha $k \leq n$, akkor

$$u_n \circ \mathrm{p}_{k,n-k} = \mathrm{p}_B \circ (u_k \times u_{n-k}), \tag{1}$$

ahol p_B a B algebra szorzását jelöli. Itt négy eset lehetséges.
1) $n = 0$. Ekkor $k = 0$ és $n - k = 0$, ezért minden $\lambda, \sigma \in K = \mathbf{T}^0(E)$ esetén

$$\begin{gathered}(u_0 \circ \mathrm{p}_{0,0})(\lambda, \sigma) = u_0(\lambda\sigma) = (\lambda\sigma)\mathbf{1}_B = (\lambda\mathbf{1}_B)(\sigma\mathbf{1}_B) = \\ = \mathrm{p}_B(\lambda\mathbf{1}_B, \sigma\mathbf{1}_B) = (\mathrm{p}_B \circ (u_0 \times u_0))(\lambda, \sigma),\end{gathered}$$

tehát $u_0 \circ \mathrm{p}_{0,0} = \mathrm{p}_B \circ (u_0 \times u_0)$.
2) $n > 0$ és $k = 0$. Ekkor $n - k = n$, ezért minden $\lambda \in K = \mathbf{T}^0(E)$ és $(y_i)_{i\in n} \in \mathbf{T}^n(E)$ esetén

$$\begin{gathered}(u_n \circ \mathrm{p}_{0,n})\left(\lambda, \bigotimes_{i\in n} y_i\right) = u_n\left(\lambda. \bigotimes_{i\in n} y_i\right) = \lambda.u_n\left(\bigotimes_{i\in n} y_i\right) = (\lambda.\mathbf{1}_B)\, u_n\left(\bigotimes_{i\in n} y_i\right) = \\ = \mathrm{p}_B\left(\lambda.\mathbf{1}_B, u_n\left(\bigotimes_{i\in n} y_i\right)\right) = (\mathrm{p}_B \circ (u_0 \times u_n))\left(\lambda, \bigotimes_{i\in n} y_i\right),\end{gathered}$$

tehát $u_n \circ \mathrm{p}_{0,n} = \mathrm{p}_B \circ (u_0 \times u_n)$.
3) $n > 0$ és $k = n$. Ekkor $n - k = 0$, ezért minden $(x_i)_{i\in n} \in \mathbf{T}^n(E)$ és $\lambda \in K = \mathbf{T}^0(E)$ esetén

$$\begin{gathered}(u_n \circ \mathrm{p}_{n,0})\left(\bigotimes_{i\in n} x_i, \lambda\right) = u_n\left(\lambda. \bigotimes_{i\in n} x_i\right) = \lambda.u_n\left(\bigotimes_{i\in n} x_i\right) = u_n\left(\bigotimes_{i\in n} x_i\right)(\lambda.\mathbf{1}_B) = \\ = \mathrm{p}_B\left(u_n\left(\bigotimes_{i\in n} x_i\right), \lambda.\mathbf{1}_B\right) = (\mathrm{p}_B \circ (u_n \times u_0))\left(\bigotimes_{i\in n} y_i, \lambda\right),\end{gathered}$$

tehát $u_n \circ \mathrm{p}_{n,0} = \mathrm{p}_B \circ (u_n \times u_0)$.
4) $n > 0$ és $0 < k < n$. Ekkor minden $(x_i)_{i\in k} \in \mathbf{T}^k(E)$ és $(y_i)_{i\in n-k} \in \mathbf{T}^{n-k}(E)$ esetén

$$\begin{gathered}(u_n \circ \mathrm{p}_{k,n-k})\left(\bigotimes_{i\in k} x_i, \bigotimes_{i\in n-k} y_i\right) = u_n\left(\bigotimes_{i\in n} z_i\right) = \prod_{i=0}^{n-1} u(z_i) = \\ = \left(\prod_{i=0}^{k-1} u(x_i)\right)\left(\prod_{i=0}^{n-k-1} u(y_i)\right) = \mathrm{p}_B\left(\prod_{i=0}^{k-1} u(x_i), \prod_{i=0}^{n-k-1} u(y_i)\right) = \\ \mathrm{p}_B\left(u_n\left(\bigotimes_{i\in k} x_i\right), u_n\left(\bigotimes_{i\in n-k} y_i\right)\right) = (\mathrm{p}_B \circ (u_k \times u_{n-k}))\left(\bigotimes_{i\in k} x_i, \bigotimes_{i\in n-k} y_i\right),\end{gathered}$$

ahol $(z_i)_{i\in n} \in E^n$ az a rendszer, amelyre $i \in k$ esetén $z_i := x_i$ és $k \leq i < n$ esetén $z_i := y_{i-k}$.

Ezzel az (1) egyenlőséget igazoltuk. Az $\tilde{u} : \mathbf{T}(E) \to B$ leképezés multiplikativitásának bizonyításához legyen $t = (t_n)_{n \in N} \in \mathbf{T}(E)$ és $t' = (t'_n)_{n \in N} \in \mathbf{T}(E)$. Vegyünk olyan $N \in \mathbb{N}$ számot, amely $\mathbb{N}$-ben felső korlátja a $\{n \in \mathbb{N} | t_n \neq 0\} \cup \{n \in \mathbb{N} | t'_n \neq 0\}$ halmaznak. Ekkor $2N$ felső korlátja a $\{n \in \mathbb{N} | (t \cdot t')_n \neq 0\}$ halmaznak, ezért (1) alkalmazásával 14.2.5. alapján kapjuk, hogy

$$\tilde{u}(t \cdot t') = \tilde{u}\left(\left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k}\left(t_k, t'_{n-k}\right) \right)_{n \in \mathbb{N}} \right) = \sum_{n=0}^{2N} u_n \left(\sum_{k=0}^{n} \mathrm{p}_{k,n-k}\left(t_k, t'_{n-k}\right) \right) =$$
$$= \sum_{n=0}^{2N} \left(\sum_{k=0}^{n} (u_n \circ \mathrm{p}_{k,n-k}) \left(t_k, t'_{n-k}\right) \right) = \sum_{n=0}^{2N} \left(\sum_{k=0}^{n} (\mathrm{p}_B \circ (u_k \times u_{n-k})) \left(t_k, t'_{n-k}\right) \right) =$$
$$= \sum_{n=0}^{2N} \left(\sum_{k=0}^{n} u_k\left(t_k\right) u_{n-k}\left(t'_{n-k}\right) \right) = \left(\sum_{n=0}^{N} u_k\left(t_k\right) \right) \left(\sum_{n=0}^{N} u_{n-k}\left(t'_{n-k}\right) \right) = \tilde{u}(t)\tilde{u}(t').$$

Ezzel az előírt tulajdonságú $\tilde{u} : \mathbf{T}(E) \to B$ egységelem-tartó algebra-morfizmus létezését igazoltuk. Az $\tilde{u}$ leképezés egyértelműsége abból következik, hogy az $\tilde{u} \circ \mathrm{in}_{E,\mathbf{T}(E)} = u$ feltétel meghatározza $\tilde{u}$-t az $\mathrm{Im}\left(\mathrm{in}_{E,\mathbf{T}(E)}\right)$ halmazon, amely által generált egységelemes részalgebra a $\mathbf{T}(E)$ tenzoralgebrában egyenlő $\mathbf{T}(E)$-vel.

b) Legyen (A, i) olyan pár, amelyre A egységelemes algebra K felett, és $i : E \to A$ olyan lineáris operátor, hogy teljesül a (TEN) állítás.

Mivel A egységelemes algebra a K test felett, és $i : E \to A$ lineáris operátor, így a) alapján egyértelműen létezik olyan $\pi : \mathbf{T}(E) \to A$ egységelem-tartó algebra-morfizmus, amelyre $\pi \circ \mathrm{in}_{E,\mathbf{T}(E)} = i$. Mivel $\mathbf{T}(E)$ egységelemes algebra a K test felett, és $\mathrm{in}_{E,\mathbf{T}(E)} : E \to \mathbf{T}(E)$ lineáris operátor, így (TEN) alapján egyértelműen létezik olyan $\sigma : A \to \mathbf{T}(E)$ egységelem-tartó algebra-morfizmus, amelyre $\sigma \circ i = \mathrm{in}_{E,\mathbf{T}(E)}$. Ekkor $\pi \circ \sigma : A \to A$ olyan egységelem-tartó algebra-morfizmus, amelyre $(\pi \circ \sigma) \circ i = i = \mathrm{id}_A \circ i$, így a (TEN) állításban szereplő egyértelműségi feltétel szerint $\pi \circ \sigma = \mathrm{id}_A$. Ugyanakkor $\sigma \circ \pi : \mathbf{T}(E) \to \mathbf{T}(E)$ olyan egységelem-tartó algebra-morfizmus, amelyre $(\sigma \circ \pi) \circ \mathrm{in}_{E,\mathbf{T}(E)} = \mathrm{in}_{E,\mathbf{T}(E)} = \mathrm{id}_{\mathbf{T}(E)} \circ \mathrm{in}_{E,\mathbf{T}(E)}$, így az a) állításban szereplő egyértelműségi feltétel szerint $\sigma \circ \pi = \mathrm{id}_{\mathbf{T}(E)}$. Tehát a π leképezés izomorfizmus a $\mathbf{T}(E)$ és A algebrák között. Mivel π és $\mathrm{in}_{E,\mathbf{T}(E)}$ injekciók, így $i = \pi \circ \mathrm{in}_{E,\mathbf{T}(E)}$ miatt az $i : E \to A$ leképezés is injekció. Továbbá, ebből az egyenlőségből következik, hogy $\mathrm{Im}(i) = \pi\langle \mathrm{Im}(\mathrm{in}_{E,\mathbf{T}(E)})\rangle$, és az $\mathrm{Im}\left(\mathrm{in}_{E,\mathbf{T}(E)}\right)$ halmaz által generált egységelemes részalgebra a $\mathbf{T}(E)$ tenzoralgebrában egyenlő $\mathbf{T}(E)$-vel, így az $\mathrm{Im}(i)$ halmaz által generált egységelemes részalgebra a $\mathbf{T}(E)$ tenzoralgebrában szintén egyenlő $\mathbf{T}(E)$-vel. ■

21.9.11. Állítás. *Legyenek E és F vektorterek, valamint $u : E \to F$ lineáris operátor. Ekkor létezik egyetlen olyan $\widetilde{u} : \mathbf{T}(E) \to \mathbf{T}(F)$ egységelem-tartó algebra-morfizmus, amelyre $\mathrm{in}_{F,\mathbf{T}(F)} \circ u = \widetilde{u} \circ \mathrm{in}_{E,\mathbf{T}(E)}$, vagyis a következő diagram kommutatív*

$$\begin{tikzcd}
E \arrow[r, "u"] \arrow[d, "\mathrm{in}_{E,\mathbf{T}(E)}"'] & F \arrow[d, "\mathrm{in}_{F,\mathbf{T}(F)}"] \\
\mathbf{T}(E) \arrow[r, "\widetilde{u}"'] & \mathbf{T}(F)
\end{tikzcd}$$

Bizonyítás. Az $\mathrm{in}_{F,\mathbf{T}(F)} \circ u : E \to \mathbf{T}(F)$ leképezés lineáris, és $\mathbf{T}(F)$ egységelemes algebra, így az előző tétel b) pontja szerint létezik egyetlen olyan $\widetilde{u} : \mathbf{T}(E) \to \mathbf{T}(F)$ egységelem-tartó algebra-morfizmus, amelyre $\mathrm{in}_{F,\mathbf{T}(F)} \circ u = \widetilde{u} \circ \mathrm{in}_{E,\mathbf{T}(E)}$. ■

21.9.12. Definíció. *Ha E és F vektorterek, valamint $u : E \to F$ lineáris operátor, akkor $\mathbf{T}(u)$ jelöli azt az egyértelműen meghatározott $\mathbf{T}(E) \to \mathbf{T}(F)$ egységelem-tartó algebra-morfizmust, amelyre $\mathrm{in}_{F,\mathbf{T}(F)} \circ u = \mathbf{T}(u) \circ \mathrm{in}_{E,\mathbf{T}(E)}$.*

Könnyen látható, hogy ha E vektortér, akkor $\mathbf{T}(\mathrm{id}_E) = \mathrm{id}_{\mathbf{T}(E)}$, hiszen $\mathrm{id}_{\mathbf{T}(E)} : \mathbf{T}(E) \to \mathbf{T}(E)$ olyan egységelem-tartó algebra-morfizmus, amelyre $\mathrm{in}_{E,\mathbf{T}(E)} \circ \mathrm{id}_E = \mathrm{id}_{\mathbf{T}(E)} \circ \mathrm{in}_{E,\mathbf{T}(E)}$.

21.9.13. Állítás. *Ha E, F és G vektorterek, valamint $u : E \to F$ és $v : F \to G$ lineáris operátorok, akkor $\mathbf{T}(v \circ u) = \mathbf{T}(v) \circ \mathbf{T}(u)$.*

Bizonyítás. A $\mathbf{T}(v) \circ \mathbf{T}(u) : \mathbf{T}(E) \to \mathbf{T}(G)$ és $\mathbf{T}(v \circ u) : \mathbf{T}(E) \to \mathbf{T}(G)$ leképezések egységelem-tartó algebra-morfizmusok a $\mathbf{T}(E)$ és $\mathbf{T}(G)$ tenzoralgebrák között, továbbá

$$\begin{aligned}(\mathbf{T}(v) \circ \mathbf{T}(u)) \circ \mathrm{in}_{E,\mathbf{T}(E)} &= \mathbf{T}(v) \circ \left(\mathbf{T}(u) \circ \mathrm{in}_{E,\mathbf{T}(E)}\right) = \mathbf{T}(v) \circ \left(\mathrm{in}_{F,\mathbf{T}(F)} \circ u\right) = \\ &= \left(\mathbf{T}(v) \circ \mathrm{in}_{F,\mathbf{T}(F)}\right) \circ u = \left(\mathrm{in}_{G,\mathbf{T}(G)} \circ v\right) \circ u = \mathrm{in}_{G,\mathbf{T}(G)} \circ (v \circ u)\end{aligned}$$

teljesül, így $\mathbf{T}(v \circ u) = \mathbf{T}(v) \circ \mathbf{T}(u)$. ■

21.9.14. Következmény. *Ha u izomorfizmus az E és F vektorterek között, akkor $\mathbf{T}(u)$ izomorfizmus a $\mathbf{T}(E)$ és $\mathbf{T}(F)$ tenzoralgebrák között. Ha E vektortér, akkor a*

$$\mathbf{GL}(E) \to \mathbf{G}(\mathbf{T}(E)); \quad u \mapsto \mathbf{T}(u)$$

leképezés injektív csoport-morfizmus.

Bizonyítás. Ha $v : F \to E$ olyan lineáris operátor, hogy $v \circ u = \mathrm{id}_E$ és $u \circ v = \mathrm{id}_F$, akkor az előző állítás alapján $\mathbf{T}(v) \circ \mathbf{T}(u) = \mathbf{T}(\mathrm{id}_E) = \mathrm{id}_{\mathbf{T}(E)}$ és $\mathbf{T}(u) \circ \mathbf{T}(v) = \mathbf{T}(\mathrm{id}_F) = \mathrm{id}_{\mathbf{T}(F)}$, tehát $\mathbf{T}(u) : \mathbf{T}(E) \to \mathbf{T}(F)$ algebra-izomorfizmus.

Ebből és az előző állításból azonnal következik, hogy a $\mathbf{GL}(E) \to \mathbf{G}(\mathbf{T}(E))$; $u \mapsto \mathbf{T}(u)$ leképezés csoport-morfizmus. Ha $u \in \mathbf{GL}(E)$ olyan, hogy $\mathbf{T}(u) = \mathrm{id}_{\mathbf{T}(E)}$, akkor

$$\mathrm{in}_{E,\mathbf{T}(E)} = \mathbf{T}(u) \circ \mathrm{in}_{E,\mathbf{T}(E)} = \mathrm{in}_{E,\mathbf{T}(E)} \circ u,$$

ezért $\mathrm{in}_{E,\mathbf{T}(E)}$ injektivitása folytán $u = \mathrm{id}_E$, tehát a $\mathbf{GL}(E) \to \mathbf{G}(\mathbf{T}(E))$; $u \mapsto \mathbf{T}(u)$ csoport-morfizmus injektív. ■

21.10. Vektortér szimmetrikus algebrája

21.10.1. Definíció. *Legyenek E, F vektorterek és $n \in \mathbb{N}$. Egy $u \in \mathbf{L}_n(E; F)$ multilineáris operátort* **szimmetrikusnak** *nevezünk, ha minden $\sigma \in \mathfrak{S}_n$ permutációra és $E^n \ni (x_i)_{i \in n}$-re fennáll az*

$$u((x_{\sigma(i)})_{i \in n}) = u((x_i)_{i \in n})$$

egyenlőség. Az $E^n \to F$ szimmetrikus multilineáris operátorok halmazát $\mathbf{L}_n^s(E; F)$ vagy $\mathbf{S}_n(E; F)$ jelöli.

A definíció természete alapján nyilvánvaló, hogy ha E, F vektorterek (illetve normált terek) és $n \in \mathbb{N}$, akkor $\mathbf{L}_n^s(E; F)$ *lineáris altere* $\mathbf{Mult}(E^n; F)$-nek.

21.10.2. Állítás. (A szimmetrikus multilineáris operátorok meghatározottságának tétele) *Legyenek E, F vektorterek a K test felett és $n \in \mathbb{N}^*$. Tegyük fel, hogy $n < \mathrm{Char}(K)$ vagy $\mathrm{Char}(K) = 0$. Ha $u \in \mathbf{L}_n^s(E; F)$ olyan, hogy minden $E \ni x$-re $u(x^{[n]}) = 0$, akkor $u = 0$.*

Bizonyítás. Legyen $u \in \mathbf{L}_n^s(E;F)$ és $(x_i)_{i\in n} \in E^n$. Azt kell megmutatni, hogy a K testre és az u-ra vonatkozó feltételek teljesülése esetén $u((x_i)_{i\in n}) = 0$.

Legyen $(t_i)_{i\in n} \in K^n$, továbbá $i \in n$ esetén $J_i := n$, és minden $J_i \ni j$-re $z_{i,j} := t_j.x_j$. Ekkor fennállnak a következő egyenlőségek:

$$\begin{aligned}
0 = u\Big(\Big(\sum_{j\in n} t_j.x_j\Big)^{[n]}\Big) &= u\Big(\Big(\sum_{j\in J_i} z_{i,j}\Big)_{i\in n}\Big) \stackrel{(1)}{=} \sum_{\sigma\in\mathscr{F}(n;n)} u((z_{i,\sigma(i)})_{i\in n}) = \\
= \sum_{\sigma\in\mathscr{F}(n;n)} u((t_{\sigma(i)}.x_{\sigma(i)})_{i\in n}) &\stackrel{(2)}{=} \sum_{\sigma\in\mathscr{F}(n;n)} \Big(\prod_{i\in n} t_{\sigma(i)}\Big).u((x_{\sigma(i)})_{i\in n}) \stackrel{(3)}{=} \\
\stackrel{(3)}{=} \sum_{\sigma\in\mathfrak{S}_n} \Big(\prod_{i\in n} t_{\sigma(i)}\Big).u((x_{\sigma(i)})_{i\in n}) &+ \sum_{\sigma\in\mathscr{F}(n;n)\setminus\mathfrak{S}_n} \Big(\prod_{i\in n} t_{\sigma(i)}\Big).u((x_{\sigma(i)})_{i\in n}) \stackrel{(4)}{=} \\
\stackrel{(4)}{=} n!\Big(\prod_{i\in n} t_i\Big).u((x_i)_{i\in n}) &+ \sum_{\sigma\in\mathscr{F}(n;n)\setminus\mathfrak{S}_n} \Big(\prod_{i\in n} t_{\sigma(i)}\Big).u((x_{\sigma(i)})_{i\in n}),
\end{aligned}$$

ahol

– az $\stackrel{(1)}{=}$ egyenlőségnél felhasználtuk u multiadditivitását és azt, hogy $\prod_{i\in n} J_i = \mathscr{F}(n;n)$;

– a $\stackrel{(2)}{=}$ egyenlőségnél felhasználtuk u multihomogenitását;

– a $\stackrel{(3)}{=}$ egyenlőségnél az $\mathscr{F}(n;n)$ halmazt az $\mathfrak{S}_n$ és $\mathscr{F}(n;n) \setminus \mathfrak{S}_n$ halmazok diszjunkt uniójaként írtuk fel, és ennek megfelelően felbontottuk az összegzést;

– a $\stackrel{(4)}{=}$ egyenlőségnél alkalmaztuk u szimmetrikusságát, így minden $\sigma \in \mathfrak{S}_n$ permutációra $u((\sigma(x_i))_{i\in n}) = u((x_i)_{i\in n})$, és felhasználtuk a K-beli szorzás általános kommutativitását, így minden $\sigma \in \mathfrak{S}_n$ permutációra $\prod_{i\in n} t_{\sigma(i)} = \prod_{i\in n} t_i$.

Tehát azt kaptuk, hogy minden $(x_i)_{i\in n} \in E^n$ esetén az

$$f_{(x_i)_{i\in n}} : K^n \to F; \quad (t_i)_{i\in n} \mapsto n!\Big(\prod_{i\in n} t_i\Big).u((x_i)_{i\in n}) + \sum_{\sigma\in\mathscr{F}(n;n)\setminus\mathfrak{S}_n} \Big(\prod_{i\in n} t_{\sigma(i)}\Big).u((x_{\sigma(i)})_{i\in n})$$

leképezés azonosan nulla. Azonban minden $(x_i)_{i\in n} : K^n \to F$ *polinomiális vektorfüggvény*, ezért a polinomiális vektorfüggvények együtthatóinak egyértelműségi tétele (**??**) alapján kapjuk, hogy $n!.u((x_i)_{i\in n}) = 0$ (és mellesleg minden $\sigma \in \mathscr{F}(n;n)\setminus\mathfrak{S}_n$ függvényre $u((x_{\sigma(i)})_{i\in n}) = 0$). Mivel a K test karakterisztikájára tett feltevés szerint $n!$ invertálható elem K-ban, ebből következik, hogy minden $(x_i)_{i\in n} \in E^n$ esetén $u((x_i)_{i\in n}) = 0$, vagyis $u = 0$. ■

Z Vigyázzunk arra, hogy ha E, F vektorterek a K test felett, $n \in \mathbb{N}^*$, és $u \in \mathbf{L}_n(E;F)$ *nem szimmetrikus* multilineáris operátor, akkor lehetséges az, hogy minden $E \ni x$-re $u(x^{[n]}) = 0$, de $u \neq 0$ (még akkor is, ha a K test nulla karakterisztikájú). Például, tetszőleges K test esetén az

$$u : K^2 \times K^2 \to K; \quad ((x_0,x_1),(y_0,y_1)) \mapsto x_1y_0 - x_0y_1$$

leképezés olyan bilineáris funkcionál a K^2 vektortér felett, hogy minden $(x_0,x_1) \in K^2$ esetén $u((x_0,x_1),(x_0,x_1)) = 0$, de $u \neq 0$.

Legyenek E, F vektorterek a K test felett, és tegyük fel, hogy a $\mathbb{Z} \to K$ kanonikus leképezés injektív (vagyis a K test nulla karakterisztikájú). Legyen továbbá $n \in \mathbb{N}^*$ rögzített. Ekkor minden $u \in \mathbf{L}_n(E;F)$ multilineáris operátorra az

$$\mathbb{S}(u) : E^n \to F; \quad (x_i)_{i\in n} \mapsto \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} u((x_{\sigma(i)})_{i\in n})$$

leképezés eleme $\mathbf{L}^s_n(E;F)$-nek; az $\mathbb{S}(u)$ operátort nevezzük u *szimmetrizáltjának.* Ha $u \in \mathbf{L}_n(E;F)$, akkor $u = \mathbb{S}(u)$ ekvivalens azzal, hogy u szimmetrikus.

21.10.3. Definíció. *Legyen E vektortér a K test felett. Ha $n \in \mathbb{N}^*$, akkor minden $(x_i)_{i\in n} \in E^n$ esetén*

$$\bigovee_{i\in n} x_i := \sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} x_{\sigma(i)},$$

*és $\overset{n}{\bigovee} E$ jelöli az $\left\{ \bigovee_{i\in n} x_i \;\middle|\; (x_i)_{i\in n} \in E^n \right\}$ halmaz által generált lineáris alteret $\mathbf{T}^n(E)$-ben, és $\overset{n}{\bigovee} E$ elemeit E **feletti n-ed rendű szimmetrikus tenzoroknak** nevezzük. Továbbá $\overset{0}{\bigovee} E := K$ és*

$$\bigovee E := \bigoplus_{n\in\mathbb{N}} \Big(\overset{n}{\bigovee} E\Big).$$

Megjegyezzük, hogy $\overset{n}{\bigovee} E$ helyett a $\mathbf{TS}^n(E)$ jelölést is szokták alkalmazni, és ezt a vektorteret az E vektortér n-edik *szimmetrikus tenzorszorzatának* is nevezik.

21.10.4. Állítás. *Legyen E vektortér a K test felett és $n \in \mathbb{N}^*$. Ekkor $\overset{n}{\bigovee} E$ olyan vektortér, hogy az*

$$s_n : E^n \to \overset{n}{\bigovee} E; \quad (x_i)_{i\in n} \mapsto \bigovee_{i\in n} x_i$$

leképezés szimmetrikus multilineáris operátor, és ha $n <$ Char(K) vagy Char$(K) = 0$, akkor minden K feletti F vektortérhez, és minden $u : E^n \to F$ szimmetrikus multilineáris operátorhoz létezik egyetlen olyan $\widetilde{u} : \overset{n}{\bigovee} E \to F$ lineáris operátor, amelyre $\widetilde{u} \circ s_n = u$, vagyis minden $(x_i)_{i\in n} \in E^n$ esetén

$$u\left((x_i)_{i\in n}\right) = \widetilde{u}\Big(\bigovee_{i\in n} x_i\Big),$$

ami azt jelenti, hogy a következő diagram kommutatív:

$$\begin{tikzcd} E^n \arrow[r, "s_n"] \arrow[dr, "u"'] & \overset{n}{\bigovee} E \arrow[d, "\tilde{u}"] \\ & F \end{tikzcd}$$

Bizonyítás. Megmutatjuk, hogy az s_n leképezés multilineáris operátor. Ehhez legyen $\mathbf{x} := (x_i)_{i\in n} \in E^n$ és $k \in n$ rögzítve. Ha $x \in E$, akkor

$$\left(s_n \circ \mathrm{in}_{k,\mathbf{x}}\right)(x) = s_n\left((x'_i)_{i\in n}\right) = \bigovee_{i\in n} x'_i = \sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} x'_{\sigma(i)},$$

ahol $(x'_i)_{i\in n} := \mathrm{in}_{k,\mathbf{x}}(x)$, tehát minden $i \in n$ esetén

$$x'_i := \begin{cases} x & \text{, ha } i = k, \\ x_i & \text{, ha } i \neq k, \end{cases}$$

ami azt jelenti, hogy minden $\sigma \in \mathfrak{S}_n$ permutációra és $i \in n$ indexre

$$x'_{\sigma(i)} = \begin{cases} x & \text{, ha } i = \sigma^{-1}(k), \\ x_i & \text{, ha } i \neq \sigma^{-1}(k), \end{cases}$$

vagyis

$$(s_n \circ \mathrm{in}_{k,\mathbf{x}})(x) = \sum_{\sigma\in\mathfrak{S}_n} \left(\bigotimes \circ \mathrm{in}_{\sigma^{-1}(k),\mathbf{x}}\right)(x),$$

ahol $\bigotimes : E^n \to \mathbf{T}^n(E)$ a kanonikus multilineáris operátor. Ez azt jelenti, hogy

$$s_n \circ \mathrm{in}_{k,\mathbf{x}} = \sum_{\sigma\in\mathfrak{S}_n} \left(\bigotimes \circ \mathrm{in}_{\sigma^{-1}(k),\mathbf{x}}\right),$$

és minden $\sigma \in \mathfrak{S}_n$ esetén $\bigotimes \circ \mathrm{in}_{\sigma^{-1}(k),\mathbf{x}} : E \to \mathbf{T}^n(E)$ lineáris operátor, így $s_n \circ \mathrm{in}_{k,\mathbf{x}} : E \to \overset{n}{\bigvee} E$ lineáris operátor. Ezért az $s_n : E^n \to \overset{n}{\bigvee} E$ leképezés multilineáris operátor.

Az s_n leképezés szimmetrikus, mert ha $(x_i)_{i\in n} \in E^n$ és $\tau \in \mathfrak{S}_n$, akkor

$$s_n\Big((x_{\tau(i)})_{i\in n}\Big) = \bigvee_{i\in n} x_{\tau(i)} = \sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} x_{\tau(\sigma(i))} = \sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} x_{(\tau\circ\sigma)(i)} = \sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} x_{\sigma(i)},$$

mert az $\mathfrak{S}_n \to \mathfrak{S}_n$; $\sigma \mapsto \tau \circ \sigma$ leképezés bijekció, így alkalmazhatjuk $\mathbf{T}^n(E)$ összeadásának általános kommutativitását.

Legyen F vektortér K felett, és $u : E^n \to F$ szimmetrikus multilineáris operátor. A tenzorszorzat univerzalitási tulajdonsága szerint létezik egyetlen olyan $v : \mathbf{T}^n(E) \to F$ lineáris operátor, amelyre minden $(x_i)_{i\in n} \in E^n$ esetén $v\Big(\bigotimes_{i\in n} x_i\Big) = u((x_i)_{i\in n})$. Ha $(x_i)_{i\in n} \in E^n$, akkor v additivitása miatt

$$v\Big(\bigvee_{i\in n} x_i\Big) = v\Big(\sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} x_{\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_n} v\Big(\bigotimes_{i\in n} x_{\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_n} u\left((x_{\sigma(i)})_{i\in n}\right) = n!u\left((x_i)_{i\in n}\right).$$

Ha $\mathrm{Char}(K) = 0$, vagy $n < \mathrm{Char}(K)$, akkor $n!$ invertálható elem K-ban, így a fentiek szerint $\widetilde{u} := \dfrac{1}{n!}\Big(v \,\Big|\, {}_{\overset{n}{\bigvee} E}\Big) : \overset{n}{\bigvee} E \to F$ olyan lineáris operátor, amelynek létezését állítottuk. Az $\widetilde{u}$ operátor egyértelműsége nyilvánvaló, mert a definíció szerint $\Big\{ \bigvee_{i\in n} x_i \,\Big|\, (x_i)_{i\in n} \in E^n \Big\}$ generátorhalmaz a $\overset{n}{\bigvee} E$ vektortérben. ■

21.10.5. Következmény. *Legyen E vektortér a K test felett és $n \in \mathbb{N}^*$. Ha $n <$ $\mathrm{Char}(K)$ vagy $\mathrm{Char}(K) = 0$, akkor a*

$$\Big(\overset{n}{\bigvee} E\Big)^* \to \mathbf{S}_n(E); \quad \Big(f \mapsto \Big((x_i)_{i\in n} \mapsto f\Big(\bigvee_{i\in n} x_i\Big)\Big)\Big)$$

leképezés lineáris bijekció, ahol $\mathbf{S}_n(E)$ az $E^n \to K$ szimmetrikus multilineáris funkcionálok vektortere. ■

21.10.6. Tétel. *Legyen E vektortér a K test felett és $n \in \mathbb{N}^*$ olyan, hogy $n < \mathrm{Char}(K)$ vagy $\mathrm{Char}(K) = 0$.*

a) *Létezik olyan (S, s) pár, hogy S vektortér a K test felett, és $s : E^n \to S$ olyan szimmetrikus multilineáris operátor, amelyre teljesül a következő állítás.*

(TS) *Minden K feletti F vektortérhez, és minden $u : E^n \to F$ szimmetrikus multilineáris operátorhoz létezik egyetlen olyan $\widetilde{u} : S \to F$ lineáris operátor, amelyre $\widetilde{u} \circ s = u$, vagyis a következő diagram kommutatív:*

$$\begin{tikzcd} E^n \arrow[r, "s"] \arrow[dr, "u"'] & S \arrow[d, "\tilde{u}"] \\ & F \end{tikzcd}$$

b) *Ha (S', s') szintén olyan pár, hogy S' vektortér a K test felett, és $s' : E^n \to S'$ olyan szimmetrikus multilineáris operátor, hogy minden F vektortérhez és minden $u : E^n \to F$ szimmetrikus multilineáris operátorhoz létezik egyetlen olyan $\widetilde{u} : S' \to F$ lineáris operátor, hogy $\widetilde{u} \circ s' = u$, akkor létezik egyetlen olyan $v : S \to S'$ lineáris bijekció, amelyre $v \circ s = s'$.*

Bizonyítás. Az 21.10.4. állítás szerint az $(S, s) := (\overset{n}{\bigovee} E, s_n)$ pár eleget tesz a (TS) feltételnek, tehát a) teljesül.

Legyen (S, s) olyan pár, amelyre (TS) teljesül, és legyen (S', s') olyan pár, amely rendelkezik a b) állításban megfogalmazott tulajdonságokkal. Ekkor S' vektortér K felett és $s' : E^n \to S'$ szimmetrikus multilineáris operátor, így egyértelműen létezik olyan $v : S \to S'$ lineáris operátor, hogy $v \circ s = s'$. Felcseréve az (S, s) és (S', s') párok szerepét, hasonló érveléssel kapjuk, hogy egyértelműen létezik olyan $v' : S' \to S$ lineáris operátor, amelyre $v' \circ s' = s$. Mivel S vektortér K felett, és $s : E^n \to S$ szimmetrikus multilineáris operátor, így (TS) alapján egyértelműen létezik olyan $w : S \to S$ lineáris operátor, amelyre $w \circ s = s$. Világos, hogy az egyértelműségi feltételből $w = \mathrm{id}_S$ következik, hiszen $\mathrm{id}_S : S \to S$ nyilvánvalóan olyan lineáris operátor, hogy $\mathrm{id}_S \circ s = s$. Ugyanakkor $v' \circ v : S \to S$ is olyan lineáris operátor, hogy $(v' \circ v) \circ s = v' \circ (v \circ s) = v' \circ s' = s$, így az egyértelműség miatt $v' \circ v = \mathrm{id}_S$. Felcseréve az (S, s) és (S', s') párok szerepét, teljesen hasonlóan kapjuk, hogy $v \circ v' = \mathrm{id}_{S'}$. Ez azt jelenti, hogy $v : S \to S'$ lineáris bijekció és $v \circ s = s'$. A v operátor egyértelműsége még a $\{w \in \mathbf{L}(S; S') | w \circ s = s'\}$ operátorhalmazban is teljesül. ■

21.10.7. Állítás. *Legyenek E és F vektorterek, valamint $n \in \mathbb{N}^*$. Ha $u : E \to F$ lineáris operátor, akkor létezik egyetlen olyan*

$$\overset{n}{\bigovee} u : \overset{n}{\bigovee} E \to \overset{n}{\bigovee} F$$

lineáris operátor, amelyre minden $(x_i)_{i \in n} \in E^n$ esetén

$$\Big(\overset{n}{\bigovee} u\Big)\Big(\bigovee_{i \in n} x_i\Big) = \bigovee_{i \in n} u(x_i).$$

Továbbá, fennáll az $\overset{n}{\bigovee} \mathrm{id}_E = \mathrm{id}_{\overset{n}{\bigovee} E}$ egyenlőség.

Bizonyítás. A $\bigvee^{n} u$ lineáris operátor egyértelműsége nyilvánvalóan következik abból, hogy $\left\{ \bigvee_{i\in n} x_i \;\middle|\; (x_i)_{i\in n} \in E^n \right\}$ generátorhalmaz a $\bigvee^{n} E$ vektortérben. A $\bigvee^{n} u$ lineáris operátor létezésének bizonyításához először megjegyezzük, hogy 19.7.6. szerint u-hoz egyértelműen létezik olyan $\widetilde{u} : \mathbf{T}^n(E) \to \mathbf{T}^n(F)$ lineáris operátor, amelyre minden $(x_i)_{i\in n} \in E^n$ esetén $\widetilde{u}\Big(\bigotimes_{i\in n} x_i\Big) = \bigotimes_{i\in n} u(x_i)$. Ekkor a definíció szerint minden $(x_i)_{i\in n} \in E^n$ esetén

$$\widetilde{u}\Big(\bigvee_{i\in n} x_i\Big) = \widetilde{u}\Big(\sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} x_{\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_n} \widetilde{u}\Big(\bigotimes_{i\in n} x_{\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_n} \bigotimes_{i\in n} u(x_{\sigma(i)}) = \bigvee_{i\in n} u(x_i).$$

Ebből látható, hogy $\widetilde{u}\left\langle \bigvee^{n} E \right\rangle \subseteq \bigvee^{n} F$, következésképpen az $\widetilde{u}$ leképezés $\bigvee^{n} E$-re vett leszűkítése olyan $\bigvee^{n} E \to \bigvee^{n} F$ lineáris operátor, amelynek a létezését állítottuk.
Ha $(x_i)_{i\in n} \in E^n$, akkor a definíció szerint

$$\Big(\bigvee^{n} \mathrm{id}_E\Big)\Big(\bigvee_{i\in n} x_i\Big) = \bigvee_{i\in n} \mathrm{id}_E(x_i) = \bigvee_{i\in n} x_i,$$

tehát a $\bigvee^{n} \mathrm{id}_E$ és $\mathrm{id}_{\bigvee^{n} E}$ lineáris operátorok megegyeznek a $\left\{ \bigvee_{i\in n} x_i \;\middle|\; (x_i)_{i\in n} \in E^n \right\}$ generátorhalmazon, ezért ezek az operátorok egyenlőek. ■

21.10.8. Állítás. *Legyenek E, F és G vektorterek, valamint $n \in \mathbb{N}^*$. Ha $u : E \to F$ és $v : F \to G$ lineáris operátorok, akkor*

$$\bigvee^{n}(v \circ u) = \Big(\bigvee^{n} v\Big) \circ \Big(\bigvee^{n} u\Big).$$

Bizonyítás. A $v \circ u : E \to G$ lineáris operátorra teljesül az, hogy minden $(x_i)_{i\in n} \in E^n$ esetén

$$\begin{aligned}\Big(\bigvee^{n}(v \circ u)\Big)\Big(\bigvee_{i\in n} x_i\Big) &= \bigvee_{i\in n}(v \circ u)(x_i) = \bigvee_{i\in n} v(u(x_i)) = \Big(\bigvee^{n} v\Big)\Big(\bigvee_{i\in n} u(x_i)\Big) = \\ &= \Big(\bigvee^{n} v\Big)\Big(\Big(\bigvee^{n} u\Big)((x_i)_{i\in n})\Big) = \Big(\Big(\bigvee^{n} v\Big) \circ \Big(\bigvee^{n} u\Big)\Big)((x_i)_{i\in n}),\end{aligned}$$

ami az előző állításban szereplő egyértelműségi tulajdonság alapján az operátoregyenlőséget bizonyítja. ■

21.10.9. Következmény. *Legyenek E és F vektorterek, valamint $n \in \mathbb{N}^*$. Ha az $u : E \to F$ lineáris operátor injektív (illetve szürjektív), akkor az*

$$\bigvee^{n} u : \bigvee^{n} E \to \bigvee^{n} F$$

lineáris operátor is injektív (illetve szürjektív). Ha $u : E \to F$ lineáris izomorfizmus az E és F vektorterek között, akkor $\bigvee^{n} u$ lineáris izomorfizmus a $\bigvee^{n} E$ és $\bigvee^{n} F$ vektorterek között.

Bizonyítás. A második állítás nyilvánvalóan következik az elsőből.

Tegyük fel, hogy az $u : E \to F$ lineáris operátor injektív. Ekkor 17.7.5. szerint létezik u-nak lineáris balinverze, vagyis olyan $v : F \to E$ lineáris operátor, hogy $v \circ u = \mathrm{id}_E$. Ekkor 21.10.7. és 21.10.8. szerint

$$\left(\overset{n}{\ovee} v\right) \circ \left(\overset{n}{\ovee} u\right) = \overset{n}{\ovee}(v \circ u) = \overset{n}{\ovee}\mathrm{id}_E = \mathrm{id}_{\overset{n}{\ovee} E},$$

tehát a $\overset{n}{\ovee} v : \overset{n}{\ovee} F \to \overset{n}{\ovee} E$ leképezés balinverze az $\overset{n}{\ovee} u$ leképezésnek, így $\overset{n}{\ovee} u : \overset{n}{\ovee} E \to \overset{n}{\ovee} F$ injekció.

Tegyük fel, hogy az $u : E \to F$ lineáris operátor szürjektív. Ekkor 17.4.7. szerint létezik u-nak lineáris jobbinverze, vagyis olyan $w : F \to E$ lineáris operátor, hogy $u \circ w = \mathrm{id}_F$. Ekkor 21.10.7. és 21.10.8. szerint

$$\left(\overset{n}{\ovee} u\right) \circ \left(\overset{n}{\ovee} w\right) = \overset{n}{\ovee}(u \circ w) = \overset{n}{\ovee}\mathrm{id}_F = \mathrm{id}_{\overset{n}{\ovee} F},$$

tehát a $\overset{n}{\ovee} w : \overset{n}{\ovee} F \to \overset{n}{\ovee} E$ leképezés jobbinverze az $\overset{n}{\ovee} u$ leképezésnek, így $\overset{n}{\ovee} u : \overset{n}{\ovee} E \to \overset{n}{\ovee} F$ szürjekció. ■

21.10.10. Definíció. *Legyen E vektortér, és legyen $\mathfrak{m}$ az*

$$\left\{\mathrm{in}_{E,\mathbf{T}(E)}(x) \cdot \mathrm{in}_{E,\mathbf{T}(E)}(y) - \mathrm{in}_{E,\mathbf{T}(E)}(y) \cdot \mathrm{in}_{E,\mathbf{T}(E)}(x) \;\middle|\; (x \in E) \wedge (y \in E)\right\}$$

halmaz által generált ideál a $\mathbf{T}(E)$ tenzoralgebrában. Ekkor a $\mathbf{T}(E)/\mathfrak{m}$ faktoralgebrát az E vektortér **szimmetrikus algebrájának** *nevezzük, és az $\mathbf{S}(E)$ szimbólummal jelöljük, továbbá $\mathrm{s}_E := \pi_{\mathbf{T}(E)/\mathfrak{m}} \circ \mathrm{in}_{E,\mathbf{T}(E)}$, ahol $\pi_{\mathbf{T}(E)/\mathfrak{m}}$ a $\mathbf{T}(E) \to \mathbf{S}(E)$ kanonikus szürjekció és $\mathrm{in}_{E,\mathbf{T}(E)} : E \to \mathbf{T}(E)$ kanonikus injekció.*

21.10.11. Tétel. *Legyen E vektortér a K test felett.*

a) *Az $(\mathbf{S}(E), \mathrm{s}_E))$ pár rendelkezik azzal a tulajdonsággal, hogy $\mathbf{S}(E)$ kommutatív egységelemes algebra a K test felett, és s_E olyan $E \to \mathbf{S}(E)$ lineáris operátor, hogy az $\mathrm{Im}(\mathrm{s}_E)$ halmaz generálja az $\mathbf{S}(E)$ algebrát, továbbá, minden A kommutatív egységelemes algebrához és $u : E \to A$ lineáris operátorhoz létezik egyetlen olyan $\tilde{u} : \mathbf{S}(E) \to B$ egységelem-tartó algebra-morfizmus, amelyre $\tilde{u} \circ \mathrm{s}_E = u$, vagyis a következő diagram kommutatív.*

$$\begin{tikzcd} E \arrow[r, "\mathrm{s}_E"] \arrow[dr, "u"'] & \mathbf{S}(E) \arrow[d, "\tilde{u}"] \\ & A \end{tikzcd}$$

b) *Tegyük fel, hogy (S, s) olyan pár, amelyre S kommutatív egységelemes algebra K felett, és $s : E \to S$ lineáris operátor, és teljesül a következő állítás.*

(TS) *Minden K feletti B kommutatív egységelemes algebrához, és minden $u : E \to B$ lineáris operátorhoz, létezik egyetlen olyan $\tilde{u} : S \to B$ egységelem-tartó algebra-morfizmus, hogy $\tilde{u} \circ i = u$, vagyis a következő diagram kommutatív.*

$$\begin{tikzcd} E \arrow[r, "s"] \arrow[dr, "u"'] & S \arrow[d, "\tilde{u}"] \\ & B \end{tikzcd}$$

Ekkor létezik egyetlen olyan $\pi : \mathbf{T}(E) \to A$ egységelem-tartó algebra-morfizmus, amelyre $\pi \circ \mathrm{in}_{E,\mathbf{T}(E)} = i$, továbbá ekkor π izomorfizmus a $\mathbf{T}(E)$ tenzoralgebra ás az A algebra között, és $i : E \to A$ szükségképpen injekció, és A egyenlő az $\mathrm{Im}(i)$ halmaz által generált egységelemes részalgebrával.

Bizonyítás. ■

21.11. Vektortér külső algebrája

21.11.1. Definíció. *Legyen E vektortér és $p \in \mathbb{N}^*$. Ekkor minden $(x_i)_{i\in p} \in E^p$ esetén*

$$\bigwedge_{i\in p} x_i := \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) \bigotimes_{i\in p} x_{\sigma(i)},$$

és $\overset{p}{\bigwedge} E$ jelöli az $\left\{ \bigwedge_{i\in p} x_i \;\middle|\; (x_i)_{i\in p} \in E^p \right\}$ halmaz által generált lineáris alteret $\mathbf{T}^p(E)$-ben, és $\overset{p}{\bigwedge} E$ elemeit E **feletti p-ed rendű antiszimmetrikus tenzoroknak** *vagy E* **feletti p-vektoroknak** *nevezzük. Továbbá $\overset{0}{\bigwedge} E := K$ és*

$$\bigwedge E := \bigoplus_{p\in\mathbb{N}} \left(\overset{p}{\bigwedge} E\right).$$

21.11.2. Állítás. *Legyen E vektortér a K test felett és $p \in \mathbb{N}^*$. Ekkor $\overset{p}{\bigwedge} E$ olyan vektortér, hogy az*

$$a_p : E^p \to \overset{p}{\bigwedge} E; \quad (x_i)_{i\in p} \mapsto \bigwedge_{i\in p} x_i$$

leképezés alternáló multilineáris operátor, vagyis $a_n \in \mathbf{Alt}_p(E; \overset{p}{\bigwedge} E)$ (20.1.1.).

Bizonyítás. Megmutatjuk, hogy az a_p leképezés multilineáris operátor. Ehhez legyen $\mathbf{x} := (x_i)_{i\in p} \in E^p$ és $k \in p$ rögzítve. Ha $x \in E$, akkor

$$(a_p \circ \mathrm{in}_{k,\mathbf{x}})(x) = a_p\left((x'_i)_{i\in p}\right) = \bigwedge_{i\in p} x'_i = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_n(\sigma) \bigotimes_{i\in p} x'_{\sigma(i)},$$

ahol $(x'_i)_{i\in p} := \mathrm{in}_{k,\mathbf{x}}(x)$, tehát minden $i \in p$ esetén

$$x'_i := \begin{cases} x & \text{, ha } i = k, \\ x_i & \text{, ha } i \neq k, \end{cases}$$

ami azt jelenti, hogy minden $\sigma \in \mathfrak{S}_p$ permutációra és $i \in p$ indexre

$$x'_{\sigma(i)} = \begin{cases} x & \text{, ha } i = \sigma^{-1}(k), \\ x_i & \text{, ha } i \neq \sigma^{-1}(k), \end{cases}$$

vagyis

$$(a_p \circ \mathrm{in}_{k,\mathbf{x}})(x) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_n(\sigma) \left(\otimes \circ \mathrm{in}_{\sigma^{-1}(k),\mathbf{x}}\right)(x),$$

ahol $\otimes : E^p \to \mathbf{T}^p(E)$ a kanonikus multilineáris operátor. Ez azt jelenti, hogy

$$a_p \circ \mathrm{in}_{k,\mathbf{x}} = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon_n(\sigma) \left(\otimes \circ \mathrm{in}_{\sigma^{-1}(k),\mathbf{x}}\right),$$

és minden $\sigma \in \mathfrak{S}_p$ esetén $\otimes \circ \mathrm{in}_{\sigma^{-1}(k),\mathbf{x}} : E \to \mathbf{T}^p(E)$ lineáris operátor, így $a_p \circ \mathrm{in}_{k,\mathbf{x}} : E \to \overset{p}{\owedge} E$ lineáris operátor. Ezért az $a_p : E^p \to \overset{p}{\owedge} E$ leképezés multilineáris operátor.

Megmutatjuk, hogy az $a_p : E^p \to \overset{p}{\owedge} E$ leképezés alternáló. Ehhez legyen $(x_i)_{i \in p} \in E^p$ olyan rendszer és legyenek $j, k \in n$ olyan számok, hogy $j \neq k$ és $x_j = x_k$. Vezessük be az

$$f : \mathfrak{S}_p \to \mathbf{T}^p(E); \quad \sigma \mapsto \varepsilon_n(\sigma) \bigotimes_{i \in p} x_{\sigma(i)}$$

függvényt, amelyre a definíció szerint

$$a_p\left((x_i)_{i \in p}\right) = \sum_{\sigma \in \mathfrak{S}_p} f(\sigma) \tag{$*$}$$

teljesül. Jelölje $\tau_{j,k} \in \mathfrak{S}_p$ azt a permutációt, amelyre $\tau_{j,k}(j) = k$ és $\tau_{j,k}(k) = j$ és minden $i \in p$ esetén, ha $i \neq j$ és $i \neq k$, akkor $\tau_{j,k}(i) = i$. Ekkor $\sigma \in \mathfrak{S}_p$ esetén minden $i \in p$ indexre

$$x_{\tau_{j,k}(\sigma(i))} = \begin{cases} x_{\sigma(i)} & \text{, ha } i \neq \sigma^{-1}(j) \text{ és } i \neq \sigma^{-1}(k), \\ x_k & \text{, ha } i = \sigma^{-1}(j), \\ x_j & \text{, ha } i = \sigma^{-1}(k). \end{cases}$$

Tehát $\sigma \in \mathfrak{S}_p$ esetén

– ha $i = \sigma^{-1}(j)$, akkor $x_{\tau_{j,k}(\sigma(i))} = x_k = x_j = x_{\sigma(i)}$,

– ha $i = \sigma^{-1}(k)$, akkor $x_{\tau_{j,k}(\sigma(i))} = x_j = x_k = x_{\sigma(i)}$.

Ez azt jelenti, hogy minden $i \in p$ esetén $x_{\tau_{j,k}(\sigma(i))} = x_{\sigma(i)}$, ezért

$$f\left(\tau_{j,k} \circ \sigma\right) = \varepsilon_n(\tau_{j,k} \circ \sigma) \bigotimes_{i \in p} x_{\tau_{j,k}(\sigma(i))} = \varepsilon_n(\tau_{j,k}) \varepsilon_n(\sigma) \bigotimes_{i \in p} x_{\sigma(i)} = -f(\sigma).$$

Ezért 13.2.2. alapján $\sum_{\sigma \in \mathfrak{S}_p} f(\sigma) = 0$, így a $(*)$ egyenlőségből $a_p\left((x_i)_{i \in p}\right) = 0$ következik, vagyis a_p alternáló multilineáris operátor. ■

21.11.3. Állítás. *Legyen E vektortér a K test felett és $p \in \mathbb{N}^*$. Ekkor az*

$$a_p : E^p \to \overset{p}{\owedge} E; \quad (x_i)_{i \in p} \mapsto \owedge_{i \in p} x_i$$

alternáló multilineáris operátorra teljesül az, hogy ha $p < \mathrm{Char}(K)$ vagy $\mathrm{Char}(K) = 0$, akkor minden K feletti F vektortérhez, és minden $u : E^p \to F$ antiszimmetrikus multilineáris operátorhoz létezik egyetlen olyan $\widetilde{u} : \overset{p}{\owedge} E \to F$ lineáris operátor, amelyre $\widetilde{u} \circ a_p = u$, vagyis minden $(x_i)_{i \in p} \in E^p$ esetén

$$u\left((x_i)_{i \in p}\right) = \widetilde{u}\Big(\owedge_{i \in p} x_i\Big),$$

ami azt jelenti, hogy a következő diagram kommutatív:

$$\begin{tikzcd} E^p \arrow[r, "a_p"] \arrow[dr, "u"'] & \overset{p}{\owedge} E \arrow[d, "\tilde{u}"] \\ & F \end{tikzcd}$$

Bizonyítás. Legyen F vektortér K felett, és $u : E^p \to F$ antiszimmetrikus multilineáris operátor. A tenzorszorzat univerzalitási tulajdonsága szerint létezik egyetlen olyan $v : \mathbf{T}^p(E) \to F$ lineáris operátor, amelyre minden $(x_i)_{i\in p} \in E^p$ esetén $v\Big(\bigotimes\limits_{i\in p} x_i\Big) = u\left((x_i)_{i\in p}\right)$. Ha $(x_i)_{i\in p} \in E^p$, akkor v additivitása miatt

$$v\Big(\bigwedge_{i\in p} x_i\Big) = v\Big(\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_n(\sigma) \bigotimes_{i\in p} x_{\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_n(\sigma) v\Big(\bigotimes_{i\in p} x_{\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_n(\sigma) u\left((x_{\sigma(i)})_{i\in p}\right) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_n(\sigma)\varepsilon_n(\sigma) u\left((x_i)_{i\in p}\right) = p!u\left((x_i)_{i\in p}\right).$$

Ha $\mathrm{Char}(K) = 0$, vagy $p < \mathrm{Char}(K)$, akkor $p!$ invertálható elem K-ban, mert $p! = \prod\limits_{0<k\leq p} k$, és minden $0 < k \leq p$ természetes számra k invertálható K-ban, így a fentiek szerint $\widetilde{u} := \dfrac{1}{p!}\Big(v \,\Big|\, {}_{\overset{p}{\bigwedge} E}\Big) : \overset{p}{\bigwedge} E \to F$ olyan lineáris operátor, amelynek létezését állítottuk. Az $\widetilde{u}$ operátor egyértelműsége nyilvánvaló, mert a definíció szerint $\Big\{ \bigwedge\limits_{i\in p} x_i \mid (x_i)_{i\in p} \in E^p \Big\}$ generátorhalmaz a $\overset{p}{\bigwedge} E$ vektortérben. ■

21.11.4. Következmény. *Legyen E vektortér a K test felett és $p \in \mathbb{N}^*$. Ha $p <$ $\mathrm{Char}(K)$ vagy $\mathrm{Char}(K) = 0$, akkor a*

$$\Big(\overset{p}{\bigwedge} E\Big)^* \to \mathbf{A}_p(E); \quad \Big(f \mapsto \Big((x_i)_{i\in p} \mapsto f\Big(\bigwedge_{i\in p} x_i\Big)\Big)\Big)$$

leképezés lineáris bijekció, ahol $\mathbf{A}_p(E)$ az $E^p \to K$ antiszimmetrikus multilineáris funkcionálok vektortere. ■

21.11.5. Állítás. *Legyen E véges dimenziós vektortér a K test felett és $n := \dim(E) >$ 0. Legyen $(e_j)_{j\in n}$ bázis az E vektortérben.*

a) *Ha $p \in \mathbb{N}^*$ és $p \leq n$, akkor az*

$$\Big(\bigwedge_{i\in p} e_{\varrho(i)}\Big)_{\varrho\in\mathscr{M}(p;n)}$$

rendszer generátorrendszer a $\overset{p}{\bigwedge} E$ vektortérben, ahol $\mathscr{M}(p;n)$ a $p \to n$ szigorúan monoton növő függvények halmaza, tehát $\overset{p}{\bigwedge} E$ véges dimenziós vektortér és

$$\dim\Big(\overset{p}{\bigwedge} E\Big) \leq \binom{\dim(E)}{p}.$$

b) *Ha $p \in \mathbb{N}$ és $p > n$, akkor $\overset{p}{\bigwedge} E = \{0\}$.*

c) *Ha $p \in \mathbb{N}^*$ és $p \leq n$, továbbá $p < \mathrm{Char}(K)$ vagy $\mathrm{Char}(K) = 0$, akkor az*

$$\Big(\bigwedge_{i\in p} e_{\varrho(i)}\Big)_{\varrho\in\mathscr{M}(p;n)}$$

rendszer bázis a $\overset{p}{\bigwedge} E$ vektortérben, és

$$\dim\Big(\overset{p}{\bigwedge} E\Big) = \binom{\dim(E)}{p}.$$

Bizonyítás. (I) Tegyük fel, hogy K tetszőleges test. Rögzítsünk egy $(x_i)_{i\in p} \in E^p$ rendszert, és legyen $(X_{i,j})_{(i,j)\in p\times n} \in \mathrm{M}_{p,n}(K)$ az a $p\times n$-es mátrix, amelyre minden $i\in p$ esetén $x_i = \sum_{j\in n} X_{i,j}.e_j$. Ekkor

$$\bigwedge_{i\in p} x_i = \bigwedge_{i\in p}\Big(\sum_{j\in n} X_{i,j}.e_j\Big) \overset{(1)}{=} \sum_{f\in\mathscr{F}(p;n)} \bigwedge_{i\in p}(X_{i,f(i)}.e_{f(i)}) \overset{(2)}{=} \sum_{f\in\mathscr{F}(p;n)} \Big(\mathrm{P}_{i\in p} X_{i,f(i)}\Big).\bigwedge_{i\in p} e_{f(i)},$$

ahol az $E^p \to \overset{p}{\bigwedge} E$ kanonikus leképezés multilinearitása miatt az $\overset{(1)}{=}$ egyenlőségnél a multiadditivitás formulát, és a $\overset{(2)}{=}$ egyenlőségnél a multihomogenitás formulát alkalmaztuk. Ha $f\in\mathscr{F}(p;n)$ és f nem injektív, akkor $\bigwedge_{i\in p} e_{f(i)} = 0$, mert az $E^p \to \overset{p}{\bigwedge} E$ kanonikus leképezés alternáló, ezért

$$\bigwedge_{i\in p} x_i = \sum_{f\in\mathscr{I}(p;n)} \Big(\mathrm{P}_{i\in p} X_{i,f(i)}\Big).\bigwedge_{i\in p} e_{f(i)}, \tag{1}$$

ahol $\mathscr{I}(p;n)$ jelöli a $p\to n$ injekciók halmazát. Ebből azonnal látható, hogy $p>n$ esetén $\bigwedge_{i\in p} x_i = 0$, hiszen ekkor $\mathscr{I}(p;n)=\emptyset$. Mivel $\Big\{\bigwedge_{i\in p} x_i \mid (x_i)_{i\in p}\in E^p\Big\}$ generátorhalmaz a $\overset{p}{\bigwedge} E$ vektortérben, ebből következik, hogy $p>n$ esetén $\overset{p}{\bigwedge} E = \{0\}$, vagyis b) teljesül.

Ettől kezdve feltehetjük, hogy $p\le n$. A 9.4.7. b) állítás szerint

$$\mathscr{I}(p;n) = \bigcup_{\varrho\in\mathscr{M}(p;n)} \{\varrho\circ\sigma | \sigma\in\mathfrak{S}_p\},$$

ahol $\mathscr{M}(p;n)$ a $p\to n$ szigorúan monoton növő függvények halmaza, ugyanakkor a $\Big(\{\varrho\circ\sigma|\sigma\in\mathfrak{S}_p\}\Big)_{\varrho\in\mathscr{M}(p;n)}$ halmazrendszer diszjunkt, így (1) alapján

$$\begin{aligned}
\bigwedge_{i\in p} x_i &= \sum_{\varrho\in\mathscr{M}(p;n)}\left(\sum_{\sigma\in\mathfrak{S}_p}\Big(\mathrm{P}_{i\in p} X_{i,\varrho(\sigma(i))}\Big).\bigwedge_{i\in p} e_{\varrho(\sigma(i))}\right) \overset{(3)}{=} \\
&\overset{(3)}{=} \sum_{\varrho\in\mathscr{M}(p;n)}\left(\sum_{\sigma\in\mathfrak{S}_p}\Big(\mathrm{P}_{i\in p} X_{i,\varrho(\sigma(i))}\Big).\varepsilon_p(\sigma)\bigwedge_{i\in p} e_{\varrho(i)}\right) = \\
&= \sum_{\varrho\in\mathscr{M}(p;n)}\left(\sum_{\sigma\in\mathfrak{S}_p}\varepsilon_p(\sigma)\Big(\mathrm{P}_{i\in p} X_{i,\varrho(\sigma(i))}\Big)\right).\bigwedge_{i\in p} e_{\varrho(i)} \overset{(4)}{=} \\
&\overset{(4)}{=} \sum_{\varrho\in\mathscr{M}(p;n)}\Big(\det\big((X_{i,\varrho(k)})_{(i,k)\in p\times p}\big)\Big).\bigwedge_{i\in p} e_{\varrho(i)},
\end{aligned}$$

ahol a $\overset{(3)}{=}$ egyenlőségnél felhasználtuk, hogy az $E^p\to\overset{p}{\bigwedge} E$ kanonikus leképezés alternáló, ezért antiszimmetrikus (20.1.2.), tehát minden $\sigma\in\mathfrak{S}_p$ permutációra $\bigwedge_{i\in p} e_{\varrho(\sigma(i))} = \varepsilon_p(\sigma)\bigwedge_{i\in p} e_{\varrho(i)}$, és a $\overset{(4)}{=}$ egyenlőségnél felhasználtuk a determináns definícióját (15.2.1.).

Ezzel megmutattuk, hogy ha $(x_i)_{i\in p}\in E^p$ és $(X_{i,j})_{(i,j)\in p\times n}\in \mathrm{M}_{p,n}(K)$ az a $p\times n$-es mátrix, amelyre minden $i\in p$ esetén $x_i=\sum\limits_{j\in n}X_{i,j}.e_j$, akkor

$$\bigwedge_{i\in p} x_i=\sum_{\varrho\in\mathscr{M}(p;n)}\left(\det\left((X_{i,\varrho(k)})_{(i,k)\in p\times p}\right)\right).\bigwedge_{i\in p} e_{\varrho(i)}, \tag{2}$$

A definíció szerint $\left\{\bigwedge\limits_{i\in p} x_i \mid (x_i)_{i\in p}\in E^p\right\}$ generátorhalmaz a $\overset{p}{\bigwedge}E$ vektortérben, ezért $\left(\bigwedge\limits_{i\in p} e_{\varrho(i)}\right)_{\varrho\in\mathscr{M}(p;n)}$ generátorrendszer a $\overset{p}{\bigwedge}E$ vektortérben. Ebből 17.5.8. alapján kapjuk, hogy $\overset{p}{\bigwedge}E$ véges dimenziós vektortér és $\dim\left(\overset{p}{\bigwedge}E\right)\le \mathrm{Card}(\mathscr{M}(p;n))=\binom{\dim(E)}{p}$, ahol az egyenlőségnél a 9.4.7. a) állítást alkalmaztuk. Ezzel az a) kijelentést igazoltuk.
(II) Tegyük fel, hogy $p\in\mathbb{N}^*$ és $p\le n$, valamint $p<\mathrm{Char}(K)$ vagy $\mathrm{Char}(K)=0$. Az a) állítás szerint $\mathscr{G}:=\left\{\bigwedge\limits_{i\in p} e_{\varrho(i)} \;\middle|\; \varrho\in\mathscr{M}(p;n)\right\}$ generátorhalmaz az $\overset{p}{\bigwedge}E$ vektortérben. A 17.5.8. tétel szerint van olyan $\mathscr{B}\subseteq\mathscr{G}$ részhalmaz, amely bázishalmaz $\overset{p}{\bigwedge}E$-ben. Ekkor

$$\mathrm{Card}(\mathscr{B})=\dim\left(\overset{p}{\bigwedge}E\right)\overset{(5)}{=}\dim\left(\left(\overset{p}{\bigwedge}E\right)^*\right)\overset{(6)}{=}\dim(\mathbf{A}_p(E))\overset{(7)}{=}\binom{\dim(E)}{p},$$

ahol

- az $\overset{(5)}{=}$ egyenlőségnél a 17.9.10. állítást alkalmaztuk,
- a $\overset{(6)}{=}$ egyenlőségnél felhasználtuk a 21.11.4. állítást,
- a $\overset{(7)}{=}$ egyenlőségnél a 20.5.4. állításra hivatkoztunk, felhasználva azt, hogy $\mathbf{A}_p(E)=\mathbf{Alt}_p(E)$.

Ugyanakkor, az $\mathscr{M}(p;n)\to\mathscr{G};\ \varrho\mapsto\bigwedge\limits_{i\in p} e_{\varrho(i)}$ leképezés szürjekció, ezért

$$\mathrm{Card}(\mathscr{G})\le\mathrm{Card}(\mathscr{M}(p;n))\overset{(8)}{=}\binom{n}{p}=\mathrm{Card}(\mathscr{B})\le\mathrm{Card}(\mathscr{G}),$$

ahol a $\overset{(8)}{=}$ egyenlőségnél ismét a 9.4.7. a) állítást alkalmaztuk. Ebből 8.1.15. alapján következik, hogy $\mathscr{G}=\mathscr{B}$, tehát $\mathscr{G}$ lineárisan független halmaz, vagyis $\left(\bigwedge\limits_{i\in p} e_{\varrho(i)}\right)_{\varrho\in\mathscr{M}(p;n)}$ lineárisan független rendszer a $\overset{p}{\bigwedge}E$ vektortérben. Tehát ez a rendszer bázis $\overset{p}{\bigwedge}E$-ben, amivel a c) állítást is igazoltuk. ■

21.11.6. Tétel. *Legyen E vektortér a K test felett és $p\in\mathbb{N}^*$ olyan, hogy $p<\mathrm{Char}(K)$ vagy $\mathrm{Char}(K)=0$.*

a) *Létezik olyan (A,a) pár, hogy A vektortér a K test felett, és $a:E^p\to A$ olyan antiszimmetrikus multilineáris operátor, amelyre teljesül a következő állítás.*

(TA) *Minden K feletti F vektortérhez, és minden $u:E^p\to F$ antiszimmetrikus multilineáris operátorhoz létezik egyetlen olyan $\widetilde{u}:A\to F$ lineáris operátor, amelyre*

$\widetilde{u} \circ a = u$, vagyis a következő diagram kommutatív:

$$\begin{tikzcd} E^p \arrow[r, "a"] \arrow[dr, "u"'] & A \arrow[d, "\tilde{u}"] \\ & F \end{tikzcd}$$

b) *Ha (A', a') szintén olyan pár, hogy A' vektortér a K test felett, és $a' : E^p \to A$ olyan antiszimmetrikus multilineáris operátor, hogy minden F vektortérhez és minden $u : E^p \to F$ antiszimmetrikus multilineáris operátorhoz létezik egyetlen olyan $\widetilde{u} : A \to F$ lineáris operátor, hogy $\widetilde{u} \circ a' = u$, akkor létezik egyetlen olyan $v : A \to A'$ lineáris bijekció, amelyre $v \circ a = a'$.*

Bizonyítás. Az előző állítás szerint az $(A, a) := \left(\overset{p}{\bigowedge} E, a_p\right)$ pár eleget tesz a (TA) feltételnek, tehát a) teljesül.

Legyen (A, a) olyan pár, amelyre (TA) teljesül, és legyen (A', a') olyan pár, amely rendelkezik a b) állításban megfogalmazott tulajdonságokkal. Ekkor A' vektortér K felett és $a' : E^p \to A'$ antiszimmetrikus multilineáris operátor, így egyértelműen létezik olyan $v : A \to A'$ lineáris operátor, hogy $v \circ a = a'$. Felcseréve az (A, a) és (A', a') párok szerepét, hasonló érveléssel kapjuk, hogy egyértelműen létezik olyan $v' : A' \to A$ lineáris operátor, amelyre $v' \circ a' = a$. Mivel A vektortér K felett, és $a : E^p \to A$ szimmetrikus multilineáris operátor, így (TA) alapján egyértelműen létezik olyan $w : A \to A$ lineáris operátor, amelyre $w \circ a = a$. Világos, hogy az egyértelműségi feltételből $w = \mathrm{id}_A$ következik, hiszen $\mathrm{id}_A : A \to A$ nyilvánvalóan olyan lineáris operátor, hogy $\mathrm{id}_A \circ a = a$. Ugyanakkor $v' \circ v : A \to A$ is olyan lineáris operátor, hogy $(v' \circ v) \circ a = v' \circ (v \circ a) = v' \circ a' = a$, így az egyértelműség miatt $v' \circ v = \mathrm{id}_A$. Felcserélve az (A, a) és (A', a') párok szerepét, teljesen hasonlóan kapjuk, hogy $v \circ v' = \mathrm{id}_{A'}$. Ez azt jelenti, hogy $v : A \to A'$ lineáris bijekció és $v \circ a = a'$. A v operátor egyértelműsége még a $\{w \in \mathbf{L}(A; A') | w \circ a = a'\}$ operátorhalmazban is teljesül. ■

21.11.7. Állítás. *Legyenek E és F vektorterek, valamint $p \in \mathbb{N}^*$. Ha $u : E \to F$ lineáris operátor, akkor létezik egyetlen olyan*

$$\overset{p}{\bigowedge} u : \overset{p}{\bigowedge} E \to \overset{p}{\bigowedge} F$$

lineáris operátor, amelyre minden $(x_i)_{i \in p} \in E^p$ esetén

$$\left(\overset{p}{\bigowedge} u\right)\left(\bigowedge_{i \in p} x_i\right) = \bigowedge_{i \in p} u(x_i).$$

Továbbá, fennáll az $\overset{p}{\bigowedge} \mathrm{id}_E = \mathrm{id}_{\overset{p}{\bigowedge} E}$ egyenlőség.

Bizonyítás. A $\overset{p}{\bigowedge} u$ lineáris operátor egyértelműsége nyilvánvalóan következik abból, hogy $\left\{ \bigowedge_{i \in p} x_i \;\middle|\; (x_i)_{i \in p} \in E^p \right\}$ generátorhalmaz a $\overset{p}{\bigowedge} E$ vektortérben. A $\overset{p}{\bigowedge} u$ lineáris operátor létezésének bizonyításához először megjegyezzük, hogy 19.7.6. szerint u-hoz egyértelműen létezik olyan $\widetilde{u} : \mathbf{T}^p(E) \to \mathbf{T}^p(F)$ lineáris operátor, amelyre minden

$(x_i)_{i\in p} \in E^p$ esetén $\widetilde{u}\Big(\bigotimes_{i\in p} x_i\Big) = \bigotimes_{i\in p} u(x_i)$. Ekkor a definíció szerint minden $(x_i)_{i\in p} \in E^p$ esetén

$$\widetilde{u}\Big(\bigwedge_{i\in p} x_i\Big) = \widetilde{u}\Big(\sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) \bigotimes_{i\in p} x_{\sigma(i)}\Big) = \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma)\widetilde{u}\Big(\bigotimes_{i\in p} x_{\sigma(i)}\Big) =$$
$$= \sum_{\sigma\in\mathfrak{S}_p} \varepsilon_p(\sigma) \bigotimes_{i\in p} u(x_{\sigma(i)}) = \bigwedge_{i\in p} u(x_i).$$

Ebből látható, hogy $\widetilde{u}\left\langle \overset{p}{\bigwedge} E\right\rangle \subseteq \overset{p}{\bigwedge} F$, következésképpen az $\widetilde{u}$ leképezés $\overset{p}{\bigwedge} E$-re vett leszűkítése olyan $\overset{p}{\bigwedge} E \to \overset{p}{\bigwedge} F$ lineáris operátor, amelynek a létezését állítottuk.
Ha $(x_i)_{i\in p} \in E^p$, akkor a definíció szerint

$$\Big(\overset{p}{\bigwedge}\mathrm{id}_E\Big)\Big(\bigwedge_{i\in p} x_i\Big) = \bigwedge_{i\in p} \mathrm{id}_E(x_i) = \bigwedge_{i\in p} x_i,$$

tehát a $\overset{p}{\bigwedge}\mathrm{id}_E$ és $\mathrm{id}_{\overset{p}{\bigwedge} E}$ lineáris operátorok megegyeznek a $\Big\{ \bigwedge_{i\in p} x_i \;\Big|\; (x_i)_{i\in p} \in E^p\Big\}$ generátorhalmazon, ezért ezek az operátorok egyenlőek. ■

21.11.8. Állítás. *Legyenek E, F és G vektorterek, valamint $p \in \mathbb{N}^*$. Ha $u : E \to F$ és $v : F \to G$ lineáris operátorok, akkor*

$$\overset{p}{\bigwedge}(v\circ u) = \Big(\overset{p}{\bigwedge} v\Big)\circ\Big(\overset{p}{\bigwedge} u\Big).$$

Bizonyítás. A $v \circ u : E \to G$ lineáris operátorra teljesül az, hogy minden $(x_i)_{i\in p} \in E^p$ esetén

$$\Big(\overset{p}{\bigwedge}(v\circ u)\Big)\Big(\bigwedge_{i\in p} x_i\Big) = \bigwedge_{i\in p}(v\circ u)(x_i) = \bigwedge_{i\in p} v(u(x_i)) = \Big(\overset{p}{\bigwedge} v\Big)\Big(\bigwedge_{i\in p} u(x_i)\Big) =$$
$$= \Big(\overset{p}{\bigwedge} v\Big)\Big(\Big(\overset{p}{\bigwedge} u\Big)((x_i)_{i\in p})\Big) = \Big(\Big(\overset{p}{\bigwedge} v\Big)\circ\Big(\overset{p}{\bigwedge} u\Big)\Big)((x_i)_{i\in p}),$$

ami az előző állításban szereplő egyértelműségi tulajdonság alapján az operátoregyenlőséget bizonyítja. ■

21.11.9. Következmény. *Legyenek E és F vektorterek, valamint $p \in \mathbb{N}^*$. Ha az $u : E \to F$ lineáris operátor injektív (illetve szürjektív), akkor az*

$$\overset{p}{\bigwedge} u : \overset{p}{\bigwedge} E \to \overset{p}{\bigwedge} F$$

lineáris operátor is injektív (illetve szürjektív). Ha $u : E \to F$ lineáris izomorfizmus az E és F vektorterek között, akkor $\overset{p}{\bigwedge} u$ lineáris izomorfizmus a $\overset{p}{\bigwedge} E$ és $\overset{p}{\bigwedge} F$ vektorterek között.

Bizonyítás. A második állítás nyilvánvalóan következik az elsőből.
Tegyük fel, hogy az $u : E \to F$ lineáris operátor injektív. Ekkor 17.7.5. szerint létezik

u-nak lineáris balinverze, vagyis olyan $v : F \to E$ lineáris operátor, hogy $v \circ u = \mathrm{id}_E$. Ekkor 21.11.7. és 21.11.8. szerint

$$\left(\bigwedge^p v\right) \circ \left(\bigwedge^p u\right) = \bigwedge^p (v \circ u) = \bigwedge^p \mathrm{id}_E = \mathrm{id}_{\bigwedge^p E},$$

tehát a $\bigwedge^p v : \bigwedge^n F \to \bigwedge^p E$ leképezés balinverze az $\bigwedge^p u$ leképezésnek, így $\bigwedge^p u : \bigwedge^p E \to \bigwedge^p F$ injekció.

Tegyük fel, hogy az $u : E \to F$ lineáris operátor szürjektív. Ekkor 17.4.7. szerint létezik u-nak lineáris jobbinverze, vagyis olyan $w : F \to E$ lineáris operátor, hogy $u \circ w = \mathrm{id}_F$. Ekkor 21.11.7. és 21.11.8. szerint

$$\left(\bigwedge^p u\right) \circ \left(\bigwedge^p w\right) = \bigwedge^p (u \circ w) = \bigwedge^p \mathrm{id}_F = \mathrm{id}_{\bigwedge^p F},$$

tehát a $\bigwedge^p w : \bigwedge^p F \to \bigwedge^p E$ leképezés jobbinverze az $\bigwedge^p u$ leképezésnek, így $\bigwedge^p u : \bigwedge^p E \to \bigwedge^p F$ szürjekció. ■

21.12. Clifford-algebrák

21.13. Algebrák ábrázolásai

22. fejezet

Hálók és ortohálók

22.1. Hálóműveletek és hálószerű rendezések

22.1.1. Definíció. *Azt mondjuk, hogy az L halmaz feletti $\leq$ rendezés* **hálószerű**, *ha L minden nem üres véges részhalmazának létezik szuprémuma és infimuma L-ben $\leq$ szerint.*

22.1.2. Állítás. *Legyen L halmaz.*
a) *Ha $\leq$ hálószerű rendezés L felett, akkor az*

$$L \times L \to L; \quad (e, f) \mapsto e \vee f := \sup\{e, f\},$$
$$L \times L \to L; \quad (e, f) \mapsto e \wedge f := \inf\{e, f\}$$

leképezések olyan kommutatív, asszociatív és idempotens műveletek, amelyek kölcsönösen elnyelőek egymásra nézve, és amelyekre teljesül az, hogy minden $e, f \in L$ esetén

$$e \leq f \Leftrightarrow e = e \wedge f \Leftrightarrow f = e \vee f.$$

b) *Ha $\vee$ és $\wedge$ olyan kommutatív, asszociatív és idempotens műveletek, amelyek kölcsönösen elnyelőek egymásra nézve, akkor minden $e, f \in L$ esetén*

$$e = e \wedge f \Leftrightarrow f = e \vee f,$$

és az L halmaz feletti

$$\leq \ := \ \{(e, f) \in L \times L \mid e = e \wedge f\}$$

reláció olyan hálószerű rendezés L felett, amelyre minden $e, f \in L$ esetén

$$\sup\{e, f\} = e \vee f,$$
$$\inf\{e, f\} = e \wedge f.$$

Bizonyítás. ■

22.1.3. Definíció. *Az L rendezett halmazt* **hálónak** *nevezzük, ha az L feletti rendezés hálószerű.*

A továbbiakban egy L rendezett halmazt *korlátosnak* nevezünk, ha létezik L-nek legnagyobb és legkisebb eleme. Korlátos rendezett halmaz legnagyobb (illetve legkisebb) elemét az **1** (illetve **0**) szimbólummal jelöljük, ha ez a jelölés nem vezet félreértésre.

22.2. Részhálók, ideálok és faktorhálók

22.2.1. Definíció. *Az L háló* **részhálójának** *nevezünk minden olyan $M \subseteq L$ halmazt, amelyre teljesül az, hogy minden $e, f \in M$ esetén $e \vee f \in M$ és $e \wedge f \in M$.*

Nyilvánvaló, hogy ha M részhálója az L hálónak, akkor M az L rendezésének M-re vett megszorításával ellátva olyan háló, amelyben minden nem üres véges rendszer szuprémuma (illetve infimuma) megegyezik ugyanezen rendszer L-ben vett szuprémumával (illetve infimumával).

22.2.2. Állítás. *Legyen L háló és $\mathfrak{p} \subseteq L$ nem üres halmaz. A következő állítások ekvivalensek.*

(i) *Minden $e, f \in \mathfrak{p}$ esetén $e \vee f \in \mathfrak{p}$, valamint minden $e \in \mathfrak{p}$ és $f \in L$ esetén $e \wedge f \in \mathfrak{p}$.*

(ii) *Minden $e, f \in \mathfrak{p}$ esetén $e \vee f \in \mathfrak{p}$, valamint minden $e \in \mathfrak{p}$ és $f \in L$ esetén, ha $f \leq e$, akkor $f \in \mathfrak{p}$.*

(iii) *Minden $e, f \in L$ esetén*

$$e \vee f \in \mathfrak{p} \quad \Leftrightarrow \quad (e \in \mathfrak{p}) \wedge (f \in \mathfrak{p}).$$

Bizonyítás. (i)⇒(ii) Ha $e \in \mathfrak{p}$ és $f \in L$, akkor (i) alapján $f \wedge e \in \mathfrak{p}$, tehát ha $f \leq e$, akkor $f = f \wedge e$ miatt $f \in \mathfrak{p}$, vagyis (ii) teljesül.

(ii)⇒(iii) Ha $e, f \in L$ és $e \vee f \in \mathfrak{p}$, akkor (ii) és $e, f \leq e \vee f$ alapján $e \in \mathfrak{p}$ és $f \in \mathfrak{p}$. Megfordítva, ha $e, f \in L$ és $e \in \mathfrak{p}$ és $f \in \mathfrak{p}$, akkor (ii) szerint $e \vee f \in \mathfrak{p}$. Ezért (ii)⇒(iii) teljesül.

(iii)⇒(i) Ha $e, f \in \mathfrak{p}$, akkor (iii) alapján $e \vee f \in \mathfrak{p}$. Továbbá, ha $e \in \mathfrak{p}$ és $f \in L$, akkor $e \vee (e \wedge f) = e \in \mathfrak{p}$ és (iii) alapján $e \wedge f \in \mathfrak{p}$. Ezért (iii)⇒(i) teljesül. ■

22.2.3. Definíció. *Az L hálóban* **ideálnak** *nevezünk minden olyan $\mathfrak{p} \subseteq L$ nem üres halmazt, amelyre teljesülnek az előző állításban megfogalmazott* (i), (ii) *és* (iii) *tulajdonságok. Az L háló $\mathfrak{p}$ ideálját* **valódinak** *nevezzük, ha $\mathfrak{p} \neq L$.*

Triviális, hogy alulról korátos hálóban minden ideálnak eleme a háló legkisebb eleme. Továbbá, felülről korlátos hálóban egy ideál akkor és csak akkor **valódi** (vagyis alaphalmaztól különböző), ha nem eleme a háló legnagyobb eleme.

Ha L háló és $e \in L$, akkor a $\mathfrak{p} :=] \leftarrow, e]$ intervallum nyilvánvalóan olyan ideál L-ben, amelyre $e \in \mathfrak{p}$: ezt az ideált nevezzük az e elem által generált **főideálnak**.

A definíció szerint nyilvánvaló, hogy háló ideáljai nem üres rendszerének a metszete pontosan akkor ideál, ha a metszet nem üres. Ha $(e_i)_{i \in I}$ olyan nem üres rendszer az L hálóban, amely nem korlátos alulról, akkor $\bigcap\limits_{i \in I}] \leftarrow, e_i] = \emptyset$, tehát ez a metszet nem ideál.

22.2.4. Állítás. *Legyen L háló és $H \subseteq L$ nem üres halmaz. Jelölje $\mathfrak{p}$ azon $e \in L$ elemek halmazát, amelyekhez létezik olyan H-ban haladó $(h_i)_{i \in I}$ nem üres véges rendszer, hogy $e \leq \bigvee\limits_{i \in I} h_i$. Ekkor $\mathfrak{p}$ ideál L-ben, és $H \subseteq \mathfrak{p}$, és $\mathfrak{p}$ az ilyen tulajdonságú ideálok között tartalmazás tekintetében a legkisebb.*

Bizonyítás. Nyilvánvaló, hogy $H \subseteq \mathfrak{p}$, ezért $H \neq \emptyset$ miatt $\mathfrak{p} \neq \emptyset$.

Ha $e \in \mathfrak{p}$ és $f \in L$, akkor van olyan H-ban haladó $(h_i)_{i \in I}$ nem üres véges rendszer, hogy

$e \leq \bigvee_{i \in I} h_i$, ezért $e \wedge f \leq e$ miatt $e \wedge f \leq \bigvee_{i \in I} h_i$ is teljesül, tehát $e \wedge f \in \mathfrak{p}$.

Legyenek $e, f \in \mathfrak{p}$ tetszőlegesek, és vegyünk olyan H-ban haladó $(h_i)_{i \in I}$ és $(g_j)_{j \in J}$ nem üres véges rendszereket, amelyekre $e \leq \bigvee_{i \in I} h_i$ és $f \leq \bigvee_{j \in J} g_j$. Legyen $(p_\alpha)_{\alpha \in I \bigsqcup J}$ az a rendszer, amelyre minden $\alpha \in I \bigsqcup J = (\{0\} \times I) \cup (\{1\} \times J)$ esetén

– ha $i \in I$ és $\alpha = (0, i)$, akkor $p_\alpha := h_i$;

– ha $j \in J$ és $\alpha = (1, j)$, akkor $p_\alpha := g_j$.

Ekkor $(p_\alpha)_{\alpha \in I \bigsqcup J}$ olyan H-ban haladó nem üres véges rendszer, hogy

$$\bigvee_{\alpha \in I \bigsqcup J} p_\alpha = \Big(\bigvee_{\alpha \in \{0\} \times I} p_\alpha \Big) \vee \Big(\bigvee_{\alpha \in \{1\} \times J} p_\alpha \Big) = \Big(\bigvee_{i \in I} p_{(0,i)} \Big) \vee \Big(\bigvee_{j \in J} p_{(1,j)} \Big) = \Big(\bigvee_{i \in I} h_i \Big) \vee \Big(\bigvee_{j \in J} g_j \Big),$$

tehát $e \vee f \leq \bigvee_{\alpha \in I \bigsqcup J} p_\alpha$, így $e \vee f \in \mathfrak{p}$ is teljesül. Ezzel megmutattuk, hogy $\mathfrak{p}$ olyan ideál L-ben, amelyre $H \subseteq \mathfrak{p}$.

Legyen $\mathfrak{q}$ olyan ideál L-ben, amelyre $H \subseteq \mathfrak{q}$. Legyen $e \in \mathfrak{p}$, és vegyünk olyan H-ban haladó $(h_i)_{i \in I}$ nem üres véges rendszert, hogy $e \leq \bigvee_{i \in I} h_i$. Minden $i \in I$ esetén $h_i \in H \subseteq \mathfrak{q}$, ezért $\bigvee_{i \in I} h_i \in \mathfrak{q}$, amiből azonnal következik, hogy $e \in \mathfrak{q}$. Ez azt jelenti, hogy $\mathfrak{p} \subseteq \mathfrak{q}$. ■

22.2.5. Következmény. *Ha L háló, $e \in L$ és $\mathfrak{p} \subseteq L$ ideál, akkor a*

$$\mathfrak{q} := \{ f \in L \mid (\exists p \in \mathfrak{p}) : f \leq e \vee p \}$$

halmaz a legkisebb olyan ideál L-ben, amelyre $\{e\} \cup \mathfrak{p} \subseteq \mathfrak{q}$.

Bizonyítás. Mivel $\mathfrak{p}$ zárt a véges szuprémum-képzésre nézve, így $f \in L$ esetén a $\mathfrak{q}$ halmaz definíciójában szereplő "$(\exists p \in \mathfrak{p}) : f \leq e \vee p\}$" kijelentés ekvivalens azzal, hogy létezik olyan $\{e\} \cup \mathfrak{p}$-ben haladó $(p_i)_{i \in I}$ nem üres véges rendszer, hogy $e \leq \bigvee_{i \in I} p_i$. Ezután alkalmazhatjuk az előző állítást. ■

22.2.6. Definíció. *Az L hálóban* **szűrőnek** *nevezünk minden olyan $\mathfrak{f} \subseteq L$ nem üres halmazt, amelyre teljesülnek a következők*

– *minden $e \in \mathfrak{f}$ és $f \in L$ esetén, ha $e \vee f \in \mathfrak{f}$;*

– *minden $e, f \in \mathfrak{f}$ esetén $e \wedge f \in \mathfrak{f}$.*

22.3. Disztributív hálók és moduláris hálók

Ha L háló, akkor $e, f, g \in L$ esetén $e \leq e \vee f$ és $e \leq e \vee g$ miatt $e \leq (e \vee f) \wedge (e \vee g)$, továbbá $f \wedge g \leq f \leq e \vee f$ és $f \wedge g \leq g \leq e \vee g$ miatt $f \wedge g \leq (e \vee f) \wedge (e \vee g)$, amiből következik, hogy

$$e \vee (f \wedge g) \leq (e \vee f) \wedge (e \vee g).$$

Hasonlóan látható, hogy minden $e, f, g \in L$ esetén

$$e \wedge (f \vee g) \geq (e \wedge f) \vee (e \wedge g).$$

Azonban egyik egyenlőtlenség megfordítása sem teljesül általában. Ezen egyenlőtlenségek megfordításainak kapcsolatáról szól a következő állítás.

22.3.1. Állítás. *Ha L háló, akkor a következő állítások ekvivalensek.*

(i) *Minden $a, b, c \in L$ esetén*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$

vagyis a $\vee$ művelet disztibutív a $\wedge$ műveletre nézve.

(ii) *Minden $a, b, c \in L$ esetén*

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$

vagyis a $\wedge$ művelet disztibutív a $\vee$ műveletre nézve.

(iii) *Minden $e, f, g \in L$ esetén*

$$e \vee (f \wedge g) = (e \vee f) \wedge (e \vee g),$$
$$e \wedge (f \vee g) = (e \wedge f) \vee (e \wedge g),$$

vagyis a $\vee$ és $\wedge$ műveletek mindketten disztributívak a másikra nézve.

Bizonyítás. Világos, hogy (iii)-ból (i) is és (ii) is következik, ezért elég azt igazolni, hogy (i)$\Rightarrow$(iii) *és* (ii)$\Rightarrow$(iii) is igaz.

(i)$\Rightarrow$(iii) Legyenek $e, f, g \in L$. Ekkor

$$(e \wedge f) \vee (e \wedge g) \overset{(1)}{=} ((e \wedge f) \vee e) \wedge ((e \wedge f) \vee g) \overset{(2)}{=} e \wedge ((e \wedge f) \vee g) \overset{(3)}{=}$$
$$\overset{(3)}{=} e \wedge ((e \vee g) \wedge (f \vee g)) \overset{(4)}{=} (e \wedge (e \vee g)) \wedge (f \vee g) \overset{(5)}{=} e \wedge (f \vee g),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél (i)-t alkalmaztuk az $a := e \wedge f$, $b := e$ és $c := g$ választással;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk, hogy $(e \wedge f) \vee e = e$, mert a $\vee$ művelet elnyelő $\wedge$-ra nézve;

– a $\overset{(3)}{=}$ egyenlőségnél ismét (i)-t alkalmaztuk az $a := g$, $b := e$ és $c := f$ választással;

– a $\overset{(4)}{=}$ egyenlőségnél kihasználtuk a $\wedge$ művelet asszociativitását, végül:

– az $\overset{(5)}{=}$ egyenlőségnél az $e \wedge (e \vee g) = e$ egyenlőségre hivatkoztunk, mivel a $\wedge$ művelet elnyelő a $\vee$ műveletre nézve.

(ii)$\Rightarrow$(iii) Legyenek $e, f, g \in L$. Ekkor

$$(e \vee f) \wedge (e \vee g) \overset{(1)}{=} ((e \vee f) \wedge e) \wedge ((e \vee f) \wedge g) \overset{(2)}{=} e \vee ((e \vee f) \wedge g) \overset{(3)}{=}$$
$$\overset{(3)}{=} e \vee ((e \wedge g) \vee (f \wedge g)) \overset{(4)}{=} (e \vee (e \wedge g)) \vee (f \wedge g) \overset{(5)}{=} e \vee (f \wedge g),$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél (ii)-t alkalmaztuk az $a := e \vee f$, $b := e$ és $c := g$ választással;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk, hogy $(e \vee f) \wedge e = e$, mert a $\wedge$ művelet elnyelő $\vee$-ra nézve;

– a $\overset{(3)}{=}$ egyenlőségnél ismét (ii)-t alkalmaztuk az $a := g$, $b := e$ és $c := f$ választással;

– a $\overset{(4)}{=}$ egyenlőségnél kihasználtuk a $\vee$ művelet asszociativitását, végül:

– az $\overset{(5)}{=}$ egyenlőségnél az $e \vee (e \wedge g) = e$ egyenlőségre hivatkoztunk, mivel a $\vee$ művelet elnyelő a $\wedge$ műveletre nézve. ■

22.3.2. Definíció. *Azt mondjuk, hogy az L háló* **disztributív**, *ha L-ben a $\vee$ és $\wedge$ műveletek mindketten disztributívak a másikra nézve.*

Világos, hogy a 22.3.1. állításnak az az értéke, hogy e szerint egy háló disztributivitásának bizonyításához *elegendő* az (i) *vagy* (ii) állítások valamelyikét igazolni.

Példa. Legyen E halmaz és $L \subseteq \mathscr{P}(E)$ olyan halmaz, hogy minden $X, Y \in L$ esetén $X \cap Y \in L$ és $X \cup Y \in L$. Nyilvánvaló, hogy ekkor az L halmaz feletti tartalmazás reláció olyan rendezés, amelyre minden $X, Y \in L$ esetén

$$X \wedge Y = X \cap Y, \quad X \vee Y = X \cup Y,$$

következésképpen minden $X, Y, Z \in L$ esetén

$$X \vee (Y \wedge Z) = X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) = (X \vee Y) \wedge (X \vee Z),$$

ezért 22.3.1. alapján L disztributív háló.

22.3.3. Definíció. *Ha L háló, akkor azt mondjuk, hogy $(e, f) \in L \times L$* **moduláris pár**, *ha minden $g \in L$, $g \leq f$ esetén $g \vee (e \wedge f) = (g \vee e) \wedge f$. Az L hálót* **modulárisnak** *nevezzük, ha minden L-beli elempár moduláris.*

Ha L disztributív háló, és $e, f, g \in L$ olyanok, hogy $g \leq f$, akkor $g \vee f = f$ miatt $g \vee (e \wedge f) = (g \vee e) \wedge (g \vee f) = (g \vee e) \wedge f$, tehát (e, f) moduláris pár. Ez azt jelenti, hogy minden disztributív háló moduláris, vagyis a modularitás a disztributivitás gyengítése. Azonban a következő példa mutatja, hogy létezik nem disztributív moduláris háló.

22.3.4. Állítás. *Ha E vektortér a K test felett, akkor az E lineáris altereinek halmaza a $\subseteq$ relációval ellátva moduláris háló, és ha E legalább kétdimenziós, akkor ez nem disztributív háló.*

Bizonyítás. Nyilvánvaló, hogy ha X és Y lineáris alterei E-nek, akkor $X \wedge Y = X \cap Y$ a $\subseteq$ rendezés szerint, mert $X \cap Y$ a tartalmazás tekintetében legnagyobb lineáris altere E-nek, amely részhalmaza X-nek és Y-nak (sőt ez a tartalmazás tekintetében legnagyobb *halmaz*, amely részhalmaza X-nek és Y-nak). De az X és Y lineáris alterek szuprémuma általában nem egyenlő $X \cup Y$-nal, mert lehetséges az, hogy $X \cup Y$ nem lineáris altér (ti. nem zárt az összeadásra nézve). Azonban létezik tartalmazás tekintetében legkisebb lineáris altér E-ben, amely tartalmazza X-t és Y-t, éspedig az $X + Y$ halmaz. Tehát az E vektortér bármely két X és Y lineáris alterére

$$X \wedge Y = X \cap Y, \quad X \vee Y = X + Y.$$

Ebből már látható, hogy ha E legalább két dimenziós, akkor a lineáris altereinek hálója nem disztributív. Legyenek ugyanis $y, z \in E$ lineárisan független vektorok, és $x := y + z$. Ekkor az $X := K.x$, $Y := K.y$ és $Z := K.z$ egy dimenziós lineáris alterekre könnyen ellenőrizhező, hogy $X \cap Y = \{0\}$, $X \cap Z = \{0\}$, ugyanakkor $X \subseteq Y + Z$, ezért

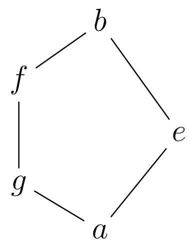
$$X \wedge (Y \vee Z) = X \cap (Y + Z) = X \neq \{0\} = (X \cap Y) + (X \cap Z) = (X \wedge Y) \vee (X \wedge Z).$$

Ugyanakkor az E vektortér lineáris altereinek hálója moduláris. Legyenek ugyanis X, Y és Z olyan lineáris alterei E-nek, hogy $Z \subseteq Y$. Legyen $y \in (Z+X) \cap Y$ tetszőleges. Ekkor van olyan $z \in Z$ és $x \in X$, hogy $y = z + x$. Mivel $z \in Z \subseteq Y$, így $x = y - z \in Y - Y \subseteq Y$, vagyis $y \in Z + (X \cap Y)$. Ez azt jelenti, hogy $(Z + X) \cap Y \subseteq Z + (X \cap Y)$, ugyanakkor a $Z + (X \cap Y) \subseteq (Z + X) \cap Y$ tartalmazás $Z \subseteq Y$ miatt nyilvánvalóan igaz, tehát

$$Z \vee (X \wedge Y) = Z + (X \cap Y) = (Z + X) \cap Y = (Z \vee X) \wedge Y,$$

vagyis (X, Y) moduláris pár. ■

Nem moduláris hálóra példát ad a következő Hasse-diagram:



Ez valóban nem moduláris, mert $e \wedge f = a$ és $g \vee e = b$, következésképpen

$$g \vee (e \wedge f) = g \vee a = g < f = b \wedge f = (g \vee e) \wedge f,$$

tehát (e, f) nem moduláris pár. Ezt a nem moduláris hálót az N_5 szimbólummal jelöljük.

Világos, hogy moduláris háló minden részhálója moduláris, továbbá izomorf hálók egyszerre modulárisak vagy nem modulárisak. Ezért moduláris hálónak nem létezik olyan részhálója, amely izomorf N_5-tel. Ennek megfordítása is igaz.

22.3.5. Tétel. (**Moduláris hálók jellemzése részhálókkal – Dedekind-tétel**) *Háló pontosan akkor moduláris, ha nincs* N_5*-tel izomorf részhálója.*

Bizonyítás. Tegyük fel, hogy L nem moduláris háló. Megmutatjuk, hogy L-nek létezik N_5-tel izomorf részhálója.

Legyen $(e, f) \in L \times L$ nem moduláris pár, és vegyünk olyan $g \in L$ elemet, amelyre $g \leq f$ és $g \vee (e \wedge f) < (g \vee e) \wedge f$. Természetesen ekkor $g < f$, mert $g = f$ esetén a $\wedge$ és $\vee$ műveletek elnyelési tulajdonsága miatt $g \vee (e \wedge f) = g = (g \vee e) \wedge f$ teljesülne. Legyenek

$$g' := g \vee (e \wedge f), \quad f' := (g \vee e) \wedge f,$$

tehát $g' < f'$.

Megmutatjuk, hogy e nem hasonlítható össze sem g'-vel, sem f'-vel.

– Ha $e \leq g'$ teljesülne, akkor

$$g' = e \vee g' = e \vee (g \vee (e \wedge f)) = (e \vee (e \wedge f)) \vee g = e \vee g \geq (g \vee e) \wedge f = f',$$

tehát $g' \geq f'$ lenne, holott $g' < f'$. Ezért $e \not\leq g'$.

– Ha $g' \leq e$ teljesülne, akkor $g \leq g \vee (e \wedge f) = g' \leq e$, tehát $g \leq e$, így $g \vee e = e$, következésképpen

$$f' = (g \vee e) \wedge f = e \wedge f \leq g \vee (e \wedge f) = g',$$

tehát $f' \leq g'$ lenne, holott $g' < f'$. Ezért $g' \not\leq e$.

– Ha $e \leq f'$ teljesülne, akkor $e \leq f' = (g \vee e) \wedge f \leq f$, tehát $e \leq f$, így $e \wedge f = e$, következésképpen

$$g' = g \vee (e \wedge f) = g \vee e \geq (g \vee e) \wedge f = f',$$

tehát $g' \geq f'$ lenne, holott $g' < f'$. Ezért $e \nleq f'$.

– Ha $f' \leq e$ teljesülne, akkor

$$f' = f' \wedge e = ((g \vee e) \wedge f) \wedge e = ((g \vee e) \wedge e) \wedge f = e \wedge f \leq g \vee (e \wedge f) = g',$$

tehát $f' \leq g'$ lenne, holott $g' < f'$. Ezért $f' \nleq e$.

Tehát $e, f', g' \in L$ olyan elemek, amelyekre $g' < f'$ és e nem hasonlítható össze sem g'-vel, sem f'-vel.

Megmutatjuk, hogy $e \wedge g' = e \wedge f'$. Valóban, $g' \leq f'$ miatt $e \wedge g' \leq e \wedge f'$, másfelől

$$e \wedge f' = e \wedge ((g \vee e) \wedge f) = (e \wedge (e \vee g)) \wedge f = e \wedge f \leq g \vee (e \wedge f) = g',$$

tehát $e \wedge f' \leq g'$, és természetesen $e \wedge f' \leq e$, ezért $e \wedge f' \leq e \wedge g'$.

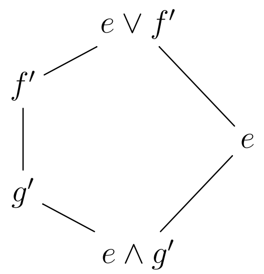
Megmutatjuk, hogy $e \vee g' = e \vee f'$. Valóban, $g' \leq f'$ miatt $e \vee g' \leq e \vee f'$, másfelől

$$e \vee g' = e \vee (g \vee (e \wedge f)) = g \vee (e \vee (e \wedge f)) = g \vee e \geq (g \vee e) \wedge f = f',$$

tehát $e \vee g' \geq f'$, és természetesen $e \vee g' \geq e$, ezért $e \vee g' \geq e \vee f'$.

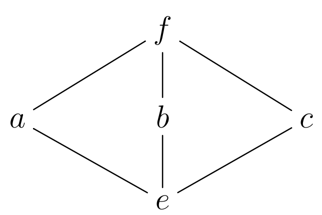
Végül, $f' < e \vee f'$ és $e < e \vee f'$, különben e és f' összehasonlíthatóak volnának, valamint $e \wedge g' < g'$ és $e \wedge g' < e$, különben e és g' összehasonlíthatóak volnának.

Ez azt jelenti, hogy az $\{e, f', g', e \wedge g', e \vee f'\}$ halmaz olyan részhálója L-nek amelynek rendezési viszonyait a következő Hasse-diagram mutatja:



vagyis ez a részháló izomorf N_5-tel. ■

Nem disztributív hálóra példát ad a következő Hasse-diagram:



Ez valóban nem disztributív, mert ebben $a \wedge c = e$, $b \vee a = f = b \vee c$, tehát

$$b \vee (a \wedge c) = b \vee e = b < f = f \wedge f = (b \vee a) \wedge (b \vee c).$$

Ezt a nem disztributív hálót az M_5 szimbólummal jelöljük. A Dedekind-tétel alapján ez a háló moduláris.

Világos, hogy disztributív háló minden részhálója disztributív, továbbá izomorf hálók egyszerre disztributívak vagy nem disztributívak. Ezért disztributív hálónak nem létezik olyan részhálója, amely izomorf M_5-tel. Azonban könnyen látható, hogy N_5 olyan nem disztributív (sőt nem is moduláris) háló, amelynek nincs M_5-tel izomorf részhálója. Tehát minden mellékfeltétel nélkül nem igaz, hogy egy háló pontosan akkor disztributív, ha nincs M_5-tel izomorf részhálója. Azonban a következő tétel szerint a modularitás mellékfeltételt kikötve az állítás igaz lesz. Ennek bizonyítását egy lemmával készítjük elő.

22.3.6. Lemma. *Ha L moduláris háló és $a, b, c \in L$, akkor a következő állítások ekvivalensek:*

(i) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

(ii) $c \vee (a \wedge b) = (c \vee a) \wedge (c \vee b)$.

(iii) $b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c)$.

(iv) $a \vee (c \wedge b) = (a \vee c) \wedge (a \vee b)$.

(v) $c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b)$.

(vi) $b \vee (a \wedge c) = (b \vee a) \wedge (b \vee c)$.

Bizonyítás. (i)$\Rightarrow$(ii) Mivel $c \leq c \vee b$ és $(a, c \vee b)$ moduláris pár, így

$$c \vee (a \wedge (c \vee b)) = (c \vee a) \wedge (c \vee b),$$

ugyanakkor (i) és $c \vee (a \wedge c) = c$ alkalmazásával

$$c \vee (a \wedge (c \vee b)) = c \vee ((a \wedge b) \vee (a \wedge c)) = (c \vee (a \wedge c)) \vee (a \wedge b) = c \vee (a \wedge b).$$

(ii)$\Rightarrow$(iii) Mivel $b \wedge a \leq b$ és (c, b) moduláris pár, így

$$(b \wedge a) \vee (c \wedge b) = ((b \wedge a) \vee c) \wedge b,$$

ugyanakkor (ii) és $(c \vee b) \wedge b = b$ alkalmazásával

$$((b \wedge a) \vee c) \wedge b = ((c \vee a) \wedge (c \vee b)) \wedge b = (c \vee a) \wedge ((c \vee b) \wedge b) = (c \vee a) \wedge b.$$

(iii)$\Rightarrow$(iv) Mivel $a \leq a \vee c$ és $(b, a \vee c)$ moduláris pár, így

$$a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c),$$

ugyanakkor (iii) és $a \vee (b \wedge a) = a$ alkalmazásával

$$a \vee (b \wedge (a \vee c)) = a \vee ((b \wedge a) \vee (b \wedge c)) = (a \vee (b \wedge a)) \vee (b \wedge c) = a \vee (b \wedge c).$$

(iv)$\Rightarrow$(v) Mivel $c \wedge b \leq c$ és (a, c) moduláris pár, így

$$(c \wedge b) \vee (a \wedge c) = ((c \wedge b) \vee a) \wedge c,$$

ugyanakkor (iv) és $(a \vee c) \wedge c = c$ alkalmazásával

$$((c \wedge b) \vee a)) \wedge c = ((a \vee c) \wedge (a \vee b)) \wedge c = (a \vee b) \wedge ((a \vee c) \wedge c) = (a \vee b) \wedge c.$$

(v)$\Rightarrow$(vi) Mivel $b \leq b \vee a$ és $(c, b \vee a)$ moduáris pár, így

$$b \vee (c \wedge (b \vee a)) = (b \vee c) \wedge (b \vee a),$$

ugyanakkor (v) és $b \vee (c \wedge b) = b$ alkalmazásával

$$b \vee (c \wedge (b \vee a)) = b \vee ((c \wedge a) \vee (c \wedge b)) = (b \vee (c \wedge b)) \vee (c \wedge a) = b \vee (c \wedge a).$$

(vi)$\Rightarrow$(i) Mivel $a \wedge c \leq a$ és (b, a) moduláris pár, így

$$(a \wedge c) \vee (b \wedge a) = ((a \wedge c) \vee b) \wedge a,$$

ugyanakkor (vi) és $(b \vee a) \wedge a = a$ alkalmazásával

$$((a \wedge c) \vee b) \wedge a = ((b \vee a) \wedge (b \vee c)) \wedge a = ((b \vee a) \wedge a) \wedge (b \vee c) = a \wedge (b \vee c). \blacksquare$$

22.3.7. Lemma. *Ha L moduláris háló és $a, b, c \in L$, akkor a következő állítások ekvivalensek:*

(i) $a \wedge (b \vee c) > (a \wedge b) \vee (a \wedge c)$.

(ii) $c \vee (a \wedge b) < (c \vee a) \wedge (c \vee b)$.

(iii) $b \wedge (a \vee c) > (b \wedge a) \vee (b \wedge c)$.

(iv) $a \vee (c \wedge b) < (a \vee c) \wedge (a \vee b)$.

(v) $c \wedge (a \vee b) > (c \wedge a) \vee (c \wedge b)$.

(vi) $b \vee (a \wedge c) < (b \vee a) \wedge (b \vee c)$.

Bizonyítás. Nyilvánvalóan fennállnak az

$$a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c), \quad c \vee (a \wedge b) \leq (c \vee a) \wedge (c \vee b), \quad b \wedge (a \vee c) \geq (b \wedge a) \vee (b \wedge c),$$
$$a \vee (c \wedge b) \leq (a \vee c) \wedge (a \vee b), \quad c \wedge (a \vee b) \geq (c \wedge a) \vee (c \wedge b), \quad b \vee (a \wedge c) \leq (b \vee a) \wedge (b \vee c)$$

egyenlőtlenségek, ezért minden itt szereplő szigorú egyenlőtlenség az előző lemma ugyanolyan sorszámú egyenlőségének negációjával ekvivalens. ■

22.3.8. Tétel. (**Birkhoff-tétel**) *Moduláris háló pontosan akkor disztributív, ha nincs* M_5*-tel izomorf részhálója.*

Bizonyítás. Legyen L nem disztributív moduláris háló. Megmutatjuk, hogy L-nek létezik M_5-tel izomorf részhálója.

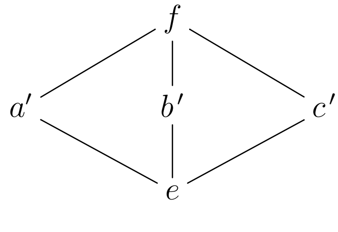
Az L háló nem disztributív, ezért rögzíthetünk olyan $a, b, c \in L$ elemeket, amelyekre

$$a \wedge (b \vee c) > (a \wedge b) \vee (a \wedge c).$$

Értelmezzük a következő elemeket:

$$e := (a \wedge b) \vee (b \wedge c) \vee (c \wedge a), \quad f := (a \vee b) \wedge (b \vee c) \wedge (c \vee a),$$
$$a' := e \vee (a \wedge f), \quad b' := e \vee (b \wedge f), \quad c' := e \vee (c \wedge f).$$

Bebizonyítjuk, hogy az $\{e, a', b', c', f\}$ halmaz olyan részhálója L-nek, amelynek rendezési viszonyait a következő Hasse-diagram mutatja:



tehát ez a részháló M_5-tel izomorf.

(I) Először megmutatjuk, hogy

$$e \leq a' \leq f; \quad e \leq b' \leq f; \quad e \leq c' \leq f.$$

Valóban, teljesülnek a következő egyenlőtlenségek:

$$a \wedge b \leq a \leq a \vee b, \quad a \wedge b \leq b \leq b \vee c, \quad a \wedge b \leq a \leq c \vee a,$$
$$b \wedge c \leq b \leq a \vee b, \quad b \wedge c \leq b \leq b \vee c, \quad b \wedge c \leq c \leq c \vee a,$$
$$c \wedge a \leq a \leq a \vee b, \quad c \wedge a \leq c \leq b \vee c, \quad c \wedge a \leq c \leq c \vee a,$$

tehát $a \wedge b,\ b \wedge c,\ c \wedge a \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$, amiből következik, hogy

$$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a),$$

vagyis $e \leq f$. Ebből azonnal következik, hogy

$$e \leq e \vee (a \wedge f) \leq f, \quad e \leq e \vee (b \wedge f) \leq f, \quad e \leq e \vee (c \wedge f) \leq f.$$

(II) A továbbiakban felhasználjuk a következő összefüggéseket, amelyek triválisan következnek a $\wedge$ és $\vee$ műveletek elnyelőségéből és a definíciókból:

$$\begin{aligned} a \vee e &= a \vee (b \wedge c), & b \vee e &= b \vee (c \wedge a), & c \vee e &= c \vee (a \wedge b), \\ a \wedge f &= a \wedge (b \vee c), & b \wedge f &= b \wedge (c \vee a), & c \wedge f &= c \wedge (a \vee b). \end{aligned}$$

(III) Bebizonyítjuk a következő egyenlőségeket:

$$\begin{aligned} e \wedge a &= (c \wedge a) \vee (a \wedge b), & e \wedge b &= (a \wedge b) \vee (b \wedge c), & e \wedge c &= (b \wedge c) \vee (c \wedge a), \\ a \vee f &= (a \vee b) \wedge (c \vee a), & b \vee f &= (a \vee b) \wedge (b \vee c), & c \vee f &= (b \vee c) \wedge (c \vee a). \end{aligned}$$

Világos, hogy $(c \wedge a) \vee (a \wedge b) \leq a$ és $(b \wedge c, a)$ moduláris pár, ezért

$$((c \wedge a) \vee (a \wedge b)) \vee ((b \wedge c) \wedge a) = ((c \wedge a) \vee (a \wedge b) \vee (b \wedge c)) \wedge a,$$

és $b \wedge c \wedge a \leq (c \wedge a) \vee (a \wedge b)$, amiből következik, hogy $(c \wedge a) \vee (a \wedge b) = e \wedge a$.
Világos, hogy $(a \wedge b) \vee (b \wedge c) \leq b$ és $(c \wedge a, b)$ moduláris pár, ezért

$$((a \wedge b) \vee (b \wedge c)) \vee ((c \wedge a) \wedge b) = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) \wedge b,$$

és $c \wedge a \wedge b \leq (a \wedge b) \vee (b \wedge c)$, amiből következik, hogy $(a \wedge b) \vee (b \wedge c) = e \wedge b$.
Világos, hogy $(b \wedge c) \vee (c \wedge a) \leq c$ és $(a \wedge b, c)$ moduláris pár, ezért

$$((b \wedge c) \vee (c \wedge a)) \vee ((a \wedge b) \wedge c) = ((b \wedge c) \vee (c \wedge a) \vee (a \wedge b)) \wedge c,$$

és $a \wedge b \wedge c \leq (b \wedge c) \vee (c \wedge a)$, amiből következik, hogy $(b \wedge c) \vee (c \wedge a) = e \wedge c$.
Világos, hogy $a \leq (a \vee b) \wedge (c \vee a)$ és $(b \vee c, (a \vee b) \wedge (c \vee a))$ moduláris pár, ezért

$$a \vee ((b \vee c) \wedge ((a \vee b) \wedge (c \vee a))) = (a \vee (b \vee c)) \wedge ((a \vee b) \wedge (c \vee a)),$$

és $a \vee b \vee c \geq (a \vee b) \wedge (c \vee a)$ amiből következik, hogy $a \vee f = (a \vee b) \wedge (c \vee a)$.
Világos, hogy $b \leq (a \vee b) \wedge (b \vee c)$ és $(c \vee a, (a \vee b) \wedge (b \vee c))$ moduláris pár, ezért

$$b \vee ((c \vee a) \wedge ((a \vee b) \wedge (b \vee c)) = (b \vee (c \vee a)) \wedge ((a \vee b) \wedge (b \vee c)),$$

és $b \vee c \vee a \geq (a \vee b) \wedge (b \vee c)$, amiből következik, hogy $b \vee f = (a \vee b) \wedge (b \vee c)$.
Világos, hogy $c \leq (b \vee c) \wedge (c \vee a)$ és $(a \vee b, (b \vee c) \wedge (c \vee a))$ moduláris pár, ezért

$$c \vee ((a \vee b) \wedge ((b \vee c) \wedge (c \vee a)) = (c \vee (a \vee b)) \wedge ((b \vee c) \wedge (c \vee a)),$$

és $c \vee a \vee b \geq (b \vee c) \wedge (c \vee a)$, amiből következik, hogy $c \vee f = (b \vee c) \wedge (c \vee a)$.
(IV) Megmutatjuk, hogy

$$\begin{aligned} a' &= (b \wedge c) \vee (a \wedge (b \vee c)) = ((b \wedge c) \vee a) \wedge (b \vee c), \\ b' &= (c \wedge a) \vee (b \wedge (c \vee a)) = ((c \vee a) \vee b) \wedge (c \vee a), \\ c' &= (a \wedge b) \vee (c \wedge (a \vee b)) = ((a \wedge b) \vee c) \wedge (a \vee b). \end{aligned}$$

A definíció, valamint $(a \wedge b) \vee (c \wedge a) \leq a \wedge (b \vee c)$ és (II) alapján

$$a' = e \vee (a \wedge f) = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) \vee (a \wedge (b \vee c)) = (b \wedge c) \vee (a \wedge (b \vee c)).$$

Továbbá, $b \wedge c \leq b \vee c$ és $(a, b \vee c)$ moduláris pár, ezért

$$a' = (b \wedge c) \vee (a \wedge (b \vee c)) = ((b \wedge c) \vee a) \wedge (b \vee c).$$

A definíció, valamint $(a \wedge b) \vee (b \wedge c) \leq b \wedge (c \vee a)$ és (II) alapján

$$b' = e \vee (b \wedge f) = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) \vee (b \wedge (c \vee a)) = (c \wedge a) \vee (b \wedge (c \vee a)).$$

Továbbá, $c \wedge a \leq c \vee a$ és $(b, c \vee a)$ moduláris pár, ezért

$$b' = (c \wedge a) \vee (b \wedge (c \vee a)) = ((c \wedge a) \vee b) \wedge (c \vee a).$$

A definíció, valamint $(b \wedge c) \vee (c \wedge a) \leq c \wedge (a \vee b)$ és (II) miatt

$$c' = e \vee (c \wedge f) = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) \vee (c \wedge (a \vee b)) = (a \wedge b) \vee (c \wedge (a \vee b)).$$

Továbbá, $a \wedge b \leq a \vee b$ és $(c, a \vee b)$ moduláris pár, ezért

$$c' = (a \wedge b) \vee (c \wedge (a \vee b)) = ((a \wedge b) \vee c) \wedge (a \vee b).$$

(V) Most bebizonyítjuk az

$$e < a' < f; \quad e < b' < f; \quad e < c' < f$$

szigorú egyenlőtlenségeket.

A 22.3.7. lemma, valamint (III) és (IV) alkalmazásával kapjuk, hogy

$$\begin{aligned}
a \wedge a' &= a \wedge (((b \wedge c) \vee a) \wedge (b \vee c) = a \wedge (b \vee c)) > (a \wedge b) \vee (a \wedge c) = a \wedge e,\\
a \vee a' &= a \vee ((b \wedge c) \vee (a \wedge (b \vee c))) = a \vee (b \wedge c) < (a \vee b) \wedge (a \vee c) = a \vee f,\\
b \wedge b' &= b \wedge (((c \vee a) \vee b) \wedge (c \vee a)) = b \wedge (c \vee a) > (b \wedge c) \vee (b \wedge a) = b \wedge e,\\
b \vee b' &= b \vee ((c \wedge a) \vee (b \wedge (c \vee a))) = b \vee (c \wedge a) < (b \vee c) \wedge (b \vee a) = b \vee f,\\
c \wedge c' &= c \wedge (((a \wedge b) \vee c) \wedge (a \vee b)) = c \wedge (a \vee b) > (c \wedge a) \vee (c \wedge b) = c \wedge e,\\
c \vee c' &= c \vee ((a \wedge b) \vee (c \wedge (a \vee b))) = c \vee (a \wedge b) < (c \vee a) \wedge (c \vee b) = c \vee f,
\end{aligned}$$

és (I) alapján ebből rendre következnek az $a' > e$, $a' < f$, $b' > e$, $b' < f$, $c' > e$ és $c' < f$ szigorú egyenlőtlenségek.

(VI) Bebizonyítjuk, hogy $a' \wedge b' = e$ és $a' \vee b' = f$.

A definíció szerint

$$a' \wedge b' = (e \vee (a \wedge f)) \wedge (e \vee (b \wedge f)).$$

Világos, hogy $e \leq e \vee (b \wedge f)$ és $(a \wedge f, e \vee (b \wedge f))$ moduláris pár, ezért

$$e \vee ((a \wedge f) \wedge (e \vee (b \wedge f))) = (e \vee (a \wedge f)) \wedge (e \vee (b \wedge f)) = a' \wedge b'.$$

Vezessük be a $g := (a \wedge f) \wedge (e \vee (b \wedge f))$ elemet, amelyre a fentiek szerint $a' \wedge b' = e \vee g$. Most a g elemet fogjuk vizsgálni. Láttuk, hogy $e \leq f$ és (b, f) moduláris pár, ezért $e \vee (b \wedge f) = (e \vee b) \wedge f$, tehát

$$g = (a \wedge f) \wedge (e \vee (b \wedge f)) = (a \wedge f) \wedge ((e \vee b) \wedge f) = (a \wedge f) \wedge (e \vee b).$$

Ugyanakkor (II) miatt $a \wedge f = a \wedge (b \vee c)$ és $e \vee b = (c \wedge a) \vee b$, amiből következik, hogy

$$g = (a \wedge (b \vee c)) \wedge ((c \wedge a) \vee b).$$

Világos, hogy $b \leq b \vee c$ és $(c \wedge a, b \vee c)$ moduláris pár, ezért

$$b \vee ((c \wedge a) \wedge (b \vee c)) = (b \vee (c \wedge a)) \wedge (b \vee c),$$

amiből $c \wedge (b \vee c) = c$ alapján következik, hogy

$$g = a \wedge (b \vee ((c \wedge a) \wedge (b \vee c))) = a \wedge (b \vee (c \wedge a)).$$

Mivel $a \wedge c \leq a$ és (b, a) moduláris pár, így $(a \wedge c) \vee (b \wedge a) = ((a \wedge c) \vee b) \wedge a$, vagyis $g = (a \wedge c) \vee (b \wedge a)$. Ebből következik, hogy

$$a' \wedge b' = e \vee g = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) \vee ((a \wedge c) \vee (b \wedge a)) = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = e,$$

vagyis $a' \wedge b' = e$.

Az $a' \vee b' = f$ egyenlőség bizonyításához megjegyezzük, hogy (I) szerint $e \leq f$ és (b, f) moduláris pár, így $b' = e \vee (b \wedge f) = (e \vee b) \wedge f$, ezért

$$a' \vee b' = (e \vee (a \wedge f)) \vee ((e \vee b) \wedge f).$$

Világos, hogy $e \leq f$ miatt $e \vee (a \wedge f) \leq f$, és $(e \vee b, f)$ moduláris pár, ezért

$$a' \vee b' = (e \vee (a \wedge f)) \vee ((e \vee b) \wedge f) = ((e \vee (a \wedge f)) \vee (e \vee b)) \wedge f = ((a \wedge f) \vee (e \vee b)) \wedge f.$$

Vezessük be a $h := (a \wedge f) \vee (e \vee b)$ elemet, amelyre a fentiek szerint $a' \vee b' = h \wedge f$. Most a h elemet fogjuk vizsgálni. (II) szerint $a \wedge f = a \wedge (b \vee c)$ és $e \vee b = (c \wedge a) \vee b$, tehát

$$h = (a \wedge (b \vee c)) \vee ((c \wedge a) \vee b) = (b \vee (a \wedge (b \vee c))) \vee (c \wedge a).$$

Világos, hogy $b \leq b \vee c$ és $(a, b \vee c)$ moduláris pár, ezért

$$b \vee (a \wedge (b \vee c)) = (b \vee a) \wedge (b \vee c),$$

amiből következik, hogy

$$h = ((b \vee a) \wedge (b \vee c)) \vee (c \wedge a) = (b \vee a) \wedge (b \vee c) \geq (b \vee a) \wedge (b \vee c) \wedge (c \vee a) = f,$$

hiszen nyilvánvalóan $(b \vee a) \wedge (b \vee c) \geq c \wedge a$. Ezért $a' \vee b' = h \wedge f = f$.

(VII) Bebizonyítjuk, hogy $b' \wedge c' = e$ és $b' \vee a' = f$.

A definíció szerint

$$b' \wedge c' = (e \vee (b \wedge f)) \wedge (e \vee (c \wedge f)).$$

Világos, hogy $e \leq e \vee (c \wedge f)$ és $(b \wedge f, e \vee (c \wedge f))$ moduláris pár, ezért

$$e \vee ((b \wedge f) \wedge (e \vee (c \wedge f))) = (e \vee (b \wedge f)) \wedge (e \vee (c \wedge f)) = b' \wedge c'.$$

Vezessük be a $g := (b \wedge f) \wedge (e \vee (c \wedge f))$ elemet, amelyre a fentiek szerint $b' \wedge c' = e \vee g$. Most a g elemet fogjuk vizsgálni. Láttuk, hogy $e \leq f$ és (c, f) moduláris pár, ezért $e \vee (c \wedge f) = (e \vee c) \wedge f$, tehát

$$g = (b \wedge f) \wedge (e \vee (c \wedge f)) = (b \wedge f) \wedge ((e \vee c) \wedge f) = (b \wedge f) \wedge (e \vee c).$$

Ugyanakkor (II) miatt $b \wedge f = b \wedge (c \vee a)$ és $e \vee c = (a \wedge b) \vee c$, amiből következik, hogy

$$g = (b \wedge (c \vee a)) \wedge ((a \wedge b) \vee c).$$

Világos, hogy $c \leq c \vee a$ és $(a \wedge b, c \vee a)$ moduláris pár, ezért

$$c \vee ((a \wedge b) \wedge (c \vee a)) = (c \vee (a \wedge b)) \wedge (c \vee a),$$

amiből $a \wedge (c \vee a) = a$ alapján következik, hogy

$$g = b \wedge (c \vee ((a \wedge b) \wedge (c \vee a))) = b \wedge (c \vee (a \wedge b)).$$

Mivel $a \wedge b \leq b$ és (c, b) moduláris pár, így $(a \wedge b) \vee (c \wedge b) = ((a \wedge b) \vee c) \wedge b$, vagyis $g = (a \wedge b) \vee (c \wedge b)$. Ebből következik, hogy

$$b' \wedge c' = e \vee g = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) \vee ((a \wedge b) \vee (c \wedge b)) = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = e,$$

vagyis $b' \wedge c' = e$.

A $b' \vee c' = f$ egyenlőség bizonyításához megjegyezzük, hogy (I) szerint $e \leq f$ és (c, f) moduláris pár, így $c' = e \vee (c \wedge f) = (e \vee c) \wedge f$, ezért

$$b' \vee c' = (e \vee (b \wedge f)) \vee ((e \vee c) \wedge f).$$

Világos, hogy $e \leq f$ miatt $e \vee (b \wedge f) \leq f$, és $(e \vee c, f)$ moduláris pár, ezért

$$b' \vee c' = (e \vee (b \wedge f)) \vee ((e \vee c) \wedge f) = ((e \vee (b \wedge f)) \vee (e \vee c)) \wedge f = ((b \wedge f) \vee (e \vee c)) \wedge f.$$

Vezessük be a $h := (b \wedge f) \vee (e \vee c)$ elemet, amelyre a fentiek szerint $b' \vee c' = h \wedge f$. Most a h elemet fogjuk vizsgálni. (II) szerint $b \wedge f = b \wedge (c \vee a)$ és $e \vee c = (a \wedge b) \vee c$, tehát

$$h = (b \wedge (c \vee a)) \vee ((a \wedge b) \vee c) = (c \vee (b \wedge (c \vee a))) \vee (a \wedge b).$$

Világos, hogy $c \leq c \vee a$ és $(b, c \vee a)$ moduláris pár, ezért

$$c \vee (b \wedge (c \vee a)) = (c \vee b) \wedge (c \vee a),$$

amiből következik, hogy

$$h = ((c \vee b) \wedge (c \vee a)) \vee (a \wedge b) = (c \vee b) \wedge (c \vee a) \geq (c \vee b) \wedge (c \vee a) \wedge (a \vee b) = f,$$

hiszen nyilvánvalóan $(c \vee b) \wedge (c \vee a) \geq a \wedge b$. Ezért $b' \vee c' = h \wedge f = f$.

(VIII) Bebizonyítjuk, hogy $a' \wedge c' = e$ és $a' \vee c' = f$.

A definíció szerint

$$a' \wedge c' = (e \vee (a \wedge f)) \wedge (e \vee (c \wedge f)).$$

Világos, hogy $e \leq e \vee (c \wedge f)$ és $(a \wedge f, e \vee (c \wedge f))$ moduláris pár, ezért

$$e \vee ((a \wedge f) \wedge (e \vee (c \wedge f))) = (e \vee (a \wedge f)) \wedge (e \vee (c \wedge f)) = a' \wedge c'.$$

Vezessük be a $g := (a \wedge f) \wedge (e \vee (c \wedge f))$ elemet, amelyre a fentiek szerint $a' \wedge c' = e \vee g$. Most a g elemet fogjuk vizsgálni. Láttuk, hogy $e \leq f$ és (c, f) moduláris pár, ezért $e \vee (c \wedge f) = (e \vee c) \wedge f$, tehát

$$g = (a \wedge f) \wedge (e \vee (c \wedge f)) = (a \wedge f) \wedge ((e \vee c) \wedge f) = (a \wedge f) \wedge (e \vee c).$$

Ugyanakkor (II) miatt $a \wedge f = a \wedge (b \vee c)$ és $e \vee c = (a \wedge b) \vee c$, amiből következik, hogy

$$g = (a \wedge (b \vee c)) \wedge ((a \wedge b) \vee c).$$

Világos, hogy $c \leq b \vee c$ és $(a \wedge b, b \vee c)$ moduláris pár, ezért

$$c \vee ((a \wedge b) \wedge (b \vee c)) = (c \vee (a \wedge b)) \wedge (b \vee c),$$

amiből $b \wedge (b \vee c) = b$ alapján következik, hogy

$$g = a \wedge (c \vee ((a \wedge b) \wedge (b \vee c))) = a \wedge (c \vee (a \wedge b)).$$

Mivel $a \wedge b \leq a$ és (c, a) moduláris pár, így $(a \wedge b) \vee (c \wedge a) = ((a \wedge b) \vee c) \wedge a$, vagyis $g = (a \wedge b) \vee (c \wedge a)$. Ebből következik, hogy

$$a' \wedge c' = e \vee g = ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a)) \vee ((a \wedge b) \vee (c \wedge a)) = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = e,$$

vagyis $a' \wedge c' = e$.

Az $a' \vee c' = f$ egyenlőség bizonyításához megjegyezzük, hogy (I) szerint $e \leq f$ és (c, f) moduláris pár, így $c' = e \vee (c \wedge f) = (e \vee c) \wedge f$, ezért

$$a' \vee c' = (e \vee (a \wedge f)) \vee ((e \vee c) \wedge f).$$

Világos, hogy $e \leq f$ miatt $e \vee (a \wedge f) \leq f$, és $(e \vee c, f)$ moduláris pár, ezért

$$a' \vee c' = (e \vee (a \wedge f)) \vee ((e \vee c) \wedge f) = ((e \vee (a \wedge f)) \vee (e \vee c)) \wedge f = ((a \wedge f) \vee (e \vee c)) \wedge f.$$

Vezessük be a $h := (a \wedge f) \vee (e \vee c)$ elemet, amelyre a fentiek szerint $a' \vee c' = h \wedge f$. Most a h elemet fogjuk vizsgálni. (II) szerint $a \wedge f = a \wedge (b \vee c)$ és $e \vee c = (a \wedge b) \vee c$, tehát

$$h = (a \wedge (b \vee c)) \vee ((a \wedge b) \vee c) = (c \vee (a \wedge (b \vee c))) \vee (a \wedge b).$$

Világos, hogy $c \leq b \vee c$ és $(a, b \vee c)$ moduláris pár, ezért

$$c \vee (a \wedge (b \vee c)) = (c \vee a) \wedge (b \vee c),$$

amiből következik, hogy

$$h = ((c \vee a) \wedge (b \vee c)) \vee (a \wedge b) = (c \vee a) \wedge (b \vee c) \geq (b \vee a) \wedge (b \vee c) \wedge (c \vee a) = f,$$

hiszen nyilvánvalóan $(c \vee a) \wedge (b \vee c) \geq a \wedge b$. Ezért $a' \vee c' = h \wedge f = f$.

(IX) Végül megmutatjuk, hogy az a', b' és c' elemek páronként nem összehasonlíthatóak az L háló rendezése szerint.

Ha $a' \leq b'$ teljesülne, akkor (VI) szerint $e = a' \wedge b' = a'$, holott (V) miatt $e < a'$. Ha $b' \leq a'$ teljesülne, akkor (VI) szerint $e = a' \wedge b' = b'$, holott (V) miatt $e < b'$. Ezért a' és b' nem összehasonlíthatóak az L háló rendezése szerint.

Ha $b' \leq c'$ teljesülne, akkor (VII) szerint $e = b' \wedge c' = b'$, holott (VI) miatt $e < b'$. Ha $c' \leq b'$ teljesülne, akkor (VII) szerint $e = b' \wedge c' = c'$, holott (V) miatt $e < c'$. Ezért b' és c' nem összehasonlíthatóak az L háló rendezése szerint.

Ha $a' \leq c'$ teljesülne, akkor (VIII) szerint $e = a' \wedge c' = a'$, holott (VI) miatt $e < a'$. Ha $c' \leq a'$ teljesülne, akkor (VIII) szerint $e = a' \wedge c' = c'$, holott (V) miatt $e < c'$. Ezért a' és c' nem összehasonlíthatóak az L háló rendezése szerint. ■

22.3.9. Tétel. (**Disztributív hálók jellemzése részhálókkal.**) *Háló pontosan akkor disztributív, ha nincs sem* M_5*-tel, sem* N_5*-tel izomorf részhálója.*

Bizonyítás. Ha egy hálónak létezik N_5-tel izomorf részhálója, akkor nem moduláris, tehát nem disztributív, és ha egy hálónak létezik M_5-tel izomorf részhálója, akkor nem disztributív. Tehát ha egy hálónak létezik M_5-tel vagy N_5-tel izomorf részhálója, akkor nem disztributív.

Megfordítva, ha egy háló nem moduláris, akkor a Dedekind-tétel szerint létezik N_5-tel izomorf részhálója, és ha a háló moduláris és nem disztributív, akkor a Birkhoff-tétel alapján létezik M_5 izomorf részhálója. ■

22.4. Halmazfélgyűrűk és disztributív hálók reprezentációs tétele*

22.4.1. Definíció. *Ha E halmaz, akkor az $L \subseteq \mathscr{P}(E)$ halmazt E feletti* **halmazfélgyűrűnek** *nevezzük, ha minden $X, Y \in L$ esetén $X \cap Y \in L$ és $X \cup Y \in L$.*

Világos, hogy minden halmazfélgyűrű a $\subseteq$ relációval ellátva disztributív háló. Ebben a pontban megmutatjuk, hogy minden disztributív háló izomorf egy halmazfélgyűrűvel. Ez a disztributív hálók Stone-féle reprezentációs tétele.

22.4.2. Definíció. *Az L hálóban* **prímideálnak** *nevezünk minden olyan $\mathfrak{p}$ ideált, amelyre $\mathfrak{p} \neq L$ és teljesül az, hogy minden $e, f \in L$ esetén, ha $e \notin \mathfrak{p}$ és $f \notin \mathfrak{p}$, akkor $e \wedge f \notin \mathfrak{p}$. Az L háló prímideáljainak halmazát $\mathrm{Spec}(L)$ jelöli, és ezt a halmazt az L háló* **egyszerű spektrumának** *nevezzük.*

22.4.3. Definíció. *Az L háló* **Stone-reprezentációjának** *nevezzük a*

$$\mathscr{S}_L : L \to \mathscr{P}(\mathrm{Spec}(L)); \quad e \mapsto \{\, \mathfrak{p} \in \mathrm{Spec}(L) \mid e \notin \mathfrak{p} \,\}$$

leképezést.

Nyilvánvaló, hogy ha $\mathbf{0}$ az L háló legkisebb eleme, akkor $\mathscr{S}_L(\mathbf{0}) = \emptyset$, mert minden $\mathfrak{p} \in \mathrm{Spec}(L)$ esetén $\mathbf{0} \in \mathfrak{p}$, azaz $\mathfrak{p} \notin \mathscr{S}_L(\mathbf{0})$. Továbbá, ha $\mathbf{1}$ az L háló legnagyobb eleme, akkor $\mathscr{S}_L(\mathbf{1}) = \mathrm{Spec}(L)$, mert minden $\mathfrak{p} \in \mathrm{Spec}(L)$ esetén $\mathbf{1} \notin \mathfrak{p}$, hiszen $\mathfrak{p}$ valódi ideál.

22.4.4. Lemma. *Disztributív hálóban minden maximális valódi ideál prímideál.*

Bizonyítás. Legyen $\mathfrak{p}$ tartalmazás tekintetében maximális valódi ideál az L disztributív hálóban. Indirekt bizonyítunk, tehát feltesszük olyan $e, f \in L$ elemek létezését, amelyekre $e \notin \mathfrak{p}$, $f \notin \mathfrak{p}$ és $e \wedge f \in \mathfrak{p}$. Készítsük el a

$$\mathfrak{q} := \{f \in L \mid (\exists p \in \mathfrak{p}) : f \leq e \vee p\}$$

halmazt, amelyről a 22.2.5. állítás alapján tudjuk, hogy a legkisebb olyan ideál L-ben, amelyre $\{e\} \cup \mathfrak{p} \subseteq \mathfrak{q}$. A $\mathfrak{p}$ ideál maximalitása miatt $\mathfrak{q} = L$ vagy $\mathfrak{q} = \mathfrak{p}$.

Ha $\mathfrak{q} = L$, akkor $f \in \mathfrak{q}$, tehát létezik olyan $p \in \mathfrak{p}$, hogy $f \leq e \vee p$. A hipotézis szerint $f \wedge e \in \mathfrak{p}$, és $p \in \mathfrak{p}$ miatt $f \wedge p \in \mathfrak{p}$, következésképpen az L háló disztributivitását alkalmazva $f = f \wedge (e \vee p) = (f \wedge e) \vee (f \wedge p) \in \mathfrak{p}$ adódik, holott $f \notin \mathfrak{p}$.

Ezért $\mathfrak{q} = \mathfrak{p}$, vagyis $e \in \mathfrak{q}$ miatt $e \in \mathfrak{p}$, ami ellentmond annak, hogy $e \notin \mathfrak{p}$. ■

22.4.5. Lemma. *Ha L disztributív háló, és $e, f \in L$, akkor az $e \not\leq f$ kijelentés azzal ekvivalens, hogy létezik olyan $\mathfrak{p}$ prímideál L-ben, hogy $e \notin \mathfrak{p}$ és $f \in \mathfrak{p}$.*

Bizonyítás. Ha $\mathfrak{p}$ olyan ideál L-ben, hogy $e \notin \mathfrak{p}$ és $f \in \mathfrak{p}$, akkor $e \leq f$ lehetetlen (még akkor is, ha L nem disztributív és $\mathfrak{p}$ nem prímideál).

Tegyük fel, hogy $e, f \in L$ olyan elemek, amelyekre $e \not\leq f$. Jelölje $\mathfrak{P}$ azon $\mathfrak{p} \subseteq L$ ideálok halmazát, amelyekre $e \notin \mathfrak{p}$ és $f \in \mathfrak{p}$. Világos, hogy $\mathfrak{P} \neq \emptyset$, mert $]\leftarrow, f] \in \mathfrak{P}$. Lássuk el a $\mathfrak{P}$ halmazt a tartalmazás relációval.

Megmutatjuk, hogy a $\mathfrak{P}$ rendezett halmaz *induktívan rendezett.* Ehhez legyen $(\mathfrak{p}_i)_{i\in I}$ olyan $\mathfrak{P}$-ben haladó nem üres rendszer, amelyre minden $i, j \in I$ esetén $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ vagy $\mathfrak{p}_j \subseteq \mathfrak{p}_i$. Ekkor $\mathfrak{p} := \bigcup_{i\in I} \mathfrak{p}_i \in \mathfrak{P}$. Valóban, ha $p \in \mathfrak{p}$ és $q \in L$ olyan, hogy $q \leq p$, akkor van olyan $i \in I$, hogy $p \in \mathfrak{p}_i$, ezért $q \in \mathfrak{p}_i \subseteq \mathfrak{p}$, hiszen $\mathfrak{p}_i$ ideál. Továbbá, ha $p, q \in \mathfrak{p}$, akkor lézenek olyan $i, j \in I$, hogy $p \in \mathfrak{p}_i$ és $q \in \mathfrak{p}_j$. Ekkor $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ esetén $p, q \in \mathfrak{p}_j$, tehát $p \vee q \in \mathfrak{p}_j$, hiszen $\mathfrak{p}_j$ ideál. Ha viszont $\mathfrak{p}_j \subseteq \mathfrak{p}_i$, akkor $p, q \in \mathfrak{p}_i$, tehát $p \vee q \in \mathfrak{p}_i$, hiszen $\mathfrak{p}_i$ ideál. Ezért $p \vee q \in \mathfrak{p}$, ami azt jelenti, hogy $\mathfrak{p}$ ideál L-ben. Világos, hogy $e \notin \mathfrak{p}$, mert minden $i \in I$ esetén $\mathfrak{p}_i \in \mathfrak{P}$, tehát $e \notin \mathfrak{p}_i$. Továbbá, $f \in \mathfrak{p}$ nyilvánvaló, mert $I \neq \emptyset$ és minden $i \in I$ esetén $\mathfrak{p}_i \in \mathfrak{P}$. Tehát $\mathfrak{p} \in \mathfrak{P}$, és nyilvánvaló, hogy $\mathfrak{p}$ felső korlátja (sőt szuprémuma) a $(\mathfrak{p}_i)_{i\in I}$ rendszernek a $\mathfrak{P}$ rendezett halmazban.

A Zorn-lemma szerint vehetjük a $\mathfrak{P}$ rendezett halmaznak egy $\mathfrak{p}$ maximális elemét. Ekkor $\mathfrak{p}$-re $e \notin \mathfrak{p}$ teljesül, tehát $\mathfrak{p}$ valódi ideál. Ugyanakkor $f \in \mathfrak{p}$ is teljesül, ezért elég azt igazolni, hogy minden $q, q' \in L$ esetén, ha $q \notin \mathfrak{p}$ és $q' \notin \mathfrak{p}$, akkor $q \wedge q' \notin \mathfrak{p}$.

Indirekt bizonyítunk, tehát feltesszük, hogy $q, q' \in L$ olyan elemek, amelyekre $q \notin \mathfrak{p}$, $q' \notin \mathfrak{p}$ és $q \wedge q' \in \mathfrak{p}$. Tekintsük a

$$\mathfrak{q} := \{g \in L \mid (\exists p \in \mathfrak{p}) : g \leq q \vee p\},$$
$$\mathfrak{q}' := \{g \in L \mid (\exists p \in \mathfrak{p}) : g \leq q' \vee p\}$$

halmazokat, amelyekről tudjuk, hogy olyan ideálok L-ben, hogy $\{q\} \cup \mathfrak{p} \subseteq \mathfrak{q}$, valamint $\{q'\} \cup \mathfrak{p} \subseteq \mathfrak{q}'$.

Megmutatjuk, hogy $e \notin \mathfrak{q}$ *vagy* $e \notin \mathfrak{q}'$. Indirekt tegyük fel, hogy $e \in \mathfrak{q} \cap \mathfrak{q}'$. Ekkor $\mathfrak{q}$ és $\mathfrak{q}'$ definíciója szerint vehetünk olyan $p, p' \in \mathfrak{p}$ elemeket, hogy $e \leq q \vee p$ és $e \leq q' \vee p'$. Ekkor $\overline{p} := p \vee p' \in \mathfrak{p}$ olyan, hogy $e \leq q \vee p \leq q \vee \overline{p}$ és $e \leq q' \vee p' \leq q' \vee \overline{p}$, amiből L disztributivitása alapján következik, hogy

$$e \leq (q \vee \overline{p}) \wedge (q' \vee \overline{p}) = (q \wedge q') \vee \overline{p},$$

tehát $e \in \mathfrak{p}$, hiszen a hipotézis szerint $q \wedge q' \in \mathfrak{p}$ és $\overline{p} \in \mathfrak{p}$, így $(q \wedge q') \vee \overline{p} \in \mathfrak{p}$, hiszen $\mathfrak{p}$ ideál. Azonban $e \notin \mathfrak{p}$, és ez az ellentmondás igazolja, hogy $e \notin \mathfrak{q}$ vagy $e \notin \mathfrak{q}'$.

Tegyük fel, hogy $e \notin \mathfrak{q}$. Mivel $f \in \mathfrak{p} \subseteq \mathfrak{q}$, így $\mathfrak{q} \in \mathfrak{P}$. Ugyanakkor $\mathfrak{p} \subseteq \mathfrak{q}$, ezért $\mathfrak{p}$ maximalitásából következik, hogy $\mathfrak{p} = \mathfrak{q}$. Azonban $q \in \mathfrak{q}$ és a hipotézis szerint $q \notin \mathfrak{p}$, ezért $\mathfrak{p} \neq \mathfrak{q}$, ami ellentmondás.

Tegyük fel, hogy $e \notin \mathfrak{q}'$. Mivel $f \in \mathfrak{p} \subseteq \mathfrak{q}'$, így $\mathfrak{q}' \in \mathfrak{P}$. Ugyanakkor $\mathfrak{p} \subseteq \mathfrak{q}'$, ezért $\mathfrak{p}$ maximalitásából következik, hogy $\mathfrak{p} = \mathfrak{q}'$. Azonban $q' \in \mathfrak{q}'$ és a hipotézis szerint $q' \notin \mathfrak{p}$, ezért $\mathfrak{p} \neq \mathfrak{q}'$, ami ellentmondás.

Ez azt jelenti, hogy $\mathfrak{p}$ olyan prímideál L-ben, amelyre $e \notin \mathfrak{p}$ és $f \in \mathfrak{p}$. ■

22.4.6. Tétel. (**Stone-féle reprezentációs tétel.**) *Ha L disztributív háló, akkor a*

$$\mathscr{S}_L : L \to \mathscr{P}(\mathrm{Spec}(L)); \quad e \mapsto \{\ \mathfrak{p} \in \mathrm{Spec}(L) \mid e \notin \mathfrak{p}\ \}$$

Stone-reprezentáció olyan, hogy $\mathrm{Im}(\mathscr{S}_L)$ *halmazfélgyűrű a* $\mathrm{Spec}(L)$ *halmaz felett, és* $\mathscr{S}_L$ *háló-izomorfizmus* L *és az* $\mathrm{Im}(\mathscr{S}_L)$ *halmazfélgyűrű között.*

Bizonyítás. Először megmutatjuk, hogy $\mathscr{S}_L$ *injektív.* Ehhez legyenek $e, f \in L$ olyanok, hogy $e \neq f$. Ekkor a rendezés antiszimmetriája miatt $e \not\leq f$ vagy $f \not\leq e$. Ha $e \not\leq f$, akkor az előző lemma szerint van olyan $\mathfrak{p} \in \mathrm{Spec}(L)$, hogy $e \notin \mathfrak{p}$ és $f \in \mathfrak{p}$, vagyis $\mathfrak{p} \in \mathscr{S}_L(e)$ és $\mathfrak{p} \notin \mathscr{S}_L(f)$, így $\mathscr{S}_L(e) \neq \mathscr{S}_L(f)$. Ha $f \not\leq e$, akkor az előző lemma szerint van olyan $\mathfrak{p} \in \mathrm{Spec}(L)$, hogy $f \notin \mathfrak{p}$ és $e \in \mathfrak{p}$, vagyis $\mathfrak{p} \in \mathscr{S}_L(f)$ és $\mathfrak{p} \notin \mathscr{S}_L(e)$, így $\mathscr{S}_L(e) \neq \mathscr{S}_L(f)$.
Ha $e, f \in L$ tetszőlegesek és $\mathfrak{p} \in \mathrm{Spec}(L)$, akkor fennállnak a következő ekvivalenciák

$$\mathfrak{p} \in \mathscr{S}_L(e \wedge f) \Leftrightarrow e \wedge f \notin \mathfrak{p} \overset{(*)}{\Leftrightarrow} (\ (e \notin \mathfrak{p}) \text{ és } (f \notin \mathfrak{p})\ ) \Leftrightarrow \mathfrak{p} \in \mathscr{S}_L(e) \cap \mathscr{S}_L(f),$$

ahol a $\overset{(*)}{\Leftrightarrow}$ ekvivalenciánál használtuk ki azt, hogy $\mathfrak{p}$ prímideál. Ez azt jelenti, hogy minden $e, f \in L$ esetén $\mathscr{S}_L(e \wedge f) = \mathscr{S}_L(e) \cap \mathscr{S}_L(f)$. Ebből az is látható, hogy $\mathrm{Im}(\mathscr{S}_L)$ zárt a véges metszet-képzésre nézve.

Ha $e, f \in L$ tetszőlegesek és $\mathfrak{p} \in \mathrm{Spec}(L)$, akkor fennállnak a következő ekvivalenciák

$$\mathfrak{p} \in \mathscr{S}_L(e \vee f) \Leftrightarrow e \vee f \notin \mathfrak{p} \overset{(**)}{\Leftrightarrow} (\ (e \notin \mathfrak{p}) \text{ vagy } (f \notin \mathfrak{p})\ ) \Leftrightarrow \mathfrak{p} \in \mathscr{S}_L(e) \cup \mathscr{S}_L(f),$$

ahol a $\overset{(**)}{\Leftrightarrow}$ ekvivalenciánál csak annyit használtuk ki, hogy $\mathfrak{p}$ ideál. Ez azt jelenti, hogy minden $e, f \in L$ esetén $\mathscr{S}_L(e \vee f) = \mathscr{S}_L(e) \cup \mathscr{S}_L(f)$. Ebből az is látható, hogy $\mathrm{Im}(\mathscr{S}_L)$ zárt a véges unió-képzésre nézve.

Tehát $\mathrm{Im}(\mathscr{S}_L)$ halmazfélgyűrű a $\mathrm{Spec}(L)$ halmaz felett, és a $\mathscr{S}_L : L \to \mathscr{P}(\mathrm{Spec}(L))$ leképezés olyan injekció, amely megtartja a hálóműveleteket, ezért $\mathscr{S}_L$ háló-izomorfizmus L és az $\mathrm{Im}(\mathscr{S}_L)$ halmazfélgyűrű között. ■

Ha L disztributív háló, akkor $\mathfrak{p} \in \mathrm{Spec}(L)$ esetén $\mathfrak{p} \neq L$, így van olyan $e \in L$, hogy $e \notin \mathfrak{p}$, tehát ha $\mathscr{S}_L$ jelöli a Stone-féle reprezentációs tételben értelmezett függvényt, akkor $\mathfrak{p} \in \mathscr{S}_L(e)$. Ez azt jelenti, hogy a $(\mathscr{S}_L(e))_{e \in L}$ halmazrendszer olyan befedése $\mathrm{Spec}(L)$-nek, amely zárt a véges metszet-képzésre nézve. Ezért értelmes a következő definíció.

22.4.7. Definíció. *Legyen* L *disztributív háló. A* $\mathrm{Spec}(L)$ *egyszerű spektrum feletti* **Stone-topológiának** *nevezzük azt a topológiát, amelynek a* $\{\mathscr{S}_L(e) | e \in L\}$ *halmaz topologikus bázisa. A* $\mathrm{Spec}(L)$ *halmazt a Stone-topológiával ellátva az* L *disztributív háló* **Stone-terének** *nevezzük.*

Tehát ha L disztributív háló és $\mathscr{S}_L$ jelöli a Stone-féle reprezentációs tételben értelmezett függvényt, akkor egy $\Omega \subseteq \mathrm{Spec}(L)$ halmaz pontosan akkor nyílt a Stone-topológia szerint, ha létezik olyan L-ben haladó $(e_i)_{i \in I}$ rendszer, hogy $\Omega = \bigcup_{i \in I} \mathscr{S}_L(e_i)$.
Speciálisan, ha $\mathfrak{p} \in \mathrm{Spec}(L)$, akkor a $V \subseteq \mathrm{Spec}(L)$ halmaz pontosan akkor környezete $\mathfrak{p}$-nek a Stone-topológia szerint, ha létezik olyan $e \in L$, hogy $\mathfrak{p} \in \mathscr{S}_L(e) \subseteq V$, vagyis $e \notin \mathfrak{p}$ és minden $\mathfrak{q} \in \mathrm{Spec}(L)$ esetén, ha $e \notin \mathfrak{q}$ (azaz $\mathfrak{q} \in \mathscr{S}_L(e)$), akkor $\mathfrak{q} \in V$.

22.4.8. Lemma. *Ha* $\mathfrak{p}$ *valódi ideál az* L *felülről korlátos hálóban, akkor létezik olyan maximális valódi ideál* L*-ben, amely tartalmazza* $\mathfrak{p}$*-t.*

Bizonyítás. Jelölje S az L háló $\mathfrak{p}$-t tartalmazó valódi ideáljainak halmazát, amely nem üres, mert $\mathfrak{p} \in S$. Az S halmazt rendezzük a tartalmazás relációval.

Az S feletti rendezés *induktív*. Valóban, legyen $(\mathfrak{p}_\alpha)_{\alpha\in A}$ olyan S-ben haladó nem üres rendszer, hogy minden $\alpha, \beta \in A$ esetén $\mathfrak{p}_\alpha \subseteq \mathfrak{p}_\beta$ vagy $\mathfrak{p}_\beta \subseteq \mathfrak{p}_\alpha$. Ekkor a $\mathfrak{q} := \bigcup_{\alpha\in A} \mathfrak{p}_\alpha$ halmaz ideál L-ben, mert $e, f \in \mathfrak{q}$ esetén léteznek olyan $\alpha, \beta \in A$ indexek, hogy $e \in \mathfrak{p}_\alpha$ és $f \in \mathfrak{p}_\beta$, és ekkor $\mathfrak{p}_\alpha \subseteq \mathfrak{p}_\beta$ esetén $e \vee f \in \mathfrak{p}_\beta$, míg $\mathfrak{p}_\beta \subseteq \mathfrak{p}_\alpha$ esetén $e \vee f \in \mathfrak{p}_\alpha$, így $e \vee f \in \mathfrak{q}$. Világos, hogy $\mathfrak{p} \subseteq \mathfrak{q}$ és ha $\mathbf{1}$ jelöli L legnagyobb elemét, akkor minden $\alpha \in A$ esetén $\mathbf{1} \notin \mathfrak{p}_\alpha$, következésképpen $\mathbf{1} \notin \mathfrak{q}$, vagyis $\mathfrak{q}$ valódi ideál, így $\mathfrak{q} \in S$. Ez azt jelenti, hogy $\mathfrak{q}$ felső korlátja (sőt szuprémuma) a $(\mathfrak{p}_\alpha)_{\alpha\in A}$ rendszernek, tehát S induktívan rendezett halmaz.

A Zorn-lemma szerint vehetünk S-ben maximális elemet: legyen $\mathfrak{q}$ ilyen. Ha $\mathfrak{p}'$ olyan valódi ideál L-ben, hogy $\mathfrak{q} \subseteq \mathfrak{p}'$, akkor $\mathfrak{p} \subseteq \mathfrak{p}'$, így $\mathfrak{p}' \in S$, amiből következik, hogy $\mathfrak{q} = \mathfrak{p}'$. Tehát $\mathfrak{q}$ maximális valódi ideál L-ben és tartalmazza a $\mathfrak{p}$ ideált. ■

22.4.9. Állítás. *Disztributív háló Stone-tere* T_0*-tér, és ha a hálónak van legnagyobb eleme, akkor kompakt* T_0*-tér.*

Bizonyítás. Legyen L disztributív háló, és legyenek $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(L)$ olyanok, hogy $\mathfrak{p} \neq \mathfrak{q}$. Ekkor $\mathfrak{q} \nsubseteq \mathfrak{p}$ vagy $\mathfrak{p} \nsubseteq \mathfrak{q}$. Az első esetben van olyan $e \in \mathfrak{q}$, hogy $e \notin \mathfrak{p}$: ekkor $\mathscr{S}_L(e)$ olyan környezete $\mathfrak{p}$-nek a Stone-topológia szerint, amelyre $\mathfrak{q} \notin \mathscr{S}_L(e)$. A második esetben van olyan $e \in \mathfrak{p}$, hogy $e \notin \mathfrak{q}$: ekkor $\mathscr{S}_L(e)$ olyan környezete $\mathfrak{q}$-nak a Stone-topológia szerint, amelyre $\mathfrak{p} \notin \mathscr{S}_L(e)$. Ezért a Stone-topológia T_0-topológia $\mathrm{Spec}(L)$ felett.

Tegyük fel, hogy L-nek van legnagyobb eleme és jelölje ezt $\mathbf{1}$. Legyen $(\Omega_i)_{i\in I}$ a Stone-topológia szerint nyílt befedése $\mathrm{Spec}(L)$-nek.

Minden $\mathfrak{p} \in \mathrm{Spec}(L)$ esetén van olyan $i \in I$, hogy $\mathfrak{p} \in \Omega_i$, és Ω_i nyílt a Stone-topológia szerint, tehát létezik olyan $e \in L$, hogy $\mathfrak{p} \in \mathscr{S}_L(e)$, vagyis $e \notin \mathfrak{p}$ és $\mathscr{S}_L(e) \subseteq \Omega$. Ez azt jelenti, hogy minden $\mathfrak{p} \in \mathrm{Spec}(L)$ esetén $\{\, (e,i) \in L \times I \mid (e \notin \mathfrak{p}) \wedge (\mathscr{S}_L(e) \subseteq \Omega_i) \,\} \neq \emptyset$. Ezért a kiválasztási axióma alapján vehetünk egy

$$f \in \prod_{\mathfrak{p}\in\mathrm{Spec}(L)} \{\, (e,i) \in L \times I \mid (e \notin \mathfrak{p}) \wedge (\mathscr{S}_L(e) \subseteq \Omega_i) \,\}$$

kiválasztó függvényt, és vezessük be a

$$\begin{aligned} \varepsilon &: \mathrm{Spec}(L) \to L; \quad \mathfrak{p} \mapsto \mathrm{pr}_1(f(\mathfrak{p})) \\ \iota &: \mathrm{Spec}(L) \to I; \quad \mathfrak{p} \mapsto \mathrm{pr}_2(f(\mathfrak{p})) \end{aligned}$$

függvényeket. Ekkor $\varepsilon : \mathrm{Spec}(L) \to L$ és $\iota : \mathrm{Spec}(L) \to I$ olyan függvények, amelyekre teljesül az, hogy minden $\mathfrak{p} \in \mathrm{Spec}(L)$ esetén $\varepsilon(\mathfrak{p}) \notin \mathfrak{p}$ és $\mathscr{S}_L(\varepsilon(\mathfrak{p})) \subseteq \Omega_{\iota(\mathfrak{p})}$.

Jelölje $\overline{\mathfrak{p}}$ az $\mathrm{Im}(\varepsilon) \subseteq L$ halmaz által generált ideált L-ben, vagyis 22.2.4. szerint $\overline{\mathfrak{p}} \subseteq L$ az a halmaz, amelynek az $e \in L$ elem pontosan akkor eleme, ha létezik olyan $\mathrm{Spec}(L)$-ben haladó $(\mathfrak{p}_j)_{j\in J}$ nem üres véges rendszer, amelyre $e \leq \bigvee_{j\in J} \varepsilon(\mathfrak{p}_j)$.

Ha $\mathbf{1} \in \overline{\mathfrak{p}}$, akkor tehát vehetünk olyan $\mathrm{Spec}(L)$-ben haladó $(\mathfrak{p}_j)_{j\in J}$ nem üres véges rendszert, amelyre $\mathbf{1} \leq \bigvee_{j\in J} \varepsilon(\mathfrak{p}_j)$, vagyis $\mathbf{1} = \bigvee_{j\in J} \varepsilon(\mathfrak{p}_j)$, amiből 22.4.6. alapján kapjuk, hogy

$$\mathrm{Spec}(L) = \mathscr{S}_L(\mathbf{1}) = \mathscr{S}_L\Big(\bigvee_{j\in J} \varepsilon(\mathfrak{p}_j)\Big) = \bigcup_{j\in J} \mathscr{S}_L(\varepsilon(\mathfrak{p}_j)) \subseteq \bigcup_{j\in J} \Omega(\iota(\mathfrak{p}_j)),$$

tehát az $\big(\Omega_{\iota(\mathfrak{p}_j)}\big)_{j\in J}$ halmazrendszer véges befedése $\mathrm{Spec}(L)$-nek.

Ez azt jelenti, hogy a bizonyítás befejezéséhez elegendő megmutatni, hogy $\mathbf{1} \notin \overline{\mathfrak{p}}$

lehetetlen. Az állítással ellentétben tegyük fel, hogy $\mathbf{1} \notin \overline{\mathfrak{p}}$, vagyis $\overline{\mathfrak{p}}$ valódi ideál L-ben. Az előző lemma szerint van olyan $\mathfrak{q}$ maximális valódi ideál L-ben, amelyre $\overline{\mathfrak{p}} \subseteq \mathfrak{q}$. Ekkor 22.4.4. alapján $\mathfrak{q} \in \mathrm{Spec}(L)$, és a definíció szerint *minden* $\mathfrak{p} \in \mathrm{Spec}(L)$ esetén $\varepsilon(\mathfrak{p}) \in \overline{\mathfrak{p}}$, tehát $\varepsilon(\mathfrak{p}) \in \mathfrak{q}$, vagyis $\mathfrak{q} \notin \mathscr{S}_L(\varepsilon(\mathfrak{p}))$, ami lehetetlen, mert $\mathfrak{q} \notin \mathscr{S}_L(\varepsilon(\mathfrak{q}))$. ■

22.5. Ortokomplementációk és ortohálók

22.5.1. Definíció. *Ha L korlátos rendezett halmaz, akkor egy*

$$L \to L; \quad e \mapsto e^{\perp}$$

leképezést **ortokomplementációnak** *nevezünk L felett, ha teljesülnek a következők:*

$(\mathrm{ORT_I})$ *minden $e \in L$ esetén $(e^{\perp})^{\perp} = e$;*

$(\mathrm{ORT_{II}})$ *minden $e, f \in L$ esetén, ha $e \leq f$, akkor $f^{\perp} \leq e^{\perp}$;*

$(\mathrm{ORT_{III}})$ *minden $e \in L$ esetén* $\sup\{e, e^{\perp}\} = \mathbf{1}$.

Azt mondjuk, hogy L **ortokomplementált rendezett halmaz**, *ha L korlátos rendezett halmaz, és adott egy L feletti ortokomplementáció. Azt mondjuk, hogy L* **ortoháló**, *ha L olyan ortokomplementált rendezett halmaz, amelynek a rendezése hálószerű. A disztributív ortohálókat* **Boole-hálóknak** *nevezzük.*

22.5.2. Definíció. *Legyen L ortokomplementált rendezett halmaz. Az $(e, f) \in L \times L$ párt* **ortogonálisnak** *nevezzük, ha $e \leq f^{\perp}$, és ekkor azt írjuk, hogy $e \perp f$. Az L-ben haladó $(e_i)_{i \in I}$ rendszert ortogonálisnak nevezzük, ha minden $i, j \in I$, $i \neq j$ esetén $e_i \perp e_j$.*

22.5.3. Állítás. *Ha L ortokomplementált rendezett halmaz, akkor teljesülnek a következő állítások.*

a) $\mathbf{0}^{\perp} = \mathbf{1}$ *és* $\mathbf{1}^{\perp} = \mathbf{0}$.

b) *Minden $e \in L$ esetén* $\inf\{e, e^{\perp}\} = \mathbf{0}$.

c) *Minden L-ben haladó $(e_i)_{i \in I}$ rendszerre, ha $\sup_{i \in I} e_i$ létezik L-ben, akkor $\inf_{i \in I} e_i^{\perp}$ létezik L-ben, és*

$$\left(\sup_{i \in I} e_i\right)^{\perp} = \inf_{i \in I} e_i^{\perp}.$$

(de Morgan-egyenlőség).

d) *Minden L-ben haladó $(e_i)_{i \in I}$ rendszerre, ha $\inf_{i \in I} e_i$ létezik L-ben, akkor $\sup_{i \in I} e_i^{\perp}$ létezik L-ben, és*

$$\left(\inf_{i \in I} e_i\right)^{\perp} = \sup_{i \in I} e_i^{\perp}.$$

(de Morgan-egyenlőség).

Bizonyítás. a) Minden $e \in L$ esetén $\mathbf{0} \leq e^{\perp}$, ezért az $(\mathrm{ORT_I})$ és $(\mathrm{ORT_{II}})$ alapján $e = (e^{\perp})^{\perp} \leq \mathbf{0}^{\perp}$, ami azt jelenti, hogy $\mathbf{0}^{\perp}$ az L rendezett halmaz legnagyobb eleme, vagyis $\mathbf{0}^{\perp} = \mathbf{1}$. Ebből az $(\mathrm{ORT_I})$ alkalmazásával nyerjük, hogy $\mathbf{1}^{\perp} = (\mathbf{0}^{\perp})^{\perp} = \mathbf{0}$.

b) Ha $e, f \in L$, $f \leq e$ és $f \leq e^{\perp}$, akkor az $(\mathrm{ORT_I})$ és $(\mathrm{ORT_{II}})$ alapján $e^{\perp} \leq f^{\perp}$ és $e = (e^{\perp})^{\perp} \leq f^{\perp}$, tehát $f^{\perp}$ felső korlátja az $\{e, e^{\perp}\}$ halmaznak, így az $(\mathrm{ORT_{III}})$ szerint $f^{\perp} = \mathbf{1}$. Ebből az $(\mathrm{ORT_I})$ és az a) alkalmazásával $f = (f^{\perp})^{\perp} = \mathbf{1}^{\perp} = \mathbf{0}$ adódik.

c) Tegyük fel, hogy $(e_i)_{i \in I}$ olyan L-ben haladó rendszer, amelynek létezik a szuprémuma;

legyen $e := \sup_{i \in I} e_i$. Megmutatjuk, hogy $e^\perp$ az $(e_i^\perp)_{i\in I}$ rendszer infimuma L-ben, vagyis a legnagyobb alsó korlátja. Valóban, minden $i \in I$ esetén $e_i \leq e$, ezért az ($\mathrm{ORT_{II}}$) alapján $e^\perp \leq e_i^\perp$, tehát $e^\perp$ alsó korlátja az $(e_i^\perp)_{i\in I}$ rendszernek. Ha $f \in L$ alsó korlátja az $(e_i^\perp)_{i\in I}$ rendszernek, akkor minden $I \ni i$-re $f \leq e_i^\perp$, így az ($\mathrm{ORT_I}$) és ($\mathrm{ORT_{II}}$) alapján $e_i = (e_i^\perp)^\perp \leq f^\perp$, így $e \leq f^\perp$, hiszen e az $(e_i^\perp)_{i\in I}$ rendszer legkisebb felső korlátja; ezért ismét az ($\mathrm{ORT_I}$) és ($\mathrm{ORT_{II}}$) alkalmazásával kapjuk, hogy $f = (f^\perp)^\perp \leq e^\perp$. Tehát $e^\perp$ az $(e_i^\perp)_{i\in I}$ rendszer legnagyobb alsó korlátja L-ben.

d) Tegyük fel, hogy $(e_i)_{i\in I}$ olyan L-ben haladó rendszer, amelynek létezik a infimuma; legyen $e := \inf_{i\in I} e_i$. Megmutatjuk, hogy $e^\perp$ az $(e_i^\perp)_{i\in I}$ rendszer szuprémuma L-ben, vagyis a legkisebb felső korlátja. Valóban, minden $i \in I$ esetén $e \leq e_i$, ezért az ($\mathrm{ORT_{II}}$) alapján $e_i^\perp \leq e^\perp$, tehát $e^\perp$ felső korlátja az $(e_i^\perp)_{i\in I}$ rendszernek. Ha $f \in L$ felső korlátja az $(e_i^\perp)_{i\in I}$ rendszernek, akkor minden $I \ni i$-re $e_i^\perp \leq f$, így az ($\mathrm{ORT_I}$) és ($\mathrm{ORT_{II}}$) alapján $f^\perp \leq (e_i^\perp)^\perp = e_i$, így $f^\perp \leq e$, hiszen e az $(e_i^\perp)_{i\in I}$ rendszer legnagyobb alsó korlátja; ezért ismét az ($\mathrm{ORT_I}$) és ($\mathrm{ORT_{II}}$) alkalmazásával kapjuk, hogy $e^\perp \leq (f^\perp)^\perp = f$. Tehát $e^\perp$ az $(e_i^\perp)_{i\in I}$ rendszer legkisebb felső korlátja L-ben. ■

22.5.4. Következmény. *Korlátos disztributív háló felett legfeljebb egy ortokomplementáció létezik.*

Bizonyítás. Legyen L korlátos disztributív háló. Az ($\mathrm{ORT_{III}}$) feltétel és az előző állítás b) pontja alapján elegendő azt igazolni, hogy minden $e \in L$ esetén legfeljebb egy olyan $e' \in L$ létezik, amelyre $e \wedge e' = \mathbf{0}$ és $e \vee e' = \mathbf{1}$. Valóban, legyen $e \in L$ rögzített elem, és $f, g \in L$ olyanok, hogy $e \vee f = e \vee g = \mathbf{1}$ és $e \wedge f = e \wedge g = \mathbf{0}$. L disztributivitása folytán

$$g = g \wedge (e \vee g) = g \wedge (e \vee f) = (g \wedge e) \vee (g \wedge f) = \mathbf{0} \vee (g \wedge f) = g \wedge f \leq f,$$

tehát $g \leq f$. Szintén az L disztributivitása miatt

$$f = f \wedge (e \vee f) = f \wedge (e \vee g) = (f \wedge e) \vee (f \wedge g) = \mathbf{0} \vee (f \wedge g) = f \wedge g \leq g,$$

tehát $f \leq g$. Ebből következik, hogy $f = g$. ■

Figyeljük meg, hogy az előző állítás bizonyításában megmutattuk, hogy ha L alulról korlátos disztributív háló és $e, f, g \in L$ olyanok, hogy $e \vee f = e \vee g$ és $e \wedge f = e \wedge g = \mathbf{0}$, akkor $f = g$.

Könnyen látható, hogy ha L ortoháló és $(e, f) \in L \times L$ ortogonális pár, akkor $e \wedge f = \mathbf{0}$, de ha $e, f \in L$ olyanok, hogy $e \wedge f = \mathbf{0}$, akkor (e, f) nem szükségképpen ortogonális pár. Azonban Boole-háló esetében az $e \wedge f = \mathbf{0}$ és $e \perp f$ összefüggések ekvivalensek, mert ha $e \wedge f = \mathbf{0}$, akkor

$$e \leq f^\perp \vee e = (f^\perp \vee e) \wedge \mathbf{1} = (f^\perp \vee e) \wedge (f^\perp \vee f) = f^\perp \vee (e \wedge f) = f^\perp \vee \mathbf{0} = f^\perp,$$

vagyis $e \leq f^\perp$.

22.6. Boole-hálók reprezentációs tétele*

22.6.1. Definíció. *Ha E halmaz, akkor $\mathscr{A} \subseteq \mathscr{P}(E)$ halmazt E feletti* **halmazalgebrának** *nevezünk, ha $E \in \mathscr{A}$, és minden $X, Y \in \mathscr{A}$ esetén $X \cup Y \in \mathscr{A}$ és $X \setminus Y \in \mathscr{A}$.*

Nyilvánvaló, hogy ha $\mathscr{A}$ halmazalgebra az E halmaz felett, akkor:

– $\emptyset = E \setminus E \in \mathscr{A}$;

– $X, Y \in \mathscr{A}$ esetén $X \cap Y = (X \cup Y) \setminus ((X \setminus Y) \cup (Y \setminus X)) \in \mathscr{A}$, tehát $\mathscr{A}$ olyan halmazfélgyűrű E felett, amelynek $\emptyset$ a legkisebb és E a legnagyobb eleme;

– az $\mathscr{A} \to \mathscr{A}$; $X \mapsto E \setminus X$ leképezés (az egyetlen) ortokomplementáció az $\mathscr{A}$ korlátos disztributív háló felett, tehát $\mathscr{A}$ Boole-háló.

22.6.2. Állítás. *Ha B Boole-háló és $\mathfrak{p}$ ideál B-ben, akkor a következő állítások ekvivalensek.*

(i) *$\mathfrak{p}$ maximális valódi ideál B-ben.*

(ii) *$\mathfrak{p}$ prímideál B-ben, vagyis $\mathfrak{p} \in \mathrm{Spec}(B)$.*

(iii) *$\mathfrak{p} \neq B$ és $\mathfrak{p} \cup \mathfrak{p}^{\perp} = B$, vagyis minden $e \in B$ esetén $e \in \mathfrak{p}$ vagy $e^{\perp} \in \mathfrak{p}$.*

Bizonyítás. (i)⇒(ii) A 22.4.4. állítás szerint ez minden disztributív hálóra igaz.

(ii)⇒(iii) Ha $e \in B$ olyan, hogy $e \notin \mathfrak{p}$ és $e^{\perp} \notin \mathfrak{p}$, akkor $\mathfrak{p} \in \mathrm{Spec}(B)$ esetén $\mathbf{0} = e \wedge e^{\perp} \notin \mathfrak{p}$, holott $\mathbf{0}$ a B háló minden ideáljának eleme.

(iii)⇒(i) Ha $\mathfrak{q}$ olyan ideál B-ben, hogy $\mathfrak{p} \subseteq \mathfrak{q}$ és $e \in \mathfrak{q}$ olyan elem, hogy $e \notin \mathfrak{p}$, akkor (iii) szerint $e^{\perp} \in \mathfrak{p}$, ezért $\mathbf{1} = e \vee e^{\perp} \in \mathfrak{q}$, így $\mathfrak{q} = B$. ■

22.6.3. Tétel. *Legyen B Boole-háló.*

a) *Az $\mathscr{S}_B : B \to \mathscr{P}(\mathrm{Spec}(B))$ Stone-reprezentáció értékkészlete halmazalgebra a $\mathrm{Spec}(B)$ halmaz felett, és $\mathscr{S}_B$ ortoizomorfizmus B és $\mathrm{Im}(\mathscr{S}_B)$ között.*

b) *$\mathrm{Im}(\mathscr{S}_B)$ egyenlő a $\mathrm{Spec}(B)$ Stone-tér nyílt-zárt részhalmainak halmazával és a $\mathrm{Spec}(B)$ Stone-tér teljesen összefüggéstelen kompakt Hausdorff-tér.*

Bizonyítás. a) A Stone-féle reprezentációs tétel (22.4.6.) szerint $\mathrm{Im}(\mathscr{S}_B)$ halmazfélgyűrű $\mathrm{Spec}(B)$ felett, és tudjuk, hogy $\mathscr{S}_B(\mathbf{0}) = \emptyset$ és $\mathscr{S}_B(\mathbf{1}) = \mathrm{Spec}(B)$. Szintén a Stone-féle reprezentációs tétel szerint az $\mathscr{S}_B : B \to \mathscr{P}(\mathrm{Spec}(B))$ Stone-reprezentáció izomorfizmus a B háló és az $\mathrm{Im}(\mathscr{S}_B)$ halmazfélgyűrű között. Ezért elég azt igazolni, hogy minden $e \in B$ esetén $\mathscr{S}_B(e^{\perp}) = \mathrm{Spec}(B) \setminus \mathscr{S}_B(e)$, hiszen ha ez igaz, akkor $\mathrm{Im}(\mathscr{S}_B)$ zárt az alaphalmazra vonatkozó komplementum-képzésre nézve, vagyis $\mathrm{Im}(\mathscr{S}_B)$ halmazalgebra a $\mathrm{Spec}(B)$ halmaz felett, és az $\mathscr{S}_B$ Stone-reprezentáció ortokomplementáció-tartó, következésképpen ortoizomorfizmus a B és $\mathrm{Im}(\mathscr{S}_B)$ Boole-hálók között.

Legyen tehát $e \in B$ rögzített elem. Ha $\mathfrak{p} \in \mathrm{Spec}(B)$, akkor az előző állítás szerint $e \in \mathfrak{p}$ *vagy* $e^{\perp} \in \mathfrak{p}$. Ugyanakkor $e \in \mathfrak{p}$ *és* $e^{\perp} \in \mathfrak{p}$ nem lehet igaz, különben $\mathbf{1} = e \vee e^{\perp} \in \mathfrak{p}$ teljesülne, tehát $\mathfrak{p} = B$ igaz volna, holott $\mathfrak{p}$ valódi ideál B-ben. Ebből a Stone-reprezentáció definícióját alkalmazva következik, hogy

$$\mathfrak{p} \in \mathscr{S}_B(e^{\perp}) \Leftrightarrow e^{\perp} \notin \mathfrak{p} \Leftrightarrow e \in \mathfrak{p} \Leftrightarrow \mathfrak{p} \notin \mathscr{S}_B(e) \Leftrightarrow \mathfrak{p} \in \mathrm{Spec}(B) \setminus \mathscr{S}_B(e),$$

ami azt jelenti, hogy $\mathscr{S}_B(e^{\perp}) = \mathrm{Spec}(B) \setminus \mathscr{S}_B(e)$.

b) Mivel B olyan disztributív háló, amelynek létezik legnagyobb eleme, így 22.4.9. szerint a $\mathrm{Spec}(B)$ Stone-tér kompakt T_0-tér.

Megmutatjuk, hogy a Stone-topológia Hausdorff-topológia $\mathrm{Spec}(B)$ felett. Legyenek $\mathfrak{p}$, $\mathfrak{p}' \in \mathrm{Spec}(B)$ olyanok, hogy $\mathfrak{p} \neq \mathfrak{p}'$. Ekkor $\mathfrak{p}' \not\subseteq \mathfrak{p}$ vagy $\mathfrak{p} \not\subseteq \mathfrak{p}'$. Tegyük fel, hogy $e \in \mathfrak{p}'$ és $e \notin \mathfrak{p}$. Ekkor $\mathscr{S}_B(e)$ olyan nyílt-zárt környezete $\mathfrak{p}'$-nek, hogy $\mathfrak{p} \notin \mathscr{S}_B(e)$, vagyis $\mathfrak{p} \in \mathrm{Spec}(B) \setminus \mathscr{S}_B(e) = \mathscr{S}_B(e^{\perp})$. Tehát $\mathscr{S}_B(e)$, illetve $\mathscr{S}_B(e^{\perp})$ diszjunkt nyílt környezetei

$\mathfrak{p}'$-nek, illetve $\mathfrak{p}$-nek. Ebből $\mathfrak{p}$ és $\mathfrak{p}'$ felcserélésével nyerjük, hogy ha $e \in \mathfrak{p}$ és $e \notin \mathfrak{p}'$, akkor $\mathscr{S}_B(e)$, illetve $\mathscr{S}_B(e^\perp)$ diszjunkt nyílt környezetei $\mathfrak{p}$-nek, illetve $\mathfrak{p}'$-nek.

A Stone-topológia definíciója szerint minden $e \in B$ esetén $\mathscr{S}_B(e)$ nyílt részhalmaza $\mathrm{Spec}(B)$-nek, ezért a) alapján a $\mathrm{Spec}(B) \setminus \mathscr{S}_B(e) = \mathscr{S}_B(e^\perp)$ halmaz is nyílt, vagyis $\mathscr{S}_B(e)$ zárt is a Stone-topológia szerint.

Legyen $\Omega \subseteq \mathrm{Spec}(B)$ a Stone-topológia szerint nem triviális nyílt-zárt halmaz. Mivel az $(\mathscr{S}_B(e))_{e\in B}$ halmazrendszer topologikus bázisa a Stone-topológiának, így létezik olyan B-ben haladó $(e_i)_{i\in I}$ nem üres rendszer, hogy $\Omega = \bigcup\limits_{i\in I} \mathscr{S}_B(e_i)$. Az Ω halmaz zárt a Stone-topológia szerint és B-nek létezik legnagyobb eleme, így a Stone-tétel szerint a $\mathrm{Spec}(B)$ halmaz feletti Stone-topológia kompakt Hausdorff-topológia. Ezért Ω kompakt halmaz a Stone-topológia szerint, és az $(\mathscr{S}_B(e_i))_{i\in I}$ halmazrendszer nyílt befedése Ω-nak. Ezért van olyan $J \subseteq I$ nem üres véges halmaz, hogy $\Omega = \bigcup\limits_{i\in J} \mathscr{S}_B(e_i)$. A Stone-reprezentáció izomorfizmus a B háló és az $\mathrm{Im}(\mathscr{S}_B)$ halmazfélgyűrű között, ezért $\bigcup\limits_{i\in J} \mathscr{S}_B(e_i) = \mathscr{S}_B\Big(\bigvee\limits_{i\in J} e_i\Big)$. Tehát az $e := \bigvee\limits_{i\in J} e_i$ elemre $\Omega = \mathscr{S}_B(e) \in \mathrm{Im}(\mathscr{S}_B)$ teljesül. ■

22.7. Ortomoduláris hálók

22.7.1. Definíció. *Az L ortohálót* **ortomodulárisnak** *nevezzük, ha L minden ortogonális elempárja moduláris pár.*

Világos, hogy minden moduláris ortoháló ortomoduláris, tehát az ortohálók körében az ortomodularitás a modularitás gyengítése. Azonban létezik nem moduláris ortomoduláris háló. Például, ha $\mathscr{H}$ végtelen dimenziós Hilbert-tér, akkor a $\mathscr{H}$ zárt lineáris altereinek halmaza a $\subseteq$ relációval és az altér-ortokomplementációval ellátva nem moduláris ortomoduláris háló.

Vigyázzunk arra, hogy a modularitás fogalmát tetszőleges hálóra értelmezzük, de az ortomodularitás az ortokomplementációhoz kötött fogalom.

22.7.2. Állítás. (**Az ortomodularitás jellemzése**) *Ha L ortoháló, akkor a következő állítások ekvivalensek.*

(i) *L ortomoduláris.*

(ii) *Minden $e \in L$ esetén az $(e, e^\perp)$ pár moduláris.*

(iii) *Minden $e, f \in L$ esetén, ha $e \leq f$, akkor $e \vee (e^\perp \wedge f) = f$.*

(iv) *Minden $e, f \in L$ esetén, ha $e \leq f$, akkor létezik olyan $g \in L$, amelyre $e \perp g$ és $e \vee g = f$.*

(v) *Minden $e, f, g \in L$ esetén, ha $e \leq f$, $e \perp g$ és $e \vee g = f$, akkor $g = e^\perp \wedge f$.*

(vi) *Minden $e, f \in L$ esetén, ha $e \perp f$ és $e \vee f = \mathbf{1}$, akkor $f = e^\perp$.*

Bizonyítás. (i)⇒(ii) Nyilvánvaló, mert az $(\mathrm{ORT_I})$ alapján minden $L \ni e$-re $e = (e^\perp)^\perp$, tehát az $(e, e^\perp)$ pár ortogonális.

(ii)⇒(iii) Legyenek $e, f \in L$ olyanok, hogy $e \leq f$. Az $(\mathrm{ORT_{II}})$ alapján $f^\perp \leq e^\perp$ és a (ii) szerint az $(e, e^\perp)$ pár moduláris, ezért $f^\perp = f^\perp \vee \mathbf{0} = f^\perp \vee (e \wedge e^\perp) = (f^\perp \vee e) \wedge e^\perp$. Ebből a de Morgan-egyenlőség és az $(\mathrm{ORT_I})$ alkalmazásával $f = (f^\perp)^\perp = ((f^\perp)^\perp \wedge e^\perp) \vee (e^\perp)^\perp = (f \wedge e^\perp) \vee e = e \vee (e^\perp \wedge f)$ következik.

(iii)⇒(iv) Ha $e, f \in L$ és $e \leq f$, akkor $g := e^\perp \wedge f$ a (iii) alapján olyan, hogy $e \vee g = f$ és $g \leq e^\perp$, vagyis $g \perp e$.

(iv)⇒(v) Legyenek $e, f, g \in L$ olyanok, hogy $e \leq f$, $e \perp g$ és $e \vee g = f$. Ekkor $e \leq g^\perp$, tehát az $(\mathrm{ORT_I})$ és $(\mathrm{ORT_{II}})$ alapján $g = (g^\perp)^\perp \leq e^\perp$. Továbbá $g \leq e \vee g = f$, tehát $g \leq e^\perp \wedge f$. Ezért a (iv) alapján van olyan $h \in L$, hogy $g \perp h$ és $g \vee h = e^\perp \wedge f$; megmutatjuk, hogy $h = \mathbf{0}$, amiből következik a bizonyítandó $g = e^\perp \wedge f$ egyenlőség. A h-ra vonatkozó feltételek alapján $h \leq g \vee h \leq e^\perp$ és $g \perp h$ miatt $h \perp g$, vagyis $h \leq g^\perp$. Ezért a de Morgan-egyenlőtlenség alkalmazásával $h \leq e^\perp \wedge g^\perp = (e \vee g)^\perp = f^\perp$. Ugyanakkor $h \leq g \vee h \leq f$, így $h \leq f \wedge f^\perp = \mathbf{0}$, vagyis $h = \mathbf{0}$.

(v)⇒(vi) A (vi) állítás az (v)-ből alkalmas szereposztással nyilvánvalóan következik.

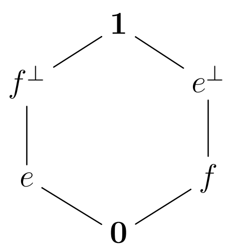
(vi)⇒(i) Legyenek $e, f \in L$ és $g \in L$ olyanok, hogy $e \perp f$ és $g \leq f$. Azt kell igazolni, hogy ha (vi) teljesül, akkor $g \vee (e \wedge f) = (g \vee e) \wedge f$, ami $e \wedge f = \mathbf{0}$ miatt azzal egyenértékű, hogy $g = (g \vee e) \wedge f$. Az nyilvánvaló, hogy fennáll a $g \leq (g \vee e) \wedge f$ egyenlőtlenség, ami az $(\mathrm{ORT_I})$ miatt úgy is írható, hogy $g \perp ((g \vee e) \wedge f)^\perp$. Ha $g \vee ((g \vee e) \wedge f)^\perp = \mathbf{1}$ teljesülne, akkor a (vi)-ból és $(\mathrm{ORT_I})$-ből következne, hogy $g = (((g \vee e) \wedge f)^\perp)^\perp = (g \vee e) \wedge f$, es éppen ezt kell igazolni. A $g \vee ((g \vee e) \wedge f)^\perp = \mathbf{1}$ egyenlőség bizonyításához háromszor alkalmazva a de Morgan-egyenlőtlenséget és kihasználva, hogy $e^\perp \geq f$ kapjuk, hogy

$$g \vee ((g \vee e) \wedge f)^\perp = g \vee ((g \vee e)^\perp \vee f^\perp) = g \vee ((g^\perp \wedge e^\perp) \vee f^\perp) = (g \vee f^\perp) \vee (g^\perp \wedge e^\perp) \geq$$
$$\geq (g \vee f^\perp) \vee (g^\perp \wedge f) = (g^\perp \wedge f)^\perp \vee (g^\perp \wedge f) = \mathbf{1},$$

tehát $g \vee ((g \vee e) \wedge f)^\perp = \mathbf{1}$. ■

Könnyen igazolható az ortomodularitás következő jellemzése: az L ortoháló pontosan akkor ortomoduláris, ha *nem léteznek* olyan $e, f \in L$ elemek, amelyekre $\mathbf{0} < e < f < \mathbf{1}$ és $e \wedge f^\perp = \mathbf{0}$.

Nem ortomoduláris ortohálóra példát ad a következő Hasse-diagram:



Ez valóban nem ortomoduláris, mert $e \vee f = \mathbf{1}$, következésképpen

$$e \vee (e^\perp \wedge f^\perp) = e \vee (e \vee f)^\perp = e \vee \mathbf{1}^\perp = e \vee \mathbf{0} = e < f^\perp.$$

Ezt a nem ortomoduláris ortohálót az O_6 szimbólummal jelöljük.

Világos, hogy ortomoduláris háló minden ortorészhálója ortomoduláris háló, továbbá ortoizomorf ortohálók egyszerre ortomodulárisak, vagy nem ortomodulárisak. Ezért ortomoduláris hálónak nem létezik olyan ortorészhálója, amely ortoizomorf O_6-tal. Ennek megfordítása is igaz.

22.7.3. Tétel. *Ortoháló pontosan akkor ortomoduláris, ha nem létezik olyan ortorészhálója, amely ortoizomorf az* O_6 *ortohálóval.*

Bizonyítás. Legyen L nem ortomoduláris háló. Megmutatjuk, hogy L-nek létezik O_6-tal ortoizomorf ortorészhálója. Valóban, mivel L nem ortomoduláris, így vehetünk olyan

$a, b \in L$ elemeket, amelyekre $a \le b$ és $a \vee \big(a^\perp \wedge b\big) < b$. Ekkor $a < b$, mert $a = b$ esetén $a \vee \big(a^\perp \wedge b\big) = a \vee \big(a^\perp \wedge a\big) = a \vee \mathbf{0} = a = b$ teljesülne. Ebből azonnal következik, hogy $b^\perp < a^\perp$. Világos, hogy $a^\perp \le b \vee a^\perp$ és $a \le a \vee \big(a^\perp \wedge b\big) \le b \le b \vee a^\perp$, ezért $\mathbf{1} = a^\perp \vee a \le b \vee a^\perp$, így $b \vee a^\perp = \mathbf{1}$. A de Morgan egyenlőség alapján ebből $a \wedge b^\perp = \big(b \vee a^\perp\big)^\perp = \mathbf{1}^\perp = \mathbf{0}$ következik. Nyilvánvaló, hogy $b < \mathbf{1}$, különben $a \vee \big(a^\perp \wedge b\big) = a \vee a^\perp = \mathbf{1} = b$ teljesülne. Ebből következik, hogy $a \wedge b^\perp = \mathbf{0} < b^\perp < a^\perp$. Végül, $a^\perp < \mathbf{1}$, különben $a = \mathbf{0}$, így $a \vee \big(a^\perp \wedge b\big) = \mathbf{0} \vee (\mathbf{1} \wedge b) = b$ teljesülne. Tehát $e := a$ és $f := b^\perp$ olyan elemek, hogy a $\{\mathbf{0}, e, f, e^\perp, f^\perp, \mathbf{1}\}$ halmaz O_6-tal ortoizomorf ortorészhálója L-nek. ■

22.8. Ortomoduláris háló σ-teljessége

22.8.1. Állítás. (**Ortomoduláris háló monoton disztributivitása**) *Legyen L ortomoduláris háló, $(f_i)_{i\in I}$ monoton növő általánosított sorozat L-ben, és $g \in L$ olyan elem, amelyhez létezik olyan $i \in I$, hogy $g \le f_i$. Ekkor $\sup_{i\in I} f_i$ pontosan akkor létezik L-ben, ha $\sup_{i\in I}(f_i \wedge g^\perp)$ létezik L-ben. Továbbá, ha $\sup_{i\in I} f_i$ létezik L-ben, akkor*

$$\Big(\sup_{i\in I} f_i\Big) \wedge g^\perp = \sup_{i\in I}(f_i \wedge g^\perp).$$

Bizonyítás. (I) Tegyük fel, hogy $f := \sup_{i\in I} f_i$ létezik L-ben. Minden $I \ni i$-re $f_i \le f$, ezért $f_i \wedge g^\perp \le f \wedge g^\perp$, vagyis $f \wedge g^\perp$ felső korlátja az $(f_i \wedge g^\perp)_{i\in I}$ rendszernek. Legyen $h \in L$ tetszőleges felső korlátja a $(f_i \wedge g^\perp)_{i\in I}$ rendszernek. Ekkor minden $i \in I$ esetén $f_i \wedge g^\perp \le h \wedge g^\perp$. Rögzítsünk olyan $i_0 \in I$ indexet, amelyre minden $i \in I$ esetén, ha $i \ge i_0$, akkor $g \le f_i$. Ha $i \in I$ és $i \ge i_0$, akkor az L ortomodularitása és $g \le f_i$ miatt

$$f_i = g \vee (f_i \wedge g^\perp) \le g \vee (h \wedge g^\perp),$$

következésképpen $f := \sup_{i\in I} f_i = \sup_{\substack{i\in I \\ i_0 \le i}} f_i \le g \vee (h \wedge g^\perp)$, hiszen az $(f_i)_{i\in I}$ általánosított sorozat monoton növő. Ugyanakkor $h \wedge g^\perp \le g^\perp$, tehát $g \le (h \wedge g^\perp)^\perp$, így ismét az L ortomodularitása szerint $(h \wedge g^\perp)^\perp = g \vee (g^\perp \wedge (h \wedge g^\perp)^\perp) = g \vee (g^\perp \wedge (h^\perp \vee g))$. Ebből ortokomplementálással kapjuk, hogy $h \wedge g^\perp = g^\perp \wedge (g \vee (h \wedge g^\perp))$. Ezért $f \wedge g^\perp \le g^\perp \wedge (g \vee (h \wedge g^\perp)) = h \wedge g^\perp \le h$, vagyis $f \wedge g^\perp$ a legkisebb felső korlátja az $(f_i \wedge g^\perp)_{i\in I}$ rendszernek.

(II) Tegyük fel, hogy $f' := \sup_{i\in I}(f_i \wedge g^\perp)$ létezik. Ismét legyen $i_0 \in I$ olyan, hogy minden $I \ni i$-re, ha $i \ge i_0$, akkor $g \le f_i$, tehát az L ortomodularitása miatt $f_i = g \vee (f_i \wedge g^\perp) \le g \vee f'$. Ebből az I előrendezett halmaz felfelé irányítottsága és az $(f_i)_{i\in I}$ rendszer monoton növése alapján kapjuk, hogy minden $I \ni i$-re $f_i \le g \vee f'$, vagyis $g \vee f'$ felső korlátja az $(f_i)_{i\in I}$ rendszernek. Tegyük fel, hogy $h \in L$ felső korlátja az $(f_i)_{i\in I}$ rendszernek. Ekkor $i \in I$ esetén $f_i \wedge g^\perp \le h \wedge g^\perp$, tehát $f' \le h \wedge g^\perp \le h$. Ugyanakkor $g \le f_{i_0} \le h$, tehát $g \vee f' \le h$, ami azt jelenti, hogy $g \vee f'$ az $(f_i)_{i\in I}$ rendszer legkisebb felső korlátja, vagyis létezik a $\sup_{i\in I} f_i$ elem L-ben. ■

22.8.2. Definíció. *Az L ortohálót* **σ-additívnak** *nevezzük, ha minden L-ben haladó ortogonális sorozatnak létezik szuprémuma L-ben. Az L hálót* **σ-teljesnek** (*illetve* **teljesnek**) *nevezzük, ha minden L-ben haladó sorozatnak* (*illetve L-ben haladó rendszernek*) *létezik szuprémuma L-ben.*

Nyilvánvaló, hogy minden σ-teljes ortoháló σ-additív. A következő állítás szerint ennek megfordítása is igaz, ha L ortomoduláris, vagyis az ortomoduláris hálók körében a σ-teljesség és σ-additivitás ekvivalens tulajdonságok.

22.8.3. Állítás. *Ortomoduláris háló pontosan akkor σ-teljes, ha σ-additív.*

Bizonyítás. Legyen L σ-additív ortomoduláris háló, és $(e_k)_{k\in\mathbb{N}}$ tetszőleges L-ben haladó sorozat. Legyen $f_0 := e_0$, és minden $\mathbb{N}^* \ni n$-re

$$f_n := \Big(\sup_{0\le k\le n} e_k\Big) \wedge \Big(\sup_{0\le k\le n-1} e_k\Big)^{\perp}.$$

Könnyen látható, hogy $(f_n)_{n\in\mathbb{N}}$ ortogonális sorozat L-ben, mert $m,n \in \mathbb{N}$ és $m < n$ esetén

$$f_m \le \sup_{0\le k\le m} e_k \le \sup_{0\le k\le n-1} e_k \le \Big(\sup_{0\le k\le n} e_k\Big)^{\perp} \vee \Big(\sup_{0\le k\le n-1} e_k\Big) = f_n^{\perp}.$$

Teljes indukcióval igazoljuk, hogy minden $n\in\mathbb{N}$ esetén $\sup\limits_{0\le k\le n} e_k = \sup\limits_{0\le k\le n} f_k$. Ez $n = 0$ esetén igaz; tegyük fel, hogy $n \in \mathbb{N}^*$ és $\sup\limits_{0\le k\le n} e_k = \sup\limits_{0\le k\le n} f_k$. Ekkor

$$\sup_{0\le k\le n+1} f_k = \Big(\sup_{0\le k\le n} e_k\Big) \vee f_{n+1} =$$

$$= \Big(\sup_{0\le k\le n} e_k\Big) \vee \bigg(\Big(\sup_{0\le k\le n+1} e_k\Big) \wedge \Big(\sup_{0\le k\le n} e_k\Big)^{\perp}\bigg) = \sup_{0\le k\le n+1} e_k,$$

ahol az utolsó egyenlőségnél kihasználtuk az L ortomodularitását. Az L σ-additivitása folytán $\sup\limits_{k\in\mathbb{N}} f_k$ létezik L-ben, ezért az imént bizonyított egyenlőségből következik, hogy $\sup\limits_{k\in\mathbb{N}} e_k$ is létezik L-ben (és még $\sup\limits_{k\in\mathbb{N}} e_k = \sup\limits_{k\in\mathbb{N}} f_k$ is teljesül). ■

22.9. σ-teljes Boole-hálók reprezentációs tétele

22.10. Ortoállapotok és ortoháló duálisa*

22.10.1. Definíció. *Ha L ortoháló, akkor egy $p : L \to [0,1]$ függvényt L feletti* **ortoállapotnak** *nevezünk, ha $p(\mathbf{1}) = 1$ és minden $e, f \in L$ esetén, ha $e \perp f$, akkor $p(e \vee f) = p(e) + p(f)$. Az L ortoháló feletti ortoállapotok halmazát L^* jelöli, és ezt a halmazt az L ortoháló* **duálisának** *nevezzük.*

Nyilvánvaló, hogy ha L ortoháló, és $p \in L^*$, akkor $p(\mathbf{0}) = 0$, mert $(\mathbf{0},\mathbf{0})$ ortogonális pár L-ben, tehát $p(\mathbf{0}) = p(\mathbf{0}\vee\mathbf{0}) = p(\mathbf{0}) + p(\mathbf{0})$. Könnyen látható továbbá, hogy ha L ortoháló és $p \in L^*$, akkor minden L-ben haladó $(e_i)_{i\in I}$ *véges ortogonális* rendszerre

$$p\Big(\sup_{i\in I} e_i\Big) = \sum_{i\in I} p(e_i)$$

teljesül; ez az I indexhalmaz számossága szerinti teljes indukcióval igazolható.

22.10.2. Állítás. *Legyen L ortoháló és $p \in L^*$.*

a) *Ha $e \in L$, akkor $p(e^{\perp}) = 1 - p(e)$.*

b) *Ha $e, f \in L$ és $e \le f$, akkor $p(e) \le p(f)$, vagyis p monoton növő.*

c) *Ha L ortomoduláris, akkor $e, f \in L$ és $e \le f$ esetén $p(f \wedge e^{\perp}) = p(f) - p(e)$, vagyis p szubtraktív.*

Bizonyítás. a) Ha $e \in L$, akkor $e \perp e^{\perp}$ és $e \vee e^{\perp} = \mathbf{1}$, ezért $1 = p(\mathbf{1}) = p(e \vee e^{\perp}) = p(e) + p(e^{\perp})$.

b) Ha $e, f \in L$ és $e \leq f$, akkor $e \perp f^{\perp}$, ezért az a) szerint $1 \geq p(e \vee f^{\perp}) = p(e) + p(f^{\perp}) = p(e) + 1 - p(f)$, amiből $p(f) \geq p(e)$ következik.

c) Ha L ortomoduláris, akkor $e, f \in L$ és $e \leq f$ esetén $e \vee (e^{\perp} \wedge f) = f$ és $e \perp e^{\perp} \wedge f$, tehát fennáll a $p(f) = p(e) + p(e^{\perp} \wedge f)$ egyenlőség. ■

A következő állítás szerint az ortomodularitás *szükséges* ahhoz, hogy egy ortoháló felett "elég sok" ortoállapot létezzen.

22.10.3. Állítás. *Ha L olyan ortoháló, hogy L^* szétválasztja az L pontjait, vagyis minden $e, f \in L$, $e \neq f$ esetén van olyan $p \in L^*$, hogy $p(e) \neq p(f)$, akkor L ortomoduláris.*

Bizonyítás. Tegyük fel, hogy L *nem* ortomoduláris. Az ortomodularitás jellemzési tétele alapján ekkor léteznek olyan $e, f \in L$, hogy $e \perp f$ és $e \vee f = \mathbf{1}$, de $f \neq e^{\perp}$. Ha $p \in L^*$, akkor $1 = p(\mathbf{1}) = p(e \vee f) = p(e) + p(f)$, tehát $p(f^{\perp}) = 1 - p(f) = p(e)$, így az L^* halmaz az e és $f^{\perp}$ különböző elmeket nem választja szét, tehát L^* *nem* szétválasztó L felett. ■

Azonban van olyan véges alaphalmazú ortomoduláris háló, amely felett egyáltalán nem létezik ortoállapot, vagyis az ortomodularitás imént igazolt szükséges feltétele nem elégséges.

22.10.4. Állítás. *Ha L ortoháló, akkor L^* olyan kompakt konvex halmaz a pontonkénti konvergencia topológiájával ellátott $\mathscr{F}(L;\mathbb{R})$ függvénytérben, hogy minden $e \in L$ esetén az $L^* \to \mathbb{R}$; $p \mapsto p(e)$ leképezés folytonos.*

Bizonyítás. A definíció szerint $L^* \subseteq [0,1]^L$, és a Tyihonov-tétel (28.3.2.) alapján a $[0,1]^L$ halmaz kompakt a szorzattopológia szerint (természetesen a $[0,1]$ intervallumon az $\mathbb{R}$ euklidészi topológiájának leszűkítését véve). Az $\mathscr{F}(L;\mathbb{R})$ függvénytér feletti pontonkénti konvergencia topológiája megegyezik az $\mathbb{R}^L$ szorzattopológiájával, és könnyen látható, hogy ennek a topológiának $[0,1]^L$-re vett leszűkítése egyenlő a $[0,1]^L$ feletti szorzattopológiával. Ez azt jelenti, hogy a $[0,1]^L$ halmaz kompakt a pontonkénti konvergencia topológiájával ellátott $\mathscr{F}(L;\mathbb{R})$ függvénytérben, tehát L^* pontosan akkor kompakt, ha *zárt* a pontonkénti konvergencia topológiája szerint. Ez viszont az L^* értelmezése alapján triviális. ■

Legyen L ortoháló és $(e_k)_{k\in\mathbb{N}}$ olyan ortogonális sorozat L-ben, amelyre $\sup_{k\in\mathbb{N}} e_k$ létezik L-ben. Ekkor minden $p \in L^*$ esetén a $\sum_{k\in\mathbb{N}} p(e_k)$ valós sor konvergens $\mathbb{R}$-ben és

$$\sum_{k=0}^{\infty} p(e_k) \leq p\left(\sup_{k\in\mathbb{N}} e_k\right),$$

hiszen minden $\mathbb{N}^* \ni n$-re a p ortoadditivitása és monotonitása folytán

$$\sum_{k\in n} p(e_k) = p\Big(\sup_{k\in n} e_k\Big) \leq p\Big(\sup_{k\in\mathbb{N}} e_k\Big).$$

Azonban létezhet olyan $p \in L^*$, amelyhez van olyan $(e_k)_{k\in\mathbb{N}}$ ortogonális sorozat L-ben, hogy $\sup_{k\in\mathbb{N}} e_k$ létezik L-ben, de

$$\sum_{k=0}^{\infty} p(e_k) < p\Big(\sup_{k\in\mathbb{N}} e_k\Big).$$

Ilyen ortohálókra két fontos példát mutatunk a következőkben. Tehát kifejezetten tartalmas a következő definíció.

22.10.5. Definíció. *Ha L ortoháló, akkor egy $p \in L^*$ ortoállapotot* **σ-additívnak** *nevezünk, ha minden L-ben haladó $(e_k)_{k\in\mathbb{N}}$ ortogonális sorozatra, ha $\sup\limits_{k\in\mathbb{N}} e_k$ létezik L-ben, akkor*

$$\sum_{k=0}^{\infty} p(e_k) = p\left(\sup_{k\in\mathbb{N}} e_k\right).$$

Az L ortoháló feletti σ-additív ortoállapotok halmazát $L^\#$ jelöli.

22.10.6. Állítás. (**Ortoállapot σ-additivitásának jellemzése**) *Legyen L ortomoduláris háló és $p \in L^*$. A következő állítások ekvivalensek.*

(i) *Minden L-ben haladó $(e_k)_{k\in\mathbb{N}}$ monoton növő sorozatra, ha $\sup\limits_{k\in\mathbb{N}} e_k$ létezik L-ben, akkor*

$$p\Big(\sup_{k\in\mathbb{N}} e_k\Big) = \sup_{k\in\mathbb{N}} p(e_k).$$

(ii) *Minden L-ben haladó $(e_k)_{k\in\mathbb{N}}$ monoton fogyó sorozatra, ha $\inf\limits_{k\in\mathbb{N}} e_k$ létezik L-ben, akkor*

$$p\Big(\inf_{k\in\mathbb{N}} e_k\Big) = \inf_{k\in\mathbb{N}} p(e_k).$$

(iii) *Minden L-ben haladó $(e_k)_{k\in\mathbb{N}}$ monoton fogyó sorozatra, ha $\inf\limits_{k\in\mathbb{N}} e_k = \mathbf{0}$, akkor*

$$\inf_{k\in\mathbb{N}} p(e_k) = 0.$$

(iv) *Minden L-ben haladó $(e_k)_{k\in\mathbb{N}}$ ortogonális sorozatra, ha $\sup\limits_{k\in\mathbb{N}} e_k$ létezik L-ben, akkor*

$$\sum_{k=0}^{\infty} p(e_k) = p\Big(\sup_{k\in\mathbb{N}} e_k\Big)$$

(*vagyis a p ortoállapot σ-additív*).

Bizonyítás. (i)$\Rightarrow$(ii) Legyen $(e_k)_{k\in\mathbb{N}}$ olyan monoton fogyó L-ben haladó sorozat, amelyre $\inf\limits_{k\in\mathbb{N}} e_k$ létezik L-ben. Ekkor a de Morgan-tétel szerint az $(e_k^\perp)_{k\in\mathbb{N}}$ sorozat monoton növő L-ben, és $\sup\limits_{k\in\mathbb{N}} e_k^\perp$ létezik L-ben, valamint $\sup\limits_{k\in\mathbb{N}} e_k^\perp = (\inf\limits_{k\in\mathbb{N}} e_k)^\perp$. Ebből a p ortoadditivitása és az (i) alapján következik, hogy

$$\begin{aligned}1 - p\Big(\inf_{k\in\mathbb{N}} e_k\Big) &= p\bigg(\Big(\inf_{k\in\mathbb{N}} e_k\Big)^\perp\bigg) = p\Big(\sup_{k\in\mathbb{N}} e_k^\perp\Big) = \sup_{k\in\mathbb{N}} \, p(e_k^\perp) = \\ &= \sup_{k\in\mathbb{N}}(1 - p(e_k)) = 1 - \inf_{k\in\mathbb{N}} p(e_k),\end{aligned}$$

tehát $p\Big(\inf\limits_{k\in\mathbb{N}} e_k\Big) = \inf\limits_{k\in\mathbb{N}} p(e_k)$.

(ii)$\Rightarrow$(iii) Nyilvánvaló, mert $p(\mathbf{0}) = 0$.

(iii)$\Rightarrow$(iv) Legyen $(e_k)_{k\in\mathbb{N}}$ olyan ortogonális sorozat L-ben, amelyre $e := \sup\limits_{k\in\mathbb{N}} e_k$ létezik, továbbá minden $n \in \mathbb{N}$ esetén legyen $f_n := \sup\limits_{0\le k\le n} e_k$. Ekkor $(f_n)_{n\in\mathbb{N}}$ olyan monoton növő sorozat L-ben, amelyre $\sup_{n\in\mathbb{N}} f_n = \sup_{k\in\mathbb{N}} e_k$. Minden $\mathbb{N} \ni n$-re $f_n \leq e$, ezért az L ortomodularitása miatt $f_n \vee (f_n^\perp \wedge e) = e$ és persze $f_n \perp f_n^\perp \wedge e$, tehát a p ortoadditivitása folytán

$$\sum_{k=0}^{n} p(e_k) + p(f_n^\perp \wedge e) = p(f_n) + p(f_n^\perp \wedge e) = p(e) = p\Big(\sup_{k\in\mathbb{N}} e_k\Big).$$

Ebből látható, hogy a bizonyítandó

$$\sum_{k=0}^{\infty} p(e_k) = p\left(\sup_{k\in\mathbb{N}} e_k\right)$$

egyenlőség ekvivalens azzal, hogy $\lim_{n\to\infty} p(f_n^\perp \wedge e) = 0$. Ugyanakkor az $(f_n^\perp \wedge e)_{n\in\mathbb{N}}$ sorozat monoton fogyó L-ben, tehát a $(p(f_n^\perp \wedge e))_{n\in\mathbb{N}}$ valós számsorozat is monoton fogyó, így azt kell igazolni, hogy $\inf_{n\in\mathbb{N}} p(f_n^\perp \wedge e) = 0$. A (iii) alapján ehhez elegendő azt megmutatni, hogy $\inf_{n\in\mathbb{N}} (f_n^\perp \wedge e) = \mathbf{0}$. Ez viszont így van, mert ha $g \in L$ alsó korlátja az $(f_n^\perp \wedge e)_{n\in\mathbb{N}}$ sorozatnak, akkor minden $n \in \mathbb{N}$ esetén $g \leq f_n^\perp$, tehát $f_n \leq g^\perp$, így $e := \sup_{k\in\mathbb{N}} e_k = \sup_{n\in\mathbb{N}} f_n \leq g^\perp$, vagyis $g \leq e^\perp$, ugyanakkor $g \leq e$, következésképpen $g \leq e \wedge e^\perp = \mathbf{0}$, azaz $g = \mathbf{0}$.

(iv)$\Rightarrow$(i) Legyen $(e_k)_{k\in\mathbb{N}}$ monoton növő sorozat L-ben, és tegyük fel, hogy $\sup_{k\in\mathbb{N}} e_k$ létezik. Legyen $f_0 := e_0$ és minden $n \in \mathbb{N}^*$ esetén $f_n := e_n \wedge e_{n-1}^\perp$. Az $(f_n)_{n\in\mathbb{N}}$ sorozat ortogonális, mert $m, n \in \mathbb{N}$ és $m < n$ esetén az $(e_k)_{k\in\mathbb{N}}$ sorozat monoton növése miatt

$$f_n^\perp = (e_n \wedge e_{n-1}^\perp)^\perp = e_n^\perp \vee e_{n-1} \geq e_{n-1} \geq e_m \geq f_m,$$

azaz $f_m \perp f_n$. Teljes indukcióval könnyen igazolható, hogy minden $n \in \mathbb{N}$ esetén $\sup_{0\leq k\leq n} f_k = e_n$, hiszen ez igaz, ha $n = 0$, továbbá, ha az $n \in \mathbb{N}$ számra igaz, akkor $e_n \leq e_{n+1}$ és az L ortomodularitása miatt

$$e_{n+1} = e_n \vee (e_n^\perp \wedge e_{n+1}) = \Big(\sup_{0\leq k\leq n} f_k\Big) \vee f_{n+1} = \sup_{0\leq k\leq n+1} f_k.$$

Ezért $\sup_{n\in\mathbb{N}} f_n$ létezik L-ben és $\sup_{n\in\mathbb{N}} f_n = \sup_{k\in\mathbb{N}} e_k$. Az L ortomodularitása miatt p szubtraktív, így minden $k \in \mathbb{N}^*$ esetén $p(f_k) = p(e_k) - p(e_{k-1})$, ezért minden $\mathbb{N}^* \ni n$-re

$$\sum_{k=0}^{n} p(f_k) = p(f_0) + \sum_{k=1}^{n} p(f_k) = p(e_0) + \sum_{k=1}^{n} (p(e_k) - p(e_{k-1})) = p(e_n).$$

A (iv) feltételből következik, hogy

$$p\Big(\sup_{k\in\mathbb{N}} e_k\Big) = p\Big(\sup_{k\in\mathbb{N}} f_k\Big) = \sum_{k=0}^{\infty} p(f_k) =$$

$$= \sup_{n\in\mathbb{N}^*} \left(\sum_{k=0}^{n} p(f_k)\right) = \sup_{n\in\mathbb{N}^*} p(e_n) = \sup_{n\in\mathbb{N}} p(e_n),$$

amit bizonyítani kellett. ■

22.10.7. Állítás. *Legyen L olyan ortomoduláris háló, amelyre teljesülnek a következő állítások.*

a) *Minden* $e \in L \setminus \{\mathbf{0}\}$ *esetén* $\sup_{p \in L^{\#}} p(e) = 1$.

b) *Létezik olyan* $(e_n)_{n\in\mathbb{N}}$ *monoton fogyó sorozat* L*-ben, amelyre* $\inf_{n\in\mathbb{N}} e_n = \mathbf{0}$*, és minden* $\mathbb{N} \ni n$*-re* $e_n \neq \mathbf{0}$.

Ekkor az $L^* \setminus L^{\#}$ *halmaz nem üres, vagyis létezik* L *felett nem* σ*-additív ortoállapot.*

Bizonyítás. Megmutatjuk, hogy *nem létezik* olyan $L^{\#}$ feletti kompakt topológia, amely szerint minden $L \ni e$-re az $L^{\#} \to \mathbb{R}$; $p \mapsto p(e)$ leképezés folytonos. Tegyük fel, hogy az állítással ellentétben $\mathscr{T}$ ilyen tulajdonságú $L^{\#}$ feletti kompakt topológia. A b) alapján vegyünk olyan $(e_n)_{n\in\mathbb{N}}$ monoton fogyó sorozatot L-ben, amelyre $\inf_{n\in\mathbb{N}} e_n = \mathbf{0}$, és minden $\mathbb{N} \ni n$-re $e_n \neq \mathbf{0}$. Minden $\mathbb{N} \ni n$-re értelmezzük az $e_n^{\#} : L^{\#} \to \mathbb{R}$; $p \mapsto p(e_n)$ függvényt. Az indirekt hipotézis szerint minden $n \in \mathbb{N}$ esetén $e_n^{\#}$ folytonos a $\mathscr{T}$ topológia szerint. Ugyanakkor az $\left(e_n^{\#}\right)_{n\in\mathbb{N}}$ függvénysorozat monoton fogyó, és az ortoállapotok σ-additivitásának jellemzési tétele alapján ez a függvénysorozat az $L^{\#}$ halmazon pontonként konvergál az $L^{\#} \to \mathbb{R}$ azonosan 0 függvényhez, hiszen $p \in L^{\#}$ esetén a p ortoállapot σ-additivitása miatt $\inf_{n\in\mathbb{N}} e_n^{\#}(p) = \inf_{n\in\mathbb{N}} p(e_n) = 0$. A Dini-tételből (**TOP** 29.4.4.) következik, hogy az $\left(e_n^{\#}\right)_{n\in\mathbb{N}}$ függvénysorozat *egyenletesen konvergál* az $L^{\#}$ halmazon az $L^{\#} \to \mathbb{R}$ azonosan 0 függvényhez, tehát

$$\lim_{n\to\infty} \Big(\sup_{p\in L^{\#}} p(e_n) \Big) = \lim_{n\to\infty} \Big(\sup_{p\in L^{\#}} e_n^{\#}(p) \Big) = \lim_{n\to\infty} |||e_n^{\#}|||_{L^{\#}} = 0.$$

Azonban az a) feltétel alapján minden $n \in \mathbb{N}$ esetén $|||e_n^{\#}|||_{L^{\#}} = \sup_{p\in L^{\#}} p(e_n) = 1$, ami ellentmond a)-nak.

Tehát nem létezik olyan $L^{\#}$ feletti kompakt topológia, amely szerint minden $L \ni e$-re az $L^{\#} \to \mathbb{R}$; $p \mapsto p(e)$ leképezés folytonos. Ugyanakkor L^* felett a pontonkénti konvergencia topológiája olyan kompakt topológia, amely szerint minden $L \ni e$-re az $L^* \to \mathbb{R}$; $p \mapsto p(e)$ leképezés folytonos. Ebből azonnal következik, hogy $L^{\#} \neq L^*$, tehát az $L^* \setminus L^{\#}$ halmaz nem üres. ■

Ha $\mathscr{H}$ *végtelen dimenziós* Hilbert-tér, akkor az $L := \mathbf{P}(\mathscr{L}(\mathscr{H}))$ projektorhálóra teljesülnek az előző állítás a) és b) feltételei. Ha T *nem kompakt*, de σ*-kompakt Hausdorff-tér*, akkor az $L := \mathscr{B}(T)$ Borel-féle σ-algebrára szintén teljesülnek az előző állítás a) és b) feltételei. Sőt mindkét L ortomoduláris háló rendelkezik a következő, a)-nál erősebb tulajdonsággal is.

a′) Minden $e \in L \setminus \{\mathbf{0}\}$ esetén van olyan $p \in L^{\#}$, hogy $p(e) > 0$.

22.11. Ortoadditív függvények

22.11.1. Definíció. *Legyen* $\mathscr{R}$ *halmazgyűrű és* L *ortokomplementált rendezett halmaz. Egy* $u : \mathscr{R} \to L$ *függvényt* **ortoadditívnak** *nevezünk, ha minden* $E, F \in \mathscr{R}$ *esetén, ha* $E \cap F = \emptyset$*, akkor* $u(E) \perp u(F)$ *és* $u(E \cup F) = u(E) \vee u(F)$*. Azt mondjuk, hogy az* $u : \mathscr{R} \to L$ *függvény* σ**-ortoadditív***, ha minden* $\mathscr{R}$*-ben haladó* $(E_k)_{k\in\mathbb{N}}$ *diszjunkt sorozatra,* $\bigcup_{k\in\mathbb{N}} E_k \in \mathscr{R}$ *esetén az* $(u(E_k))_{k\in\mathbb{N}}$ *rendszer ortogonális* L*-ben, és* $u\Big(\bigcup_{k\in\mathbb{N}} E_k\Big) = \sup_{k\in\mathbb{N}} u(E_k)$.

Legyen $\mathscr{R}$ halmazgyűrű, L ortokomplementált rendezett halmaz, és $u : \mathscr{R} \to L$ ortoadditív függvény. Ekkor $u(\emptyset) = \mathbf{0}$, mert a feltevés alapján $u(\emptyset) \perp u(\emptyset)$, hiszen $\emptyset \in \mathscr{R}$

és $\emptyset \cap \emptyset = \emptyset$. De ha $T \in \mathscr{R}$, akkor $u(T) \neq \mathbf{1}$ lehetséges; például az $\mathscr{R} \to L$ azonosan $\mathbf{0}$ függvény nyilvánvalóan σ-ortoadditív.

Az **ALN** 24.1. pontban majd bevezetjük a halmazgyűrűn értelmezett, egységelemes *-algebrába ható, projektor-értékű ortoadditív (illetve σ-ortoadditív) függvényeket. Azt a definíciót összevetve az előzővel látható, hogy ha A egységelemes *-algebra, akkor A projektorainak $\mathbf{P}(A)$ halmaza a természetes rendezéssel és ortokomplementációval ellátva ortokomplementált rendezett halmaz, és ha $\mathscr{R}$ halmazgyűrű, akkor az $\mathscr{R} \to A$ projektor-értékű ortoadditív (illetve σ-ortoadditív) függvények halmaza megegyezik az itt értelmezett $\mathscr{R} \to \mathbf{P}(A)$ ortoadditív (illetve σ-ortoadditív) függvények halmazával.

22.11.2. Állítás. *Legyen $\mathscr{R}$ halmazgyűrű, L ortoháló, és $u : \mathscr{R} \to L$ ortoadditív függvény.*

a) *Ha $E, F \in \mathscr{R}$ és $E \subseteq F$, akkor $u(E) \leq u(F)$, tehát u monoton növő.*

b) *Ha $(E_i)_{i\in I}$ véges (nem feltétlenül diszjunkt) rendszer $\mathscr{R}$-ben, akkor*

$$u\Big(\bigcup_{i\in I} E_i\Big) = \sup_{i\in I} u(E_i).$$

c) *Ha L ortomoduláris, akkor $E, F \in \mathscr{R}$ és $E \subseteq F$ esetén $u(F \setminus E) = u(F) \wedge u(E)^{\perp}$, tehát u szubtraktív.*

Bizonyítás. a) Ha $E, F \in \mathscr{R}$ és $E \subseteq F$, akkor $F\setminus E \in \mathscr{R}$, $E\cap(F\setminus E) = \emptyset$ és $E\cup(F\setminus E) = F$, tehát az u ortoadditivitása miatt $u(E) \leq u(E) \vee u(F \setminus E) = u(F)$.

b) Az ortoadditivitás definíciójából látható, hogy ha $(E_i)_{i\in I}$ véges *diszjunkt* rendszer $\mathscr{R}$-ben, akkor $u\Big(\bigcup_{i\in I} E_i\Big) = \sup_{i\in I} u(E_i)$; ez az I halmaz számossága szerinti teljes indukcióval könnyen igazolható.

Legyenek $E, F \in \mathscr{R}$ tetszőleges halmazok. Ekkor $E \setminus F$, $F \setminus E$ és $E \cap F$ olyan páronként diszjunkt halmazok $\mathscr{R}$-ben, amelyekre

$$E = (E \setminus F) \cup (E \cap F), \quad F = (F \setminus E) \cup (E \cap F), \quad E \cup F = (E \setminus F) \cup (F \setminus E) \cup (E \cap F),$$

ezért

$$\begin{aligned} u(E) \vee u(F) &= (u(E \setminus F) \vee u(E \cap F)) \vee (u(F \setminus E) \vee u(E \cap F)) = \\ &= u(E \setminus F) \vee u(F \setminus E) \vee u(E \cap F) = u(E \cup F). \end{aligned}$$

Ebből kapjuk, hogy ha $(E_i)_{i\in I}$ véges (nem feltétlenül diszjunkt rendszer) $\mathscr{R}$-ben, akkor $u\Big(\bigcup_{i\in I} E_i\Big) = \sup_{i\in I} u(E_i)$; ez az I halmaz számossága szerinti teljes indukcióval könnyen igazolható.

c) Ha $E, F \in \mathscr{R}$ és $E \subseteq F$, akkor az a) iménti bizonyítása szerint $u(E) \vee u(F\setminus E) = u(F)$ és $u(E) \perp u(F \setminus E)$, ezért ha L ortomoduláris, akkor $u(F \setminus E) = u(F) \wedge u(E)^{\perp}$. ■

22.11.3. Állítás. *Legyen $\mathscr{R}$ halmazgyűrű, L ortoháló, és $u : \mathscr{R} \to L$ σ-ortoadditív függvény. Ekkor minden $\mathscr{R}$-ben haladó (nem feltétlenül diszjunkt) $(E_k)_{k\in\mathbb{N}}$ sorozatra, ha $\bigcup_{k\in\mathbb{N}} E_k \in \mathscr{R}$, akkor $\sup_{k\in\mathbb{N}} u(E_k)$ létezik L-ben, és $u\Big(\bigcup_{k\in\mathbb{N}} E_k\Big) = \sup_{k\in\mathbb{N}} u(E_k)$.*

Bizonyítás. Legyen $(E_k)_{k\in\mathbb{N}}$ tetszőleges olyan sorozat $\mathscr{R}$-ben, amelyre $\bigcup_{k\in\mathbb{N}} E_k \in \mathscr{R}$. Legyen $F_0 := E_0$ és minden $n \in \mathbb{N}^*$ esetén

$$F_n := E_n \setminus \left(\bigcup_{k=0}^{n-1} E_k\right).$$

Nyilvánvaló, hogy $(F_k)_{k\in\mathbb{N}}$ olyan diszjunkt sorozat $\mathscr{R}$-ben, hogy $\bigcup_{k\in\mathbb{N}} F_k = \bigcup_{k\in\mathbb{N}} E_k \in \mathscr{R}$, ezért az u függvény σ-ortoadditivitása miatt létezik az $e := \sup_{k\in\mathbb{N}} u(F_k)$ elem L-ben és $e := u\Big(\bigcup_{k\in\mathbb{N}} F_k\Big) = u\Big(\bigcup_{k\in\mathbb{N}} E_k\Big)$.

Minden $k \in \mathbb{N}$ esetén $F_k \subseteq E_k$, ezért $u(F_k) \leq u(E_k)$. Ebből következik, hogy ha $f \in L$ az $(u(E_k))_{k\in\mathbb{N}}$ sorozatnak felső korlátja L-ben, akkor f az $(u(F_k))_{k\in\mathbb{N}}$ sorozatnak is felső korlátja, így $e \leq f$. Ugyanakkor, teljes indukcióval könnyen belátható, hogy az $e \in L$ elem az $(u(E_k))_{k\in\mathbb{N}}$ sorozatnak felső korlátja L-ben, mert $u(E_0) = u(F_0) \leq e$, és ha $n \in \mathbb{N}^*$ olyan, hogy minden $k < n$ természetes számra $u(E_k) \leq e$, akkor $E_n = F_n \cup \Big(\bigcup_{k=0}^{n-1}(E_k \cap E_n)\Big)$ miatt

$$u(E_n) = u(F_n) \vee \sup_{0\leq k\leq n-1} u(E_k \cap E_n) \leq u(F_n) \vee \sup_{0\leq k\leq n-1} u(E_k) \leq e,$$

ahol felhasználtuk, hogy u monoton növő, és minden $\mathscr{R}$-ben haladó $(H_i)_{i\in I}$ véges rendszerre $u\Big(\bigcup_{i\in I} H_i\Big) = \sup_{i\in I} u(H_i)$. Tehát az $e \in L$ elem a legkisebb felső korlátja L-ben az $(u(E_k))_{k\in\mathbb{N}}$ sorozatnak, így $\sup_{k\in\mathbb{N}} u(E_k)$ létezik L-ben és $u\Big(\bigcup_{k\in\mathbb{N}} E_k\Big) = e = \sup_{k\in\mathbb{N}} u(E_k)$. ■

22.11.4. Következmény. *Legyen $\mathscr{R}$ olyan halmazgyűrű a T halmaz felett, amelyre $T \in \mathscr{R}$. Legyen L ortomoduláris háló, és $u : \mathscr{R} \to L$ olyan ortoadditív függvény, amelyre $u(T) = \mathbf{1}$.*

a) *Minden $E \in \mathscr{R}$ esetén $u(T \setminus E) = u(E)^\perp$.*

b) *Ha u σ-ortoadditív, akkor minden $\mathscr{R}$-ben haladó $(E_k)_{k\in\mathbb{N}}$ sorozatra, $\bigcap_{k\in\mathbb{N}} E_k \in \mathscr{R}$ esetén $\inf_{k\in\mathbb{N}} u(E_k)$ létezik L-ben, és $u\Big(\bigcap_{k\in\mathbb{N}} E_k\Big) = \inf_{k\in\mathbb{N}} u(E_k)$.*

Bizonyítás. a) Az L ortomodularitása és $u(T) = \mathbf{1}$ miatt minden $E \in \mathscr{R}$ esetén $u(T \setminus E) = u(T) \wedge u(E)^\perp = u(E)^\perp$, ahol kihasználtuk az u szubtraktivitását.

b) Ha $(E_k)_{k\in\mathbb{N}}$ olyan sorozat $\mathscr{R}$-ben, hogy $\bigcap_{k\in\mathbb{N}} E_k \in \mathscr{R}$, akkor a feltevés alapján $(T \setminus E_k)_{k\in\mathbb{N}}$ olyan $\mathscr{R}$-ben haladó sorozat, hogy $\bigcup_{k\in\mathbb{N}}(T \setminus E_k) = T \setminus \Big(\bigcap_{k\in\mathbb{N}} E_k\Big) \in \mathscr{R}$, tehát, ha az u függvény σ-ortoadditív, akkor az előző állításból kapjuk, hogy $\sup_{k\in\mathbb{N}} u(T \setminus E_k)$ létezik L-ben és $\sup_{k\in\mathbb{N}} u(T \setminus E_k) = u\Big(\bigcup_{k\in\mathbb{N}}(T \setminus E_k)\Big)$. Az a) alapján minden $\mathbb{N} \ni k$-ra

$u(T \setminus E_k) = u(E_k)^{\perp}$, tehát a de Morgan-egyenlőségből kapjuk, hogy $\inf\limits_{k \in \mathbb{N}} u(E_k)$ létezik L-ben és $\Big(\inf\limits_{k \in \mathbb{N}} u(E_k)\Big)^{\perp} = \sup\limits_{k \in \mathbb{N}} u(E_k)^{\perp} = u\Big(T \setminus \Big(\bigcap\limits_{k \in \mathbb{N}} E_k\Big)\Big) = \Big(u\Big(\bigcap\limits_{k \in \mathbb{N}} E_k\Big)\Big)^{\perp}$. ■

23. fejezet

Rendezett testek

23.1. Rendezett testek alaptulajdonságai

23.1.1. Definíció. *A* $(K,+,\cdot,\leq)$ *négyest* **rendezett testnek** *nevezzük, ha* $(K,+,\cdot)$ *test és* $\leq$ *olyan lineáris rendezés a* K *halmaz felett, amelyre teljesülnek a következők:*

$(\mathrm{KO_I})$ *Minden* $x,y,z\in K$ *elemre, ha* $x\leq y$*, akkor* $x+z\leq y+z$*.*

$(\mathrm{KO_{II}})$ *Minden* $x,y\in K$ *elemre, ha* $x\geq \mathbf{0}$ *és* $y\geq\mathbf{0}$*, akkor* $x\cdot y\geq\mathbf{0}$*.*

Ha $(K,+,\cdot,\leq)$ *rendezett test, akkor az* $\{x\in K|x\geq\mathbf{0}\}$ *halmazt a* K_+ *szimbólummal jelöljük, és ennek elemeit* K **pozitív** *elemeinek nevezzük (a* $\leq$ *rendezés szerint).*

A rendezett testeket is általában egyetlen betűvel, az alaphalmaz szimbólumával jelöljük, és a rendezését a $\leq$ szimbólummal jelöljük, ha ez nem vezet félreértésre.

Példa. A racionális számok teste a természetes rendezéssel rendezett test (16.1.10.).

Tegyük fel, hogy K rendezett test. Ha $x,y\in K$, akkor az $x\leq y$ és $-y\leq -x$ egyenlőtlenségek ekvivalensek egymással; ez $(\mathrm{KO_I})$-ből következik. Ha $x\in K$, akkor $x^2\geq\mathbf{0}$, mert ha $x\geq\mathbf{0}$, akkor ez a $(\mathrm{KO_{II}})$ alapján nyilvánvaló, ha pedig $x<\mathbf{0}$, akkor $-x>\mathbf{0}$, tehát ismét $(\mathrm{KO_{II}})$-t alkalmazva kapjuk, hogy $x^2=(-x)^2\geq\mathbf{0}$. Teljesül az, hogy $\mathbf{0}<\mathbf{1}$, mert $\mathbf{0}\neq\mathbf{1}=\mathbf{1}^2$. A $-\mathbf{1}$ elem nem állítható elő négyzetelemek összegeként; ez az előzőek alapján nyilvánvaló. Speciálisan, ha p prímszám, akkor az $\mathbb{F}_p$ test felett *nem létezik* olyan rendezés, amellyel $\mathbb{F}_p$ rendezett test volna, mert ebben $-\mathbf{1}=\sum_{k=1}^{p-1}\mathbf{1}^2$ teljesül. Ha $x\in K$ és $x>\mathbf{0}$, akkor $x^{-1}>\mathbf{0}$, mert ellenkező esetben $\mathbf{0}<-x^{-1}$ igaz lenne, tehát a $(\mathrm{KO_{II}})$ alkalmazásával $\mathbf{0}<(-x^{-1})\cdot x=-\mathbf{1}$ adódna, vagyis $\mathbf{1}<\mathbf{0}$ teljesülne, ami nem igaz. Ha $x,y\in K$, akkor minden $z\in K_+$ elemre, $x\leq y$ esetén $x\cdot z\leq y\cdot z$ teljesül; ez a $(\mathrm{KO_I})$ és $(\mathrm{KO_{II}})$ feltételekből nyilvánvalóan következik.

23.1.2. Állítás. *Ha* K *rendezett test, akkor minden* $n\in\mathbb{N}$ *páratlan számra a*

$$K\to K;\quad x\mapsto x^n$$

hatványozás-függvény szigorúan monoton növő, és minden $n\in\mathbb{N}^*$ *számra a*

$$K_+\to K_+;\quad x\mapsto x^n$$

függvény szigorúan monoton növő.

Bizonyítás. Először megjegyezzük, hogy minden $n \in \mathbb{N}^*$ és $x, y \in K$ esetén

$$y^n - x^n = (y-x) \sum_{k=0}^{n-1} y^{n-1-k} x^k$$

teljesül. Ez teljes indukcióval könnyen igazolható, hiszen az állítás triviálisan igaz, ha $n = 1$, és ha n-re igaz, akkor

$$\begin{aligned} y^{n+1} - x^{n+1} &= y(y^n - x^n) + (y-x)x^n \overset{(*)}{=} y\left((y-x)\sum_{k=0}^{n-1} y^{n-1-k}x^k\right) + (y-x)x^n = \\ &= (y-x)\left(y\sum_{k=0}^{n-1} y^{n-1-k}x^k + x^n\right) = (y-x)\left(\sum_{k=0}^{n-1} y^{n-k}x^k + x^n\right) = \\ &= (y-x)\sum_{k=0}^{n} y^{n-k}x^k = (y-x)\sum_{k=0}^{(n+1)-1} y^{(n+1)-1-k}x^k, \end{aligned}$$

ahol a $\overset{(*)}{=}$ egyenlőségnél alkalmaztuk az indukciós hipotézist, így az állítás igaz az $n+1$ számra is.

Ebből azonnal kapjuk az állítás második részét, mert ha $n \in \mathbb{N}^*$ és $x, y \in K_+$ olyanok, hogy $x < y$, akkor az előző egyenlőség alapján $y^n - x^n \geq (y-x)y^{n-1}$, így $y^n > x^n$, hiszen $y - x > \mathbf{0}$ és $y^{n-1} > \mathbf{0}$.

Tegyük fel, hogy $n \in \mathbb{N}$ páratlan, és $x, y \in K$ olyanok, hogy $x < y$. Ha $x \geq \mathbf{0}$, akkor az előzőek szerint $x^n < y^n$. Ha $x < \mathbf{0}$ és $y \geq \mathbf{0}$, akkor $-x > \mathbf{0}$, tehát $-x^n = (-x)^n > \mathbf{0}$, vagyis $x^n < \mathbf{0} \leq y^n$. Végül, ha $x < \mathbf{0}$ és $y < \mathbf{0}$, akkor $\mathbf{0} < -y < -x$, így az n szám páratlansága miatt $-y^n = (-y)^n < (-x)^n = -x^n$, vagyis $x^n < y^n$. ∎

23.1.3. Állítás. *Ha K rendezett test, akkor a $\mathbb{Z}$ és K közötti kanonikus leképezés injektív, és a $J : \mathbb{Q} \to K$ kanonikus leképezés olyan, hogy minden $r, s \in \mathbb{Q}$ számra $r \leq s$ a $\mathbb{Q}$ természetes rendezése szerint pontosan akkor teljesül, ha $J(r) \leq J(s)$ a K rendezése szerint (vagyis J szigorúan rendezéstartó).*

Bizonyítás. Jelölje j a $\mathbb{Z}$ és K közötti kanonikus leképezést. A $j(1) = \mathbf{1} > \mathbf{0}$ egyenlőtlenségből kiindulva, teljes indukcióval könnyen kapjuk, hogy minden $n \in \mathbb{N}^*$ számra $j(n) > \mathbf{0}$. Ezért minden $p \in \mathbb{Z}$ esetén, ha $p > 0$, akkor $j(p) > \mathbf{0}$, és ha $p < 0$, akkor $-p > 0$, így $-j(p) = j(-p) > \mathbf{0}$, vagyis $j(p) < \mathbf{0}$. Ez azt mutatja, hogy j injektív, és minden $p \in \mathbb{Z}$ esetén $p > 0$ pontosan akkor igaz, ha $j(p) > \mathbf{0}$. Nyilvánvalóan ez azzal egyenértékű, hogy minden $q, p \in \mathbb{Z}$ esetén, a $q < p$ és $j(q) < j(p)$ kijelentések ekvivalensek.

Legyenek $(q, p), (q', p') \in \mathbb{Z} \times (\mathbb{N}^*)$ olyan párok, hogy $q \cdot p' < q' \cdot p$, vagyis $q/p < q'/p'$. A j tulajdonságai alapján ekkor $j(q) \cdot j(p') < j(q') \cdot j(p)$, ugyanakkor $j(p), j(p') > \mathbf{0}$, ezért $J(q/p) = j(q) \cdot j(p)^{-1} < j(q') \cdot j(p')^{-1} = J(q'/p')$, következésképpen J szigorúan monoton növő.

Megfordítva, legyenek $(q, p), (q', p') \in \mathbb{Z} \times (\mathbb{N}^*)$ olyan párok, hogy $J(q/p) < J(q'/p')$. Ekkor $j(q) \cdot j(p)^{-1} = J(q/p) < J(q'/p') = j(q') \cdot j(p')^{-1}$ és $j(p), j(p') > \mathbf{0}$, ezért $j(q) \cdot j(p') < j(q') \cdot j(p)$. Ez azt jelenti, hogy a $q \cdot p'$ és $q' \cdot p$ egész számokra $j(q \cdot p') < j(q' \cdot p)$ teljesül, tehát $q \cdot p' < q' \cdot p$, amiből kapjuk, hogy $q/p < q'/p'$. Ezzel igazoltuk, hogy J szigorúan rendezéstartó. ∎

23.2. Artin–Schreier-tétel

23.2.1. Definíció. *Legyen K test. A $\mathscr{P}(K)$ hatványhalmazon értelmezzük a következő műveleteket:*

$$\begin{aligned}\mathscr{P}(K)\times\mathscr{P}(K)\to\mathscr{P}(K); \quad (A,B)\mapsto A+B &:= \{a+b \mid (a\in A)\wedge(b\in B)\},\\ \mathscr{P}(K)\times\mathscr{P}(K)\to\mathscr{P}(K); \quad (A,B)\mapsto A\cdot B &:= \{a\cdot b \mid (a\in A)\wedge(b\in B)\}.\end{aligned}$$

Ezt a $+$ műveletet a K test feletti **komplexus-összeadásnak**, *és a $\cdot$ műveletet a K test feletti* **komplexus-szorzásnak** *nevezzük.*

A testműveletek tulajdonságait felhasználva könnyen belátható, hogy a komplexus-össszeadás asszociatív, kommutatív, neutrális elemes (és $\{\mathbf{0}\}$ a neutrális elem), azonban csak a test egy elemű részhalmazainak létezik inverze. Továbbá, a komplexus-szorzás asszociatív, kommutatív, neutrális elemes (és $\{\mathbf{1}\}$ a neutrális elem), azonban csak a K azon egy elemű részhalmazainak létezik inverze, amelyek invertálható elemet tartalmaznak.

23.2.2. Állítás. (**A rendezett testek pozitivitás-tartományának jellemzése**) *Legyen K test.*

a) *Ha $\leq$ olyan rendezés K felett, amellyel ellátva K rendezett test* (*tehát $\leq$ olyan lineáris rendezés K felett, amelyre* (KO$_{\mathrm{I}}$) *és* (KO$_{\mathrm{II}}$) *teljesül*)*, akkor a*

$$P := \{x\in K \mid x\geq \mathbf{0}\}$$

halmazra teljesülnek a következő összefüggések:

$$P+P\subseteq P, \quad P\cdot P\subseteq P, \quad P\cap(-P)=\{\mathbf{0}\}, \quad P\cup(-P)=K,$$

ahol $-P := \{-x \mid x\in P\}$. Továbbá, ekkor fennáll a $K^2\subseteq P$ tartalmazás is, ahol $K^2 := \{x^2|x\in K\}$ a négyzetelemek halmaza.

b) *Megfordítva, ha $P\subseteq K$ olyan halmaz, amely rendelkezik az* a)*-ban megfogalmazott tulajdonságokkal, akkor egyértelműen létezik K felett az a $\leq$ rendezés, amellyel ellátva K rendezett test, és amelyre $P=\{x\in K \mid x\geq\mathbf{0}\}$ teljesül. Ez a $\leq$ rendezés olyan, hogy minden $x,y\in K$ esetén*

$$x\leq y \;\Leftrightarrow\; y-x\in P$$

teljesül.

Bizonyítás. a) Nyilvánvaló, hogy (KO$_{\mathrm{I}}$) *ekvivalens* a $P+P\subseteq P$ össszefüggéssel, és (KO$_{\mathrm{II}}$) *ekvivalens* a $P\cdot P\subseteq P$ össszefüggéssel. Ha $x\in K$, akkor $x\in P\cap(-P)$ esetén $x\geq\mathbf{0}$ és $-x\geq\mathbf{0}$, így (KO$_{\mathrm{I}}$) alapján $\mathbf{0}=(-x)+x\geq 0+x=x$, tehát a K feletti rendezés *antiszimmetrikussága* folytán $x=\mathbf{0}$. Ezért $P\cap(-P)=\{\mathbf{0}\}$ is teljesül. Ha $x\in K$, akkor a K feletti rendezés *linearitása* folytán $x\geq\mathbf{0}$, vagy $x\leq\mathbf{0}$, és az utóbbi esetben (KO$_{\mathrm{I}}$) alapján $\mathbf{0}=x+(-x)\leq\mathbf{0}+(-x)=-x$, tehát $x\in P$ vagy $-x\in P$. Ezért $P\cup(-P)=K$ is teljesül. Végül, a négyzetelemek pozitívak rendezett tesben, ezért $K^2\subseteq P$.

b) Legyen $P\subseteq K$ olyan halmaz, amely rendelkezik az a)-ban megfogalmazott tulajdonságokkal. Vezessük be azt a $\leq$ relációt, amelyre $x,y\in K$ esetén

$$x\leq y \;\stackrel{\mathrm{df}}{\Leftrightarrow}\; y-x\in P.$$

Mivel $\mathbf{0} \in P$, így minden $x \in K$ esetén $x - x = \mathbf{0} \in P$, vagyis $x \leq x$, ami azt jelenti, hogy a $\leq$ reláció *reflexív* K felett. Ha $x, y \in K$ olyanok, hogy $x \leq y$ és $y \leq x$, akkor $y - x \in P$ és $-(y-x) = x - y \in P$, tehát $y - x \in P \cap (-P) = \{\mathbf{0}\}$, következésképpen $y - x = \mathbf{0}$, vagyis $x = y$. Ez azt jelenti, hogy a $\leq$ reláció *antiszimmetrikus*. Ha $x, y, z \in K$ olyanok, hogy $x \leq y$ és $y \leq z$, akkor $y - x, z - y \in P$, ezért $z - x = (z-y) + (y-x) \in P + P \subseteq P$, tehát $x \leq z$, ami azt jelenti, hogy a $\leq$ reláció *tranzitív*. Ha $x, y \in K$ tetszőlegesek, akkor $y - x \in K = (P \cup (-P))$, tehát $y - x \in K$ (és ekkor $x \leq y$) vagy $y - x \in -P$, azaz $x - y = -(y-x) \in P$ (és ekkor $y \leq x$). Ezzel megmutattuk, hogy $\leq$ *lineáris rendezés* K felett. Továbbá nyilvánvaló, hogy minden $x \in K$ esetén $x \geq \mathbf{0}$ ekvivalens azzal, hogy $x = x - \mathbf{0} \in P$, tehát $P = \{x \in K | x \geq \mathbf{0}\}$.

Ha $x, y, z \in K$ és $x \leq y$, akkor $y - x \in P$, és $(y+z) - (x+z) = y - x$, ezért $x + z \leq y + z$. Ez azt jelenti, hogy a $\leq$ rendezésre (KO$_{\mathrm{I}}$) teljesül. Ha $x, y \in K$ olyanok, hogy $x \geq \mathbf{0}$ és $y \geq \mathbf{0}$, akkor $x \in P$ és $y \in P$, ezért $x \cdot y \in P \cdot P \subseteq P$, vagyis $x \cdot y \geq \mathbf{0}$. Ez azt jelenti, hogy a $\leq$ rendezésre (KO$_{\mathrm{II}}$) is teljesül, tehát $\leq$ olyan rendezés K felett, amellyel ellátva *K rendezett test.*

Ha $\leq'$ szintén olyan rendezés K felett, amellyel ellátva K rendezett test és $P = \{x \in K | x \geq' \mathbf{0}\}$, akkor minden $x, y \in K$ esetén $x \leq' y$ a $\leq'$ rendezésre vonatkozó (KO$_{\mathrm{I}}$) feltétel alapján ekvivalens azzal, hogy $\mathbf{0} = x + (-x) \leq' y + (-x) = y - x$, vagyis $y - x \in P$, azaz $x \leq y$. Ez azt jelenti, hogy $\leq$ az *egyetlen* olyan K feletti rendezés, amellyel ellátva K rendezett test és $P = \{x \in K | x \geq \mathbf{0}\}$. ■

23.2.3. Tétel. (**Artin–Schreier-tétel**) *Ha K test, akkor a következő állítások ekvivalensek:*

(i) *Létezik olyan $\leq$ rendezés K felett, amellyel ellátva K rendezett test* (*tehát $\leq$ olyan lineáris rendezés K felett, amelyre* (KO$_{\mathrm{I}}$) *és* (KO$_{\mathrm{II}}$) *teljesül*).

(ii) *A $-\mathbf{1}$ elem nem áll elő K-ban négyzetelemek összegeként* (*tehát nem létezik olyan K-ban haladó $(x_i)_{i \in I}$ véges rendszer, amelyre $-\mathbf{1} = \sum_{i \in I} x_i^2$ teljesül*).

(iii) *Ha $(x_i)_{i \in I}$ olyan K-ban haladó véges rendszer, amelyre $\sum_{i \in I} x_i^2 = \mathbf{0}$, akkor minden $I \ni i$-re $x_i = \mathbf{0}$.*

Bizonyítás. Az (i)⇒(ii) és (ii)⇒(iii) implikációk könnyen igazolhatóak. A (iii)⇒(i) következtetés igazolásához jelölje $\mathfrak{P}$ azon $P \subseteq K$ hamazok halmazát, amelyekre teljesülnek a következő összefüggések:

$$P + P \subseteq P, \quad P \cdot P \subseteq P, \quad P \cap (-P) = \{\mathbf{0}\}, \quad K^2 \subseteq P,$$

ahol $-P := \{-x | x \in P\}$, és $K^2 := \{x^2 | x \in K\}$ a négyzetelemek halmaza.

Először megjegyezzük, hogy $\mathfrak{P} \neq \emptyset$, mert a K négyzetelemeinek véges összegeként előálló elemek P halmazára $P + P \subseteq P$, $P \cdot P \subseteq P$ és $K^2 \subseteq P$ nyilvánvalóan teljesül, továbbá a (iii) miatt $P \cap (-P) = \{\mathbf{0}\}$ is igaz, tehát $P \in \mathfrak{P}$.

A $\mathfrak{P}$ halmazt a tartalmazás-relációval rendezzük. Megmutatjuk, hogy ez induktívan rendezett halmaz. Ehhez elég azt belátni, hogy ha $(P_i)_{i \in I}$ olyan nem üres rendszer $\mathfrak{P}$-ben, hogy minden $I \ni i, j$-re $P_i \subseteq P_j$ vagy $P_j \subseteq P_i$, akkor a $P := \bigcup_{i \in I} P_i$ halmazra $P \in \mathfrak{P}$ teljesül. Ennek bizonyításához legyenek $x, y \in P$. Ekkor van olyan $i \in I$ és $j \in I$, hogy $x \in P_i$ és $y \in P_j$. Ha $P_i \subseteq P_j$, akkor $x, y \in P_j$, így $x + y \in P_j + P_j \subseteq P_j \subseteq P$ és $x \cdot y \in P_j \cdot P_j \subseteq P_j \subseteq P$. Ha $P_j \subseteq P_i$, akkor $x, y \in P_i$, így $x + y \in P_i + P_i \subseteq P_i \subseteq P$ és

$x \cdot y \in P_i \cdot P_i \subseteq P_i \subseteq P$. Ez azt jelenti, hogy $P + P \subseteq P$ és $P \cdot P \subseteq P$ teljesül. Az $I \neq \emptyset$ feltétel alapján van olyan $i \in I$, hogy $P_i \subseteq P$, tehát $K^2 \subseteq P$. Végül, ha $x \in P \cap (-P)$, akkor $x \in P$ és $-x \in P$, tehát léteznek olyan $i \in I$ és $j \in I$, hogy $x \in P_i$ és $-x \in P_j$. Ha $P_i \subseteq P_j$, akkor $x, -x \in P_j$, így $x \in P_j \cap (-P_j) = \{\mathbf{0}\}$, vagyis $x = \mathbf{0}$. Ha $P_j \subseteq P_i$, akkor $x, -x \in P_i$, így $x \in P_i \cap (-P_i) = \{\mathbf{0}\}$, vagyis $x = \mathbf{0}$. Ez azt jelenti, hogy $P \cap (-P) = \{\mathbf{0}\}$, tehát $P \in \mathfrak{P}$.

Megmutatjuk, hogy ha $P \in \mathfrak{P}$ és $x \in K \setminus P$, akkor a $P' := P + \{-x\} \cdot P$ halmaz olyan, hogy $P' \in \mathfrak{P}$, és $P \subseteq P'$, valamint $-x \in P'$ teljesül. Világos, hogy $\mathbf{0} \in P$ miatt $P \subseteq P'$, és

$$P' + P' = (P + \{-x\} \cdot P) + (P + \{-x\} \cdot P) = (P + P) + \{-x\} \cdot (P + P) \subseteq P + \{-x\} \cdot P = P',$$

mert $P + P \subseteq P$. Továbbá:

$$\begin{aligned} P' \cdot P' &= (P + \{-x\} \cdot P) \cdot (P + \{-x\} \cdot P) = (P \cdot P) + \{x^2\} \cdot (P \cdot P) + \{-x\} \cdot (P \cdot P + P \cdot P) \\ &\subseteq P + K^2 \cdot P + \{-x\} \cdot (P + P) \subseteq P + P \cdot P + \{-x\} \cdot P \subseteq P + P + \{-x\} \cdot P \subseteq P + \{-x\} \cdot P = P'. \end{aligned}$$

Nyilvánvaló, hogy $K^2 \subseteq P \subseteq P + \{-x\} \cdot P = P'$ és $-x = \mathbf{0} + (-x) \cdot \mathbf{1} \in P'$, mert $\mathbf{1} = \mathbf{1}^2 \in K^2 \subseteq P$. Ezért már csak azt kell igazolni, hogy $P' \cap (-P') \subseteq \{\mathbf{0}\}$. Ehhez legyen $y \in P' \cap (-P')$, tehát $y \in P'$ és $-y \in P'$. Legyenek $a, b, c, d \in P$ olyan elemek, amelyekre $y = a - x \cdot b$ és $-y = c - x \cdot d$. Ekkor $a - x \cdot b = -(c - x \cdot d)$, amiből következik, hogy $a + c = x \cdot (b + d)$. Ha $b + d \neq \mathbf{0}$ teljesülne, akkor ebből

$$x = (a + c) \cdot (b + d) \cdot ((b + d)^{-1})^2 \in (P + P) \cdot (P + P) \cdot K^2 \subseteq P \cdot P \cdot P \subseteq P$$

adódna, holott $x \notin P$. Ezért $b + d = \mathbf{0}$, így szükségképpen $a + c = \mathbf{0}$ is teljesül, hiszen $x \neq \mathbf{0}$, mert $\mathbf{0} \in P$. Ekkor $b = -d \in P \cap (-P) = \{\mathbf{0}\}$ és $a = -c \in P \cap (-P) = \{\mathbf{0}\}$, vagyis $a = b = c = d = \mathbf{0}$, így $y = \mathbf{0}$.

A Kuratowski–Zorn-lemma alapján létezik maximális elem a $\mathfrak{P}$ rendezett halmazban; legyen P ilyen. Ekkor $P \cup (-P) = K$ is teljesül, mert ha $x \in K$ és $x \notin P$, akkor az előző bekezdés szerint van olyan $P' \in \mathfrak{P}$, amelyre $P \subseteq P'$ és $-x \in P'$: ekkor a P maximalitása miatt $P = P'$, tehát $-x \in P$, vagyis $x \in -P$.

Tehát a rendezett testek pozitivitás-tartományának jellemzése alapján *létezik* K felett olyan $\leq$ rendezés, amellyel ellátva K rendezett test, és amelyre $P = \{x \in K | x \geq \mathbf{0}\}$ teljesül. ■

23.3. Archimédészi módon rendezett testek

23.3.1. Definíció. *A K rendezett testet* **archimédészi módon rendezett testnek** *mondjuk, ha minden $x \in K$ és $y \in K$ elemhez, $y > \mathbf{0}$ esetén létezik olyan $n \in \mathbb{N}$, hogy $x < n \cdot y$.*

23.3.2. Állítás. *A racionális számok rendezett teste archimédészi módon rendezett test.*

Bizonyítás. Legyenek $x \in \mathbb{Q}$ és $y \in \mathbb{Q}$ olyanok, hogy $y > 0$. Ekkor léteznek olyan $q, q', p' \in \mathbb{N}^*$ és $p \in \mathbb{Z}$, hogy $x = p/q$ és $y = p'/q'$. Olyan $n \in \mathbb{N}$ számot keresünk, amelyre $p/q < n(p'/q')$, vagyis $pq' < np'q$. Ha $p \leq 0$, akkor $pq' \leq 0$, ugyanakkor $p'q \in \mathbb{N}^*$, így ekkor *bármely* $n \in \mathbb{N}^*$ számra $pq' \leq 0 < np'q$. Ha $p > 0$, azaz $p \in \mathbb{N}^*$, akkor $n := pq' + 1 \in \mathbb{N}^*$ olyan szám, amelyre $pq' < pq' + 1 \leq (pq' + 1)(p'q) = np'q$. ■

23.3.3. Tétel. (Az archimédészi módon rendezett testek jellemzése) *Ha K rendezett test, akkor a következő állítások ekvivalensek.*

(i) *K archimédészi módon rendezett test.*

(ii) *Minden $x \in K$ esetén van olyan $n \in \mathbb{N}$, hogy $x < n$, vagyis az $\mathbb{N}$ halmaz nem korlátos felülről K-ban.*

(iii) *Minden $x \in K$ elemhez létezik olyan $p \in \mathbb{Z}$, hogy $p \leq x < p + 1$.*

(iv) *Minden $x, y \in K$, $x < y$ esetén létezik olyan $r \in \mathbb{Q}$, hogy $x < r < y$.*

(v) *Minden $x \in K$ esetén az $\{r \in \mathbb{Q} | r < x\}$ halmaznak létezik szuprémuma K-ban, és $x = \sup_K\{r \in \mathbb{Q} | r < x\}$.*

Bizonyítás. (i)⇒(ii) Tudjuk, hogy $\mathbf{0} < \mathbf{1}$, ezért (i) alapján, $x \in K$ esetén van olyan $n \in \mathbb{N}$, hogy $x < n \cdot \mathbf{1} = n$.

(ii)⇒(iii) Először tegyük fel, hogy $x \in K$ olyan, hogy $x \geq \mathbf{0}$. A (ii) feltevés alapján létezik olyan $n \in \mathbb{N}$, hogy $x < n$, vagyis $\{n \in \mathbb{N} | x < n\} \neq \emptyset$. Az $\mathbb{N}$ halmaz jólrendezettsége miatt létezik legkisebb elem az $\{n \in \mathbb{N} | x < n\}$ halmazban; legyen ez m. Ekkor $x \geq \mathbf{0}$ miatt $m > 0$, tehát $p := m - 1 \in \mathbb{N}$. Továbbá $x < m = p + 1$, és $p < m$ miatt $x < p$ nem igaz, vagyis $p \leq x$. Tehát $p \in \mathbb{N}$ olyan, hogy $p \leq x < p + 1$.

Legyen most $x \in K$ olyan, hogy $x < \mathbf{0}$. Ekkor $-x > \mathbf{0}$, tehát az előző bekezdés szerint van olyan $q \in \mathbb{N}$, amelyre $q \leq -x < q + 1$, így $-q - 1 < x \leq -q$ is teljesül. Ha $x \neq -q$, akkor $p := -q - 1 \in \mathbb{Z}$ olyan elem, amelyre $p \leq x < p + 1$. Ha viszont $x = -q$, akkor $p := -q \in \mathbb{Z}$ olyan, hogy $p \leq x < p + 1$.

Ezzel igazoltuk, hogy minden $x \in K$ elemhez van olyan $p \in \mathbb{Z}$, hogy $p \leq x < p + 1$.

(iii)⇒(iv) Legyenek $x, y \in K$ olyanok, hogy $x < y$. A feltevés szerint $y - x > \mathbf{0}$, így $(y - x)^{-1} > \mathbf{0}$, és (iii) alapján létezik olyan $q \in \mathbb{Z}$, hogy $\mathbf{0} < (y - x)^{-1} < q$, tehát $q \in \mathbb{N}^*$ és $\mathbf{1} < q \cdot (y - x)$. Ha q ilyen, akkor ismét (iii) alapján, van olyan $p \in \mathbb{Z}$, hogy $p \leq q \cdot x < p + 1$. Ekkor az $r := (p + 1)/q$ racionális számra $x < r < y$ teljesül. Valóban, $p + 1 \leq q \cdot x + \mathbf{1} < q \cdot y$, így az $q^{-1} \in K$ pozitív elemmel való szorzás után azt kapjuk, hogy $r < y$. Továbbá, $q \cdot x < p + 1$, így az $q^{-1} \in K$ pozitív elemmel való szorzás után azt kapjuk, hogy $x < r$.

(iv)⇒(v) Legyen $x \in K$. Az $\{r \in \mathbb{Q} | r < x\} \subseteq K$ halmaznak x természetesen felső korlátja. Ha $y \in K$ is felső korlátja, akkor $y < x$ lehetetlen, különben a (iv) miatt létezne olyan $r \in \mathbb{Q}$, hogy $y < r < x$, márpedig $r < x$ és $r \in \mathbb{Q}$ esetén $r \leq y$. Ez azt jelenti, hogy x az $\{r \in \mathbb{Q} | r < x\}$ halmaz legkisebb felső korlátja a K rendezett halmazban, tehát $x = \sup_K\{r \in \mathbb{Q} | r < x\}$.

(v)⇒(i) Legyenek $x, y \in K$ olyanok, hogy $y > \mathbf{0}$. Ekkor az (v) miatt létezik olyan $r \in \mathbb{Q}$, hogy $\mathbf{0} < r < y$. Továbbá, $x < x + \mathbf{1}$ és (v) miatt létezik olyan $r' \in \mathbb{Q}$, hogy $x < r' < x + \mathbf{1}$. A racionális számok rendezett teste archimédészi módon rendezett, ezért van olyan $n \in \mathbb{N}$, hogy $r' < nr$. Ekkor $x < r' < nr < n \cdot y$, így K archimédészi módon rendezett test. ■

Megjegyezzük, hogy ha K archimédészi módon rendezett test, akkor minden $x \in K$ elemhez *egyetlen* olyan $p \in \mathbb{Z}$ létezik, hogy $p \leq x < p + 1$. Valóban, ha $x \in K$ és $p, p' \in \mathbb{Z}$ olyanok, hogy $p \leq x < p + 1$ és $p' \leq x < p' + 1$ egyszerre teljesül, akkor $p \leq x < p' + 1$ miatt $p < p' + 1$, vagyis $p - p' < 1$, és hasonlóan kapjuk, hogy $p' - p < 1$ is teljesül, tehát $-1 < p - p' < 1$. De $\mathbb{Z}$-ben a 0 az egyetlen elem, amely szigorúan -1 és 1 közé esik, következésképpen $p - p' = 0$. Ezért értelmes a következő definíció.

23.3.4. Definíció. *Ha K archimédészi módon rendezett test, akkor minden $x \in K$ esetén $[x]$ jelöli azt az egyetlen egész számot, amelyre $[x] \leq x < [x] + 1$ teljesül, és az $[x] \in \mathbb{Z}$ számot az x elem* **egész részének** *nevezzük.*

Megjegyezzük még, hogy az archimédészi módon rendezett testek jellemzési tételében szereplő (iv) tulajdonságot úgy fejezzük ki, hogy $\mathbb{Q}$ *rendezés-sűrű* az archimédészi módon rendezett testekben.

23.4. Teljesen rendezett testek

23.4.1. Definíció. *A K rendezett testet* **teljesen rendezett testnek** *mondjuk, ha K minden nem üres, felülről korlátos részhalmazának létezik szuprémuma a K rendezett halmazban.*

23.4.2. Állítás. *A K rendezett test pontosan akkor teljesen rendezett test, ha teljesül rá a következő állítás.*

(C) *Minden $X, Y \subseteq K$ halmazra, ha $X \neq \emptyset \neq Y$ és minden $x \in X$ és $y \in Y$ esetén $x \leq y$, akkor létezik olyan $z \in K$, hogy minden $x \in X$ és $y \in Y$ esetén $x \leq z \leq y$.*

Bizonyítás. Tegyük fel, hogy K teljesen rendezett test, és legyenek $X, Y \subseteq K$ olyan halmazok, hogy $X \neq \emptyset \neq Y$ és minden $x \in X$ és $y \in Y$ esetén $x \leq y$. Ekkor $X \neq \emptyset$ és Y minden eleme felső korlátja X-nek, valamint $Y \neq \emptyset$, így X nem üres, felülről korlátos részhalmaza K-nak. Ezért K teljes rendezettsége miatt létezik X-nek szuprémuma: legyen $z := \sup(X)$. Ekkor $x \in X$ esetén $x \leq z$, és ha $y \in Y$, akkor y felső korlátja X-nek, így $z \leq y$. Ez azt jelenti, hogy K-ra (C) teljesül.

Megfordítva, tegyük fel, hogy K rendelkezik a (C) tulajdonsággal. Legyen $X \subseteq K$ nem üres, felülről korlátos halmaz, és jelölje Y az X halmaz felső korlátjainak halmazát. Ekkor $Y \neq \emptyset$ és minden $x \in X$ és $y \in Y$ esetén $x \leq y$. Ezért (C) alapján vehetünk olyan $z \in K$ elemet, amelyre minden $x \in X$ és $y \in Y$ esetén $x \leq z \leq y$. Ekkor z felső korlátja X-nek és z kisebb-egyenlő Y minden eleménél, vagyis X minden felső korlátjánál. Tehát z az X halmaz legkisebb felső korlátja, vagyis $z = \sup(X)$. Ez azt jelenti, hogy K teljesen rendezett test. ∎

Megjegyezzük, hogy az előző állításban szereplő (C) tulajdonságot *Cantor-féle szétválasztási tulajdonságnak* nevezzük.

Természetes kérdés az, hogy *létezik-e* teljesen rendezett test? A racionális számok rendezett teste nem teljesen rendezett test, mert például az $\{r \in \mathbb{Q} | (r \geq 0) \wedge (r^2 \leq 2)\}$ halmaznak nincs szuprémuma $\mathbb{Q}$-ban, holott nem üres és felülről korlátos. A következő állítás megmutatja, hogy teljesen rendezett testet csakis az archimédészi módon rendezett testek között lehet találni.

23.4.3. Állítás. *Minden teljesen rendezett test archimédészi módon rendezett.*

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy K teljesen rendezett test, és $x, y \in K$ olyan elemek, hogy $y > \mathbf{0}$, de nem létezik olyan $n \in \mathbb{N}$, amelyre $x < n \cdot y$ teljesülne. Ekkor az $\{n \cdot y | n \in \mathbb{N}\} \subseteq K$ halmaznak x felső korlátja, így a K teljes rendezettsége miatt létezik szuprémuma; legyen $z := \sup\{n \cdot y | n \in \mathbb{N}\}$. Ekkor $z - y < z$ miatt $z - y$ nem felső korlátja $\{n \cdot y | n \in \mathbb{N}\}$-nek, tehát van olyan $n \in \mathbb{N}$, amelyre $z - y < n \cdot y$. De ekkor $z < (n + 1) \cdot y$, holott minden $m \in \mathbb{N}$ számra $m \cdot y \leq z$ teljesül. Ez az ellentmondás az állítást bizonyítja. ∎

23.4.4. Állítás. *Legyen K archimédészi módon rendezett test. Ekkor az*

$$f_K : K \to \mathscr{P}(\mathbb{Q}); \quad x \mapsto \{r \in \mathbb{Q} | r < x\}$$

leképezés injektív, és $\mathrm{Im}(f_K)$ *minden eleme olyan $\lambda \subseteq \mathbb{Q}$ halmaz, amelyre teljesülnek a következők:*

($\mathrm{D_I}$) *$\lambda \neq \emptyset$ és λ felülről korlátos $\mathbb{Q}$-ban;*

($\mathrm{D_{II}}$) *λ-nak nincs legnagyobb eleme $\mathbb{Q}$-ban;*

($\mathrm{D_{III}}$) *minden $r \in \lambda$ elemre $]\leftarrow, r] \subseteq \lambda$.*

Ha K teljesen rendezett test, akkor az f_K függvény értékkészlete egyenlő azon $\lambda \subseteq \mathbb{Q}$ halmazok halmazával, amelyekre ($\mathrm{D_I}$), ($\mathrm{D_{II}}$) *és* ($\mathrm{D_{III}}$) *teljesül.*

Bizonyítás. Minden $x \in K$ esetén $x = \sup_K\{r \in \mathbb{Q} | r < x\} = \sup_K f_K(x)$, ezért az f_K függvény injektív.

Legyen $x \in K$ és $\lambda := \{r \in \mathbb{Q} | r < x\}$. Az $x < [x] + 1 \in \mathbb{Z} \subseteq \mathbb{Q}$ egyenlőtlenség miatt λ felülről korlátos halmaz $\mathbb{Q}$-ban, továbbá $[x] - 1 < [x] \leq x$ miatt $[x] - 1 \in \lambda$, így $\lambda \neq \emptyset$. Ha $r \in \lambda$, akkor $r < x$, ezért van olyan $s \in \mathbb{Q}$, hogy $r < s < x$; ekkor $s \in \lambda$ és $r < s$, tehát λ-nak nincs legnagyobb eleme. Ha $r \in \lambda$, akkor $s \in \mathbb{Q}$ és $s < r$ esetén $s < x$, ezért $s \in \lambda$. Ez azt jelenti, hogy λ-ra ($\mathrm{D_I}$), ($\mathrm{D_{II}}$) és ($\mathrm{D_{III}}$) teljesül.

Tegyük fel, hogy K teljesen rendezett test, és legyen $\lambda \subseteq \mathbb{Q}$ olyan halmaz, amelyre ($\mathrm{D_I}$), ($\mathrm{D_{II}}$) és ($\mathrm{D_{III}}$) teljesül. A λ halmazt a K részhalmazának tekintve; a ($\mathrm{D_I}$) alapján λ a K-ban is nem üres és felülről korlátos, ezért képezhető az $x := \sup_K \lambda$ elem. Megmutatjuk, hogy $\lambda = f_K(x)$. Valóban, ha $r \in \lambda$, akkor a ($\mathrm{D_{II}}$) miatt van olyan $s \in \lambda$, hogy $r < s$ a $\mathbb{Q}$ rendezése szerint, és x felső korlátja λ-nak K-ban, így $r < x$ a K rendezett halmazban. Ez azt jelenti, hogy $\lambda \subseteq f_K(x)$. Megfordítva, ha $r \in f_K(x)$, akkor $r \in \mathbb{Q}$ és $r < x$ a K rendezése szerint. A definíció szerint x a legkisebb felső korlátja λ-nak, ezért r már nem felső korlátja λ-nak K-ban, így létezik olyan $s \in \lambda$, hogy $r < s$. Ekkor a ($\mathrm{D_{III}}$) miatt $r \in \lambda$, ami azt jelenti, hogy $f_K(x) \subseteq \lambda$. ■

Az előző állításnak nyilvánvaló következménye, hogy minden archimédészi módon rendezett test alaphalmaza legfeljebb kontinuum-számosságú, és bármely két teljesen rendezett test alaphalmazai ekvipotensek egymással.

23.4.5. Definíció. Dedekind-szeletnek *nevezünk minden olyan $\lambda \subseteq \mathbb{Q}$ halmazt, amelyre az előző állítás* ($\mathrm{D_I}$), ($\mathrm{D_{II}}$) *és* ($\mathrm{D_{III}}$) *feltételei teljesülnek. A Dedekind-szeletek halmazát $\mathbb{R}$ jelöli.*

Könnyen látható, hogy minden $r \in \mathbb{Q}$ esetén az $]\leftarrow, r[$ intervallum $\mathbb{Q}$-ban Dedekind-szelet, vagyis $]\leftarrow, r[\in \mathbb{R}$ és természetesen az előző állításban értelmezett $f_{\mathbb{Q}}$ függvény egyenlő a $\mathbb{Q} \to \mathbb{R};\ r \mapsto]\leftarrow, r[$ leképezéssel, tehát a $\mathbb{Q}$ halmaz e kitüntetett injekció által azonosul az $\mathbb{R}$ egy részhalmazával.

23.5. A valós számok rendezett teste

23.5.1. Tétel. (Dedekind-tétel) *Létezik teljesen rendezett test, és ha $(K_1, +_1, \cdot_1, \leq_1)$ és $(K_2, +_2, \cdot_2, \leq_2)$ teljesen rendezett testek, akkor létezik egyetlen olyan $f : K_1 \to K_2$ bijekció, amely additív, vagyis minden $x, y \in K_1$ esetén $f(x +_1 y) = f(x) +_2 f(y)$; multiplikatív, vagyis minden $x, y \in K_1$ esetén $f(x \cdot_1 y) = f(x) \cdot_2 f(y)$; és szigorúan rendezés-tartó, vagyis minden $x, y \in K_1$ esetén $(x \leq_1 y) \Leftrightarrow (f(x) \leq_2 f(y))$.*

Bizonyítás. Először megállapodunk abban, hogy a $\subseteq$ relációt $\mathbb{R}$ felett a $\leq$ szimbólummal jelöljük; megmutatjuk, hogy ez *lineáris* rendezés az $\mathbb{R}$ felett. Legyenek $\lambda, \lambda' \in \mathbb{R}$, és tegyük fel, hogy $\lambda \not\subseteq \lambda'$. Legyen $r \in \lambda$ olyan elem, amelyre $r \notin \lambda'$. Ha $s \in \lambda'$, akkor a $(\mathrm{D_{III}})$ és $r \notin \lambda'$ miatt $r \leq s$ lehetetlen, tehát $s < r$ igaz, így ismét a $(\mathrm{D_{III}})$ és $r \in \lambda$ alapján $s \in \lambda$ adódik. Ez azt jelenti, hogy $\lambda \not\subseteq \lambda'$ esetén $\lambda' \subseteq \lambda$ teljesül. Ebből a λ és λ' felcserélésével kapjuk, hogy $\lambda' \not\subseteq \lambda$ esetén $\lambda \subseteq \lambda'$ teljesül. Ezért minden $\lambda, \lambda' \in \mathbb{R}$ elemre $\lambda \subseteq \lambda'$ vagy $\lambda' \subseteq \lambda$ teljesül.

Megmutatjuk, hogy az $\mathbb{R}$ feletti $\leq$ lineáris rendezésre teljesül az, hogy minden nem üres, felülről korlátos halmaznak létezik szuprémuma. Legyen ugyanis $E \subseteq \mathbb{R}$ olyan nem üres halmaz, amelynek $\lambda' \in \mathbb{R}$ felső korlátja $\leq$ szerint, vagyis minden $\lambda \in E$ esetén $\lambda \subseteq \lambda'$. Ekkor $\bigcup E \subseteq \lambda'$, tehát $\bigcup E$ nem üres, felülről korlátos részhalmaza $\mathbb{Q}$-nak mert a λ' minden felső korlátja $\mathbb{Q}$-ban az $\bigcup E$ halmaznak is felső korlátja. Ezért $\bigcup E$-re $(\mathrm{D_I})$ teljesül. Ha $r \in \bigcup E$, akkor van olyan $\lambda \in E$, hogy $r \in \lambda$, így a $(\mathrm{D_{II}})$ alapján olyan $s \in \lambda$ is létezik, amelyre $r < s$, és persze $s \in \bigcup E$ szintén teljesül. Ezért $\bigcup E$-re $(\mathrm{D_{II}})$ teljesül. Ha $r \in \bigcup E$ és $s < r$, akkor van olyan $\lambda \in E$, hogy $r \in \lambda$; ekkor $s \in \lambda \subseteq \bigcup E$, hiszen λ-ra $(\mathrm{D_{III}})$ igaz. Tehát $(\mathrm{D_{III}})$ a $\bigcup E$ halmazra is teljesül, így $\bigcup E \in \mathbb{R}$. Világos, hogy minden $\lambda \in E$ esetén $\lambda \subseteq \bigcup E$, vagyis $\bigcup E$ felső korlátja E-nek a $\leq$ rendezés szerint. Ha $\sigma \in \mathbb{R}$ felső korlátja E-nek a $\leq$ rendezés szerint, akkor minden $\lambda \in E$ esetén $\lambda \subseteq \sigma$, így az $\bigcup E$ halmaz definíciója szerint $\bigcup E \subseteq \sigma$. Ez azt jelenti, hogy $\bigcup E$ az E halmaz legkisebb felső korlátja $\mathbb{R}$-ben a $\leq$ rendezés szerint.

Most összeadást értelmezünk az $\mathbb{R}$ halmaz elemei között. Ehhez legyenek $\lambda, \lambda' \in \mathbb{R}$ rögzítve, és tekintsük a

$$\lambda + \lambda' := \{r + r' | (r \in \lambda) \wedge (r' \in \lambda')\}$$

halmazt. Megmutatjuk, hogy $\lambda + \lambda' \in \mathbb{R}$. Ha $\bar{r} \in \mathbb{Q}$ (illetve $\bar{r}' \in \mathbb{Q}$) a λ (illetve λ') felső korlátja $\mathbb{Q}$-ban, akkor nyilvánvaló, hogy $\bar{r} + \bar{r}'$ a $\lambda + \lambda'$ halmaz felső korlátja $\mathbb{Q}$-ban. Ezért $\lambda + \lambda'$-re $(\mathrm{D_I})$ teljesül. Ha $r \in \lambda$ és $r' \in \lambda'$, akkor a $(\mathrm{D_{II}})$ szerint létezik olyan $s \in \lambda$ és $s' \in \lambda'$, hogy $r < s$ és $r' < s'$; ekkor $r + r' < s + s' \in \lambda + \lambda'$, tehát $\lambda + \lambda'$-re $(\mathrm{D_{II}})$ teljesül. Ha $r \in \lambda$, $r' \in \lambda'$ és $t \in \mathbb{Q}$ olyan, hogy $t < r + r'$, akkor $t - r < r'$, így $t - r \in \lambda'$, hiszen $(\mathrm{D_{III}})$ teljesül λ'-re; ekkor viszont $t = r + (t - r) \in \lambda + \lambda'$, következésképpen $\lambda + \lambda'$-re $(\mathrm{D_{III}})$ teljesül.

Ezzel értelmeztünk egy $+$ műveletet $\mathbb{R}$-ben. Állítjuk, hogy $+$ olyan *kommutatív csoportművelet* $\mathbb{R}$ felett, amelyre $(\mathrm{KO_I})$ teljesül.

Ha $\lambda, \lambda', \lambda'' \in \mathbb{R}$ és $s \in (\lambda + \lambda') + \lambda''$, akkor van olyan $r \in \lambda$, $r' \in \lambda'$ és $r'' \in \lambda''$, hogy $s = (r + r') + r''$; ekkor a $\mathbb{Q}$ összeadásának asszociativitása miatt $s = r + (r' + r'') \in \lambda + (\lambda' + \lambda'')$, tehát $(\lambda + \lambda') + \lambda'' \subseteq \lambda + (\lambda' + \lambda'')$. Hasonlóan kapjuk azt is, hogy minden $\lambda, \lambda', \lambda'' \in \mathbb{R}$ esetén $\lambda + (\lambda' + \lambda'') \subseteq (\lambda + \lambda') + \lambda''$, következésképpen az $\mathbb{R}$ feletti $+$ művelet asszociatív.

Ha $\lambda, \lambda' \in \mathbb{R}$ és $s \in \lambda + \lambda'$, akkor van olyan $r \in \lambda$ és $r' \in \lambda'$, hogy $s = r + r'$; ekkor a $\mathbb{Q}$ összeadásának kommutativitása miatt $s = r' + r \in \lambda' + \lambda$, tehát $\lambda + \lambda' \subseteq \lambda' + \lambda$. Ez bármely két $\lambda, \lambda' \in \mathbb{R}$ elemre igaz, ezért fennáll a $\lambda' + \lambda \subseteq \lambda + \lambda'$ összefüggés is, így az $\mathbb{R}$ feletti $+$ művelet kommutatív.

Legyen $\mathbf{0} := \{r \in \mathbb{Q} | r < 0\}$; világos, hogy $\mathbf{0} \in \mathbb{R}$. Legyen $\lambda \in \mathbb{R}$; ekkor $s \in \mathbf{0} + \lambda$ esetén van olyan $t \in \mathbf{0}$ és $r \in \lambda$, hogy $s = t + r < 0 + r = r$, így $s \in \lambda$. Láthatóan itt azt használtuk fel, hogy $\mathbb{Q}$-ban az összeadásra és a természetes rendezésre $(\mathrm{KO_I})$, valamint

λ-ra ($\mathrm{D_{III}}$) teljesül. Ez azt jelenti, hogy $\mathbf{0} + \lambda \subseteq \lambda$. Megfordítva, ha $s \in \lambda$, akkor a ($\mathrm{D_{II}}$) miatt van olyan $r \in \lambda$, hogy $s < r$; ekkor $s = (s - r) + r \in \mathbf{0} + \lambda$, így $\lambda \subseteq \mathbf{0} + \lambda$. Ezzel megmutattuk, hogy minden $\lambda \in \mathbb{R}$ esetén $\lambda = \mathbf{0} + \lambda$, tehát a $+$ művelet kommutativitása miatt $\mathbf{0}$ a $+$ műveletnek neutrális eleme.

Legyen $\lambda \in \mathbb{R}$; olyan $\lambda' \in \mathbb{R}$ elemet keresünk, amelyre $\lambda + \lambda' = \mathbf{0}$ teljesül. Két eset lehetséges.

– Tegyük fel, hogy λ-nak létezik szuprémuma $\mathbb{Q}$-ban, és legyen ez $\bar{r}$. Ekkor a $\lambda' :=] \leftarrow, -\bar{r}[$ intervallum $\mathbb{Q}$-ban olyan, hogy $\lambda' \in \mathbb{R}$, és $\lambda + \lambda' = \mathbf{0}$ teljesül. Valóban, ha $r \in \lambda$ és $r' \in \lambda'$, akkor $r + r' < r + (-\bar{r}) \leq 0$, mert $\bar{r}$ felső korlátja λ-nak, ezért $r + r' \in \mathbf{0}$, ami azt jelenti, hogy $\lambda + \lambda' \subseteq \mathbf{0}$. Megfordítva, ha $s \in \mathbf{0}$, akkor $\bar{r} + s$ nem felső korlátja λ-nak, tehát van olyan $r \in \lambda$, hogy $\bar{r} + s < r$; ekkor $s = r + (s - r) \in \lambda + \lambda'$, mert $s - r < -\bar{r}$. Tehát $\mathbf{0} \subseteq \lambda + \lambda'$ is teljesül.

– Tegyük fel, hogy λ-nak nem létezik szuprémuma $\mathbb{Q}$-ban. Legyen

$$\lambda' := \{-r' | (r' \in \mathbb{Q}) \wedge (\forall r \in \lambda)(r \leq r')\},$$

vagyis λ' a λ felső korlátjai $\mathbb{Q}$-beli additív inverzeinek halmaza. Először igazoljuk, hogy $\lambda' \in \mathbb{R}$. A λ' halmaz nem üres, mert λ felülről korlátos $\mathbb{Q}$-ban. Ha $r \in \lambda$, akkor $-r$ felső korlátja λ'-nek $\mathbb{Q}$-ban, tehát λ' felülről korlátos $\mathbb{Q}$-ban, mert $\lambda \neq \emptyset$. Ezért λ'-re ($\mathrm{D_I}$) teljesül. Ha $s \in \lambda'$, és r' olyan felső korlátja $\mathbb{Q}$-ban λ-nak, hogy $s = -r'$, akkor van olyan r'' felső korlátja $\mathbb{Q}$-ban λ-nak, hogy $r'' < r'$, különben r' a λ szuprémuma volna $\mathbb{Q}$-ban; ekkor $s = -r' < -r'' \in \lambda'$, tehát λ'-re ($\mathrm{D_{II}}$) teljesül. Legyen $s \in \lambda'$, $t \in \mathbb{Q}$ és $t < s$; ekkor van olyan r' felső korlátja $\mathbb{Q}$-ban λ-nak, hogy $s = -r'$, tehát $r' = -s < -t$, vagyis $-t$ a felső korlátja $\mathbb{Q}$-ban λ-nak, így $t = -(-t) \in \lambda'$. Ezért λ'-re ($\mathrm{D_{III}}$) is teljesül, vagyis $\lambda' \in \mathbb{R}$. Most megmutatjuk, hogy $\lambda + \lambda' = \mathbf{0}$. Ha $r \in \lambda$ és r' felső korlátja $\mathbb{Q}$-ban λ-nak, akkor $r \leq r'$, tehát $r - r' \leq 0$, és $r - r' \neq 0$, különben r' a λ szuprémuma volna $\mathbb{Q}$-ban; ez azt jelenti, hogy $r + (-r') \in \mathbf{0}$, vagyis $\lambda + \lambda' \subseteq \mathbf{0}$. Megfordítva, legyen $s \in \mathbf{0}$ tetszőleges, vagyis $s \in \mathbb{Q}$ és $s < 0$. Rögzítsünk egy $r' \in \mathbb{Q}$ számot, amely a λ halmaznak felső korlátja. Ha $r \in \lambda$, akkor $-s > 0$ és a $\mathbb{Q}$ archimédészi rendezettsége folytán van olyan $n \in \mathbb{N}$, hogy $r' - r < n \cdot (-s)$, így $r' + n \cdot s < r \in \lambda$, tehát $r' + n \cdot s$ *nem felső korlátja* λ-nak. Az $\mathbb{N}$ jólrendezettsége miatt létezik az a legkisebb $n \in \mathbb{N}$, amelyre $r' + n \cdot s$ nem felső korlátja λ-nak. Ekkor $r' + n \cdot s \in \lambda$, mert λ-ra ($\mathrm{D_{III}}$) teljesül, ugyanakkor $n > 0$, mert r' a λ-nak felső korlátja, tehát $r' + (n - 1) \cdot s$ felső korlátja λ-nak. Ekkor a λ' definíciója szerint $-(r' + (n-1) \cdot s) \in \lambda'$, és $s = (r' + n \cdot s) + (-(r' + (n-1) \cdot s)) \in \lambda + \lambda'$, amivel igazoltuk, hogy $\mathbf{0} \subseteq \lambda + \lambda'$.

Ezzel beláttuk, hogy $+$ kommutatív csoportművelet $\mathbb{R}$ felett. Legyenek most $\lambda, \lambda', \sigma \in \mathbb{R}$ olyanok, hogy $\lambda \leq \lambda'$. Ha $r \in \lambda$ és $s \in \sigma$, akkor $r \in \lambda'$, mert $\lambda \subseteq \lambda'$, tehát $r + s \in \lambda' + \sigma$. Ez azt jelenti, hogy $\lambda + \sigma \subseteq \lambda' + \sigma$, vagyis az $\mathbb{R}$ feletti $+$ műveletre és $\leq$ rendezésre ($\mathrm{KO_I}$) teljesül.

Jelölje $\mathbb{R}^+$ a $\mathbf{0}$-nál nagyobb valós számok, és $\mathbb{Q}^+$ a 0-nál nagyobb racionális számok halmazát. Nyilvánvaló, hogy $\lambda \in \mathbb{R}$ esetén $\lambda \in \mathbb{R}^+$ pontosan akkor teljesül, ha $\lambda \cap \mathbb{Q}^*_+ \neq \emptyset$. Most egy műveletet értelmezünk az $\mathbb{R}^*_+$ halmaz felett; minden $\lambda, \lambda' \in \mathbb{R}^*_+$ esetén legyen:

$$\lambda \cdot \lambda' :=] \leftarrow, 0] \cup \{r \cdot r' | (r \in \lambda \cap \mathbb{Q}^*_+) \wedge (r' \in \lambda' \cap \mathbb{Q}^*_+)\}.$$

Először megmutatjuk, hogy $\lambda, \lambda' \in \mathbb{R}^*_+$ esetén $\lambda \cdot \lambda' \in \mathbb{R}^*_+$. Világos, hogy $\lambda \cdot \lambda'$ felülről korlátos $\mathbb{Q}$-ban, mert ha s (illetve s') a λ (illetve λ') felső korlátja $\mathbb{Q}$-ban, akkor $s \cdot s'$ a $\lambda \cdot \lambda'$-nek felső korlátja $\mathbb{Q}$-ban. Ha $r \in \lambda \cap \mathbb{Q}^*_+$ és $r' \in \lambda' \cap \mathbb{Q}^*_+$, akkor van olyan $s \in \lambda$, hogy $r < s$, és van olyan $s' \in \lambda'$, hogy $r' < s'$; ekkor $s \cdot s' \in \lambda \cdot \lambda'$, és $r \cdot r' < s \cdot s'$, vagyis

$\lambda \cdot \lambda'$-ra ($\mathrm{D_{II}}$) teljesül. Ha $s \in \mathbb{Q}_+^*$, $r \in \lambda \cap \mathbb{Q}_+^*$ és $r' \in \lambda' \cap \mathbb{Q}_+^*$ olyanok, hogy $s < r \cdot r'$, akkor $s/r < r'$ miatt $s/r \in \lambda' \cap \mathbb{Q}_+^*$, és $s = r \cdot (s/r) \in \lambda \cdot \lambda'$, így $\lambda \cdot \lambda'$-re ($\mathrm{D_{III}}$) teljesül, vagyis $\lambda \cdot \lambda' \in \mathbb{R}_+^*$.

Megmutatjuk, hogy a $\cdot$ művelet asszociatív. Ehhez legyenek $\lambda, \lambda', \lambda'' \in \mathbb{R}_+^*$ rögzítve, és legyen $s \in ((\lambda \cdot \lambda') \cdot \lambda'') \cap \mathbb{Q}_+^*$. Ekkor van olyan $r \in \lambda \cap \mathbb{Q}_+^*$, $r' \in \lambda' \cap \mathbb{Q}_+^*$ és $r'' \in \lambda'' \cap \mathbb{Q}_+^*$, hogy $s = (r \cdot r') \cdot r''$. De a $\mathbb{Q}$ feletti szorzás asszociativitása miatt $(r \cdot r') \cdot r'' = r \cdot (r' \cdot r'') \in (\lambda \cdot (\lambda' \cdot \lambda'')) \cap \mathbb{Q}_+^*$, így $(\lambda \cdot \lambda') \cdot \lambda'' \subseteq \lambda \cdot (\lambda' \cdot \lambda'')$. Teljesen hasonlóan kapjuk, hogy $\lambda \cdot (\lambda' \cdot \lambda'') \subseteq (\lambda \cdot \lambda') \cdot \lambda''$ is teljesül.

Igazoljuk azt, hogy a $\cdot$ művelet kommutatív. Ehhez legyenek $\lambda, \lambda' \in \mathbb{R}_+^*$ rögzítve, és legyen $s \in (\lambda \cdot \lambda') \cap \mathbb{Q}_+^*$. Ekkor van olyan $r \in \lambda \cap \mathbb{Q}_+^*$ és $r' \in \lambda' \cap \mathbb{Q}_+^*$, hogy $s = r \cdot r'$. De a $\mathbb{Q}$ feletti szorzás kommutativitása miatt $r \cdot r' = r' \cdot r \in (\lambda' \cdot \lambda) \cap \mathbb{Q}_+^*$, így $\lambda \cdot \lambda' \subseteq \lambda' \cdot \lambda$. Ez bármely két $\lambda, \lambda' \in \mathbb{R}_+^*$ elemre igaz, ezért $\lambda \cdot \lambda' = \lambda' \cdot \lambda$.

Megmutatjuk, hogy az $\mathbf{1} := \{r \in \mathbb{Q} | r < 1\} \in \mathbb{R}_+^*$ elem a $\cdot$ műveletnek neutrális eleme. Ehhez legyen $\lambda \in \mathbb{R}_+^*$, és legyen $s \in (\mathbf{1} \cdot \lambda) \cap \mathbb{Q}_+^*$. Van olyan $t \in \mathbf{1} \cap \mathbb{Q}_+^*$ és $r \in \lambda \cap \mathbb{Q}_+^*$, hogy $s = t \cdot r$; ekkor $t < 1$ és $0 < r$ miatt $s < r$, így $s \in \lambda \cap \mathbb{Q}_+^*$, mert λ-ra ($\mathrm{D_{III}}$) teljesül. Ez azt jelenti, hogy $\mathbf{1} \cdot \lambda \subseteq \lambda$. Megfordítva, legyen $s \in \lambda \cap \mathbb{Q}_+^*$; a ($\mathrm{D_{II}}$) miatt van olyan $r \in \lambda$, hogy $s < r$; ekkor $s/r \in \mathbf{1} \cap \mathbb{Q}_+^*$, $r \in \lambda \cap \mathbb{Q}_+^*$ és $s = (s/r) \cdot r \in (\mathbf{1} \cdot \lambda) \cap \mathbb{Q}_+^*$, amiből következik, hogy $\lambda \subseteq \mathbf{1} \cdot \lambda$.

Bebizonyítjuk, hogy a $\cdot$ művelet disztributív a $+$ művelet $\mathbb{R}_+^* \times \mathbb{R}_+^*$-ra vett leszűkítésére nézve. Ehhez legyenek $\sigma, \lambda, \lambda' \in \mathbb{R}_+^*$ rögzítve. Ha $s \in \sigma \cap \mathbb{Q}_+^*$, $r \in \lambda \cap \mathbb{Q}_+^*$ és $r' \in \lambda' \cap \mathbb{Q}_+^*$, akkor $s \cdot (r + r') = s \cdot r + s \cdot r'$, mert a szorzás disztributív az összeadásra nézve $\mathbb{Q}$-ban; ugyanakkor $s \cdot r + s \cdot r' \in \sigma \cdot \lambda + \sigma \cdot \lambda'$, így $\sigma \cdot (\lambda + \lambda') \subseteq \sigma \cdot \lambda + \sigma \cdot \lambda'$. Megfordítva, legyen $t \in (\sigma \cdot \lambda + \sigma \cdot \lambda') \cap \mathbb{Q}_+^*$ tetszőleges. Ekkor van olyan $s, s' \in \sigma$, $r \in \lambda \cap \mathbb{Q}_+^*$ és $r' \in \lambda' \cap \mathbb{Q}_+^*$, hogy $t = s \cdot r + s' \cdot r'$. Ha $\bar{s} := max(s, s')$, akkor $\bar{s} \in \sigma$, és $t = s \cdot r + s' \cdot r' \le \bar{s} \cdot (r + r') \in \sigma \cdot (\lambda + \lambda')$, így $\sigma \cdot \lambda + \sigma \cdot \lambda' \subseteq \sigma \cdot (\lambda + \lambda')$.

Megmutatjuk, hogy a $\cdot$ művelet szerint az $\mathbb{R}_+^*$ minden elemének van inverze (tehát $\cdot$ az $\mathbb{R}_+^*$ halmaz felett *kommutatív csoportművelet*). Legyen $\lambda \in \mathbb{R}_+^*$; olyan $\lambda' \in \mathbb{R}_+^*$ elemet keresünk, amelyre $\lambda \cdot \lambda' = \mathbf{1}$ teljesül. Két eset lehetséges.

– Tegyük fel, hogy λ-nak létezik szuprémuma $\mathbb{Q}$-ban, és legyen ez $\bar{r}$. Ekkor a $\lambda' :=]\leftarrow, 1/\bar{r}[$ intervallum $\mathbb{Q}$-ban olyan, hogy $\lambda' \in \mathbb{R}_+^*$, és $\lambda \cdot \lambda' = \mathbf{1}$ teljesül. Valóban, ha $r \in \lambda \cap \mathbb{Q}_+^*$ és $r' \in \lambda' \cap \mathbb{Q}_+^*$, akkor $r \cdot r' < r \cdot (1/\bar{r}) \le 1$, mert $\bar{r}$ felső korlátja λ-nak, ezért $r \cdot r' \in \mathbf{1}$, ami azt jelenti, hogy $\lambda \cdot \lambda' \subseteq \mathbf{1}$. Megfordítva, ha $s \in \mathbf{1} \cap \mathbb{Q}_+^*$, akkor $0 < s < 1$, így $s \cdot \bar{r}$ nem felső korlátja λ-nak, tehát van olyan $r \in \lambda$, hogy $s \cdot \bar{r} < r$; ekkor $s = r \cdot (s/r) \in \lambda \cdot \lambda'$, mert $s/r < 1/\bar{r}$; következésképpen $\mathbf{1} \subseteq \lambda \cdot \lambda'$ is teljesül.

– Tegyük fel, hogy λ-nak nem létezik szuprémuma $\mathbb{Q}$-ban. Legyen

$$\lambda' :=]\leftarrow, 0] \cup \{1/r' | (r' \in \mathbb{Q}_+^*) \wedge (\forall r \in \lambda)(r \le r')\},$$

vagyis λ' a λ felső korlátjai $\mathbb{Q}$-beli multiplikatív inverzeinek halmaza, hozzávéve a $]\leftarrow, 0]$ intervallumot. Megmutatjuk, hogy $\lambda' \in \mathbb{R}_+^*$, és $\lambda \cdot \lambda' = \mathbf{1}$ teljesül. Valóban, ($\mathrm{D_I}$) teljesül λ'-re, mert ha $r \in \lambda \cap \mathbb{Q}_+^*$, akkor $1/r$ felső korlátja $\mathbb{Q}$-ban λ'-nek. Ha $s \in \lambda' \cap \mathbb{Q}_+^*$, akkor van olyan $r' \in \mathbb{Q}$ felső korlátja λ-nak, hogy $s = 1/r'$; ekkor létezik olyan $r'' \in \mathbb{Q}$, amely szintén felső korlátja $\mathbb{Q}$-ban λ-nak és $r'' < r'$ (különben r' a λ-nak szuprémuma volna $\mathbb{Q}$-ban); világos, hogy $s < 1/r'' \in \lambda'$, tehát λ'-re ($\mathrm{D_{II}}$) is teljesül. Legyen $s \in \lambda' \cap \mathbb{Q}_+^*$ és $r \in \mathbb{Q}_+^*$ olyan, hogy $r < s$; ekkor van olyan $r' \in \mathbb{Q}$ felső korlátja λ-nak, hogy $s = 1/r'$, vagyis ekkor $1/s$ felső korlátja $\mathbb{Q}$-ban λ-nak. Ugyanakkor $1/s < 1/r$, tehát $1/r$ is felső korlátja $\mathbb{Q}$-ban λ-nak, tehát $r = 1/(1/r) \in \lambda'$, vagyis λ'-re ($\mathrm{D_{III}}$) is teljesül, így $\lambda' \in \mathbb{R}_+^*$. Azt kell még igazolni, hogy $\lambda \cdot \lambda' = \mathbf{1}$. Ha $r \in \lambda \cap \mathbb{Q}_+^*$ és r' felső korlátja $\mathbb{Q}$-ban λ-nak, akkor $r < r'$ miatt $r \cdot (1/r') < 1$, ezért $\lambda \cdot \lambda' \subseteq \mathbf{1}$. Megfordítva, legyen $s \in \mathbf{1} \cap \mathbb{Q}_+^*$ tetszőleges, vagyis $s \in \mathbb{Q}$ és $0 < s < 1$; olyan $r \in \lambda \cap \mathbb{Q}_+^*$ és $r' \in \mathbb{Q}_+^*$ számokat keresünk, amelyekre r' a λ-nak felső korlátja $\mathbb{Q}$-ban, és $s \leq r/r'$. Ehhez legyen $r_0 \in \lambda \cap \mathbb{Q}_+^*$ és $r_0' \in \mathbb{Q}$ rögzített felső korlátja λ-nak. Értelmezzük a következő függvényt:

$$f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \times \mathbb{Q}; \quad (r, r') \mapsto \begin{cases} (\frac{r+r'}{2}, r') & \text{, ha } \frac{r+r'}{2} \in \lambda \\ (r, \frac{r+r'}{2}) & \text{, ha } \frac{r+r'}{2} \notin \lambda \end{cases},$$

és vegyük az $(r_0, r_0') \in \mathbb{Q} \times \mathbb{Q}$ kezdőpont és az f függvény által meghatározott iterációs sorozatot; jelölje ezt $((r_n, r_n')_{n \in \mathbb{N}})$. n szerinti teljes indukcióval könnyen belátható, hogy minden $n \in \mathbb{N}$ számra $r_n \in \lambda \cap \mathbb{Q}_+^*$, $r_n \leq r_{n+1}$, $r_{n+1}' \leq r_n'$, $r_n' - r_n = \frac{r_0' - r_0}{2^n}$, és r_n' felső korlátja λ-nak. Legyen $n \in \mathbb{N}$ olyan, hogy

$$2^n > \frac{\left(\frac{r_0'}{r_0}\right) - 1}{1 - s}.$$

Ekkor

$$r_n' > r_n \geq r_0 > \frac{1}{2^n} \cdot \left(\frac{r_0' - r_0}{1 - s}\right) = \frac{r_n' - r_n}{1 - s},$$

amiből azonnal kapjuk, hogy $s < r_n/r_n' \in \lambda \cdot \lambda'$. Ezért $s \in \lambda'$, ami azt jelenti, hogy $\mathbf{1} \subseteq \lambda \cdot \lambda'$, ilymódon λ' a λ inverze a $\cdot$ művelet szerint.

Most a $\cdot$ műveletet kiterjesztjük $\mathbb{R}$-re úgy, hogy minden $\lambda \in \mathbb{R}$ esetén

$$\lambda \cdot \mathbf{0} := \mathbf{0} \cdot \lambda := \mathbf{0},$$

továbbá minden $\lambda, \lambda' \in \mathbb{R} \setminus \{\mathbf{0}\}$ esetén:

$$\lambda \cdot \lambda' := \begin{cases} -(\lambda \cdot (-\lambda')) & \text{, ha } \lambda > \mathbf{0} \text{ és } \lambda' < \mathbf{0} \\ -((-\lambda) \cdot \lambda') & \text{, ha } \lambda < \mathbf{0} \text{ és } \lambda' > \mathbf{0} \\ (-\lambda) \cdot (-\lambda') & \text{, ha } \lambda < \mathbf{0} \text{ és } \lambda' < \mathbf{0} \end{cases}.$$

Kissé hosszadalmas, de teljesen elemi, esetszétválasztásos módszerrel beláthatjuk, hogy $\cdot$ olyan művelet $\mathbb{R}$, hogy az $(\mathbb{R}, +, \cdot)$ hármas test, továbbá természetesen a $\cdot$ műveletre $(\mathrm{KO_{II}})$ teljesül, vagyis az $(\mathbb{R}, +, \cdot, \leq)$ négyes teljesen rendezett test.

Legyen $(K, +, \cdot, \leq)$ teljesen rendezett test, és tekintsük az előző állításban értelmezett $f_K : K \to \mathbb{R};\ x \mapsto \{r \in \mathbb{Q} | r < x\}$ bijekciót.

Ha $x, y \in K$ és $x \leq y$, akkor $r \in f_K(x)$ esetén $r < x$, ezért $r < y$, vagyis $r \in f_K(y)$, ami azt jelenti, hogy $f_K(x) \subseteq f_K(y)$. Megfordítva, ha $x, y \in K$ és $f_K(x) \subseteq f_K(y)$, akkor $y < x$ lehetetlen, különben a K archimédészi rendezettsége folytán létezne olyan $r \in \mathbb{Q}$, amelyre $y < r < x$, vagyis $r \in f_K(x)$, de $r \notin f_K(y)$, ami ellentmondás. Ez azt jelenti, hogy $x, y \in K$ és $f_K(x) \subseteq f_K(y)$ esetén $x \leq y$, következésképpen az f_K függvény rendezés-izomorfizmus a K és $\mathbb{R}$ rendezett halmazok között.

Legyenek $x, y \in K$ rögzítve. Ha $r \in f_K(x)$ és $s \in f_K(y)$, akkor $r < x$ és $s < y$, így $r + s < x + y$, tehát $r + s \in f_K(x + y)$, amiből az $\mathbb{R}$ feletti összeadás értelmezése alapján következik, hogy $f_K(x) + f_K(y) \subseteq f_K(x + y)$. Megfordítva, tegyük fel, hogy $t \in f_K(x + y)$, vagyis $t \in \mathbb{Q}$ olyan, hogy $t < x + y$. Ekkor $t - y < x$, tehát a K archimédészi rendezettsége miatt van olyan $r \in \mathbb{Q}$, amelyre $t - y < r < x$. Ekkor $r \in f_K(x)$ és $t - r < y$, így a K archimédészi rendezettsége miatt van olyan $s \in \mathbb{Q}$, amelyre $t - r < s < y$. Ekkor $s \in f_K(y)$ és $t < r + s \in f_K(x) + f_K(y)$, tehát a Dedekind-szeletek $(\mathrm{D_{III}})$ tulajdonsága szerint $t \in f_K(x) + f_K(y)$. Ez azt jelenti, hogy $f_K(x+y) \subseteq f_K(x) + f_K(y)$, így az f_K függvény *additív.*

Legyenek most $x, y \in K$ olyanok, hogy $x > 0$ és $y > 0$. Ha $r \in f_K(x) \cap \mathbb{Q}_+^*$ és $s \in f_K(y) \cap \mathbb{Q}_+^*$, akkor $0 < r < x$ és $0 < s < y$, így $r \cdot s < x \cdot y$, tehát $r \cdot s \in f_K(x \cdot y)$, amiből az $\mathbb{R}_+^*$ feletti szorzás értelmezése alapján következik, hogy $f_K(x) \cdot f_K(y) \subseteq f_K(x \cdot y)$. Megfordítva, tegyük fel, hogy $t \in f_K(x \cdot y)$, vagyis $t \in \mathbb{Q}$ olyan, hogy $t < x \cdot y$. Ekkor $t \cdot y^{-1} < x$, tehát a K archimédészi rendezettsége miatt van olyan $r \in \mathbb{Q}$, amelyre $t \cdot y^{-1} < r < x$. Ekkor $r \in f_K(x)$ és $t \cdot r^{-1} < y$, így a K archimédészi rendezettsége miatt van olyan $s \in \mathbb{Q}$, amelyre $t \cdot r^{-1} < s < y$. Ekkor $s \in f_K(y)$ és $t < r \cdot s \in f_K(x) \cdot f_K(y)$, tehát a Dedekind-szeletek ($\mathrm{D_{III}}$) tulajdonsága szerint $t \in f_K(x) \cdot f_K(y)$. Ez azt jelenti, hogy $f_K(x \cdot y) \subseteq f_K(x) \cdot f_K(y)$, így $f_K(x \cdot y) = f_K(x) \cdot f_K(y)$ teljesül, ha $x > 0$ és $y > 0$. Ugyanakkor tetszőleges $x, y \in K$ elemekre:

$$x \cdot 0 = 0 \cdot x = 0,$$
$$x \cdot y = -(x \cdot (-y)) = -((-x) \cdot y) = (-x) \cdot (-y),$$

amiből az $\mathbb{R}$ feletti szorzás értelmezése alapján kapjuk, hogy f_K *multiplikatív.*

Legyen most $f : K \to \mathbb{R}$ tetszőleges olyan bijekció, amely additív, multiplikatív és szigorúan rendezés-tartó; megmutatjuk, hogy $f = f_K$. Ehhez legyen $L := \{x \in K | f(x) = f_K(x)\}$; azt kell igazolni, hogy $L = K$. Először is megjegyezzük, hogy az f és f_K additivitása miatt minden $x, y \in L$ esetén $x + y \in L$, továbbá az f és f_K multiplikativitása miatt minden $x, y \in L$ esetén $x \cdot y \in L$ teljesül. Az f additivitásából következik, hogy $f(0)+f(0) = f(0+0) = f(0)$, ezért $f(0) = \mathbf{0} = f_K(0)$, vagyis $0 \in L$. Ha $\lambda \in \mathbb{R}$ tetszőleges, akkor az f szürjektivitása miatt van olyan $x \in K$, amelyre $f(x) = \lambda$; ekkor az f multiplikativitása szerint $f(1) \cdot \lambda = f(1) \cdot f(x) = f(1 \cdot x) = f(x) = \lambda$, ezért $f(1) = \mathbf{1} = f_K(1)$, azaz $1 \in L$. Ebből teljes indukcióval kapjuk, hogy minden $\mathbb{N} \subseteq L$, mert ha $n \in \mathbb{N}$ és $n \in L$, akkor $n + 1 \in L$. Ugyanakkor $x \in K$ esetén $f(x) + f(-x) = f(x + (-x)) = f(0) = \mathbf{0}$, tehát $f(-x) = -f(x)$. Ezért minden $x \in L$ esetén $-x \in L$ teljesül, következésképpen $\mathbb{Z} \subseteq L$. Ha $x \in K \setminus \{0\}$, akkor az f multiplikativitása miatt $f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(1) = \mathbf{1}$, következésképpen $f(x^{-1}) = f(x)^{-1}$. Ebből kapjuk, hogy $x \in L \setminus \{0\}$ esetén $x^{-1} \in L$, így $\mathbb{Q} \subseteq L$, hiszen minden $q \in \mathbb{Z}$ és $p \in \mathbb{Z}^*$ esetén $q, p \in L$ és $p^{-1} \in L$, tehát $q \cdot p^{-1} \in L$. Legyen most $x \in K$ tetszőleges. Láttuk, hogy $x = \sup_K\{r \in \mathbb{Q} | r < x\}$ teljesül. Ekkor

$$f(x) = f(\sup_K\{r \in \mathbb{Q} | r < x\}) = \sup_{\mathbb{R}} f\langle\{r \in \mathbb{Q} | r < x\}\rangle =$$
$$= \sup_{\mathbb{R}}\{f(r) | (r \in \mathbb{Q}) \wedge (r < x)\} = \bigcup_{(r \in \mathbb{Q}) \wedge (r < x)} f(r) = \bigcup_{(r \in \mathbb{Q}) \wedge (r < x)} f_K(r),$$

mert az f függvény izomorfizmus a K és $\mathbb{R}$ rendezett halmazok között. Tehát ha $s \in f(x) = \bigcup_{(r \in \mathbb{Q}) \wedge (r < x)} f_K(r)$, akkor van olyan $r \in \mathbb{Q}$, amelyre $r < x$ és $s \in f_K(r)$; ekkor $s < r$, így $s < x$, vagyis $s \in f_K(x)$. Ez azt jelenti, hogy $f(x) \subseteq f_K(x)$. Megfordítva, ha $s \in f_K(x)$, akkor $s < x$, tehát a K archimédészi rendezettsége miatt van olyan $r \in \mathbb{Q}$, hogy $s < r < x$; ekkor $s \in f_K(r) \subseteq f(x)$, vagyis $s \in f(x)$, ami azt jelenti, hogy $f_K(x) \subseteq f(x)$. Ezzel megmutattuk, hogy $f = f_K$.

Ha most $(K_1, +_1, \cdot_1, \leq_1)$ és $(K_2, +_2, \cdot_2, \leq_2)$ teljesen rendezett testek, akkor az előzőek alapján az $f_{K_2}^{-1} \circ f_{K_1} : K_1 \to K_2$ függvény additív, multiplikatív és szigorúan rendezés-tartó bijekció; tehát ilyen tulajdonságú függvény *létezik.* Ha $f : K_1 \to K_2$ tetszőleges olyan bijekció, amely additív, multiplikatív és szigorúan rendezés-tartó, akkor az $f_{K_2} \circ f :$

$K_1 \to \mathbb{R}$ leképezés szintén additív, multiplikatív és szigorúan rendezés-tartó, így az előzőek szerint $f_{K_2} \circ f = f_{K_1}$, tehát $f = f_{K_2}^{-1} \circ f_{K_1}$, vagyis az ilyen tulajdonságú függvény *egyértelmű.* ■

19. Mutassuk meg, hogy egy rendezett test pontosan akkor archimédészi módon rendezett test, ha izomorf az $\mathbb{R}$ valamelyik rendezett résztestével. Továbbá, egy archimédészi módon rendezett test pontosan akkor teljesen rendezett, ha izomorf a valós számok testével.

(*Útmutatás.* Archimédészi módon rendezett test minden rendezett résztestе nyilvánvalóan archimédészi módon rendezett. Másfelől, láttuk hogy ha K archimédészi módon rendezett test, akkor az $f_K : K \to \mathbb{R};\ x \mapsto \{r \in \mathbb{Q} | r < x\}$ leképezés injektív, művelet-tartó és szigorúan rendezés-tartó. Ez a leképezés pontosan akkor szürjektív (tehát izomorfizmus K és $\mathbb{R}$ között), ha K teljesen rendezett.)

23.6. A komplex számok teste

A valós számtestben az $x^2 = y$ egyenlet nem oldható meg x-re akkor, ha $y < 0$. Sőt ez az egyenlet semmilyen rendezett testben nem oldható meg x-re negatív y esetén. Azonban könnyen megadhatjuk $\mathbb{R}$ olyan "testbővítését", amelyben ez az egyenlet minden y-ra megoldható.

23.6.1. Állítás. *Az $\mathbb{R} \times \mathbb{R}$ halmazon értelmezzük a $+$ és $\cdot$ műveleteket úgy, hogy minden $(x, y), (x', y') \in \mathbb{R} \times \mathbb{R}$ párra:*

$$(x, y) + (x', y') := (x + x', y + y'),$$

$$(x, y) \cdot (x', y') := (x \cdot x' - y \cdot y', x \cdot y' + x' \cdot y).$$

Ekkor az $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ hármas olyan test, amelyben az $x^2 = -\mathbf{1}$ egyenlet megoldható, és a

$$\mathrm{j} : \mathbb{R} \to \mathbb{R} \times \mathbb{R}; \quad x \mapsto (x, 0)$$

leképezés olyan injekció, hogy minden $x, x' \in \mathbb{R}$ esetén $\mathrm{j}(x + x') = \mathrm{j}(x) + \mathrm{j}(x')$ és $\mathrm{j}(x \cdot x') = \mathrm{j}(x) \cdot \mathrm{j}(x')$ teljesül.

Bizonyítás. (I) Ha $(x, y), (x', y'), (x'', y'') \in \mathbb{R} \times \mathbb{R}$, akkor

$$((x, y) + (x', y')) + (x'', y'') = (x + x', y + y') + (x'', y'') = ((x + x') + x'', (y + y') + y'') \overset{(1)}{=}$$
$$\overset{(1)}{=} (x + (x' + x''), y + (y' + y'')) = (x, y) + (x' + x'', y' + y'') = (x, y) + ((x', y') + (x'', y'')),$$

ahol az $\overset{(1)}{=}$ egyenlőségnél az $\mathbb{R}$ feletti összeadás asszociativitását alkalmaztuk. Ezért az $\mathbb{R} \times \mathbb{R}$ felett bevezetett $+$ művelet asszociatív.

Ha $(x, y), (x', y') \in \mathbb{R} \times \mathbb{R}$, akkor

$$(x, y) + (x', y') = (x + x', y + y') \overset{(2)}{=} (x' + x, y' + y) = (x', y') + (x, y),$$

ahol a $\overset{(2)}{=}$ egyenlőségnél az $\mathbb{R}$ feletti összeadás kommutativitását alkalmaztuk. Ezért az $\mathbb{R} \times \mathbb{R}$ felett bevezetett $\cdot$ művelet kommutatív.

Ha $(x, y) \in \mathbb{R} \times \mathbb{R}$, akkor $(x, y) + (0, 0) = (x + 0, y + 0) = (x, y)$, így $(0, 0)$ neutrális elem az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $+$ művelet szerint. Ha $(x,y)\in\mathbb{R}\times\mathbb{R}$, akkor $(x,y)+(-x,-y)=x+(-x),y+(-y))=(0,0)$, tehát $(-x,-y)$ az (x,y) elem inverze az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $+$ művelet szerint.

Ez azt jelenti, hogy az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $+$ műveletre a 16.2.1. definícióban szereplő $(\mathrm{K_I})$ tulajdonság teljesül.

(II) Ha $(x,y),(x',y'),(x'',y'')\in\mathbb{R}\times\mathbb{R}$, akkor

$$((x,y)\cdot(x',y'))\cdot(x'',y'')=(x\cdot x'-y\cdot y',x\cdot y'+x'\cdot y)\cdot(x'',y'')=$$
$$=((x\cdot x'-y\cdot y')\cdot x''-(x\cdot y'+x'\cdot y)\cdot y'',(x\cdot x'-y\cdot y')\cdot y''+(x\cdot y'+x'\cdot y)\cdot x'')\stackrel{(3)}{=}$$
$$\stackrel{(3)}{=}(x\cdot(x'\cdot x''-y'\cdot y'')-y\cdot(x'\cdot y''+x''\cdot y'),x\cdot(x'\cdot y''+x''\cdot y')+y\cdot(x'\cdot x''-y'\cdot y''))=$$
$$=(x,y)\cdot(x'\cdot x''-y'\cdot y'',x'\cdot y''+x''\cdot y')=(x,y)\cdot((x',y')\cdot(x'',y'')),$$

ahol a $\stackrel{(2)}{=}$ egyenlőségnél mindkét komponensben kiemeltük az x és y szorzó-tényezőket, kihasználva az $\mathbb{R}$ feletti műveletek tulajdonságait. Ezért az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $\cdot$ művelet asszociatív.

Ha $(x,y),(x',y')\in\mathbb{R}\times\mathbb{R}$, akkor

$$(x,y)\cdot(x',y')=(x\cdot x'-y\cdot y',x\cdot y'+x'\cdot y)\stackrel{(4)}{=}(x'\cdot x-y'\cdot y,x'\cdot y+y'\cdot x)=(x',y')\cdot(x,y),$$

ahol a $\stackrel{(4)}{=}$ egyenlőségnél felhasználtuk az $\mathbb{R}$ feletti szorzás és összeadás kommutativitását. Ezért az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $\cdot$ művelet kommutatív.

Ha $(x,y)\in\mathbb{R}\times\mathbb{R}$, akkor $(x,y)\cdot(1,0)=(x\cdot 1-y\cdot 0,x\cdot 0+y\cdot 1)=(x.y)$, így $(1,0)$ neutrális elem az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $\cdot$ művelet szerint, és természetesen $(1,0)\neq(0,0)$.

Legyen $(x,y)\in(\mathbb{R}\times\mathbb{R})\setminus\{(0,0)\}$, tehát $x\neq 0$ vagy $y\neq 0$. Az Artin–Schreier-tétel (**??**) alapján $x^2+y^2\neq 0$, tehát vehetjük az x^2+y^2 valós szám $(x^2+y^2)^{-1}$ multiplikatív inverzét. Ekkor

$$(x,y)\cdot\left(x\cdot(x^2+y^2)^{-1},-y\cdot(x^2+y^2)^{-1}\right)=$$
$$=\left(x^2\cdot(x^2+y^2)^{-1}+y^2\cdot(x^2+y^2)^{-1},x\cdot(-y)\cdot(x^2+y^2)^{-1}+y\cdot x\cdot(x^2+y^2)^{-1}\right)=(1,0),$$

tehát az $(x\cdot(x^2+y^2)^{-1},-y\cdot(x^2+y^2)^{-1})$ pár az (x,y) elem inverze az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $\cdot$ művelet szerint.

Ez azt jelenti, hogy az $\mathbb{R}\times\mathbb{R}$ felett bevezetett $\cdot$ műveletre a 16.2.1. definícióban szereplő $(\mathrm{K_{II}})$ tulajdonság teljesül.

(III) Ha $(x,y),(x',y'),(x'',y'')\in\mathbb{R}\times\mathbb{R}$, akkor

$$(x,y)\cdot((x',y')+(x'',y''))=(x,y)\cdot(x'+x'',y'+y'')=$$
$$=(x\cdot(x'+x'')-y\cdot(y'+y''),x\cdot(y'+y'')+y\cdot(x'+x''))\stackrel{(5)}{=}$$
$$\stackrel{(5)}{=}((x\cdot x'-y\cdot y')+(x\cdot x''-y\cdot y''),(x\cdot y'+x'\cdot y)+(x\cdot y''+x''\cdot y))=$$
$$=(x\cdot x'-y\cdot y',x\cdot y'+x'\cdot y)+(x\cdot x''-y\cdot y'',x\cdot y''+x''\cdot y)=$$
$$=(x,y)\cdot(x',y')+(x,y)\cdot(x'',y''),$$

ahol az $\stackrel{(5)}{=}$ egyenlőségnél felhasználtuk azt, hogy az $\mathbb{R}$ feletti szorzás disztributív az $\mathbb{R}$ feletti összeadásra nézve. Ezért az $\mathbb{R}\times\mathbb{R}$ feletti $\cdot$ művelet disztributív az $\mathbb{R}\times\mathbb{R}$ feletti összeadásra nézve, vagyis a 16.2.1. definícióban szereplő $(\mathrm{K_{III}})$ tulajdonság teljesül, tehát az $(\mathbb{R} \times \mathbb{R}, +\cdot)$ hármas test.

(IV) Nyilvánvaló, hogy $(0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$, és $(-1, 0)$ a multiplikatív neutrális elem additív inverze az $\mathbb{R} \times \mathbb{R}$ testben, tehát az $\mathbf{i} := (0, 1) \in \mathbb{R} \times \mathbb{R}$ elem olyan, hogy $\mathbf{i}^2 = -\mathbf{1}$.

Végül, a $\mathrm{j} : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$; $x \mapsto (x, 0)$ injekció additív (azaz összeadás-tartó), mert $x, x' \in \mathbb{R}$ esetén

$$\mathrm{j}(x + x') = (x + x', 0) = (x, 0) + (x'.0) = \mathrm{j}(x) + \mathrm{j}(x'),$$

továbbá a j függvény multiplikatív (azaz szorzás-tartó) is, mert

$$\mathrm{j}(x) \cdot \mathrm{j}(x') = (x, 0) \cdot (x', 0) = (x \cdot x' - 0 \cdot 0, x \cdot 0 + 0 \cdot x') = (x \cdot x', 0) = \mathrm{j}(x \cdot x'). \blacksquare$$

23.6.2. Definíció. *Az előző állításban bevezetett* $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ *testet a* **komplex számok testének** *nevezzük és* $\mathbb{C}$*-vel jelöljük. A* $\mathbb{C}$ *elemeit* (*tehát a valós számpárokat*) **komplex számoknak** *nevezzük.*

Látható, hogy a komplex számok teste felett nem létezik olyan rendezés, amellyel $\mathbb{C}$ rendezett test volna, azonban a $\mathbb{Z}$ és $\mathbb{C}$ közötti kanonikus leképezés injektív (vagyis a $\mathbb{C}$ test 0 karakterisztikájú), és nemcsak a $\mathbb{Q}$ test, hanem az $\mathbb{R}$ is azonosítható az $\mathbb{C}$ egy "résztestével" (**2**. gyakorlat). Ezért a továbbiakban azt írjuk, hogy $\mathbb{R} \subseteq \mathbb{C}$, amin azt értjük, hogy $\mathbb{R}$ azonosul az $\{(x, 0) | x \in \mathbb{R}\} \subseteq \mathbb{C}$ halmazzal.

Ha $z \in \mathbb{C}$, akkor a z pár első (illetve második) komponensét a z komplex szám *valós* (illetve *képzetes*) *részének* nevezzük, és a $\Re(z)$ (illetve $\Im(z)$) szimbólummal jelöljük. Ha $z \in \mathbb{C}$, akkor a $(\Re(z), -\Im(z))$ komplex számot a z *konjugáltjának* nevezzük és ezt z^* vagy $\bar{z}$ jelöli.

Ha $z \in \mathbb{C}$, akkor $z = \Re(z) + \mathbf{i} \cdot \Im(z)$ teljesül, amin pontosan azt kell érteni, hogy $z = (\Re(z), \Im(z)) = (\Re(z), 0) + (0, 1) \cdot (\Im(z), 0)$.

Később látni fogjuk, hogy $\mathbb{C}$-ben minden komplex együtthatós algebrai egyenlet megoldható, vagyis minden, legalább elsőfokú, komplex együtthatós polinomnak létezik komplex gyöke. Ez az *algebra alaptétele* **MET** (22.4.4.), amit csak jóval később bizonyítunk, mert a bizonyítása eddig még nem érintett, nem triviális analitikus tényeken alapul.

24. fejezet

Involutív algebrai objektumok

24.1. *-félcsoportok és Baer-*-félcsoportok

24.1.1. Definíció. *Azt mondjuk, hogy S* ***-félcsoport***, ha S (multiplikatívan jelölt) félcsoport, és adott egy $S \to S$; $s \mapsto s^*$ egyváltozós művelet, amelyre teljesülnek a következők:*

– *minden $s \in S$ esetén $(s^*)^* = s$* (**involutivitás**),

– *minden $s, t \in S$ esetén $(st)^* = t^* s^*$* (**antimultiplikativitás**).

*A * egyváltozós műveletet az S *-félcsoport* **involúciójának** *nevezzük.*

24.1.2. Állítás. *Legyen S *-félcsoport.*

a) *Az $e \in S$ elem pontosan akkor neutrális elem az S félcsoportban, ha $e = e^*$ és minden $s \in S$ esetén $se = s$.*

b) *A $z \in S$ elem pontosan akkor zéruselem az S félcsoportban, ha $z = z^*$ és minden $s \in S$ esetén $sz = z$.*

Bizonyítás. a) A feltétel szükséges, mert ha $e \in S$ neutrális elem, akkor $e^* = ee^*$, amiből adjungálással következik, hogy $e = (e^*)^* = (e^*)^* = (e^*)^* e^* = ee^* = e^*$, vagyis $e = e^*$. A feltétel elégséges is, mert ha $s \in S$ esetén $s^* e = s^*$, akkor $e = e^*$ alapján adjungálással kapjuk, hogy $s = (s^*)^* = (s^* e)^* = e^*(s^*)^* = es$ is teljesül, így $e \in S$ neutrális elem S-ben.

b) A feltétel szükséges, mert ha $z \in S$ zéruselem, akkor $z^* z = z$, amiből adjungálással következik, hogy $z^* = (z^* z)^* = z^*(z^*)^* = z^* z = z$, vagyis $z = z^*$. A feltétel elégséges is, mert ha $s \in S$ esetén $s^* z = z$, akkor $z = z^*$ alapján adjungálással kapjuk, hogy $z = z^* = (s^* z)^* = z^*(s^*)^* = zs$ is teljesül, így $z \in S$ zéruselem S-ben. ■

Megállapodunk abban, hogy ebben a részben minden félcsoport neutrális elemét 1 és a zéruselemét 0 jelöli, ha ezek léteznek.

24.1.3. Definíció. *Ha S *-félcsoport, akkor $\mathbf{P}(S) := \{e \in S | e = e^2 = e^*\}$, és $\mathbf{P}(S)$ elemeit S* **projektorainak** *nevezzük.*

Ha S *-félcsoport, akkor $\mathbf{P}(S)$ részhalmaza az S félcsoport idempotens elemei halmazának, amelyet $\mathbf{I}(S)$-sel jelöltünk, és amelyet elláttunk egy $\leq$-vel jelölt természetes rendezéssel (12.2.2.), amely szerint $e, f \in \mathbf{I}(S)$ esetén

$$e \leq f \quad \overset{\text{def}}{\Leftrightarrow} \quad e = ef = fe.$$

A továbbiakban a $\mathbf{P}(S)$ halmazt szintén rendezett halmaznak tekintjük, amelynek rendezése az $\mathbf{I}(S)$ feletti természetes rendezés megszorítása $\mathbf{P}(S)$-re.

24.1.4. Állítás. *Legyen S *-félcsoport.*

a) *Ha $e, f \in \mathbf{P}(S)$, akkor*

$$e \leq f \quad \Leftrightarrow \quad e = ef \quad \Leftrightarrow \quad e = fe.$$

b) *Ha S neutrális elemes, akkor $1 \in \mathbf{P}(S)$ és 1 a $(\mathbf{P}(S), \leq)$ rendezett halmaz legnagyobb eleme.*

c) *Ha S zéruselemes, akkor $0 \in \mathbf{P}(S)$ és 0 a $(\mathbf{P}(S), \leq)$ rendezett halmaz legkisebb eleme.*

Bizonyítás. a) Legyenek $e, f \in \mathbf{P}(S)$ rögzítve. Ha $e \leq f$, akkor $e = ef = fe$, tehát $e = ef$ teljesül. Ha $e = ef$, akkor adjungálással kapjuk, hogy $e = e^* = (ef)^* = f^*e^* = fe$, tehát $e = fe$. Ha $e = fe$, akkor adjungálással kapjuk, hogy $e = e^* = (fe)^* = e^*f^* = ef$, tehát ekkor $e = ef = fe$, vagyis $e \leq f$.

b) A 24.1.2. a) állítás szerint $1 = 1^*$ és természetesen 1 idempotens elem, ezért $1 \in \mathbf{P}(S)$. Az 1 elem az $(\mathbf{I}(S), \leq)$ rendezett halmaz legnagyobb eleme, ezért a $(\mathbf{P}(S), \leq)$ rendezett halmaznak még inkább a legnagyobb eleme (12.2.2.).

c) A 24.1.2. b) állítás szerint $0 = 0^*$ és természetesen 0 idempotens elem, ezért $0 \in \mathbf{P}(S)$. A 0 elem az $(\mathbf{I}(S), \leq)$ rendezett halmaz legkisebb eleme, ezért a $(\mathbf{P}(S), \leq)$ rendezett halmaznak még inkább a legkisebb eleme (12.2.2.). ■

24.1.5. Állítás. *Ha S *-félcsoport, akkor minden $e, f \in \mathbf{P}(S)$ esetén*

$$e \leq f \quad \Leftrightarrow \quad eS \subseteq fS,$$

$$e = f \quad \Leftrightarrow \quad eS = fS.$$

Bizonyítás. Ha $e \leq f$, akkor $e = fe$, ezért minden $s \in S$ esetén S szorzásának asszociativitása miatt $es = (fe)s = f(es) \in fS$, ezért $eS \subseteq fS$. Megfordítva, ha $eS \subseteq fS$, akkor $e = e^2 = ee \in eS$ miatt van olyan $s \in S$, hogy $e = fs$, ezért S szorzásának asszociativitása folytán $fe = f(fs) = (ff)s = fs = e$, így $e \leq f$. Tehát $e \leq f \Leftrightarrow eS \subseteq fS$ teljesül, így

$$e = f \quad \Leftrightarrow \quad (e \leq f) \wedge (f \leq e) \quad \Leftrightarrow \quad (eS \subseteq fS) \wedge (fS \subseteq eS) \quad \Leftrightarrow \quad eS = fS$$

is teljesül, hiszen a $\mathbf{P}(S)$ feletti $\leq$ reláció antiszimmetrikus. ■

24.1.6. Definíció. *Azt mondjuk, hogy az S *-félcsoport* **Baer-*-félcsoport***, ha S zéruselemes, és minden $s \in S$ elemhez létezik olyan $e \in \mathbf{P}(S)$ projektor, hogy*

$$eS = \{x \in S | sx = 0\}.$$

Ha S Baer--félcsoport, akkor minden $s \in S$ esetén s' jelöli azt az egyetlen projektort S-ben, amelyre $s'S = \{x \in S | sx = 0\}$.*

24.1.7. Állítás. *Ha S Baer-*-félcsoport, akkor S neutrális elemes félcsoport, valamint $1 = 0'$ és $1' = 0$.*

Bizonyítás. A definíció szerint $0'S = \{x \in S | 0x = 0\} = S$, ezért minden $s \in S$ esetén $s^* \in S = 0'S$, tehát létezik olyan $t \in S$, hogy $s^* = 0't$, így S szorzásának asszociativitása és $0'$ idempotenciája miatt $0's^* = 0'(0't) = (0'0')t = 0't = s^*$. Ebből adjungálással kapjuk, hogy minden $s \in S$ elemre $s = (s^*)^* = (0's^*)^* = (s^*)^*(0')^* = s0'$. Ebből 24.1.2. a) alapján következik, hogy $0'$ a neutrális elem S-ben, vagyis $1 = 0'$.

A definíció szerint $1'S = \{x \in S | 1x = 0\} = \{0\}$, ezért $1' = 1'1 \in 1'S = \{0\}$, vagyis $1' = 0$. ■

24.1.8. Állítás. *Ha S Baer-*-félcsoport, akkor minden $s \in S$ esetén $ss' = 0$ és $s(s')' = s$, továbbá minden $e \in \mathbf{P}(S)$ esetén $e \leq (e')'$.*

Bizonyítás. Legyen $s \in S$ rögzítve. Ekkor $s' = s'1 \in s'S = \{x \in S | sx = 0\}$, ezért $ss' = 0$. Ebből adjungálással kapjuk, hogy $s's^* = (s')^*s^* = (ss')^* = 0^* = 0$, vagyis $s^* \in \{x \in S | s'x = 0\} = (s')'S$. Ezért vehetünk olyan $t \in S$ elemet, amelyre $s^* = (s')'t$, amiből adjungálással adódik, hogy $s = (s^*)^* = t^*((s')')^* = t^*(s')'$. Ezt az egyenlőséget jobbról szorozva az $(s')'$ idempotens elemmel kapjuk, hogy $s(s')' = (t^*(s')')(s')' = t^*(s')' = s$, tehát $s(s')' = s$.

Ha $e \in \mathbf{P}(S)$, akkor az előzőek szerint $e(e')' = e$, ami azt jelenti, hogy $e \leq (e')'$. ■

24.1.9. Definíció. *Ha S Baer-*-félcsoport, akkor az $e \in \mathbf{P}(S)$ projektort* **zártnak** *nevezzük, ha $e = (e')'$. Az S Baer-*-félcsoport zárt projektorainak halmazát $\mathbf{P}_c(S)$ jelöli.*

24.1.10. Állítás. *Ha S Baer-*-félcsoport, akkor minden $s \in S$ esetén $s' = ((s')')'$.*

Bizonyítás. Legyen $s \in S$ rögzítve. A 24.1.5. állítás szerint

$$s' = ((s')')' \quad \Leftrightarrow \quad s'S = ((s')')'S \quad \Leftrightarrow \quad \{x \in S | sx = 0\} = \{x \in S | (s')'x = 0\}.$$

Ha $x \in S$ olyan, hogy $(s')'x = 0$, akkor 24.1.8. szerint $sx = (s(s')')x = s((s')'x) = s0 = 0$, tehát fennáll az $\{x \in S | sx = 0\} \supseteq \{x \in S | (s')'x = 0\}$ összefüggés.

Megfordítva, legyen $x \in S$ olyan, hogy $sx = 0$. Ekkor $x \in s'S$, tehát vehetünk olyan $t \in S$ elemet, amelyre $x = s't$. Ebből adjungálással kapjuk, hogy $x^* = t^*s'$, ezért $x^*s' = (t^*s')s' = t^*s' = x^*$. Ebből 24.1.8. alkalmazásával $x^*(s')' = (x^*s')(s')' = x^*(s'(s')') = x^*0 = 0$ adódik, tehát $x^*(s')' = 0$. Ezt adjungálva kapjuk, hogy $0 = 0^* = ((s')')^*(x^*)^* = (s')'x$. Ez azt jelenti, hogy az $\{x \in S | sx = 0\} \subseteq \{x \in S | (s')'x = 0\}$ összefüggés is teljesül. ■

24.1.11. Következmény. *Ha S Baer-*-félcsoport, akkor az $e \in \mathbf{P}(S)$ projektor pontosan akkor zárt, ha létezik olyan $s \in S$, hogy $e = s'$.*

Bizonyítás. Ha $e \in \mathbf{P}(S)$ zárt projektor, akkor $s := e' \in S$ olyan, hogy $e = s'$. Megfordítva, ha $s \in S$ olyan, hogy $e = s'$, akkor az előző állítás szerint $e = s' = ((s')')' = (e')'$, vagyis $e \in \mathbf{P}_c(S)$. ■

24.1.12. Állítás. *Ha S Baer-*-félcsoport, akkor minden $s \in S$ és $e \in \mathbf{P}(S)$ esetén, ha $es = se$, akkor $e's = se'$.*

Bizonyítás. Mivel $es = se$, így $e(se') = (es)e' = (se)e' = s(ee') = s0 = 0$, tehát $se' \in \{x \in S | ex = 0\} = e'S$, így létezik olyan $t \in S$, hogy $se' = e't$. Ebből következik, hogy $e'se' = e'(e't) = (e'e')t = e't = se'$, vagyis $se' = e'se'$. Az $es = se$ egyenlőséget adjungálva, $e = e^*$ alapján kapjuk, hogy $es^* = s^*e$, így az előző érvelést s helyett s^*-ra alkalmazva kapjuk, hogy $s^*e' = e's^*e'$. Ezt az egyenlőséget aadjungálva, $e' = (e')^*$ alapján kapjuk, hogy $e's = (e')^*(s^*)^* = (s^*e')^* = (e's^*e')^* = (e')^*(s^*)^*(e')^* = e'se'$. Ebből következik, hogy $se' = e'se' = e's$. ■

24.1.13. Állítás. *Legyen S Baer-*-félcsoport.*

a) *Ha $e, f \in \mathbf{P}(S)$, akkor*
$$e \le f \quad \Rightarrow \quad f' \le e'.$$

b) *Ha $e, f \in \mathbf{P}_{\mathrm{c}}(S)$, akkor*
$$e \le f \quad \Leftrightarrow \quad ef' = 0 \quad \Leftrightarrow \quad f'e = 0.$$

Bizonyítás. a) Tegyük fel, hogy $e \le f$. Ha $x \in S$ olyan, hogy $fx = 0$, akkor $ex = (ef)x = e(fx) = e0 = 0$, tehát $f'S = \{x \in S | fx = 0\} \subseteq \{x \in S | ex = 0\} = e'S$, amiből 24.1.5. alapján következik, hogy $f' \le e'$.

b) Adjungálással kapjuk, hogy az $ef' = 0$ és $f'e = 0$ egyenlőségek ekvivalensek (még akkor is, ha e vagy f nem zárt projektorok). Ha $e \le f$, akkor 24.1.8. szerint $ef' = (ef)f' = e(ff') = e0 = 0$, így $(e \le f) \Rightarrow (ef' = 0)$ teljesül (még akkor is, ha e vagy f nem zárt projektorok). Tegyük fel, hogy $ef' = 0$. Ekkor $f' \in \{x \in S | ex = 0\} = e'S$, tehát vehetünk olyan $s \in S$ elemet, amelyre $f' = e's$. Ebből kapjuk, hogy $e'f' = e'(e's) = (e'e')s = e's = f'$, ezért $f' \le e'$, amiből a) és az e és f projektorok zártsága alapján következik, hogy $e = (e')' \le (f')' = f$, ami azt jelenti, hogy $(ef' = 0) \Rightarrow (e \le f)$ is teljesül. ■

24.1.14. Tétel. *Legyen S Baer-*-félcsoport, és a $\mathbf{P}_{\mathrm{c}}(S)$ halmazon tekintsük a*
$$\le \; := \; \{ \, (e, f) \in \mathbf{P}_{\mathrm{c}}(S) \times \mathbf{P}_{\mathrm{c}}(S) \mid e = ef \, \}$$
relációt és a
$$\mathbf{P}_{\mathrm{c}}(S) \to \mathbf{P}_{\mathrm{c}}(S); \quad e \mapsto e^{\perp} := e'$$
leképezést. Ekkor a $(\mathbf{P}_{\mathrm{c}}(S), \le, \perp)$ hármas olyan ortomoduláris háló, amelyre minden $e, f \in \mathbf{P}_{\mathrm{c}}(S)$ esetén
$$e \wedge f = e(f'e)' = (f'e)'e = e \wedge (f'e)',$$
$$e \bigvee f = (e'(fe')')'.$$

Bizonyítás. (I) Megmutatjuk, hogy ha $e, f \in \mathbf{P}_{\mathrm{c}}(S)$ és $ef = fe$, akkor $ef \in \mathbf{P}_{\mathrm{c}}(S)$. Valóban, a 12.2.4. állítás szerint $ef \in S$ idempotens elem, továbbá $(ef)^* = f^*e^* = fe = ef$, tehát $ef \in \mathbf{P}(S)$, így csak az ef projektor zártságát kell igazolni. Nyilvánvaló, hogy ha $x \in S$ és $ex = 0$, akkor $ef = fe$ miatt $(ef)x = (fe)x = f(ex) = f0 = 0$, tehát $e'S = \{x \in S | ex = 0\} \subseteq \{x \in S | (ef)x = 0\} = (ef)'S$, amiből 24.1.5. alapján kapjuk, hogy $e' \le (ef)'$, ezért az e projektor zártsága és 24.1.13. a) szerint $((ef)')' \le (e')' = e$. Ugyanakkor, $x \in S$ és $fx = 0$ esetén $(ef)x = e(fx) = e0 = 0$, tehát $f'S = \{x \in S | fx = 0\} \subseteq \{x \in S | (ef)x = 0\} = (ef)'S$, amiből 24.1.5. alapján kapjuk, hogy $f' \le (ef)'$, ezért az f projektor zártsága és 24.1.13. a) szerint $((ef)')' \le (f')' = f$. A 12.2.4. állítás szerint $ef = \inf\{e, f\}$ az $\mathbf{I}(S)$ rendezett halmazban, vagyis ef a legnagyobb alsó korlátja az $\{e, f\}$ halmaznak az $\mathbf{I}(S)$ feletti természetes rendezés szerint, így az előzőek szerint $((ef)')' \le ef$. Mivel pedig $ef \le ((ef)')'$ is teljesül (24.1.8.), így $ef = ((ef)')'$, vagyis $ef \in \mathbf{P}_{\mathrm{c}}(S)$.

Ebből azonnal következik, hogy ha $e, f \in \mathbf{P}_{\mathrm{c}}(S)$ és $ef = fe$, akkor $ef = \inf\{e, f\}$ a $(\mathbf{P}_{\mathrm{c}}(S), \le)$ rendezett halmazban is.

(II) Megmutatjuk, hogy ha $e, f \in \mathbf{P}_{\mathrm{c}}(S)$ tetszőlegesek, akkor $e(f'e)' = (f'e)'e$.

Nyilvánvaló, hogy $e'S = \{x \in S | ex = 0\} \subseteq \{x \in S | (f'e)x = 0\} = (f'e)'S$, így 24.1.5. szerint $e' \le (f'e)'$, vagyis $e' = e'(f'e)' = (f'e)'e'$. Most alkalmazzuk a 24.1.12. állítást e

helyett $'$-ra, az $s := (f'e)'$ választással. Azt kapjuk, hogy $(e')'(f'e)' = (f'e)'(e')'$, amiből az e projektor zártsága miatt kapjuk, hogy $e(f'e)' = (f'e)'e$.

(III) Az (I) és (II) állításból következik, hogy ha $e, f \in \mathbf{P}_c(S)$ tetszőlegesek, akkor $e(f'e)' \in \mathbf{P}_c(S)$, és $e(f'e)' = \inf\{e, (f'e)'\}$ a $(\mathbf{P}_c(S), \leq)$ rendezett halmazban, vagyis $e(f'e)'$ a legnagyobb alsó korlátja az $\{e, (f'e)'\}$ halmaznak a $(\mathbf{P}_c(S), \leq)$ rendezett halmazban. Megmutatjuk, hogy ekkor $e(f'e)'$ egyenlő az $\{e, f\}$ halmaz legnagyobb alsó korlátjával $(\mathbf{P}_c(S), \leq)$ rendezett halmazban. Tehát azt kell igazolni, hogy $e(f'e)' \leq e$, és $e(f'e)' \leq f$, és minden $g \in \mathbf{P}_c(S)$ zárt projektorra, ha $g \leq e$ és $g \leq f$, akkor $g \leq e(f'e)'$ teljesül.

Az $e(f'e)' \leq e$ állítás triviálisan igaz, és $e(f'e)' \leq f$ is igaz, mert 24.1.8. szerint $f'(e(f'e)') = (f'e)(f'e)' = 0$, így a 24.1.13. állítás b) pontjából következik, hogy $e(f'e)' \leq f$. Legyen $g \in \mathbf{P}_c(S)$ olyan, hogy $g \leq e$ és $g \leq f$. Ekkor $(f'e)g = f'(eg) = f'g = f'(fg) = (f'f)g = 0g = 0$, mert f zárt projektor, így $f = f1 \in fS = (f')'S = \{x \in S | f'x = 0\}$. Ez azt jelenti, hogy $g \in \{x \in S | (f'e)x = 0\} = (f'e)'S$, tehát van olyan $s \in S$, amelyre $g = (f'e)'s$. Ekkor $(f'e)'g = (f'e)'((f'e)'s) = ((f'e)'(f'e)')s = (f'e)'s = g$, tehát $g \leq (f'e)'$. Ugyanakkor, a hipotézis szerint $g \leq e$, így $g \leq \inf\{e, (f'e)'\} = e(f'e)'$, amit bizonyítani kellett.

Ezzel bebizonyítottuk, hogy a $(\mathbf{P}_c(S), \leq)$ rendezett halmazban bármely két elemnek létezik infimuma, és ha $e, f \in \mathbf{P}_c(S)$ tetszőlegesek, akkor $e \wedge f = e(f'e)'$.

(IV) Megmutatjuk, hogy a $\mathbf{P}_c(S) \to \mathbf{P}_c(S)$; $e \mapsto e^\perp := e'$ leképezés *ortokomplementáció* (22.5.1.) a $(\mathbf{P}_c(S), \leq)$ korlátos rendezett halmaz felett.

Minden $e \in \mathbf{P}_c(S)$ esetén $(e^\perp)^\perp = (e')' = e$, hiszen e zárt projektor, ezért $(\mathrm{ORT_I})$ teljesül. Az 24.1.13. állítás a) pontjából következik, hogy $(\mathrm{ORT_{II}})$ is teljesül. Az $(\mathrm{ORT_{III}})$ feltétel ellenőrzéséhez legyenek $e, f \in \mathbf{P}_c(S)$ olyanok, hogy $e \leq f$ és $e^\perp \leq f$. Azt kell igazolni, hogy $f = 1$. A hipotézisek és 24.1.13. a) szerint $f' \leq e'$ és $f' \leq (e')' = e$, vagyis $f'e' = f'$ és $f'e = f'$. Az utolsó egyenlőséget jobbról szorozva az e' elemmel és felhasználva 24.1.8. állítást kapjuk, hogy $f' = f'e' = (f'e)e' = f'(ee') = f'0 = 0$, tehát $f' = 0$, így 24.1.7. szerint $f = (f')' = 0' = 1$.

Tehát a $\mathbf{P}_c(S) \to \mathbf{P}_c(S)$; $e \mapsto e^\perp := e'$ leképezés ortokomplementáció a $(\mathbf{P}_c(S), \leq)$ korlátos rendezett halmaz felett, vagyis a $(\mathbf{P}_c(S), \leq, \perp)$ hármas ortokomplementált rendezett halmaz. (III) szerint $\mathbf{P}_c(S)$ bármely két elemének létezik infimuma, így 22.5.3. alapján $\mathbf{P}_c(S)$ bármely két elemének létezik a szuprémuma is, tehát a $\leq$ rendezés hálószerű $\mathbf{P}_c(S)$ felett, vagyis a $(\mathbf{P}_c(S), \leq, \perp)$ hármas ortoháló. Ugyancsak a 22.5.3. állításból következik, hogy minden $e, f \in \mathbf{P}_c(S)$ esetén

$$e \vee f = (e^\perp \wedge f^\perp)^\perp = (e'((f')'e')')' = (e'(fe')')'.$$

(V) Végül igazoljuk a $(\mathbf{P}_c(S), \leq, \perp)$ ortoháló ortomodularitását. Ehhez legyenek $e, f \in \mathbf{P}_c(S)$ olyanok, hogy $e \leq f$. Azt kell belátni, hogy $e \vee (e^\perp \wedge f) = f$. A hipotézis alapján világos, hogy f felső korlátja az $\{e, e^\perp \wedge f\}$ halmaznak, tehát azt kell igazolni, hogy f a legkisebb felső korlátja ennek a halmaznak a $(\mathbf{P}_c(S), \leq)$ rendezett halmazban, vagyis, ha $g \in \mathbf{P}_c(S)$ olyan, hogy $e \leq g$ és $e^\perp \wedge f \leq g$, akkor $f \leq g$. A 24.1.13. állítás b) pontja szerint a g-re vonatkozó feltételek azt jelentik, hogy $g'e = 0$ és $g'(e' \wedge f) = 0$. Ugyanakkor

$$0 = g'(e' \wedge f) \overset{(1)}{=} g'\left(e'(f'e')'\right) \overset{(2)}{=} g'\left(e'(f')'\right) \overset{(3)}{=} (g'e')f \overset{(4)}{=} g'f,$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél felhasználtuk azt, hogy (III) szerint $e' \wedge f = e'(f'e')'$;

– a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk, hogy $e \leq f$ miatt 24.1.13. a) szerint $f' \leq e'$, vagyis $f'e' = f'$;

– a $\overset{(3)}{=}$ egyenlőségnél S műveletének asszociativitását és az f projektor zártságát alkalmaztuk;

– a $\overset{(4)}{=}$ egyenlőségnél felhasználtuk, hogy $e \leq g$ és 24.1.13. a) szerint $g' \leq e'$, vagyis $g'e' = g'$.

Tehát $g'f = 0$, ami a 24.1.13. állítás b) pontja szerint azt jelenti, hogy $f \leq g$, amit bizonyítani kellett. ■

24.2. Ortomoduláris hálók Foulis-féle reprezentációs tétele

24.2.1. Definíció. *Ha L ortoháló, akkor minden $e \in L$ esetén*

$$\phi_e : L \to L; \quad f \mapsto e \wedge (e^\perp \vee f).$$

24.2.2. Állítás. *Ha L ortomoduláris háló, akkor minden $e \in L$ esetén ϕ_e olyan $L \to L$ függvény, amelyre:*

a) *ϕ_e monoton növő, valamint $\phi_e(0) = 0$ és $\phi_e(1) = e$;*

b) *$\phi_e \circ \phi_e = \phi_e$;*

c) *minden $f \in L$ elemre $\phi_e\left(\left(\phi_e(f^\perp)\right)^\perp\right) = e \wedge f$.*

d) *minden $f, g \in L$ esetén $\phi_e(f \vee g) = \phi_e(f) \vee \phi_e(g)$ és $\phi_e(f \wedge g) \leq \phi_e(f) \wedge \phi_e(g)$.*

Bizonyítás. a) Legyenek $f, g \in L$ és $f \leq g$. Ekkor L ortomodularitásából következik, hogy $g = f \vee (f^\perp \wedge e)$, ezért

$$\phi_e(g) = e \wedge (e^\perp \vee g) = e \wedge (e^\perp \vee f \vee (f^\perp \wedge e)) \geq e \wedge (e^\perp \vee f) = \phi_e(f),$$

mert nyilvánvalóan $e \geq e \wedge (e^\perp \vee f)$ és $e^\perp \vee f \vee (f^\perp \wedge e) \geq e^\perp \vee f \geq e \wedge (e^\perp \vee f)$. Tehát a $\phi_e : L \to L$ függvény monoton növő.

Világos, hogy $\phi_e(0) = e \wedge (e^\perp \vee 0) = e \wedge e^\perp = 0$ és $\phi_e(1) = e \wedge (e^\perp \vee 1) = e \wedge 1 = e$.

b) Ha $f \in L$, akkor

$$(\phi_e \circ \phi_e)(f) = \phi_e\left(e \wedge (e^\perp \vee f)\right) = e \wedge \left(e^\perp \vee (e \wedge (e^\perp \vee f))\right) \overset{(*)}{=} e \wedge (e^\perp \vee f) = \phi_e(f),$$

ahol a $\overset{(*)}{=}$ egyenlőségnél azt használtuk fel, hogy $e^\perp \leq e^\perp \vee f$, így L ortomodularitása miatt $e^\perp \vee (e \wedge (e^\perp \vee f)) = e^\perp \vee ((e^\perp)^\perp \wedge (e^\perp \vee f)) = e^\perp \vee f$.

c) Ha $f \in L$, akkor

$$\phi_e\left(\left(\phi_e(f^\perp)\right)^\perp\right) = \phi_e\left(\left(e \wedge (e^\perp \vee f^\perp)\right)^\perp\right) \overset{(1)}{=} \phi_e\left(e^\perp \vee \left((e^\perp)^\perp \wedge (f^\perp)^\perp\right)\right) =$$
$$= \phi_e\left(e^\perp \vee (e \wedge f)\right) = e \wedge \left(e^\perp \vee \left(e^\perp \vee (e \wedge f)\right)\right) = e \wedge \left(e^\perp \vee (e \wedge f)\right) \overset{(1)}{=}$$
$$\overset{(1)}{=} \left(e^\perp \vee \left(e \wedge (e^\perp \vee f^\perp)\right)\right)^\perp \overset{(2)}{=} (e^\perp \vee f^\perp)^\perp \overset{(1)}{=} e \wedge f,$$

ahol az $\overset{(1)}{=}$ egyenlőség(ek)nél az ortokomplementált rendezett halmazokra vonatkozó de Morgan-egyenlőséget alkalmaztuk (22.5.3.), és a $\overset{(2)}{=}$ egyenlőségnél felhasználtuk azt, hogy

$e^\perp \le e^\perp \vee f^\perp$, így L ortomodularitása miatt $e^\perp \vee (e \wedge (e^\perp \vee f^\perp)) = e^\perp \vee ((e^\perp)^\perp \wedge (e^\perp \vee f^\perp)) = e^\perp \vee f^\perp$.

d) Legyenek $f, g \in L$. Az a) állítás szerint ϕ_e monoton növő, ezért $\phi_e(f \wedge g) \le \phi_e(f)$ és $\phi_e(f \wedge g) \le \phi_e(g)$, amiből $\phi_e(f \wedge g) \le \phi_e(f) \wedge \phi_e(g)$ következik. Megmutatjuk, hogy $\phi_e(f \vee g)$ a legkisebb felső korlátja a $\{\phi_e(f), \phi_e(g)\}$ halmaznak.

Mivel a) szerint ϕ_e monoton növő, így $\phi_e(f) \le \phi_e(f \vee g)$ és $\phi_e(g) \le \phi_e(f \vee g)$, vagyis $\phi_e(f \vee g)$ felső korlátja a $\{\phi_e(f), \phi_e(g)\}$ halmaznak.

Legyen $h \in L$ felső korlátja a $\{\phi_e(f), \phi_e(g)\}$ halmaznak, vagyis $\phi_e(f) \le h$ és $\phi_e(g) \le h$. Ekkor $h^\perp \le (\phi_e(f))^\perp$ és $h^\perp \le (\phi_e(g))^\perp$, így ϕ_e monoton növése folytán $\phi_e(h^\perp) \le \phi_e\left((\phi_e(f))^\perp\right)$ és $\phi_e(h^\perp) \le \phi_e\left((\phi_e(g))^\perp\right)$. Ugyanakkor c) alapján

$$\phi_e\left((\phi_e(f))^\perp\right) = \phi_e\left(\left(\phi_e\left((f^\perp)^\perp\right)\right)^\perp\right) = e \wedge f^\perp,$$
$$\phi_e\left((\phi_e(g))^\perp\right) = \phi_e\left(\left(\phi_e\left((g^\perp)^\perp\right)\right)^\perp\right) = e \wedge g^\perp,$$

következésképpen

$$\phi_e(h^\perp) \le \phi_e\left((\phi_e(f))^\perp\right) \wedge \phi_e\left((\phi_e(g))^\perp\right) = (e \wedge f^\perp) \wedge (e \wedge g^\perp) = e \wedge (f \vee g)^\perp \le (f \vee g)^\perp,$$

tehát $f \vee g = ((f \vee g)^\perp)^\perp \le \left(\phi_e(h^\perp)\right)^\perp$. Ismét ϕ_e monoton növését és c)-t alkalmazva, ebből kapjuk, hogy

$$\phi_e(f \vee g) \le \phi_e\left(\left(\phi_e(h^\perp)\right)^\perp\right) = e \wedge h = h,$$

vagyis $\phi_e(f \vee g) \le h$, így $\phi_e(f \vee g)$ a legkisebb felső korlátja a $\{\phi_e(f), \phi_e(g)\}$ halmaznak, azaz $\phi_e(f \vee g) = \phi_e(f) \vee \phi_e(g)$. ■

24.2.3. Állítás. *Ha L ortoháló, akkor minden $\varphi : L \to L$ függvényhez legfeljebb egy olyan $\psi : L \to L$ monoton növő függvény létezik, amelyre teljesül az, hogy minden $e \in L$ esetén fennállnak a $\psi\left((\varphi(e^\perp))^\perp\right) \le e$ és $\varphi\left((\psi(e^\perp))^\perp\right) \le e$ egyenlőtlenségek.*

Bizonyítás. Legyenek ψ és ψ' olyan $L \to L$ monoton növő függvények, amelyekre minden $e \in L$ esetén fennállnak a $\psi\left((\varphi(e^\perp))^\perp\right) \le e$ és $\varphi\left((\psi(e^\perp))^\perp\right) \le e$, valamint a $\psi'\left((\varphi(e^\perp))^\perp\right) \le e$ és $\varphi\left((\psi'(e^\perp))^\perp\right) \le e$ egyenlőtlenségek. Legyen $e \in L$ rögzítve. Ekkor $\varphi\left((\psi(e))^\perp\right) = \varphi\left(\left(\psi((e^\perp)^\perp)\right)^\perp\right) \le e^\perp$, tehát $e = (e^\perp)^\perp \le \left(\varphi\left((\psi(e))^\perp\right)\right)^\perp$, így a ψ' függvény monoton növése miatt $\psi'(e) \le \psi'\left(\left(\varphi\left((\psi(e))^\perp\right)\right)^\perp\right) \le \psi(e)$, vagyis $\psi'(e) \le \psi(e)$. A ψ és ψ' függvényekre vonatkozó feltételek szimmetrikusak, így ψ és ψ' felcserélésével kapjuk, hogy $\psi(e) \le \psi'(e)$ is teljesül. ■

24.2.4. Definíció. *Ha L ortoháló, akkor* $\mathrm{M}(L)$ *jelöli azon $\varphi : L \to L$ monoton növő függvények halmazát, amelyekre $\varphi(0) = 0$, továbbá,* $\mathrm{S}(L)$ *jelöli azon $\varphi \in \mathrm{M}(L)$ függvények halmazát, amelyekhez (24.2.3. szerint egyértelműen) létezik olyan $\varphi^* : L \to L$ monoton növő függvény, amelyre minden $e \in L$ esetén fennállnak a $\varphi^*\left((\varphi(e^\perp))^\perp\right) \le e$ és $\varphi\left((\varphi^*(e^\perp))^\perp\right) \le e$ egyenlőtlenségek.*

24.2.5. Állítás. *Legyen L ortoháló.*

a) *Ha $\varphi \in \mathrm{S}(L)$, akkor $\varphi^* \in \mathrm{S}(L)$ és $(\varphi^*)^* = \varphi$.*

b) *Ha $\varphi, \psi \in \mathrm{S}(L)$, akkor $\varphi \circ \psi \in \mathrm{S}(L)$ és $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$.*

c) *Ha $\varphi, \psi \in \mathrm{S}(L)$, akkor*

$$\varphi \circ \psi = 0_L \quad \Leftrightarrow \quad \psi(1) \le (\varphi^*(1))^\perp,$$

ahol 0_L *a* 0 *értékű* $L \to L$ *konstansfüggvény.*

d) *Ha* L *ortomoduláris, akkor minden* $e \in L$ *esetén* $\phi_e \in \mathrm{S}(L)$ *és* $\phi_e = \phi_e^*$.

Bizonyítás. a) Legyen $\varphi \in \mathrm{S}(L)$ rögzítve. Ekkor $\varphi^* : L \to L$ monoton növő függvény és $0 \leq (\varphi(1))^\perp$, így $\varphi^*(0) \leq \varphi^*\left((\varphi(1))^\perp\right) = \varphi^*\left((\varphi(0^\perp))^\perp\right) \leq 0$, tehát $\varphi^*(0) = 0$, így $\varphi^* \in \mathrm{M}(L)$. Továbbá, $\varphi : L \to L$ monoton növő függvény, és a hipotézis szerint minden $e \in L$ esetén $\varphi\left((\varphi^*(e^\perp))^\perp\right) \leq e$ és $\varphi^*\left((\varphi(e^\perp))^\perp\right) \leq e$, tehát $\varphi^* \in \mathrm{S}(L)$, és látható, hogy $(\varphi^*)^* = \varphi$.

b) Legyenek $\varphi, \psi \in \mathrm{S}(L)$. Mivel φ és ψ monoton növekvőek, így $\varphi \circ \psi$ is monoton növő, és $(\varphi \circ \psi)(0)\varphi(\psi(0)) = \varphi(0) = 0$. Továbbá, $\psi^* \circ \varphi^* : L \to L$ monoton növő függvény, és minden $e \in L$ esetén

$$(\psi^* \circ \varphi^*)\left(((\varphi \circ \psi)(e^\perp))^\perp\right) = \psi^*\left(\varphi^*\left(\left(\varphi\left(\psi(e^\perp)\right)\right)^\perp\right)\right), \tag{1}$$

és $\varphi^*\left(\left(\varphi\left(\psi(e^\perp)\right)\right)^\perp\right) \leq \left(\psi(e^\perp)\right)^\perp$, így ψ^* monoton növése miatt

$$\psi^*\left(\varphi^*\left(\left(\varphi\left(\psi(e^\perp)\right)\right)^\perp\right)\right) \leq \psi^*\left(\left(\psi(e^\perp)\right)^\perp\right) \leq e,$$

ami az (1) egyenlőséggel kombinálva azt adja, hogy $(\psi^* \circ \varphi^*)\left(((\varphi \circ \psi)(e^\perp))^\perp\right) \leq e$. Továbbá, minden $e \in L$ esetén

$$(\varphi \circ \psi)\left(((\psi^* \circ \varphi^*)(e^\perp))^\perp\right) = \varphi\left(\psi\left(\left(\psi^*\left(\varphi^*(e^\perp)\right)\right)^\perp\right)\right), \tag{2}$$

és $\psi\left(\left(\psi^*\left(\varphi^*(e^\perp)\right)\right)^\perp\right) \leq \left(\varphi^*(e^\perp)\right)^\perp$, így φ monoton növése miatt

$$\varphi\left(\psi\left(\left(\psi^*\left(\varphi^*(e^\perp)\right)\right)^\perp\right)\right) \leq \varphi\left(\left(\varphi^*(e^\perp)\right)^\perp\right) \leq e,$$

ami a (2) egyenlőséggel kombinálva azt adja, hogy $(\varphi \circ \psi)\left(((\psi^* \circ \varphi^*)(e^\perp))^\perp\right) \leq e$. Ez azt jelenti, hogy $\varphi \circ \psi \in \mathrm{S}(L)$ és $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$.

c) Legyenek $\varphi, \psi \in \mathrm{S}(L)$.

Ha $\psi(1) \leq (\varphi^*(1))^\perp$, akkor φ monoton növése miatt

$$\varphi(\psi(1)) \leq \varphi\left((\varphi^*(1))^\perp\right) = \varphi\left((\varphi^*(0^\perp))^\perp\right) \leq 0,$$

tehát $(\varphi \circ \psi)(1) = 0$, és mivel $\varphi \circ \psi : L \to L$ monoton növő és 1 a legnagyobb elem L-ben, így $\varphi \circ \psi = 0_L$.

Megfordítva, ha $\varphi \circ \psi = 0_L$, akkor $\varphi(\psi(1)) = 0$, ezért

$$\varphi^*(1) = \varphi^*(0^\perp) = \varphi^*\left((\varphi(\psi(1)))^\perp\right) \leq (\psi(1))^\perp,$$

amiből következik, hogy $\psi(1) = ((\psi(1))^\perp)^\perp \leq (\varphi^*(1))^\perp$.

d) Ha L ortomoduláris, akkor 24.2.2. c) alapján minden $e, f \in L$ esetén $\phi_e\left(\left(\phi_e(f^\perp)\right)^\perp\right) = e \wedge f \leq f$ és 24.2.2. a) szerint minden $e \in L$ elemre a $\phi_e : L \to L$ függvény monton növő és $\phi_e(0) = 0$, így $\phi_e \in \mathrm{S}(L)$ és $\phi_e = \phi_e^*$. ■

24.2.6. Tétel. (**Foulis-féle reprezentációs tétel.**) *Minden* L *ortomoduláris hálóra* $\mathrm{S}(L)$ *olyan Baer-*-félcsoport, hogy minden* $e \in L$ *elemre* $\phi_e \in \mathbf{P}_c(\mathrm{S}(L))$*, és az*

$$L \to \mathbf{P}_c(\mathrm{S}(L)); \quad e \mapsto \phi_e \tag{$*$}$$

leképezés ortoizomorfizmus.

Bizonyítás. A 24.2.5. állítás b) pontja szerint $\mathrm{S}(L)$ felett a függvénykompozíció egy kétváltozós művelet, és ugyanezen állítás a) és b) pontjai szerint az $\mathrm{S}(L) \to \mathrm{S}(L)$; $\varphi \mapsto \varphi^*$ leképezés olyan, amellyel $\mathrm{S}(L)$ *-félcsoport (24.1.1.). A továbbiakban $\mathrm{S}(L)$-t mindig *-félcsoportnak fogjuk tekinteni.

A 24.2.2. állítás b) pontja és a 24.2.5. állítás d) pontja szerint minden $e \in L$ esetén a ϕ_e függvény projektor az $\mathrm{S}(L)$ *-félcsoportban (24.1.3.), vagyis $\phi_e \in \mathbf{P}(\mathrm{S}(L))$.

Megmutatjuk, hogy $\mathrm{S}(L)$ Baer-*-félcsoport (24.1.6.). Ehhez elegendő azt igazolni, hogy minden $\varphi \in \mathrm{S}(L)$ esetén

$$\phi_{(\varphi^*(1))^\perp} \circ \mathrm{S}(L) = \{\psi \in \mathrm{S}(L) | \varphi \circ \psi = 0_L\},$$

ami azt is igazolja, hogy $\varphi' = \phi_{(\varphi^*(1))^\perp}$. A 24.2.5. állítás c) pontja szerint minden $\varphi \in \mathrm{S}(L)$ esetén $\{\psi \in \mathrm{S}(L) | \varphi \circ \psi = 0_L\} = \{\psi \in \mathrm{S}(L) | \psi(1) \leq (\varphi^*(1))^\perp\}$, tehát azt kell igazolni, hogy

$$\phi_{(\varphi^*(1))^\perp} \circ \mathrm{S}(L) = \{\psi \in \mathrm{S}(L) | \psi(1) \leq (\varphi^*(1))^\perp\}.$$

Legyen $\varphi \in \mathrm{S}(L)$ rögzítve. Ha $\widetilde{\psi} \in \mathrm{S}(L)$, akkor a $\phi_{(\varphi^*(1))^\perp} : L \to L$ függvény monoton növése miatt $\left(\phi_{(\varphi^*(1))^\perp} \circ \widetilde{\psi}\right)(1) = \phi_{(\varphi^*(1))^\perp}(\widetilde{\psi}(1)) \leq \phi_{(\varphi^*(1))^\perp}(1) = (\varphi^*(1))^\perp$, így $\phi_{(\varphi^*(1))^\perp} \circ \mathrm{S}(L) \subseteq \{\psi \in \mathrm{S}(L) | \psi(1) \leq (\varphi^*(1))^\perp\}$.

Megfordítva, tegyük fel, hogy $\psi \in \mathrm{S}(L)$ olyan függvény, hogy $\psi(1) \leq (\varphi^*(1))^\perp$. Legyen $e \in L$. Ekkor ψ monoton növése miatt $\psi(e) \leq \psi(1) \leq (\varphi^*(1))^\perp$, ezért $\varphi^*(1) \leq (\psi(e))^\perp$, amiből L ortomodularitása folytán következik, hogy $(\psi(e))^\perp = \varphi^*(1) \vee \left((\varphi^*(1))^\perp \wedge (\psi(e))^\perp\right)$. Ebből a de Morgan-egyenlőség alapján kapjuk, hogy

$$\psi(e) = (\varphi^*(1))^\perp \wedge (\varphi^*(1) \vee \psi(e)) = \phi_{(\varphi^*(1))^\perp}(\psi(e)).$$

Ez azt jelenti, hogy $\psi = \phi_{(\varphi^*(1))^\perp} \circ \psi \in \phi_{(\varphi^*(1))^\perp} \circ \mathrm{S}(L)$, amiből nyilvánvalóan következik, hogy $\{\psi \in \mathrm{S}(L) | \psi(1) \leq (\varphi^*(1))^\perp\} \subseteq \phi_{(\varphi^*(1))^\perp} \circ \mathrm{S}(L)$.

Tehát $\mathrm{S}(L)$ Baer-*-félcsoport, és minden $\varphi \in \mathrm{S}(L)$ esetén $\varphi' = \phi_{(\varphi^*(1))^\perp}$. Speciálisan, ha $e \in L$, akkor $\phi_e^*(1) = \phi_e(1) = e$ miatt $(\phi_e)' = \phi_{e^\perp}$, amiből azonnal következik, hogy ϕ_e *zárt* projektor az $\mathrm{S}(L)$ Baer-*-félcsoportban, hiszen $((\phi_e)')' = \left(\phi_{e^\perp}\right)' = \phi_{(e^\perp)^\perp} = \phi_e$.

Ebből az is látszik, hogy a $(*)$ leképezés ortokomplementáció-tartó. Továbbá, ez a leképezés *ráképez* $\mathbf{P}_c(\mathrm{S}(L))$-re, mert ha φ zárt projektor az $\mathrm{S}(L)$ Baer-*-félcsoportban, akkor

$$\varphi = (\varphi')' = \left(\phi_{(\varphi^*(1))^\perp}\right)' = \phi_{((\varphi^*(1))^\perp)^\perp} = \phi_{\varphi^*(1)}.$$

A $(*)$ leképezés nyilvánvalóan injektív, mert minden $e \in L$ esetén $\phi_e(1) = e$. A bizonyítást befejezéseként megmutatjuk, hogy a $(*)$ leképezés rendezés-izomorfizmus az L és $\mathbf{P}_c(\mathrm{S}(L))$ rendezett halmazok között, vagyis minden $e, f \in L$ esetén

$$e \leq f \quad L\text{-ben} \quad \Leftrightarrow \quad \phi_e \leq \phi_f \quad \mathbf{P}_c(\mathrm{S}(L))\text{-ben}.$$

Legyenek $e, f \in L$ olyanok, hogy $e \leq f$ az L rendezett halmazban. Ekkor

$$\phi_{f^\perp} \circ \mathrm{S}(L) \overset{(1)}{=} \{\psi \in \mathrm{S}(L) | \phi_f \circ \psi = 0_L\} \overset{(2)}{=} \{\psi \in \mathrm{S}(L) | \psi(1) \leq ((\phi_f)^*(1))^\perp\} \overset{(3)}{=}$$

$$= \{\psi \in \mathrm{S}(L) | \psi(1) \leq f^\perp\} \overset{(4)}{\subseteq} \{\psi \in \mathrm{S}(L) | \psi(1) \leq e^\perp\} \overset{(3)}{=} \{\psi \in \mathrm{S}(L) | \psi(1) \leq ((\phi_e)^*(1))^\perp\} \overset{(2)}{=}$$

$$\overset{(2)}{=} \{\psi \in \mathrm{S}(L) | \phi_e \circ \psi = 0_L\} \overset{(1)}{=} \phi_{e^\perp} \circ \mathrm{S}(L),$$

ahol

– az $\overset{(1)}{=}$ egyenlőség(ek)nél felhasználtuk azt, hogy minden $g \in L$ esetén $(\phi_g)' = \phi_{g^\perp}$;

– a $\overset{(2)}{=}$ egyenlőség(ek)nél a 24.2.5. állítás c) pontját alkalmaztuk;

– a $\overset{(3)}{=}$ egyenlőség(ek)nél felhasználtuk azt, hogy minden $g \in L$ esetén $(\phi_g)^* = \phi_g$ és $\phi_g(1) = g$;

– a $\overset{(4)}{\subseteq}$ összefüggésnél alkalmaztuk az $e \leq f$ feltételt, ami az L ortohálóban ekvivalens az $f^\perp \leq e^\perp$ egyenlőtlenséggel.

Tehát $\phi_{f^\perp} \circ \mathrm{S}(L) \subseteq \phi_{e^\perp} \circ \mathrm{S}(L)$, ezért $(\phi_f)' = \phi_{f^\perp} \leq \phi_{e^\perp} = (\phi_e)'$ teljesül (24.1.5.), így $\phi e = ((\phi_e)')' \leq ((\phi_f)')' = \phi_f$ teljesül a $\mathbf{P}_\mathrm{c}(\mathrm{S}(L))$ rendezett halmazban.

Megfordítva, legyenek $e, f \in L$ olyanok, hogy $\phi_e \leq \phi_f$ a $\mathbf{P}_\mathrm{c}(\mathrm{S}(L))$ rendezett halmazban. Ekkor $\phi_e = \phi_f \circ \phi_e$, következésképpen $e = \phi_e(1) = \phi_f(\phi_e(1)) = \phi_f(e) \leq \phi_f(1) = f$, vagyis $e \leq f$ az L rendezett halmazban. ■

24.3. *-algebrák

24.3.1. Definíció. *Azt mondjuk, hogy A* ***-algebra***, ha A komplex algebra, és adott egy $A \to A;\ a \mapsto a^*$ egyváltozós művelet, amelyre teljesülnek a következők:*

– *minden $a \in A$ esetén $(a^*)^* = a$* (**involutivitás**),

– *minden $a, b \in A$ és $z \in \mathbb{C}$ esetén $(a + z.b)^* = a^* + \overline{z}.b^*$* (**konjugált-linearitás**),

– *minden $a, b \in A$ esetén $(ab)^* = b^*a^*$* (**antimultiplikativitás**).

*A * egyváltozós műveletet az A *-algebra* **involúciójának** *nevezzük. Azt mondjuk, hogy az A *-algebra involúciója* **valódi***, ha minden $a \in A$ esetén, az $a^*a = 0$ feltételből $a = 0$ következik.*

A legelemibb *-algebra-konstrukciók a következők.

– *-algebra minden olyan részalgebrája, amely zárt az involúcióra nézve (vagyis **-részalgebra*) a műveletek leszűkítésével ellátva *-algebra. Ha A *-algebra és $e \in A$ olyan idempotens eleme, amelyre $e^* = e$, akkor az e-vel redukált eAe részalgebra az A-nak *-részalgebrája. Ha S olyan részhalmaza az A *-algebrának, amely zárt az involúcióra nézve (amit úgy fejezünk ki, hogy az S halmaz önadjungált), akkor a $\mathrm{C}(S)$ kommutáns az A-nak *-részalgebrája. Továbbá, ha S tetszőleges részhalmaza A-nak, akkor az A S-et tartalmazó *-részalgebráinak metszete szintén *-részalgebra A-ban; ezt nevezzük az S által generált *-részalgebrának.

– Ha $(A_i)_{i \in I}$ *-algebrák tetszőleges rendszere, akkor a szorzatalgebra a

$$\prod_{i \in I} A_i \to \prod_{i \in I} A_i; \quad (a_i)_{i \in I} \mapsto (a_i^*)_{i \in I}$$

leképezéssel ellátva *-algebra. Ezt a *-algebrát nevezzük az $(A_i)_{i \in I}$ *-algebra-rendszer *szorzatának.*

– Ha A *-algebra és $\mathfrak{m}$ olyan ideál A-ban, amely zárt az involúcióra nézve (vagyis $\mathfrak{m}$ **-ideál*), akkor az $A/\mathfrak{m}$ faktoralgebrán létezik egyetlen olyan $A/\mathfrak{m} \to A/\mathfrak{m};\ \zeta \mapsto \zeta^*$ egyváltozós művelet, amelyre teljesül az, hogy minden $a \in A$ esetén $(\pi_{A/\mathfrak{m}}(a))^* =$

$\pi_{A/\mathfrak{m}}(a^*)$. Az $A/\mathfrak{m}$ algebra ezzel a művelettel ellátva *-algebra; ezt nevezzük az A *-algebra $\mathfrak{m}$ *-ideál szerinti *faktor-*-algebrájának.*

24.4. Példák *-algebrákra

(I) Legyen T halmaz, és tekintsük az $\mathscr{F}(T;\mathbb{C})$ teljes függvényalgebrát. Az $\mathscr{F}(T;\mathbb{C})$ komplex algebra az

$$\mathscr{F}(T;\mathbb{C}) \to \mathscr{F}(T;\mathbb{C}); \quad f \mapsto \overline{f}$$

(konjugálás) egyváltozós művelettel ellátva kommutatív egységelemes *-algebra. Ennek a *-algebrának speciális *-részalgebrái a következők.

– A $T \to \mathbb{C}$ korlátos függvények $\mathscr{F}^b(T;\mathbb{C})$ halmaza *-részalgebrája $\mathscr{F}(T;\mathbb{C})$-nek. A $\mathbb{C}^{(T)} := \{f \in \mathscr{F}(T;\mathbb{C}) | "[f \neq 0] \text{ véges}"\}$ halmaz *-ideálja az $\mathscr{F}(T;\mathbb{C})$ *-algebrának.

– Ha T topologikus tér, akkor a $T \to \mathbb{C}$ folytonos (illetve korlátos és folytonos) függvények $\mathscr{C}(T;\mathbb{C})$ (illetve $\mathscr{C}^b(T;\mathbb{C})$) halmaza *-részalgebrája az $\mathscr{F}(T;\mathbb{C})$ *-algebrának.

– Ha T lokálisan kompakt tér, akkor a $T \to \mathbb{C}$ kompakt tartójú folytonos (illetve a végtelenben eltűnő folytonos) függvények $\mathscr{K}(T;\mathbb{C})$ (illetve $\overline{\mathscr{K}}(T;\mathbb{C})$) halmaza *-részalgebrája az $\mathscr{F}(T;\mathbb{C})$ *-algebrának.

– Ha $\mathscr{R}$ halmazgyűrű a T halmaz felett, akkor a $T \to \mathbb{C}$ $\mathscr{R}$-lépcsősfüggvények (illetve $\mathscr{R}$-egyszerű függvények) $\mathscr{E}_{\mathbb{C}}(T,\mathscr{R})$ (illetve $\widehat{\mathscr{E}}_{\mathbb{C}}(T,\mathscr{R})$) halmaza *-részalgebrája az $\mathscr{F}(T;\mathbb{C})$ *-algebrának.

(II) Legyen $\mathscr{H}$ komplex Hilbert-tér. Ekkor a $\mathscr{H} \to \mathscr{H}$ folytonos lineáris operátorok $\mathscr{L}(\mathscr{H})$ algebrája az operátoradjungálás művelettel ellátva egységelemes *-algebra, amely pontosan akkor kommutatív, ha $\mathscr{H}$ legfeljebb egydimenziós. Ennek a *-algebrának speciális *-részalgebrái a következők.

– A $\mathscr{H} \to \mathscr{H}$ folytonos és véges dimenziós értékű lineáris operátorok halmaza *-ideálja az $\mathscr{L}(\mathscr{H})$ *-algebrának.

– A $\mathscr{H} \to \mathscr{H}$ kompakt operátorok halmaza *-ideálja az $\mathscr{L}(\mathscr{H})$ *-algebrának.

– Ha $S \subseteq \mathscr{L}(\mathscr{H})$ önadjungált operátorhalmaz, tehát minden $s \in S$ esetén $s^* \in S$, akkor a $\mathrm{C}(S)$ kommutáns *-részalgebrája az $\mathscr{L}(\mathscr{H})$ *-algebrának. Az ilyen alakú *-algebrákat $\mathscr{H}$ feletti *Neumann-algebráknak* nevezzük.

(III) Legyen G csoport, és tekintsük az $A_{\mathbb{C}}(G)$ konvolúciós algebrát, amely egységelemes komplex algebra. Minden $a \in A_{\mathbb{C}}(G)$ esetén értelmezzük az $a^* : G \to \mathbb{C};\ s \mapsto \overline{a(s^{-1})}$ leképezést. Ekkor az $A_{\mathbb{C}}(G)$ algebra az $A_{\mathbb{C}}(G) \to A_{\mathbb{C}}(G);\ a \mapsto a^*$ egyváltozós művelettel ellátva olyan egységelemes *-algebra, amely pontosan akkor kommutatív, ha a G csoport kommutatív.

(IV) *Speciális példák.*

– Legyen A komplex vektortér és $D : A \to A$ tetszőleges olyan konjugált lineáris operátor, hogy $D \circ D = \mathrm{id}_A$. Legyen minden $a \in A$ esetén $a^* := D(a)$. Ekkor az A komplex vektortér a 0 szorzással és a * egyváltozós művelettel ellátva kommutatív *-algebra. Az ilyen alakú *-algebrákat *nulla-szorzású *-algebráknak* nevezzük.

– Jelölje A a diszk-algebrát és minden $a \in A$ esetén legyen

$$a^* : \overline{\mathrm{B}}_1(0;\mathbb{C}) \to \mathbb{C}; \quad z \mapsto \overline{a(\overline{z})}.$$

Ekkor $a \in A$ esetén $a^* \in A$, és az A komplex algebra a $*$ egyváltozós művelettel ellátva egységelemes kommutatív *-algebra. Ezt a teljesen konkrét *-algebrát szintén *diszk-algebrának* nevezzük. (Vigyázzunk arra, hogy a diszk-algebrában az involúció nem a konjugálás, mert a konjugálás elrontja a Cauchy-Riemann-egyenleteket, vagyis a holomorfitást, így a konjugálás kivezet a diszk-algebrából.)

– Legyen A egységelemes *-algebra és $j \in A$ olyan elem, amelyre $j = j^*$ és $j^2 = \mathbf{1}$. Ekkor az

$$A \to A; \quad a \mapsto a^{\#} := ja^*j$$

leképezés involúció az A komplex algebra felett, tehát A a $\#$ involúcióval ellátva szintén egységelemes *-algebra.

24.5. *-algebra egyégelemesítése

24.5.1. Definíció. *Ha A és B *-algebrák, akkor A és B közötti* ***-algebra-morfizmusnak** *nevezünk minden olyan $\pi : A \to B$ algebra-morfizmust, amely megtartja az A és B involúcióját, vagyis minden $a \in A$ esetén $\pi(a^*) = \pi(a)^*$. A bijektív *-algebra-morfizmusokat* ***-algebra-izomorfizmusoknak** *nevezzük.*

24.5.2. Állítás. *Legyen A *-algebra.*

a) *Létezik olyan (B, j) pár, hogy B egységelemes *-algebra és $j : A \to B$ *-algebra-morfizmus, és teljesül az, hogy minden C egységelemes *-algebrához és minden $\pi : A \to C$ *-algebra-morfizmushoz létezik egyetlen olyan $\tilde{\pi} : B \to C$ egységelem-tartó *-algebra-morfizmus, hogy $\tilde{\pi} \circ j = \pi$.*

b) *Legyenek (B_1, j_1) és (B_2, j_2) olyan párok, hogy B_1 és B_2 egységelemes *-algebrák, valamint $j_1 : A \to B_1$ és $j_2 : A \to B_2$ *-algebra-morfizmusok, és teljesül az, hogy minden C egységelemes *-algebrához és $\pi_1 : A \to C$ és $\pi_2 : A \to C$ *-algebra-morfizmushoz létezik egyetlen olyan olyan $\tilde{\pi}_1 : B_1 \to C$ egységelem-tartó *-algebra-morfizmus, hogy $\tilde{\pi}_1 \circ j_1 = \pi_1$, valamint létezik egyetlen olyan olyan $\tilde{\pi}_2 : B_2 \to C$ egységelem-tartó *-algebra-morfizmus, hogy $\tilde{\pi}_2 \circ j_2 = \pi_2$. Ekkor létezik egyetlen olyan $\pi : B_1 \to B_2$ *-algebra-izomorfizmus, amelyre $\pi \circ j_1 = j_2$.*

Bizonyítás. a) Legyen $\tilde{A} := \mathbb{C} \times A$ és értelmezzük a

$$+ : \tilde{A} \times \tilde{A} \to \tilde{A}; \quad \cdot : \tilde{A} \times \tilde{A} \to \tilde{A}; \quad . : \mathbb{C} \times \tilde{A} \to \tilde{A}; \quad * : \tilde{A} \to \tilde{A}$$

leképezéseket úgy, hogy $(\lambda, a), (\sigma, b) \in \tilde{A}$ esetén legyen

$$(\lambda, a) + (\sigma, b) := (\lambda + \sigma, a + b), \quad (\lambda, a) \cdot (\sigma, b) := (\lambda\sigma, \lambda.b + \sigma.a + ab),$$
$$\sigma.(\lambda, a) := (\sigma\lambda, \sigma.a), \quad (\lambda, a)^* := (\overline{\lambda}, a^*).$$

Ekkor az $\tilde{A}$ halmaz a $+, \cdot, ., *$ műveletekkel ellátva egységelemes *-algebra, amelynek $(1, 0)$ az egységeleme, és a

$$j : A \to \tilde{A}; \quad a \mapsto (0, a)$$

leképezés *-algebra-morfizmus. Világos, hogy $\mathrm{Im}(j)$ olyan 1-kodimenziós *-ideál A-ban, hogy $\tilde{A} = \mathbb{C}.\mathbf{1} \oplus \mathrm{Im}(j)$.

Legyen C egységelemes *-algebra, $\pi : A \to C$ *-algebra-morfizmus, és jelölje $\mathbf{1}_C$ a C egységelemét. Könnyen látható, hogy a

$$\tilde{\pi} : \tilde{A} \to C; \quad (\lambda, a) \mapsto \lambda.\mathbf{1}_C + \pi(a)$$

leképezés az egyetlen olyan egységelem-tartó *-algebra-morfizmus $\tilde{A}$ és C között, amelyre $\tilde{\pi} \circ j = \pi$.

b) Legyenek (B_1, j_1) és (B_2, j_2) olyan párok, amelyekre teljesülnek a b)-ben megfogalmazott feltételek. Ekkor B_2 egységelemes *-algebra és $j_2 : A \to B_2$ *-algebra-morfizmus, ezért a (B_1, j_1) pár tulajdonsága szerint létezik egyetlen olyan $\overline{j}_2 : B_1 \to B_2$ egységelem-tartó *-algebra-morfizmus, amelyre $\overline{j}_2 \circ j_1 = j_2$. Továbbá, B_1 egységelemes *-algebra és $j_1 : A \to B_1$ *-algebra-morfizmus, ezért a (B_2, j_2) pár tulajdonsága szerint létezik egyetlen olyan $\overline{j}_1 : B_2 \to B_1$ egységelem-tartó *-algebra-morfizmus, amelyre $\overline{j}_1 \circ j_2 = j_1$. Ekkor $\overline{j}_1 \circ \overline{j}_2 : B_1 \to B_1$ olyan egységelem-tartó *-algebra-morfizmus, amelyre $(\overline{j}_1 \circ \overline{j}_2) \circ j_1 = j_1$. Ugyanakkor az id_{B_1} leképezés természetesen szintén olyan $B_1 \to B_1$ egységelem-tartó *-algebra-morfizmus, amelyre $\mathrm{id}_{B_1} \circ j_1 = j_1$. De a (B_1, j_1) párra kirótt tulajdonság szerint csak egyetlen olyan $\pi : B_1 \to B_1$ egységelem-tartó *-algebra-morfizmus létezik, amelyre $\pi \circ j_1 = j_1$; ezért $\overline{j}_1 \circ \overline{j}_2 = \mathrm{id}_{B_1}$. Teljesen hasonló érvelést alkalmazva kapjuk, hogy $\overline{j}_2 \circ \overline{j}_1 = \mathrm{id}_{B_2}$. Ez azt jelenti, hogy az $\overline{j}_2 : B_1 \to B_2$ leképezés olyan *-izomorfizmus, amelyre $\overline{j}_2 \circ j_1 = j_2$, és a (B_1, j_1) párra vonatkozó tulajdonság miatt ilyen egységelem-tartó *-algebra-morfizmus csak egy létezhet. ■

24.5.3. Definíció. *Az A *-algebra* **egységelemesítésének** *nevezünk minden olyan (B, j) párt, amelyre B egységelemes *-algebra és $j : A \to B$ *-algebra-morfizmus, és teljesül az, hogy minden C egységelemes *-algebrához és minden $\pi : A \to C$ *-algebra-morfizmushoz létezik egyetlen olyan $\tilde{\pi} : B \to C$ egységelem-tartó *-algebra-morfizmus, hogy $\tilde{\pi} \circ j = \pi$. Az előző állítás bizonyításának a) részében előállított $(\tilde{A}, j)$ párt az A *-algebra* **standard egységelemesítésének** *nevezzük.*

Példa. Legyen T lokálisan kompakt tér, és jelölje T' a T egypontú kompaktifikációját. Tekintsük a $\mathscr{C}(T'; \mathbb{C})$ egységelemes *-algebrát és legyen $j : \overline{\mathscr{K}}(T; \mathbb{C}) \to \mathscr{C}(T'; \mathbb{C})$ az a leképezés, amely minden $T \to \mathbb{C}$ folytonos végtelenben eltűnő függvényhez hozzárendeli a 0-val vett kiterjesztését T'-re. Ekkor a $(\mathscr{C}(T'; \mathbb{C}), j)$ pár nem standard egységelemesítése a $\overline{\mathscr{K}}(T; \mathbb{C})$ *-algebrának.

24.6. Speciális elemek *-algebrákban

*-algebrákban értelmezhető néhány fontos elem-típus; most ezekről lesz szó.

24.6.1. Definíció. *Ha A *-algebra, akkor a következő elnevezéseket és jelöléseket alkalmazzuk.*

– *Az $a \in A$ elemet* **normálisnak** *nevezzük, ha $a^*a = aa^*$.*

– *Az $x \in A$ elemet* **önadjungáltnak** *vagy* **hermitikusnak** *nevezzük, ha $x^* = x$; az A *-algebra önadjungált elemeinek halmazát A_{sa} vagy A_h jelöli.*

– *Az $x \in A$ elemet* **pozitívnak** *nevezzük, ha létezik A-ban olyan $(a_i)_{i \in I}$ véges rendszer, amelyre $x = \sum_{i \in I} a_i^* a_i$; az A *-algebra pozitív elemeinek halmazát A_+ jelöli.*

– *Az $e \in A$ elemet* **projektornak** *nevezzük, ha $e^2 = e = e^*$; az A *-algebra projektorainak halmazát $\mathbf{P}(A)$ jelöli.*

– *Ha A egységelemes, akkor az $u \in A$ elemet* **unitérnek** *nevezzük, ha $u^*u = uu^* = \mathbf{1}$; az A *-algebra unitér elemeinek halmazát $\mathbf{U}(A)$ jelöli.*

Megjegyzések. Legyen A *-algebra.

1) Nyilvánvaló, hogy az A_{sa} halmaz $\mathbb{R}$-lineáris altere az A komplex vektortérnek, és minden $a \in A$ elemhez egyértelműen léteznek olyan $x, y \in A_{sa}$, amelyekre $a = x + \mathbf{i}.y$, ugyanis az $x := \frac{1}{2}(a + a^*)$ és $y := \frac{1}{2\mathbf{i}}(a - a^*)$ elemekre $a = x + \mathbf{i}.y$ teljesül és $x, y \in A_{sa}$; továbbá, ha $x, y \in A_{sa}$ olyanok, hogy $a = x + \mathbf{i}.y$, akkor $a^* = x - \mathbf{i}.y$, így szükségképpen $x = \frac{1}{2}(a + a^*)$ és $y = \frac{1}{2\mathbf{i}}(a - a^*)$.

Ez azt mutatja, hogy A megegyezik az A_{sa} valós vektortér *komplexifikációjával* (17.13.1.). Tehát, ha F komplex vektortér, és $u : A_{sa} \to F$ $\mathbb{R}$-lineáris operátor, akkor létezik egyetlen olyan $u_{\mathbb{C}} : A \to F$ $\mathbb{C}$-lineáris operátor, amely az u-nak kiterjesztése.

2) Az A_{sa} halmaz pontosan akkor zárt a szorzásra nézve, ha A kommutatív. Valóban, ha A kommutatív, akkor $x, y \in A_{sa}$ esetén $(xy)^* = y^*x^* = yx = xy$, tehát $xy \in A_{sa}$; továbbá, ha az A_{sa} halmaz zárt a szorzásra nézve, akkor $x, y \in A_{sa}$ esetén $xy \in A_{sa}$, vagyis $xy = (xy)^* = y^*x^* = yx$, így az A_{sa} halmaz bármely két eleme kommutál egymással, tehát az 1) alapján A kommutatív.

3) Legyen $a \in A$ és legyenek $x, y \in A_{sa}$ azok az elemek, amelyekre $a = x + \mathbf{i}.y$. Ekkor

$$\begin{aligned} a^*a &= (x - \mathbf{i}.y)(x + \mathbf{i}.y) = x^2 + y^2 + \mathbf{i}.(xy - yx), \\ aa^* &= (x + \mathbf{i}.y)(x - \mathbf{i}.y) = x^2 + y^2 - \mathbf{i}.(xy - yx), \end{aligned}$$

amiből látható, hogy az a elem pontosan akkor normális, ha $xy - yx = 0$, vagyis ha x és y felcserélhetők egymással.

4) A definíciók alapján nyilvánvaló, hogy $\mathbf{P}(A) \subseteq A_+ \subseteq A_{sa}$. Később majd részletesen foglalkozunk *-algebra projektorainak halmazával.

5) Legyen A egységelemes *-algebra. Egy $u \in A$ elem pontosan akkor unitér, ha invertálható (azaz $u \in \mathbf{G}(A)$) és $u^{-1} = u^*$. Nyilvánvaló, hogy az A minden unitér eleme normális, és az unitér elemek $\mathbf{U}(A)$ halmaza részcsoportja az invertálható elemek $\mathbf{G}(A)$ csoportjának. Az $\mathbf{U}(A)$ alakú *unitér* csoportok a harmonikus analízis alapvetően fontos objektumai.

6) Egy $a \in A$ elem pontosan akkor normális, ha az $\{a\}$ halmaz által generált *-részalgebra kommutatív, vagyis ha létezik a-t tartalmazó kommutatív *-részalgebrája A-nak. Világos ugyanis, hogy az $a \in A$ normális elem által generált *-részalgebra egyenlő a

$$\sum_{(m,n) \in \mathbb{N} \times \mathbb{N}} z_{m,n} a^m (a^*)^n$$

alakú elemek halmazával, ahol $(z_{m,n})_{(m,n) \in \mathbb{N} \times \mathbb{N}} \in \mathbb{C}^{(\mathbb{N} \times \mathbb{N})}$ olyan rendszer, amelyre $z_{0,0} = 0$; és természetesen az ilyen alakú elemek egymással felcserélhetők. Ha A egységelemes és $a \in A$ normális elem, akkor az $\{a, \mathbf{1}\}$ halmaz által generált *-részalgebra egyenlő a fenti alakú elemek halmazával, ahol $(z_{m,n})_{(m,n) \in \mathbb{N} \times \mathbb{N}} \in \mathbb{C}^{(\mathbb{N} \times \mathbb{N})}$ tetszőleges, vagyis $z_{0,0} \neq 0$ is lehetséges.

7) Az A_+ halmaz 0 csúcspontú *konvex kúp* az A_{sa} valós vektortérben, hiszen a definíció alapján nyilvánvaló, hogy $\mathbb{R}_+.A_+ \subseteq A_+$ és $A_+ + A_+ \subseteq A_+$. Az A_{sa} halmazon értelmezzük azt a $\preceq$ relációt, amelyre $x, y \in A_{sa}$ esetén $x \preceq y$ azt jelenti, hogy $y - x \in A_+$. Nyilvánvaló, hogy ez a reláció *reflexív* és *tranzitív*, tehát *előrendezés* az A_{sa} halmaz felett, továbbá ez az előrendezés abban az értelemben összhangban áll az A_{sa} valós vektortér-struktúrájával, hogy

- minden $x, y, z \in A_{sa}$ esetén, ha $x \preceq y$, akkor $x + z \preceq y + z$;
- minden $x, y \in A$ és $\alpha \in \mathbb{R}_+$ esetén, ha $x \preceq y$, akkor $\alpha.x \preceq \alpha.y$.

Ezt a $\preceq$ relációt az A_{sa} feletti *természetes előrendezésnek* nevezzük. Nyilvánvaló, hogy a $\preceq$ előrendezés pontosan akkor *rendezés*, ha $A_+ \cap (-A_+) = \{0\}$, hiszen ez a feltétel ekvivalens a $\preceq$ reláció antiszimmetrikusságával.

Világos, hogy ha minden A-beli $(a_i)_{i\in I}$ véges rendszerre, a $\sum\limits_{i\in I} a_i^* a_i = 0$ feltételből következik, hogy minden $i \in I$ esetén $a_i = 0$, akkor $A_+ \cap (-A_+) = \{0\}$.

8) Ha $a, b \in A$, akkor
$$a^*b + b^*a \preceq a^*a + b^*b,$$
mert $a^*a + b^*b - a^*b - b^*a = (a-b)^*(a-b)$. Ebből következik, hogy ha $(a_i)_{i\in I}$ tetszőleges véges rendszer A-ban, akkor
$$\sum_{j,k\in I,\ j\neq k} a_j^* a_k \preceq (\mathrm{Card}(I) - 1) \sum_{j\in I} a_j^* a_j.$$
Ez könnyen igazolható, hiszen
$$\sum_{j,k\in I,\ j\neq k} a_j^* a_k = \frac{1}{2} \sum_{j,k\in I,\ j\neq k} (a_j^* a_k + a_k^* a_j) \preceq \frac{1}{2} \sum_{j,k\in I,\ j\neq k} (a_j^* a_j + a_k^* a_k) =$$
$$= \sum_{j,k\in I,\ j\neq k} a_j^* a_j = \sum_{k\in I} \Big(\sum_{j\in I\setminus\{k\}} a_j^* a_j \Big) = \sum_{k\in I} \Big(\Big(\sum_{j\in I} a_j^* a_j \Big) - a_k^* a_k \Big) =$$
$$= \sum_{k\in I} \Big(\sum_{j\in I} a_j^* a_j \Big) - \sum_{k\in I} a_k^* a_k = (\mathrm{Card}(I) - 1) \sum_{j\in I} a_j^* a_j.$$

9) Ha $x, y \in A_{sa}$ és $x \preceq y$, akkor minden $a \in A$ esetén $a^*xa, a^*ya \in A_{sa}$ és
$$a^*xa \preceq a^*ya,$$
hiszen $y - x \in A$ esetén van olyan $(a_i)_{i\in I}$ véges rendszer A-ban, amelyre $y - x = \sum\limits_{i\in I} a_i^* a_i$, tehát
$$a^*ya - a^*xa = a^*(y-x)a = \sum_{i\in I} a^*(a_i^* a_i)a = \sum_{i\in I} (a_i a)^*(a_i a) \in A_+.$$
Ebből következik, hogy ha A egységelemes és $a \in \mathbf{G}(A)$, akkor az
$$A_{sa} \to A_{sa}; \quad x \mapsto a^*xa$$
leképezés olyan $\mathbb{R}$-*lineáris bijekció*, amelyre $x, y \in A_{sa}$ esetén $x \preceq y$ *ekvivalens* azzal, hogy $a^*xa \preceq a^*ya$, vagyis ez a leképezés *előrendezés-izomorfizmus*. Ez azon múlik, hogy ha $a \in A$ invertálható elem, akkor a^* is invertálható, és $(a^*)^{-1} = (a^{-1})^*$.

10) Legyen $n \in \mathbb{N}$, $n \geq 3$, és $z_n := \mathrm{Exp}((2\pi\mathbf{i})/n)$. Ekkor $a, b \in A$ esetén
$$b^*a = \frac{1}{n} \sum_{k=0}^{n-1} z_n^k (a + z_n^k b)^*(a + z_n^k b).$$
Ez egyszerű számolással nyerhető, felhasználva a $\sum\limits_{k=0}^{n-1} z_n^k = 0 = \sum\limits_{k=0}^{n-1} z_n^{2k}$ egyenlőségeket. Speciálisan, az $n := 4$ esetben a
$$b^*a = \frac{1}{4} \sum_{k=0}^{3} \mathbf{i}^k (a + \mathbf{i}^k b)^*(a + \mathbf{i}^k b)$$

összefüggést kapjuk, amit *polarizációs formulának* nevezünk.

11) Ha A egységelemes, akkor $A_{sa} = A_+ - A_+$, vagyis az A minden önadjungált eleme előáll pozitív elemek különbségeként, hiszen $x \in A_{sa}$ esetén

$$x = \frac{1}{4}(x + \mathbf{1})^*(x + \mathbf{1}) - \frac{1}{4}(x - \mathbf{1})^*(x - \mathbf{1}) \in A_+ - A_+.$$

Ezért az A minden eleme előáll pozitív elemek komplex lineáris kombinációjaként. Ugyanakkor a nulla-szorzású *-algebrák példája mutatja, hogy $A_+ = \{0\}$ és $A_{sa} \neq \{0\}$ lehetséges.

12) Fennáll az $A_+ = \tilde{A}_+ \cap A$ egyenlőség, ami pontosan azt jelenti, hogy $\{0\} \times A_+ = \tilde{A}_+ \cap (\{0\} \times A)$. Legyen ugyanis $(\lambda, a) \in \tilde{A}_+$; ekkor vehetünk olyan $((\lambda_i, a_i))_{i \in I}$ véges rendszert $\tilde{A}$-ban, amelyre

$$\begin{aligned}(\lambda, a) &= \sum_{i \in I} (\lambda_i, a_i)^*(\lambda_i, a_i) = \sum_{i \in I} (\overline{\lambda_i}, a_i^*)(\lambda_i, a_i) = \\ &= \left(\sum_{i \in I} |\lambda_i|^2, \sum_{i \in I} \overline{\lambda_i} a_i + \sum_{i \in I} \lambda_i a_i^* + \sum_{i \in I} a_i^* a_i \right).\end{aligned}$$

Ezért, ha $(\lambda, a) \in \{0\} \times A$ is teljesül, azaz $\lambda = 0$, akkor minden $i \in I$ esetén $\lambda_i = 0$, így $a = \sum_{i \in I} a_i^* a_i \in A_+$. Ebből az is következik, hogy $x, y \in A_{sa}$ esetén az $x \preceq y$ egyenlőtlenség pontosan akkor teljesül A-ban, ha $\tilde{A}$-ban is igaz.

24.7. Önadjungált funkcionálok

24.7.1. Definíció. *Legyen A *-algebra és $f : A \to \mathbb{C}$ lineáris funkcionál.*

– *Az f* **adjungáltjának** *nevezzük az*

$$f^* : A \to \mathbb{C}; \quad a \mapsto \overline{f(a^*)}$$

lineáris funkcionált. Azt mondjuk, hogy az f funkcionál **önadjungált**, *vagy* **hermitikus**, *ha $f^* = f$.*

– *Ha $a \in A$, akkor az*

$$\begin{aligned} a.f : A \to \mathbb{C}; &\quad x \mapsto f(ax) \\ f.a : A \to \mathbb{C}; &\quad x \mapsto f(xa) \end{aligned}$$

jelöléseket alkalmazzuk. Továbbá, $a, b \in A$ esetén $a.f.b := (a.f).b$, vagyis $a.f.b : A \to \mathbb{C}$ az a lineáris funkcionál, amelyre minden $A \ni x$-re $(a.f.b)(x) = f(axb)$.

– *Az f funkcionált pozitívnak nevezzük, ha $f\langle A_+ \rangle \subseteq \mathbb{R}_+$, vagy ami ugyanaz: minden $a \in A$ esetén $f(a^*a) \in \mathbb{R}_+$.*

Megjegyzések. Legyen A *-algebra és jelölje A^* az A komplex vektortér algebrai duálisát, vagyis az $A \to \mathbb{C}$ lineáris funkcionálok komplex vektorterét.

1) Az $A^* \to A^*$; $f \mapsto f^*$ leképezés olyan konjugált-lineáris bijekció, amely megegyezik a saját inverzével, vagyis minden $f \in A^*$ esetén $(f^*)^* = f$. Ebből az is következik, hogy

az A feletti önadjungált funkcionálok halmaza az A^* komplex vektortérnek $\mathbb{R}$-lineáris altere. Továbbá, minden $f \in A^*$ funkcionálra

$$f = \frac{1}{2}(f + f^*) + \mathbf{i}\frac{1}{2\mathbf{i}}(f - f^*)$$

teljesül, és az $\frac{1}{2}(f + f^*)$ és $\frac{1}{2\mathbf{i}}(f - f^*)$ funkcionálok önadjungáltak, tehát minden $f \in A^*$ előáll $f = f_1 + \mathbf{i}f_2$ alakban, ahol f_1 és f_2 önadjungált funkcionálok A felett. Ez az előállítás egyértelmű is, mert ha $f \in A^*$ és $f = f_1 + \mathbf{i}f_2$, ahol f_1 és f_2 önadjungált funkcionálok A felett, akkor $f^* = f_1 - \mathbf{i}f_2$, így ebből a két egyenlőségből $f_1 = \frac{1}{2}(f + f^*)$ és $f_2 = \frac{1}{2\mathbf{i}}(f - f^*)$ következik.

2) Minden $f \in A^*$ esetén a következő állítások ekvivalensek.

(i) f önadjungált.

(ii) Minden $x \in A_{sa}$ esetén $f(x) \in \mathbb{R}$.

(iii) Létezik (egyértelműen) olyan $g : A_{sa} \to \mathbb{R}$ lineáris funkcionál, amelyre f a g kiterjesztése.

Valóban, (i)$\Rightarrow$(ii) azért igaz, mert ha $x \in A_{sa}$, akkor az (i) alapján $\overline{f(x)} = \overline{f(x^*)} =: f^*(x) = f(x)$, vagyis $f(x) \in \mathbb{R}$. Továbbá, ha (ii) teljesül, akkor a $g := f|_{A_{sa}} : A_{sa} \to \mathbb{R}$ leképezés az a lineáris funkcionál, amelynek f a kiterjesztése, ezért (ii)$\Rightarrow$(iii) teljesül. Ha (iii) igaz, és $g : A_{sa} \to \mathbb{R}$ olyan lineáris funkcionál, hogy f a g kiterjesztése, akkor $x, y \in A_{sa}$ esetén $f(x) = g(x) \in \mathbb{R}$ és $f(y) = g(y) \in \mathbb{R}$, tehát

$$\begin{aligned} f^*(x + \mathbf{i}y) &:= \overline{f((x + \mathbf{i}y)^*)} = \overline{f(x - \mathbf{i}y)} = \overline{f(x) - \mathbf{i}f(y)} = \\ &= \overline{g(x) - \mathbf{i}g(y)} = g(x) + \mathbf{i}g(y) = f(x) + \mathbf{i}f(y) = f(x + \mathbf{i}y) \end{aligned}$$

tehát $f^* = f$, így (iii)$\Rightarrow$(i) teljesül.

Ebből az is következik, hogy az $f \to f|_{A_{sa}}$ leképezés bijekció az A feletti önadjungált funkcionálok valós vektortere és az A_{sa} valós vektortér algebrai duálisa között.

3) Ha $a \in A$ és $f \in A^*$, akkor $(a.f)^* = f^*.a^*$ és $(f.a)^* = a^*.f^*$; ez egyszerű számolással igazolható.

4) Vigyázzunk arra, hogy pozitív funkcionál nem szükségképpen önadjungált. Például, nulla-szorzású *-algebra felett minden lineáris funkcionál triviálisan pozitív, de sok nem önadjungált lineáris funkcionál létezhet. A pozitív funkcionálokkal később részletesen foglalkozunk. Z

5) Az A feletti önadjungált funkcionálok valós vektortere felett értelmezzük azt a $\preceq$ relációt, amelyre $f \preceq g$ pontosan akkor teljesül, ha a $g - f$ funkcionál pozitív, vagyis minden $a \in A$ esetén $f(a^*a) \leq g(a^*a)$. Világos, hogy ez a $\preceq$ reláció reflexív és tranzitív, tehát előrendezés az A feletti önadjungált funkcionálok valós vektortere felett, amit a *természetes előrendezésnek nevezük.* Ez pontosan akkor rendezés, ha minden $f : A \to \mathbb{C}$ önadjungált funkcionálra, az $A_+ \subseteq \mathrm{Ker}(f)$ feltételből $f = 0$ következik. Speciálisan, ha A előáll az A_+ halmaz lineáris burkaként (például A egységelemes), akkor ez a reláció rendezés.

24.8. Egységelemes *-algebrák típusai

Most az egységelemes *-algebrák elemi és összetett tulajdonságait vizsgáljuk, és kijelöljük az egységelemes *-algebrák legfontosabb típusait. Ezután megfogalmazzuk a *struktúra-tétellel* kapcsolatos alapvető problémát egységelemes *-algebrákra.

24.8.1. Definíció. *Az A *-algebrát* **Abel-típusúnak** *nevezzük, ha az A minden projektora kommutál az A minden elemével, vagyis $\mathbf{P}(A) \subseteq \mathrm{C}(A)$. Az A egységelemes *-algebrát* **végesnek** *nevezzük, ha minden $a \in A$ esetén az $a^*a = \mathbf{1}$ feltételből $aa^* = \mathbf{1}$ következik. Ha A *-algebra, akkor az $e \in \mathbf{P}(A)$ projektort* **Abel-projektornak** (*illetve* **véges projektornak**) *nevezzük, ha az eAe redukált *-algebra Abel-típusú* (*illetve véges*).

Nyilvánvaló, hogy minden kommutatív *-algebra Abel-típusú, és bármely *-algebrában a 0 elem egyszerre Abel-típusú és véges.

Ha $\mathscr{H}$ Hilbert-tér, akkor az $\mathscr{L}(\mathscr{H})$ operátor-*-algebra pontosan akkor véges, ha $\mathscr{H}$ véges dimenziós (innen származik az elnevezés). Valóban, ha $\mathscr{H}$ véges dimenziós és $a \in \mathscr{L}(\mathscr{H})$ olyan, hogy $a^* \circ a = \mathrm{id}_{\mathscr{H}}$, akkor az a operátor injektív, így szürjektív is és $a^{-1} = a^*$, tehát $a \circ a^* = \mathrm{id}_{\mathscr{H}}$ is teljesül. Az $\mathbf{l}^2_{\mathbb{C}}$ Hilbert-tér esetében megadható olyan $a \in \mathscr{L}(\mathbf{l}^2_{\mathbb{C}})$ operátor, amelyre $a^* \circ a = \mathrm{id}_{\mathbf{l}^2_{\mathbb{C}}}$ és az $a \circ a^*$ operátor nem injektív. Ilyen például az az $a : \mathbf{l}^2_{\mathbb{C}} \to \mathbf{l}^2_{\mathbb{C}}$ operátor, amelyre $\mathbf{s} \in \mathbf{l}^2_{\mathbb{C}}$ és $n \in \mathbb{N}$ esetén $(a(\mathbf{s}))(n) := \mathbf{s}(n-1)$, ha $n > 0$, és $(a(\mathbf{s}))(0) := 0$. Ez azt jelenti, hogy az $\mathscr{L}(\mathbf{l}^2_{\mathbb{C}})$ *-algebra nem véges. Ebből kiindulva belátható, hogy bármely $\mathscr{H}$ végtelen dimenziós Hilbert-térre az $\mathscr{L}(\mathscr{H})$ operátor-*-algebra nem véges.

24.8.2. Állítás. *Minden Abel-típusú egységelemes *-algebra véges. Minden Abel-projektor véges projektor.*

Bizonyítás. Legyen A egységelemes Abel-típusú *-algebra, és legyen $a \in A$ olyan, hogy $a^*a = \mathbf{1}$. Világos, hogy $aa^* \in A_{sa}$ és $(aa^*)(aa^*) = a(a^*a)a^* = a\mathbf{1}a^* = aa^*$, tehát $aa^* \in \mathbf{P}(A) \subseteq \mathrm{C}(A)$. Ezért fennállnak a következő egyenlőségek

$$\mathbf{1} = (a^*a)(a^*a) = (a^*(aa^*))a = ((aa^*)a^*)a = (aa^*)(a^*a) = aa^*.$$

Ez azt jelenti, hogy A véges *-algebra. Ebből következik, hogy minden Abel-típusú projektor véges. ■

24.8.3. Definíció. *Legyen A egységelemes *-algebra.*

– *Az $a \in A$ elemet* **centrálisnak** *nevezzük, ha a kommutál az A minden elemével, vagyis $a \in \mathrm{C}(A)$. Az A centrális elemeinek halmazát az A* **centrumának** *nevezzük.*

– *Azt mondjuk, hogy az $e \in \mathbf{P}(A)$ projektor* **hű**, *ha minden $f \in \mathbf{P}(A)$ centrális projektorra, $e = ef$ esetén $f = \mathbf{1}$ teljesül.*

24.8.4. Definíció. *Azt mondjuk, hogy az A egységelemes *-algebra*

– **diszkrét**, *ha létezik hű Abel-projektor A-ban,*

– **folytonos**, *ha 0 az egyetlen Abel-projektor A-ban,*

– **félig-véges**, *ha létezik hű véges projektor A-ban,*

– **tisztán végtelen**, *ha 0 az egyetlen véges projektor A-ban,*

– **valóban végtelen**, *ha 0 az egyetlen centrális véges projektor A-ban,*

– **valóban nem Abel-típusú**, *ha 0 az egyetlen centrális Abel-projektor A-ban.*

*Azt mondjuk továbbá, hogy az A egységelemes *-algebra*

– **I. típusú**, *ha diszkrét,*
– **II. típusú**, *ha folytonos és félig-véges,*
– **III. típusú**, *ha tisztán végtelen.*

Azt mondjuk, hogy két tulajdonság, amelyek egységelemes *-algebrákra vonatkoznak egymás *komplementerei*, ha csak a 0 dimenziós *-algebra rendelkezik mindkét tulajdonsággal egyszerre. Könnyen látható, hogy következő tulajdonság-párok komplementerek:

– diszkrétség és folytonosság,
– félig végesség és tisztán végtelenség,
– végesség és valóban végtelenség,
– Abel-típusosság és valóban nem Abel-típusosság.

Ebből az is következik, hogy az I., II. és III. típusosság páronként komplementer tulajdonságok. Továbbá, a definíciók alapján nyilvánvalók a következő állítások:

– minden kommutatív *-algebra Abel-típusú;
– minden Abel-típusú *-algebra diszkrét *és* véges;
– minden diszkrét *vagy* véges *-algebra félig-véges;
– minden tisztán végtelen *-algebra folytonos *és* valóban végtelen;
– minden folytonos *vagy* valóban végtelen *-algebra valóban nem Abel-típusú.

Példa. Ha $\mathscr{H}$ Hilbert-tér, akkor az $\mathscr{L}(\mathscr{H})$ *-algebra I. típusú, mert minden $P \in \mathbf{P}(\mathscr{L}(\mathscr{H}))$ projektorra, ha $\dim(\mathrm{Im}(P)) = 1$, akkor P hű Abel-projektor $\mathscr{L}(\mathscr{H})$-ban.

Legyen $\mathfrak{M}$ egységelemes *-algebráknak tetszőleges osztálya. Azt mondjuk, hogy az $\mathfrak{M}$-re teljesül a *struktúra-tétel*, ha minden $A \in \mathfrak{M}$ algebrához léteznek olyan A_I, A_{II}, $A_{III} \in \mathfrak{M}$ algebrák, amelyekre $A = A_I \oplus A_{II} \oplus A_{III}$, és A_I I. típusú, A_{II} II. típusú, és A_{III} III. típusú *-algebrák.

24.9. Természetes rendezés *-algebra projektorainak halmazán

Emlékeztetünk arra, hogy az A *-algebra projektorainak, vagyis önadjungált idempotens elemeinek halmazát $\mathbf{P}(A)$-val jelöljük. Ha A egységelemes, akkor az A egységelemét $\mathbf{1}$ jelöli.

24.9.1. Definíció. *Ha A *-algebra, akkor $e, f \in \mathbf{P}(A)$ esetén azt írjuk, hogy $e \leq f$, ha $e = ef$; ezt a $\mathbf{P}(A)$ feletti $\leq$ relációt a $\mathbf{P}(A)$* **természetes rendezésének** *nevezzük.*

Megjegyzések. 1) Az elnevezést az indokolja, hogy ha A *-algebra, akkor a $\leq$ reláció rendezés a $\mathbf{P}(A)$ halmaz felett. Valóban, a $\leq$ reláció:

– *reflexív*, mert a $\mathbf{P}(A)$ elemei idempotensek;

– *antiszimmetrikus*, mert $e \leq f$ és $f \leq e$ esetén $e = ef$ és $f = fe$, tehát az e és f elemek önadjungáltsága miatt $f = fe = f^*e^* = (ef)^* = e^* = e$;

– *tranzitív*, mert $e \leq f$ és $f \leq g$ esetén $e = ef$ valamint $f = fg$, így az A szorzásának asszociativitása miatt $e = ef = e(fg) = (ef)g = eg$, vagyis $e \leq g$.

A továbbiakban a $\mathbf{P}(A)$ halmazt mindig rendezett halmaznak tekintjük, amelynek rendezése a $\mathbf{P}(A)$ feletti természetes rendezés.

2) Ha A *-algebra, akkor nyilvánvalóan 0 a $\mathbf{P}(A)$ legkisebb eleme, és ha A egységelemes, akkor természetesen $\mathbf{1}$ a $\mathbf{P}(A)$ legnagyobb eleme, tehát ekkor $\mathbf{P}(A)$ a $\leq$ relációval ellátva *korlátos rendezett halmaz.*

3) Ha A *-algebra, akkor $e, f \in \mathbf{P}(A)$ esetén $e \leq f$ pontosan akkor teljesül, ha $f - e \in \mathbf{P}(A)$. Valóban, ha $e \leq f$, akkor $e = ef$, ezért $ef = e = e^* = f^*e^* = fe$, vagyis e és f kommutálnak egymással, így $(f-e)^2 = f^2 + e^2 - ef - fe = f + e - 2ef = f - e$, tehát $f - e \in \mathbf{P}(A)$. Megfordítva, ha $f - e \in \mathbf{P}(A)$, akkor $(f-e)^2 = f - e$, azaz $f + e - ef - fe = f - e$, vagyis $2e = ef + fe$. Ezt az egyenlőséget jobbról szorozva f-fel kapjuk, hogy $2ef = ef + fef$, tehát $ef = fef$. Ebből adjungálással nyerjük, hogy $ef = fe$, ezért $2e = ef + fe = 2ef$, vagyis $e = ef$, ami azt jelenti, hogy $e \leq f$.

4) Legyen A *-algebra. Ekkor $\mathbf{P}(A) \subseteq A_{sa}$, és az A_{sa} halmazon a 16.4. pont 7) megjegyzésében bevezettük azt a $\preceq$ relációt, amelyre teljesül az, hogy ha $x, y \in A_{sa}$, akkor $x \preceq y$ definíció szerint ekvivalens azzal, hogy $y - x \in A_+$, vagyis létezik olyan $(a_i)_{i \in I}$ véges rendszer A-ban, amelyre $y - x = \sum_{i \in I} a_i^* a_i$. Tudjuk, hogy a $\preceq$ reláció nem szükségképpen antiszimmetrikus, bár reflexív és tranzitív (vagyis *előrendezés* A_{sa} felett). A 3. példában majd megmutatjuk, hogy a $\preceq$ reláció $\mathbf{P}(A)$-ra vett leszűkitése és a $\leq$ rendezés *nem szükségképpen egyenlőek*, mert a $\preceq$ reláció még a $\mathbf{P}(A)$ halmazon sem feltétlenül antiszimmetrikus. Azonban nyilvánvaló, hogy $e, f \in \mathbf{P}(A)$ és $e \leq f$ esetén $e \preceq f$, hiszen a 3) megjegyzés szerint $f - e \in \mathbf{P}(A)$, így $f - e = (f-e)^*(f-e) \in A_+$, vagyis $e \preceq f$.

Példák (a projektorok közötti rendezésre).

1) Legyen T lokálisan kompakt tér és $A := \overline{\mathscr{K}}(T; \mathbb{C})$. Ekkor $\mathbf{P}(A) = \{\chi_E | \text{"}E \subseteq T \text{ kompakt-nyílt"}\}$, tehát $\mathbf{P}(A)$ az $E \mapsto \chi_E$ leképezés által azonosítható a T kompakt-nyílt részhalmazainak halmazával. Világos, hogy ha $E, F \subseteq T$ kompakt-nyílt halmazok,

akkor $\chi_{_E} \le \chi_{_F}$ pontosan akkor teljesül, ha $E \subseteq F$. Az is látható, hogy a $\mathbf{P}(A)$ halmazon a $\le$ és $\preceq$ relációk egyenlők. Később megmutatjuk, hogy ez nem véletlen.

2) Legyen $\mathscr{H}$ Hilbert-tér és $A := \mathscr{L}(\mathscr{H})$. Ekkor $\mathbf{P}(A)$ egyenlő a $\mathscr{H}$ Hilbert-tér *ortogonális projektorainak* halmazával, amely az $e \mapsto \mathrm{Im}(e)$ leképezés által azonosítható a $\mathscr{H}$ zárt lineáris altereinek halmazával. Nyilvánvaló, hogy $e, f \in \mathbf{P}(A)$ esetén $e \le f$ ekvivalens azzal, hogy $\mathrm{Im}(e) \subseteq \mathrm{Im}(f)$. Hamarosan igazoljuk, hogy $\mathbf{P}(A)$ felett a $\le$ és $\preceq$ relációk ebben az esetben is egyenlők.

3) Tekintsük az $\mathrm{M}_2(\mathbb{C})$ mátrixalgebrát, és jelölje $\#$ az *euklidészi involúciót* $\mathrm{M}_2(\mathbb{C})$ felett, vagyis $m \in \mathrm{M}_2(\mathbb{C})$ esetén $m^\#$ az m mátrix transzponált-konjugáltja. Legyen $j := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, és minden $m \in \mathrm{M}_2(\mathbb{C})$ esetén $m^* := jm^\# j$. Ekkor az $\mathrm{M}_2(\mathbb{C})$ komplex algebra a $*$ leképezéssel ellátva egységelemes *-algebra; jelölje A ezt a *-algebrát. Tekintsük a következő mátrixokat:

$$e := \begin{pmatrix} \frac{3}{2} & \mathbf{i}\frac{\sqrt{3}}{2} \\ \mathbf{i}\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \quad f := \begin{pmatrix} \frac{3}{2} & -\mathbf{i}\frac{\sqrt{3}}{2} \\ -\mathbf{i}\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \quad a_\pm := \begin{pmatrix} 1 & \mp\mathbf{i}\frac{\sqrt{3}}{2} \\ 1 & \pm\mathbf{i}\frac{\sqrt{3}}{2} \end{pmatrix}.$$

Ekkor $e, f \in \mathbf{P}(A)$, $f - e = a_+^* a_+$ és $e - f = a_-^* a_-$, tehát $e \preceq f$ és $f \preceq e$. Ugyanakkor $e \neq ef$, így nem igaz az $e \le f$ egyenlőtlenség. Természetesen $e \neq f$, tehát a $\preceq$ reláció $\mathbf{P}(A)$-ra vett megszorítása nem antiszimmetrikus.

24.9.2. Állítás. *Ha A olyan *-algebra, amelynek létezik hű ábrázolása, akkor a $\mathbf{P}(A)$ feletti $\le$ és $\preceq$ relációk egyenlőek.*

Bizonyítás. Legyen π hű ábrázolása A-nak a $\mathscr{H}$ Hilbert-térben, és legyenek $e, f \in \mathbf{P}(A)$ olyanok, hogy $e \preceq f$. Ekkor $\pi(e), \pi(f) \in \mathbf{P}(\mathscr{L}(\mathscr{H}))$, és a $\pi(f - e)$ operátor pozitív az $\mathscr{L}(\mathscr{H})$ *-algebrában, tehát minden $\zeta \in \mathscr{H}$ esetén

$$\|\pi(f)\zeta\|^2 - \|\pi(e)\zeta\|^2 = (\pi(f)\zeta|\zeta) - (\pi(e)\zeta|\zeta) = (\pi(f-e)\zeta|\zeta) \in \mathbb{R}_+,$$

vagyis $\|\pi(e)\zeta\| \le \|\pi(f)\zeta\|$. Ebből következik, hogy $\mathrm{Ker}(\pi(f)) \subseteq \mathrm{Ker}(\pi(e))$, tehát

$$\mathrm{Im}(\pi(e)) = (\mathrm{Ker}(\pi(e)))^\perp \subseteq (\mathrm{Ker}(\pi(f))^\perp = \mathrm{Im}(\pi(f)).$$

Ez azt jelenti, hogy $\pi(e) \preceq \pi(f)$ az $\mathscr{L}(\mathscr{H})$ *-algebrában, tehát $\pi(ef) = \pi(e)\pi(f) = \pi(e)$. Ebből a π injektivitása folytán $ef = e$, vagyis $e \le f$ következik. ■

24.9.3. Következmény. *Ha A pre-C^*-algebra, akkor a $\mathbf{P}(A)$ feletti $\preceq$ és $\le$ relációk egyenlőek.*

Bizonyítás. Láttuk, hogy egy *-algebrának pontosan akkor létezik hű ábrázolása, ha létezik felette pre-C^*-norma (**??**). Ezért az előző állításból azonnal kapjuk, hogy egy pre-C^*-algebra projektorainak halmazán a $\preceq$ és $\le$ relációk egyenlők. ■

Az előző következmény indokolja azt, hogy pre-C^*-algebrák esetében a $\preceq$ szimbólumot nem használjuk, hanem helyette a $\le$ jelet alkalmazzuk. De vigyázzunk arra, hogy ez a konvenció félreértésre vezet akkor ha a szóban forgó *-algebra projektorainak halmazán a $\preceq$ és $\le$ relációk nem egyenlőek.

Most azt a problémát vizsgáljuk, hogy ha A *-algebra, akkor a $\mathbf{P}(A)$ feletti $\le$ rendezés szerint milyen szuprémumok és infimumok léteznek? Megállapodunk abban, hogy a szuprémumokra és az infimumokra a szokásos hálóelméleti jelölést alkalmazzuk, tehát, ha A *-algebra és $e, f \in \mathbf{P}(A)$, akkor az $\{e, f\}$ halmaz $\le$ reláció szerinti szuprémumát (illetve infimumát) $e \vee f$ (illetve $e \wedge f$) jelöli, ha létezik.

24.9.4. Állítás. *Legyen A *-algebra és $e, f \in \mathbf{P}(A)$.*

a) *Ha $ef = fe$, akkor $e \vee f$ és $e \wedge f$ léteznek $\mathbf{P}(A)$-ban, és*

$$e \vee f = e + f - ef, \quad e \wedge f = ef.$$

Speciálisan, ha $ef = 0$, akkor $e \vee f$ és $e \wedge f$ léteznek $\mathbf{P}(A)$-ban, és $e \vee f = e + f$, valamint $e \wedge f = 0$.

b) *Ha $e \leq f$, akkor $f - e \in \mathbf{P}(A)$ és $e \vee (f - e) = f$.*

c) *Ha $ef = 0$ és $g \in \mathbf{P}(A)$ olyan, hogy $e \leq g \leq e \vee f$, akkor $g - e \leq f$.*

Bizonyítás. a) Tegyük fel, hogy $ef = fe$. Ekkor $ef \in \mathbf{P}(A)$, mert $(ef)^* = f^*e^* = fe = ef$ és $(ef)^2 = e(fe)f = e(ef)f = ef$. Világos továbbá, hogy $(ef)e = e(fe) = e(ef) = ef$ és $(ef)f = ef$, tehát ef alsó korlátja az $\{e, f\}$ halmaznak. Ha $g \in \mathbf{P}(A)$ olyan projektor, amely alsó korlátja az $\{e, f\}$ halmaznak, akkor $g(ef) = (ge)f = gf = g$, tehát $g \leq ef$. Ezért ef a legnagyobb alsó korlátja az $\{e, f\}$ halmaznak, vagyis $e \wedge f = ef$.

Továbbá, ha $ef = fe$, akkor $e + f - ef \in \mathbf{P}(A)$, mert $(e + f - ef)^* = e^* + f^* - (ef)^* = e + f - f^*e^* = e + f - fe = e + f - ef$, valamint $(e + f - ef)^2 = e^2 + fe - (ef)e + ef + f^2 - (ef)f - e(ef) - f(ef) + (ef)(ef) = e + fe - ef + ef + f - ef - ef - ef + ef = e + f - ef$. Világos, hogy $e(e + f - ef) = e^2 + ef - e(ef) = e + ef - ef = e$ és $f(e + f - ef) = fe + f^2 - f(ef) = fe + f - ef = f$, vagyis $e + f - ef$ felső korlátja az $\{e, f\}$ halmaznak. Ha $g \in \mathbf{P}(A)$ olyan projektor, amely felső korlátja az $\{e, f\}$ halmaznak, akkor $(e + f - ef)g = eg + fg - e(fg) = e + f - ef$, tehát $e + f - ef \leq g$. Ez azt jelenti, hogy $e + f - ef$ a legkisebb felső korlátja az $\{e, f\}$ halmaznak, vagyis $e \vee f = e + f - ef$.

Ha $ef = 0$, akkor $fe = f^*e^* = (ef)^* = 0 = ef$, tehát az előzőek alapján $e \vee f = e + f$ és $e \wedge f = 0$.

b) Tegyük fel, hogy $e \leq f$. Ekkor a 3) megjegyzés alapján $f - e \in \mathbf{P}(A)$, és világos, hogy $e(f - e) = ef - e^2 = e - e = 0$, így az a) szerint $e \vee (f - e)$ létezik és $e \vee (f - e) = e + (f - e) = f$.

c) Tegyük fel, hogy $ef = 0$ és $g \in \mathbf{P}(A)$ olyan, hogy $e \leq g \leq e \vee f$. Ekkor az a) alapján $g = g(e \vee f) = g(e + f) = ge + gf = e + gf$, tehát $g - e = gf$. Ugyanakkor $e \leq g$ miatt $g - e \in \mathbf{P}(A)$, tehát ez az elem önadjungált, így $fg = (gf)^* = (g - e)^* = g - e = gf$, vagyis az a)-ból következik, hogy $f \wedge g$ létezik és $f \wedge g = fg$. Ebből látható, hogy $g - e = gf = fg = f \wedge g \leq f$. ■

24.9.5. Következmény. *Ha A *-algebra és $(e_i)_{i \in I}$ nem üres véges kommutatív rendszer $\mathbf{P}(A)$-ban, akkor $\bigvee_{i \in I} e_i$ és $\bigwedge_{i \in I} e_i$ léteznek $\mathbf{P}(A)$-ban, valamint*

$$\bigvee_{i \in I} e_i = \sum_{H \subseteq I,\ H \neq \emptyset} (-1)^{\mathrm{Card}(H)+1} \Big(\mathrm{P}_{i \in H}\, e_i \Big), \qquad \bigwedge_{i \in I} e_i = \mathrm{P}_{i \in I}\, e_i.$$

*Ha A kommutatív *-algebra, akkor $\mathbf{P}(A)$ a $\leq$ relációval ellátva alulról korlátos disztributív háló.*

Bizonyítás. Az előző állítás a) pontja alapján, az I halmaz számossága szerinti teljes indukcióval igazolható. ■

24.9.6. Állítás. *Ha A egységelemes *-algebra, akkor a*

$$\mathbf{P}(A) \to \mathbf{P}(A); \quad e \mapsto e^{\perp} := \mathbf{1} - e$$

leképezés ortokomplementáció a $\mathbf{P}(A)$ korlátos rendezett halmaz felett (22.5.1.).

Bizonyítás. Világos, hogy $e \in \mathbf{P}(A)$ esetén $\left(e^{\perp}\right)^{\perp} = \mathbf{1}-(\mathbf{1}-e) = e$, és minden $e, f \in \mathbf{P}(A)$ esetén, ha $e \leq f$, akkor $f^{\perp}e^{\perp} = (\mathbf{1}-f)(\mathbf{1}-e) = \mathbf{1}-e-f+fe = \mathbf{1}-f = f^{\perp}$, vagyis $f^{\perp} \leq e^{\perp}$. Ha $e \in \mathbf{P}(A)$, akkor $ee^{\perp} = 0$ miatt $e \vee e^{\perp} = e + (\mathbf{1}-e) = \mathbf{1}$. ■

24.9.7. Definíció. *Ha A egységelemes *-algebra, akkor $e, f \in \mathbf{P}(A)$ esetén azt mondjuk, hogy e és f* **ortogonálisak egymásra***, ha $e \leq f^{\perp}$ teljesül; ezt a tényállást az $e \perp f$ szimbólummal jelöljük.*

Nyilvánvaló, hogy ha A egységelemes *-algebra, akkor $e, f \in \mathbf{P}(A)$ esetén $e \perp f$ pontosan akkor teljesül, ha $ef = 0$. Valóban, $ef^{\perp} = e(\mathbf{1}-f) = e - ef$, ezért $e = ef^{\perp}$ (vagyis $e \perp f$) azzal egyenértékű, hogy $e = e - ef$ (vagyis $ef = 0$).

24.9.8. Állítás. *Ha A egységelemes *-algebra, akkor $\mathbf{P}(A)$ a $\leq$ rendezéssel és $\perp$ leképezéssel ellátva olyan ortokomplementált rendezett halmaz, amelyben bármely véges ortogonális rendszernek létezik szuprémuma, és amelyben minden $e, f \in \mathbf{P}(A)$ elemre, ha $e \leq f$, akkor egyértelműen létezik olyan $g \in \mathbf{P}(A)$, amelyre $e \perp g$ és $e \vee g = f$; ez a g projektor egyenlő az $f \wedge e^{\perp}$ elemmel. Ha A kommutatív egységelemes *-algebra, akkor $\mathbf{P}(A)$ Boole-háló.*

Bizonyítás. Ha $(e_i)_{i \in I}$ nem üres ortogonális rendszer $\mathbf{P}(A)$-ban, az $(e_i)_{i \in I}$ rendszer kommutatív, így $\bigvee_{i \in I} e_i$ létezik a $\mathbf{P}(A)$ rendezett halmazban. Ha $e, f \in \mathbf{P}(A)$ és $e \leq f$, akkor $f - e \in \mathbf{P}(A)$ és $e \perp f - e$, mert $e(f-e) = ef - e = 0$, továbbá $e \vee (f-e) = e + (f-e) = f$. Ha $e, f \in \mathbf{P}(A)$, $e \leq f$ és $g \in \mathbf{P}(A)$ olyan, hogy $e \perp g$ és $e \vee g = f$, akkor $e \vee g = e + g$ miatt $g = f - e$, tehát g egyértelműen van meghatározva. Továbbá, ekkor $(f-e)f = f^2 - fe = f - e$ és $(f-e)e^{\perp} = (f-e)(\mathbf{1}-e) = f-e-fe+e^2 = f-e-e+e = f-e$, tehát $f - e$ alsó korlátja az $\{f, e^{\perp}\}$ halmaznak. Ha $g \in \mathbf{P}(A)$ alsó korlátja az $\{f, e^{\perp}\}$ halmaznak, akkor $g \leq e^{\perp}$ miatt $ge = 0$, így $g(f-e) = gf - ge = g$, vagyis $g \leq f - e$. Ez azt jelenti, hogy $e \leq f$ esetén $f - e = f \wedge e^{\perp}$.

Legyen A kommutatív egységelemes *-algebra és $e, f \in \mathbf{P}(A)$. Ekkor

$$(e \vee f) \wedge g = (e + f - ef)g = eg + fg - efg,$$

ugyanakkor

$$(e \wedge g) \vee (f \wedge g) = eg + fg - (eg)(fg) = eg + fg - efg,$$

ami azt jelenti, hogy

$$(e \wedge g) \vee (f \wedge g) = (e \vee f) \wedge g,$$

vagyis a $\mathbf{P}(A)$ ortoháló disztributív. ■

24.10. Rickart-*-algebrák és ortomoduláris projektorhálók

Algebrai szempontból érdekes kérdés, hogy egy *-algebra projektorainak halmazán a természetes rendezés milyen algebrai feltételek teljesülése esetén *hálószerű*. Az alábbiakban olyan *elégséges feltételt* adunk, amely jó motivációt ad majd a Rickart-*-algebrák bevezetéséhez.

24.10.1. Állítás. *Legyen A *-algebra és $e, f \in \mathbf{P}(A)$. Ekkor a következő állítások ekvivalensek.*

(i) *Az $R_{e,f} := \{h \in \mathbf{P}(A) | (eh = 0) \wedge ((f - fe)h = f - fe)\}$ halmaznak létezik legkisebb eleme $\mathbf{P}(A)$-ban.*

(ii) *Létezik az $e \vee f$ elem $\mathbf{P}(A)$-ban.*

Továbbá, ha (i) *teljesül, akkor $e \vee f = e + \min(R_{e,f})$.*

Bizonyítás. (i)⇒(ii) Legyen $g := \min(R_{e,f})$. Ekkor $g \in R_{e,f}$, így $eg = 0$, tehát $e \vee g$ létezik $\mathbf{P}(A)$-ban és $e \vee g = e + g$. Állítjuk, hogy $e + g$ egyenlő az $\{e, f\}$ halmaz legkisebb felső korlátjával. Valóban, $e \leq e \vee g = e + g$, továbbá $eg = 0$ és $(f - fe)g = f - fe$ miatt $fg = f - fe$, így $f(e + g) = f$, vagyis $f \leq e + g$. Ez azt jelenti, hogy $e + g$ felső korlátja az $\{e, f\}$ halmaznak. Legyen $h \in \mathbf{P}(A)$ felső korlátja az $\{e, f\}$ halmaznak. Ekkor $e \leq h$, tehát $h - e \in \mathbf{P}(A)$, és világos, hogy $e(h - e) = eh - e^2 = 0$, valamint $f = fh$ miatt $(f - fe)(h - e) = fh - (fe)h - fe + (fe)e = f - fe$, vagyis $h - e \in R_{e,f}$. A g definíciója alapján $g \leq h - e$, tehát $g = g(h - e) = gh - ge = gh$, azaz $g \leq h$. Ugyanakkor $e \leq h$ is teljesül, tehát $e + g = e \vee g \leq h$. Ez azt jelenti, hogy $e + g$ az $\{e, f\}$ halmaz legkisebb felső korlátja, és azt is látjuk, hogy $e \vee f = e + \min(R_{e,f})$.

(ii)⇒(i) Tegyük fel, hogy $e \vee f$ létezik $\mathbf{P}(A)$-ban, és legyen $g := (e \vee f) - e$. Állítjuk, hogy g az $R_{e,f}$ halmaz legkisebb eleme. Valóban, $eg = e((e \vee f) - e) = e(e \vee f) - e^2 = 0$ és $(f - fe)g = (f - fe)((e \vee f) - e) = f(e \vee f) - (fe)(e \vee f) - fe + (fe)e = f - fe$, ezért $g \in R_{e,f}$. Legyen $h \in R_{e,f}$ tetszőleges; azt kell igazolni, hogy $g \leq h$. Világos, hogy $eh = 0$ miatt $e + h \in \mathbf{P}(A)$ és $e \leq e \vee h = e + h$. Továbbá, $f - fe = (f - fe)h = fh$, vagyis $f = f(e + h)$, így $f \leq h$. Ebből következik, hogy $e \vee f \leq e + g$, így $e \vee f = (e \vee f)(e + h) = (e \vee f)e + (e \vee f)h = e + (e \vee f)h$, azaz $(e \vee f) - e = (e \vee f)h = ((e \vee f) - e)h$. Ez azt jelenti, hogy $g = gh$, vagyis $g \leq h$. ■

24.10.2. Következmény. *Ha A egységelemes *-algebra és $e, f \in \mathbf{P}(A)$ olyan elemek, amelyekre az $\{h \in \mathbf{P}(A) | (f - fe)h = f - fe\}$ halmaznak létezik legkisebb eleme $\mathbf{P}(A)$-ban, akkor $e \vee f$ létezik $\mathbf{P}(A)$-ban, és $e \vee f = e + \min(\{h \in \mathbf{P}(A) | (f - fe)h = f - fe\})$.*

Bizonyítás. Legyen $R'_{e,f} := \{h \in \mathbf{P}(A) | (f - fe)h = f - fe\}$ és $g := \min(R'_{e,f})$. Világos, hogy $R_{e,f} := \{h \in \mathbf{P}(A) | (eh = 0) \wedge ((f - fe)h = f - fe)\} \subseteq R'_{e,f}$, így g az $R_{e,f}$ halmaz minden eleménél kisebb-egyenlő $\mathbf{P}(A)$-ban. Ezért ha $g \in R_{e,f}$, akkor g az $R_{e,f}$ halmaz legkisebb eleme, így elég hivatkozni az előző állításra. A $g \in R_{e,f}$ kijelentés azzal ekvivalens, hogy $eg = 0$, vagyis $g \leq e^{\perp}$. Ez utóbbi egyenlőtlenség viszont igaz, mert $(f - fe)e^{\perp} = fe^{\perp} - (fe)e^{\perp} = fe^{\perp} = f(\mathbf{1} - e) = f - fe$, azaz $e^{\perp} \in R'_{e,f}$. ■

24.10.3. Következmény. *Legyen A egységelemes *-algebra és vezessük be az $S := \{f - fe | e, f \in \mathbf{P}(A)\}$ halmazt. Ha minden $s \in S$ esetén a $\{h \in \mathbf{P}(A) | sh = s\}$ halmaznak létezik legkisebb eleme $\mathbf{P}(A)$-ban, akkor $\mathbf{P}(A)$ ortomoduláris háló.*

Bizonyítás. Ha a feltétel teljesül, akkor az előző állítás alapján minden $e, f \in \mathbf{P}(A)$ esetén $e \vee f$ létezik $\mathbf{P}(A)$-ban. Az ortokomplementáció tulajdonságaiból következik, hogy minden $e, f \in \mathbf{P}(A)$ esetén $e \wedge f$ is létezik $\mathbf{P}(A)$-ban, hiszen $\left(e^{\perp} \vee f^{\perp}\right)^{\perp}$ az $\{e, f\}$ halmaz legkisebb felső korlátja (*de Morgan-egyenlőtlenség*) (22.5.3.), így $\mathbf{P}(A)$ ortomoduláris háló. ■

24.10.4. Definíció. *Ha A *-algebra, akkor az $a \in A$ elem* **jobboldali projektorának** *nevezünk minden olyan $e \in \mathbf{P}(A)$ projektort, amelyre minden $x \in A$ esetén az $ax = 0$ és $ex = 0$ kijelentések ekvivalensek (vagyis az a elem és az e projektor* **jobboldali anullátorai** *egyenlőek A-ban).*

Megjegyezzük, hogy *-algebrában nem szükségképpen létezik minden elemnek jobboldali projektora: erre a jelenségre hamarosan példákat látunk. Azonban *egységelemes* *-algebrában minden elemnek *legfeljebb egy* jobboldali projektora létezik. Valóban, ha A egységelemes *-algebra és $e, f \in \mathbf{P}(A)$ olyanok, hogy minden $A \ni x$-re $ex = 0$ ekvivalens azzal, hogy $fx = 0$, akkor $ee^\perp = 0$ miatt $0 = fe^\perp = f - fe$, azaz $f \leq e$, továbbá $ff^\perp = 0$ miatt $0 = ef^\perp = e - ef$, azaz $e \leq f$, így $e = f$.

24.10.5. Definíció. *Ha A egységelemes *-algebra, akkor az $a \in A$ elem jobboldali projektorát* $\mathrm{RP}(a)$ *jelöli, ha létezik. Az A egységelemes *-algebrát* **Rickart-*-algebrának** *nevezzük, ha az A minden elemének létezik jobboldali projektora.*

Megjegyezzük, hogy ha A egységelemes *-algebra, és az $a \in A$ elemnek létezik jobboldali projektora, akkor $\mathrm{RP}(a)$ a $\{h \in \mathbf{P}(A) | ah = a\}$ halmaz legkisebb eleme $\mathbf{P}(A)$-ban, hiszen $\mathrm{RP}(a)\mathrm{RP}(a)^\perp = 0$ miatt $0 = a\mathrm{RP}(a)^\perp = a - a\mathrm{RP}(a)$, így $\mathrm{RP}(a) \in \{h \in \mathbf{P}(A) | ah = a\}$, továbbá, ha $h \in \mathbf{P}(A)$ és $ah = a$, akkor $ah^\perp = a - ah = 0$, így $0 = \mathrm{RP}(a)h^\perp = \mathrm{RP}(a) - \mathrm{RP}(a)h$, vagyis $\mathrm{RP}(a) \leq h$.

24.10.6. Állítás. *Ha A Rickart-*-algebra, akkor* $\mathbf{P}(A)$ *ortomoduláris háló, és minden $e, f \in \mathbf{P}(A)$ esetén*

$$e \vee f = e + \mathrm{RP}(f - fe)$$
$$e \wedge f = e - \mathrm{RP}(e - fe).$$

Bizonyítás. Legyenek $e, f \in \mathbf{P}(A)$. Ekkor $\mathrm{RP}(f - fe)$ a $\{h \in \mathbf{P}(A) | (f - fe)h = f - fe\}$ halmaz legkisebb eleme, így $e \vee f$ létezik $\mathbf{P}(A)$-ban, és $e \vee f = e + \mathrm{RP}(f - fe)$. A de Morgan egyenlőség alapján egyszerű számolással kapjuk, hogy

$$e \wedge f = \left(e^\perp \vee f^\perp\right)^\perp = \mathbf{1} - ((\mathbf{1} - e) + \mathrm{RP}((\mathbf{1} - f) - (\mathbf{1} - f)(\mathbf{1} - e)) = e - \mathrm{RP}(e - fe). \blacksquare$$

Példák (Rickart-*-algebrákra).

1) Legyen T halmaz és $\mathscr{B}$ σ-algebra T felett. (Ilyenkor azt is mondjuk, hogy a $(T, \mathscr{B})$ pár *mérhető tér.*) Legyen $A := \widehat{\mathscr{E}}_{\mathbb{C}}(T, \mathscr{B})$, vagyis A a $T \to \mathbb{C}$ $\mathscr{B}$-egyszerű függvények *-algebrája. Könnyen igazolható, hogy egy $f : T \to \mathbb{C}$ függvény pontosan akkor eleme A-nak, ha korlátos és minden $E \subseteq \mathbb{C}$ Borel-halmazra $\overset{-1}{f}\langle E \rangle \in \mathscr{B}$. Állítjuk, hogy A Rickart-*-algebra. Valóban, ha $a \in A$, akkor nyilvánvaló, hogy minden $A \ni x$-re

$$ax = 0 \;\Leftrightarrow\; [a \neq 0] \subseteq [x = 0] \;\Leftrightarrow\; \chi_{[a \neq 0]} x = 0,$$

és $\mathbb{C} \setminus \{0\}$ Borel-halmaz $\mathbb{C}$-ben (mert nyílt), így $[a \neq 0] = \overset{-1}{a}\langle \mathbb{C} \setminus \{0\} \rangle \in \mathscr{B}$, következésképpen $\chi_{[a \neq 0]} \in \mathbf{P}(A)$. Látható, hogy $a \in A$ esetén $\mathrm{RP}(a) = \chi_{[a \neq 0]}$.

2) Legyen $\mathscr{H}$ Hilbert-tér; ekkor az $A := \mathscr{L}(\mathscr{H})$ operátoralgebra Rickart-*-algebra. Valóban, ha $a \in A$ és e jelöli a $(\mathrm{Ker}(a))^\perp$ zárt lineáris altérre vetítő ortogonális projektort, akkor minden $A \ni x$-re

$$ax = 0 \;\Leftrightarrow\; \mathrm{Im}(x) \subseteq \mathrm{Ker}(a) \;\Leftrightarrow\; (\mathrm{Ker}(a))^\perp \subseteq (\mathrm{Im}(x))^\perp = \mathrm{Ker}(x^*) \;\Leftrightarrow$$
$$\Leftrightarrow\; \mathrm{Im}(e) \subseteq \mathrm{Ker}(x^*) \;\Leftrightarrow\; x^* e = 0 \;\Leftrightarrow\; ex = 0$$

teljesül, ezért $e = \mathrm{RP}(a)$.

24.10.7. Definíció. *Az A Rickart-*-algebra* **Rickart-*-részalgebrájának** *nevezzük az A minden olyan B *-részalgebráját, amely egységelemes, és minden $b \in B$ esetén* $\mathrm{RP}(b) \in B$. (*Azonban nem követeljük meg, hogy a B egységeleme megegyezzen az A egységelemével.*)

24.10.8. Állítás. *Ha A Rickart-*-algebra és B Rickart-*-részalgebrája A-nak, akkor B az A műveleteinek leszűkítésével ellátva olyan Rickart-*-algebra, amelyre minden $b \in B$ esetén b jobboldali projektora B-ben ugyanaz, mint A-ban.*

Bizonyítás. Nyilvánvaló következménye annak, hogy minden $b \in B$ esetén a b elem jobboldali anullátora B-ben egyenlő az A-beli jobboldali anullátorának B-vel vett metszetével. ■

Példák (Rickart-*-részalgebrákra).

1) Legyen A Rickart-*-algebra és $e \in \mathbf{P}(A)$. Ekkor az eAe redukált algebra az A-nak Rickart-*-részalgebrája. Valóban, eAe az A-nak egységelemes *-részalgebrája (amelynek az egységeleme e, ami az érdekes esetben nem egyenlő az A egységelemével), továbbá, ha $b \in eAe$, akkor $be^{\perp} = b - be = 0$, így a jobboldali projektor értelmezése alapján $\mathrm{RP}(b)e^{\perp} = 0$, vagyis $\mathrm{RP}(b)e = \mathrm{RP}(b)$, tehát $\mathrm{RP}(b) \in eAe$.

2) Legyen A Rickart-*-algebra és $S \subseteq A$ önadjungált halmaz, vagyis minden $s \in S$ esetén $s^* \in S$. Ekkor a $\mathrm{C}(S)$ kommutáns az A-nak Rickart-*-részalgebrája. Valóban, $\mathrm{C}(S)$ olyan *-részalgebrája A-nak, amelynek eleme az A egységeleme, továbbá, ha $b \in \mathrm{C}(S)$ és $s \in S$, akkor $b\mathrm{RP}(b) = b$ miatt $b(s\mathrm{RP}(b) - s) = (bs)\mathrm{RP}(b) - bs = (sb)\mathrm{RP}(b) - bs = sb - bs = 0$, így a jobboldali projektor értelmezése alapján $\mathrm{RP}(b)(s\mathrm{RP}(b) - s) = 0$, vagyis $\mathrm{RP}(b)s = \mathrm{RP}(b)s\mathrm{RP}(b)$. Tehát $b \in \mathrm{C}(S)$ és $s \in S$ esetén $\mathrm{RP}(b)s^* = \mathrm{RP}(b)s^*\mathrm{RP}(b)$ is teljesül, hiszen $s^* \in S$, amiből adjungálással nyerjük, hogy $s\mathrm{RP}(b) = \mathrm{RP}(b)s\mathrm{RP}(b) = \mathrm{RP}(b)s$, azaz $\mathrm{RP}(b) \in \mathrm{C}(S)$.

Az előző példa alapján világos, hogy minden *Neumann-algebra* Rickart-*-algebra.

24.11. Clifford-*-algebrák

25. fejezet

Rendezett vektorterek és lineáris hálók

25.1. Rendezett csoportok

25.1.1. Definíció. *Azt mondjuk, hogy az* $(G, +, \leq)$ *hármas* **rendezett csoport**, *ha* $(G, +)$ *kommutatív csoport és* $\leq$ *olyan rendezés* G *felett, amelyre teljesül a következő tulajdonság.*

(GO) *Minden* $x, y, z \in G$ *esetén, ha* $x \leq y$, *akkor* $x + z \leq y + z$ (*vagyis minden* $z \in G$ *elemre az* $G \to G$; $x \mapsto x + z$ *leképezés monoton növő a* $\leq$ *rendezés szerint*).

Ha $(G, +, \leq)$ *rendezett csoport, akkor*

$$G_+ := \{ x \in G \mid 0 \leq x \},$$

és az G_+ *halmazt az* $(G, +, \leq)$ *rendezett csoport* **pozitivitás-tartományának** *nevezzük, és* G_+ *elemeit* **pozitívaknak** *nevezzük.*

A szokásos jelölési konvenciónak megfelelően minden rendezett csoportot egyetlen szimbólummal, az alaphalmaz jelével jelölünk, továbbá a kommutatív csoportműveletére a $+$, és neutrális elemére a 0, valamint rendezésére a $\leq$ szimbólumot alkalmazzuk.

Ha G rendezett csoport és $x, y \in G$, akkor

$$x \leq y \quad \Leftrightarrow \quad -y \leq -x \quad \Leftrightarrow \quad 0 \leq y - x.$$

Valóban, ha $x \leq y$, akkor (GO) szerint $0 = x + (-x) \leq y + (-x) = y - x$, ezért ismét az (GO) feltételt alkalmazva $-y = 0 + (-y) \leq (y + (-x)) + (-y) = -x$, ami azt jelenti, hogy minden $x, y \in G$ esetén $(x \leq y) \Rightarrow (-y \leq -x)$ és $(x \leq y) \Rightarrow (0 \leq y - x)$ teljesül. Ebből következik, hogy ha $-y \leq -x$, akkor $x = -(-x) \leq -(-y) = y$, ami azt jelenti, hogy minden $x, y \in G$ esetén $(-y \leq -x) \Rightarrow (x \leq y)$ is teljesül, következésképpen $(x \leq y) \Leftrightarrow (-y \leq -x)$. Ha $0 \leq y - x$, akkor (GO) alapján $x = 0 + x \leq (y - x) + x = y$. Ezért $(x \leq y) \Leftrightarrow (0 \leq y - x)$ is teljesül.

Az előző bekezdésből következik, hogy rendezett csoport rendezését egyértelműen meghatározza a pozitivitás-tartománya. A következő állításban megmutatjuk, hogy rendezett csoportok pozitivitás-tartományai milyen jellemző tulajdonságokkal rendelkeznek.

25.1.2. Állítás. *Legyen* $(G, +)$ *kommutatív csoport.*

a) *Ha* $\leq$ *olyan rendezés* G *felett, hogy* $(G, +, \leq)$ *rendezett csoport, akkor az* G_+ *halmazra*

$$G_+ + G_+ \subseteq G_+, \quad G_+ \cap (-G_+) = \{0\}$$

teljesül.

b) *Ha $P \subseteq G$ olyan halmaz, hogy*

$$P + P \subseteq P, \quad P \cap (-P) = \{0\},$$

akkor létezik egyetlen olyan $\leq$ rendezés G felett, hogy $(G, +, \leq)$ rendezett csoport és $P = \{x \in G | 0 \leq x\}$.

Bizonyítás. a) Ha $x, y \in G_+$, akkor (GO) miatt $0 \leq x = 0 + x \leq y + x = x + y$, tehát $x + y \in G_+$. Ezért $G_+ + G_+ \subseteq G_+$ teljesül.

Az nyilvánvaló, hogy $0 \in G_+ \cap (-G_+)$. Ha $x \in G_+ \cap (-G_+)$, akkor $0 \leq -x$, így (GO) miatt $x = 0 + x \leq (-x) + x = 0$, tehát $0 \leq x$ és $x \leq 0$ egyszerre teljesül, így a $\leq$ reláció antiszimmetrikussága folytán $x = 0$. Ezért $G_+ \cap (-G_+) = \{0\}$ teljesül.

b) Vezessük be a

$$\leq := \{ (x, y) \in G \times G \mid y - x \in P \}$$

relációt. Ez rendezés az G halmaz felett.

Valóban, $P \cap (-P) = \{0\}$ miatt $0 \in P$, ezért minden $x \in G$ esetén $x - x = 0 \in P$, vagyis $x \leq x$, ami azt jelenti, hogy $\leq$ reflexív az G halmazon. Ha $x, y \in G$, valamint $x \leq y$ és $y \leq x$, akkor $y - x \in P$ és $-(y - x) = x - y \in P$, tehát $y - x \in P \cap (-P) = \{0\}$, vagyis $y - x = 0$, azaz $x = y$, ami azt jelenti, hogy a $\leq$ reláció antiszimmetrikus. Ha $x, y, z \in G$, valamint $x \leq y$ és $y \leq z$, akkor $y - x \in P$ és $z - y \in P$, tehát $z - x = (z - y) + (y - x) \in P + P \subseteq P$, vagyis $x \leq z$, ami azt jelenti, hogy a $\leq$ reláció tranzitív. Tehát a $\leq$ reláció rendezés az G halmaz felett.

Ha $x, y, z \in G$, valamint $x \leq y$, akkor $(y + z) - (x + z) = y - x \in P$, tehát $x + z \leq y + z$, vagyis a $\leq$ rendezésre és a $+$ műveletre (GO) teljesül, ami azt jelenti, hogy $(G, +, \leq)$ rendezett csoport. Mivel $\leq$ definíciója szerint minden $x \in G$ elemre $0 \leq x$ és $x = x - 0 \in P$ ekvivalens kijelentések, így $P = \{x \in G | 0 \leq x\}$.

Ha $\leq'$ szintén olyan rendezés G felett, hogy $(G, +, \leq')$ rendezett csoport és fennáll a $P = \{x \in G | 0 \leq' x\}$ egyenlőség, akkor minden $x, y \in G$ esetén

$$x \leq y \Leftrightarrow y - x \in P = \{z \in G | 0 \leq' z\} \Leftrightarrow 0 \leq' (y - x) \Leftrightarrow x \leq' y,$$

tehát $\leq = \leq'$, amivel az egyértelműséget is igazoltuk. ■

25.1.3. Állítás. (**Az egyenlőtlenségek összeadásának szabálya.**) *Ha G rendezett csoport, és $(x_i)_{i \in I}$ és $(y_i)_{i \in I}$ olyan G-ben haladó véges rendszerek, hogy minden $i \in I$ esetén $x_i \leq y_i$, akkor*

$$\sum_{i \in I} x_i \leq \sum_{i \in I} y_i.$$

Bizonyítás. Az I indexhalmaz számossága szerinti teljes indukcióval bizonyítunk.

Az állítás igaz, ha $\mathrm{Card}(I) = 0$, azaz $I = \emptyset$, mert ekkor a $0 \leq 0$ egyenlőtlenségről van szó. Az állítás triviális akkor ha $\mathrm{Card}(I) = 1$, vagyis I egy elemű.

Most igazoljuk az állítást $\mathrm{Card}(I) = 2$ esetén. (Erre szükség lesz az indukciós lépés megtételénél.) Legyenek tehát α és β olyan halmazok, hogy $\alpha \neq \beta$ és $I = \{\alpha, \beta\}$. A hipotézis szerint $x_\alpha \leq y_\alpha$, ezért (GO) alapján kapjuk, hogy $x_\alpha + x_\beta \leq y_\alpha + x_\beta$. Ugyanakkor, a hipotézis szerint $x_\beta \leq y_\beta$, ezért a $+$ művelet kommutativitása és (GO) szerint $y_\alpha + x_\beta = x_\beta + y_\alpha \leq y_\beta + y_\alpha = y_\alpha + y_\beta$. Tehát $x_\alpha + x_\beta \leq y_\alpha + x_\beta$ és $y_\alpha + x_\beta \leq y_\alpha + y_\beta$ egyszerre teljesül, így a $\leq$ reláció tranzitivitása miatt

$$\sum_{i \in I} x_i = x_\alpha + x_\beta \leq y_\alpha + y_\beta = \sum_{i \in I} y_i.$$

Tegyük most fel, hogy az állítás igaz minden olyan I véges indexhalmazra, amelyre $\mathrm{Card}(I) = n$, ahol $n \in \mathbb{N}$ és $n \geq 2$. Legyenek $(x_i)_{i \in I}$ és $(y_i)_{i \in I}$ olyan G-ben haladó véges rendszerek, hogy $\mathrm{Card}(I) = n+1$, és minden $i \in I$ esetén $x_i \leq y_i$. Rögzítsünk egy $i_* \in I$ indexet és legyen $I_* := I \setminus \{i_*\}$. Ekkor $(x_i)_{i \in I_*}$ és $(y_i)_{i \in I_*}$ olyan G-ben haladó rndszerek, hogy $\mathrm{Card}(I_*) = n$, és minden $i \in I_*$ esetén $x_i \leq y_i$, ezért az indukciós hipotézis szerint $\sum\limits_{i \in I_*} x_i \leq \sum\limits_{i \in I_*} y_i$. Ugyanakkor $x_{i_*} \leq y_{i_*}$ is teljesül, ezért a két elemű indexhalmazra igazolt állítás alapján

$$\sum_{i \in I} x_i = \Big(\sum_{i \in I_*} x_i\Big) + x_{i_*} \leq \Big(\sum_{i \in I_*} y_i\Big) + y_{i_*} = \sum_{i \in I} y_i,$$

tehát az állítás igaz az n+1 számosságú I indexhalmazra is. ■

25.1.4. Állítás. *Legyen G rendezett csoport, $(x_i)_{i \in I}$ G-ben haladó rendszer.*

a) *A $\bigvee\limits_{i \in I} x_i$ szuprémum pontosan akkor létezik, ha létezik a $\bigwedge\limits_{i \in I} (-x_i)$ infimum, és ha $\bigvee\limits_{i \in I} x_i$ létezik, akkor*

$$\bigvee_{i \in I} x_i = -\bigwedge_{i \in I} (-x_i).$$

b) *A $\bigwedge\limits_{i \in I} x_i$ infimum pontosan akkor létezik, ha létezik a $\bigvee\limits_{i \in I} (-x_i)$ szuprémum, és ha $\bigwedge\limits_{i \in I} x_i$ létezik, akkor*

$$\bigwedge_{i \in I} x_i = -\bigvee_{i \in I} (-x_i).$$

c) *Ha $y \in G$, akkor a $\bigvee\limits_{i \in I} (x_i + y)$ szuprémum pontosan akkor létezik, ha létezik a $\bigvee\limits_{i \in I} x_i$ szuprémum, és ha $\bigvee\limits_{i \in I} x_i$ létezik, akkor*

$$\bigvee_{i \in I} (x_i + y) = \Big(\bigvee_{i \in I} x_i\Big) + y.$$

d) *Ha $y \in G$, akkor a $\bigwedge\limits_{i \in I} (x_i + y)$ infimum pontosan akkor létezik, ha létezik a $\bigwedge\limits_{i \in I} x_i$ infimum, és ha $\bigwedge\limits_{i \in I} x_i$ létezik, akkor*

$$\bigwedge_{i \in I} (x_i + y) = \Big(\bigwedge_{i \in I} x_i\Big) + y.$$

Bizonyítás. Az a) és b) állítások abból következnek, hogy az $G \to G;\ x \mapsto -x$ inverzió rendezés-izomorfizmus az $(G, \leq)$ rendezett halmaz és az $(G, \leq^\circ)$ ellentett rendezett halmaz között. A c) és d) állítások abból következnek, hogy minden $y \in G$ esetén (GO) miatt az $G \to G;\ x \mapsto x + y$ eltolás rendezés-automorfizmusa az $(G, \leq)$ rendezett halmaznak. (Természetesen lehetségesek elemi közvetlen bizonyítások is.) ■

25.1.5. Állítás. *Legyen G rendezett csoport, valamint $(x_i)_{i \in I}$ és $(y_j)_{j \in J}$ G-ben haladó nem üres rendszerek.*

a) *Ha léteznek a* $\bigvee_{i\in I} x_i$ *és* $\bigvee_{j\in J} y_j$ *szuprémumok, akkor létezik a* $\bigvee_{(i,j)\in I\times J}(x_i+y_j)$ *szuprémum is és*

$$\bigvee_{(i,j)\in I\times J}(x_i+y_j)=\Big(\bigvee_{i\in I} x_i\Big)+\Big(\bigvee_{j\in J} y_j\Big)$$

b) *Ha léteznek a* $\bigwedge_{i\in I} x_i$ *és* $\bigwedge_{j\in J} y_j$ *infimumok, akkor létezik a* $\bigwedge_{(i,j)\in I\times J}(x_i+y_j)$ *infimum is és*

$$\bigwedge_{(i,j)\in I\times J}(x_i+y_j)=\Big(\bigwedge_{i\in I} x_i\Big)+\Big(\bigwedge_{j\in J} y_j\Big).$$

Bizonyítás. a) Legyen $x:=\bigvee_{i\in I} x_i$ és $y:=\bigvee_{j\in J} y_j$. Minden $(i,j)\in I\times J$ esetén $x_i\le x$ és $y_j\le y$, így az egyenlőtlenségek összeadásának szabálya (25.1.3.) szerint $x_i+y_j\le x+y$, tehát $x+y$ felső korlátja az $(x_i+y_j)_{(i,j)\in I\times J}$ rendszernek. Legyen $z\in G$ felső korlátja az $(x_i+y_j)_{(i,j)\in I\times J}$ rendszernek, tehát minden $i\in I$ és $j\in J$ esetén $x_i+y_j\le z$. Ha $i\in I$, akkor minden $j\in J$ indexre $y_j\le z-x_i$, vagyis $z-x_i$ felső korlátja az $(y_j)_{j\in J}$ rendszernek, így $y=\bigvee_{j\in J} y_j\le z-x_i$. Tehát minden $i\in I$ indexre $x_i\le z-y$, vagyis $z-y$ felső korlátja az $(x_i)_{i\in I}$ rendszernek, ezért $x=\bigvee_{i\in I} x_i\le z-y$, vagyis $x+y\le z$. Ez azt jelenti, hogy $x+y$ a legkisebb felső korlátja az $(x_i+y_j)_{(i,j)\in I\times J}$ rendszernek.

b) Legyen $x:=\bigwedge_{i\in I} x_i$ és $y:=\bigwedge_{j\in J} y_j$. Minden $(i,j)\in I\times J$ esetén $x\le x_i$ és $y\le y_j$, így az egyenlőtlenségek összeadásának szabálya (25.1.3.) szerint $x+y\le x_i+y_j$, tehát $x+y$ alsó korlátja az $(x_i+y_j)_{(i,j)\in I\times J}$ rendszernek. Legyen $z\in G$ alsó korlátja az $(x_i+y_j)_{(i,j)\in I\times J}$ rendszernek, tehát minden $i\in I$ és $j\in J$ esetén $z\le x_i+y_j$. Ha $i\in I$, akkor minden $j\in J$ indexre $z-x_i\le y_j$, vagyis $z-x_i$ alsó korlátja az $(y_j)_{j\in J}$ rendszernek, így $z-x_i\le\bigwedge_{j\in J} y_j=y$. Tehát minden $i\in I$ indexre $z-y\le x_i$, vagyis $z-y$ alsó korlátja az $(x_i)_{i\in I}$ rendszernek, ezért $z-y\le x=\bigwedge_{i\in I} x_i$, vagyis $z\le x+y$. Ez azt jelenti, hogy $x+y$ a legnagyobb alsó korlátja az $(x_i+y_j)_{(i,j)\in I\times J}$ rendszernek. ■

25.2. Hálószerűen rendezett csoportok

25.2.1. Definíció. *Azt mondjuk, hogy G* **hálószerűen rendezett csoport**, *ha G olyan rendezett csoport, amelynek rendezése hálószerű.*

25.2.2. Állítás. *Ha G rendezett csoport, akkor a következő állítások ekvivalensek.*

(i) *G hálószerűen rendezett csoport.*

(ii) *Minden $x,y\in G$ esetén létezik az $x\vee y$ szuprémum.*

(iii) *Minden $x,y\in G$ esetén létezik az $x\wedge y$ infimum.*

Bizonyítás. Nyilvánvalóan következik a 25.1.4. állításból. ■

25.2.3. Definíció. *Ha G hálószerűen rendezett csoport, akkor minden $x\in G$ esetén*

$$x^+:=x\vee 0,\qquad x^-:=(-x)\vee 0,\qquad |x|=x\vee(-x),$$

és x^+-t az x elem **pozitív részének**, *x^--t az x elem* **negatív részének**, *és $|x|$-t az x elem* **abszolút értékének** *nevezzük.*

A definíció alapján nyilvánvaló, hogy ha G hálószerűen rendezett csoport, akkor minden $x \in G$ esetén

$$(-x)^+ = x^-, \quad (-x)^- = x^+, \quad |-x| = |x|.$$

Továbbá, ha G hálószerűen rendezett csoport és $x, y \in G$, akkor

$$|x+y| \ \leq \ |x| + |y|,$$

hiszen $x \leq |x|$ és $y \leq |y|$ miatt az egyenlőtlenségek összeadásának szabálya szerint $x+y \leq |x|+|y|$, valamint $-x \leq |x|$ és $-y \leq |y|$ miatt az egyenlőtlenségek összeadásának szabálya szerint $-(x+y) = (-x)+(-y) \leq |x|+|y|$, vagyis $|x+y| = (x+y) \vee (-(x+y)) \leq |x|+|y|$.

25.2.4. Állítás. *Legyen G hálószerűen rendezett csoport.*

a) *Minden $x \in G$ esetén $x^+, x^-, |x| \in G_+$ és*

$$x = x^+ - x^-, \quad |x| = x^+ + x^-,$$
$$2.x^+ = |x| + x, \quad 2.x^- = |x| - x.$$

b) *Minden $x, y \in G$ esetén*

$$x \vee y = x + (y-x)^+, \quad x \wedge y = x - (x-y)^+.$$

c) *Minden $x, y \in G$ esetén*

$$(x \wedge y) + (x \vee y) = x + y.$$

Bizonyítás. a) Legyen $x \in G$. A definíciók szerint triviális, hogy $0 \leq x^+$ és $0 \leq x^-$. Az $x = x^+ - x^-$ egyenlőség ekvivalens azzal, hogy $x \vee 0 = x^+ = x + x^-$.

Az $x \vee 0 = x + x^-$ egyenlőség bizonyításához először megjegyezzük, hogy a definíció szerint $-x \leq (-x) \vee 0 = x^-$, ezért $0 \leq x + x^-$. Továbbá, $0 \leq x^-$, ezért $x \leq x + x^-$, vagyis $x + x^-$ felső korlátja az $\{x, 0\}$ halmaznak. Legyen $y \in G$ felső korlátja az $\{x, 0\}$ halmaznak, vagyis $x \leq y$ és $0 \leq y$. Ekkor $0 \leq y - x$ és $-x \leq y - x$, ezért $x^- = (-x) \vee 0 \leq y - x$, amiből következik, hogy $x + x^- \leq y$. Tehát $x + x^-$ a legkisebb felső korlátja az $\{x, 0\}$ halmaznak, vagyis $x^+ = x \vee 0 = x + x^-$.

Bebizonyítjuk az $|x| = x^+ + x^-$ egyenlőséget, amiből $G_+ + G_+ \subseteq G_+$ miatt $|x| \in G_+$ is következik. Közvetlenül azt igazoljuk, hogy $x^+ + x^-$ az $\{-x, x\}$ halmaz legkisebb felső korlátja. Mivel $x \leq x^+$ és $0 \leq x^-$, így $x \leq x^+ + x^-$. Ugyanakkor $0 \leq x^+$ és $-x \leq x^-$, így $-x \leq x^+ + x^-$. Ez azt jelenti, hogy $x^+ + x^-$ felső korlátja az $\{-x, x\}$ halmaznak. Legyen $y \in G$ felső korlátja az $\{-x, x\}$ halmaznak, vagyis $-x \leq y$ és $x \leq y$. Ekkor az egyenlőtlenségek összeadásának szabálya szerint $0 = (-x) + x \leq y + y$, továbbá $y \leq y^+$, így $y + y \leq y^+ + y$, ezért $0 \leq y^+ + y$, vagyis $-y \leq y^+$. Ebből $0 \leq y^+$ miatt következik, hogy $y^- = (-y) \vee 0 \leq y^+$, tehát $0 \leq y^+ - y^- = y$. Ezután könnyen látható, hogy $x^+ + x^- \leq y$, vagy ami ugyanaz: $x^+ \leq y - x^-$. Valóban, $-x \leq y$ és $0 \leq y$, ezért $x^- = (-x) \vee 0 \leq y$, vagyis $0 \leq y - x^-$. Továbbá, $x \leq y$ és $0 \leq y$ miatt $x^+ = x \vee 0 \leq y$, ezért $x = x^+ - x^- \leq y - x^-$. Ezzel beláttuk, hogy $0 \leq y - x^-$ és $x \leq y - x^-$, tehát $x^+ = x \vee 0 \leq y - x^-$, vagyis $x^+ + x^- \leq y$. Ez azt jelenti, hogy $x^+ + x^-$ az $\{-x, x\}$ halmaz legkisebb felső korlátja, azaz $|x| = x \vee (-x) = x^+ + x^-$.

Tehát megmutattuk, hogy $|x| = x^+ + x^-$ és $x = x^+ - x^-$. Ezeket az egyenlőségeket összeadva és kivonva kapjuk, hogy $2.x^+ = |x| + x$ és $2.x^- = |x| - x$.

b) Legyenek $x, y \in G$.

Mivel $0 \leq (y-x)^+$, így $x \leq x + (y-x)^+$. Mivel $y - x \leq (y-x)^+$, így $y = x + (y-x) \leq$

$x+(y-x)^+$. Tehát az $x+(y-x)^+\in G$ elem felső korlátja az $\{x,y\}$ halmaznak. Legyen $z\in G$ felső korlátja az $\{x,y\}$ halmaznak, vagyis $x\le z$ és $y\le z$. Ekkor $y-x\le z-x$ és $0\le z-x$ egyszerre teljesül, így $(y-x)^+=(y-x)\vee 0\le z-x$. Ebből következik, hogy $x+(y-x)^+\le z$, tehát $x+(y-x)^+$ a legkisebb felső korlátja az $\{x,y\}$ halmaznak, vagyis $x\vee y=x+(y-x)^+$.

Mivel $0\le(x-y)^+$, így $-(x-y)^+\le 0$, tehát $x-(x-y)^+\le x$. Ugyanakkor, $x-y\le(x-y)^+$ miatt $x-(x-y)^+\le y$, tehát $x-(x-y)^+$ alsó korlátja az $\{x,y\}$ halmaznak. Legyen $z\in G$ alsó korlátja az $\{x,y\}$ halmaznak, vagyis $z\le x$ és $z\le y$. Ekkor $0\le x-z$ és $x-y\le x-z$ egyszerre teljesül, tehát $(x-y)^+=(x-y)\vee 0\le x-z$, amiből $z\le x-(x-y)^+$ következik. Ez azt jelenti, hogy $x-(x-y)^+$ a legnagyobb alsó korlátja az $\{x,y\}$ halmaznak, vagyis $x\wedge y=x-(x-y)^+$.

c) Legyenek $x,y\in G$. Felhasználva a nyilvánvaló $x\vee y=y\vee x$ egyenlőséget, b)-ből következik, hogy

$$(x\wedge y)+(x\vee y)=(x\wedge y)+(y\vee x)=x-(x-y)^++y+(x-y)^+=x+y.$$

(Másik bizonyítás: minden $x,y,z\in G$ esetén 25.1.4. c) és b) alapján

$$(z-x)\vee(z-y)=(z+(-x))\vee(z+(-y))=z+((-x)\vee(-y))=z-(x\wedge y)\,,$$

ahová a $z:=x+y$ értéket helyettesítve, és ismét felhasználva az $x\vee y=y\vee x$ összefüggést, kapjuk a bizonyítandó egyenlőséget.) ■

25.2.5. Következmény. *Ha G hálószerűen rendezett csoport, akkor minden $x\in G$ esetén:*

$$\begin{aligned} 0\le x \quad&\Leftrightarrow\quad x^-=0 \quad\Leftrightarrow\quad x^+=x \quad\Leftrightarrow\quad |x|=x.\\ x\le 0 \quad&\Leftrightarrow\quad x^-=-x \quad\Leftrightarrow\quad x^+=0 \quad\Leftrightarrow\quad |x|=-x.\end{aligned}$$

Bizonyítás. (I) Legyen $x\in G$. Ha $0\le x$, akkor $-x\le 0$, ezért $x^-=(-x)\vee 0=0$. Ha $x^-=0$, akkor az előző állítás a) pontja szerint $x=x^+-x^-=x^+$. Ha $x^+=x$, akkor $0\le x$, ezért $-x\le 0\le x$, tehát $|x|=x\vee(-x)=x$. Végül, ha $|x|=x$, akkor $0\le x$, mert az előző állítás a) pontja szerint $0\le|x|$.

(II) Az (I) ekvivalenciákat alkalmazva $x\in G$ esetén a $-x$ elemre, kapjuk a második ekvivalencia-láncot. ■

25.2.6. Állítás. (**Disztributivitás formulák.**) *Legyen G hálószerűen rendezett csoport, $(x_i)_{i\in I}$ tetszőleges G-ben haladó rendszer és $y\in G$.*

a) *Ha létezik a $\bigvee_{i\in I} x_i$ szuprémum, akkor létezik a $\bigvee_{i\in I}(y\wedge x_i)$ szuprémum is és*

$$\bigvee_{i\in I}(y\wedge x_i)=y\wedge\bigvee_{i\in I}x_i.$$

b) *Ha létezik a $\bigwedge_{i\in I} x_i$ infimum, akkor létezik a $\bigwedge_{i\in I}(y\vee x_i)$ infimum is és*

$$\bigwedge_{i\in I}(y\vee x_i)=y\vee\bigwedge_{i\in I}x_i.$$

Bizonyítás. a) Legyen $x:=\bigvee_{i\in I}x_i$. Azt kell igazolni, hogy $y\wedge x$ a legkisebb felső korlátja az $(y\wedge x_i)_{i\in I}$ rendszernek. Minden $i\in I$ esetén $y\wedge x_i\le y$ és $y\wedge x_i\le x_i\le x$, ezért

$y \wedge x_i \leq y \wedge x$, vagyis $y \wedge x$ felső korlátja az $(y \wedge x_i)_{i \in I}$ rendszernek. Legyen $z \in G$ felső korlátja az $(y \wedge x_i)_{i \in I}$ rendszernek. Ekkor 25.2.4. c) szerint minden $i \in I$ esetén $y + x_i - (y \vee x_i) = y \wedge x_i \leq z$, ezért $x_i \leq z - y + (y \vee x_i) \leq z - y + (y \vee x)$, így $x = \bigvee_{i \in I} x_i \leq z - y + (y \vee x)$ is teljesül. Tehát ismét a 25.2.4. c) állítást alkalmazva $x \wedge y = x + y - (y \vee x) \leq z$ adódik, vagyis $y \wedge x$ a legkisebb felső korlátja az $(y \wedge x_i)_{i \in I}$ rendszernek.

Legyen $x := \bigwedge_{i \in I} x_i$. Azt kell igazolni, hogy $y \vee x$ a legnagyobb alsó korlátja az $(y \vee x_i)_{i \in I}$ rendszernek. Minden $i \in I$ esetén $y \leq y \vee x_i$ és $x \leq x_i \leq y \vee x_i$, ezért $y \vee x \leq y \vee x_i$, vagyis $y \vee x$ alsó korlátja az $(y \vee x_i)_{i \in I}$ rendszernek. Legyen $z \in G$ alsó korlátja az $(y \vee x_i)_{i \in I}$ rendszernek. Ekkor 25.2.4. c) szerint minden $i \in I$ esetén $z \leq y \vee x_i = y + x_i - (y \wedge x_i)$, ezért $z - y + (y \wedge x) \leq z - y + (y \wedge x_i) \leq x_i$, így $z - y + (y \wedge x) \leq \bigwedge_{i \in I} x_i = x$ is teljesül. Tehát ismét a 25.2.4. c) állítást alkalmazva $z \leq x + y - (y \wedge x) = x \vee y$ adódik, vagyis $y \vee x$ a legnagyobb alsó korlátja az $(y \vee x_i)_{i \in I}$ rendszernek. ■

25.2.7. Következmény. *Minden hálószerűen rendezett csoport disztributív háló.* ■

25.2.8. Állítás. *Legyen $(G, +)$ kommutatív csoport.*

a) *Ha $\leq$ olyan rendezés G felett, hogy $(G, +, \leq)$ hálószerűen rendezett csoport, akkor az G_+ halmazra*

$$G_+ + G_+ \subseteq G_+, \quad G_+ \cap (-G_+) = \{0\}, \quad G_+ - G_+ = G$$

teljesül, és az $\leq$ rendezés G_+-ra vett megszorítása (vagyis a $\leq \cap (G_+ \times G_+)$ reláció) hálószerű rendezés az G_+ halmaz felett.

b) *Ha $P \subseteq G$ olyan halmaz, hogy*

$$P + P \subseteq P, \quad P \cap (-P) = \{0\}, \quad P - P = G,$$

és a $\leq := \{(x, y) \in G \times G | y - x \in P\}$ reláció P-re vett megszorítása hálószerű rendezés a P halmaz felett, akkor $\leq$ az egyetlen olyan rendezés G felett, hogy $(G, +, \leq)$ hálószerűen rendezett csoport és $P = \{x \in G | 0 \leq x\}$.

Bizonyítás. a) A 25.1.2. állítás alapján $G_+ + G_+ \subseteq G_+$ és $G_+ \cap (-G_+) = \{0\}$ teljesül, továbbá az előző állítás a) pontja szerint G minden eleme előáll két pozitív elem különbségeként, így $G_+ - G_+ = G$ is igaz. Ha $x, y \in G_+$, akkor nyilvánvaló, hogy $x \vee y \in G_+$ és $x \wedge y \in G_+$, ezért $x \vee y$ (illetve $x \wedge y$) az $\{x, y\}$ halmaz szuprémuma (illetve infimuma) a $\leq$ rendezés G_+-ra vett megszorítása szerint is, tehát ez a megszorított G_+ feletti rendezés hálószerű.

b) A 25.1.2. állítás alapján egyetlen olyan $\leq$ rendezés létezik G felett, amelyre $(G, +, \leq)$ rendezett csoport, és $P = \{x \in G | 0 \leq x\} = G_+$. Megmutatjuk, hogy a b) feltételei mellett a $\leq$ rendezés hálószerű.

Legyenek $x, y \in G$ rögzítve, és $G_+ - G_+ = G$ alapján vegyünk olyan $x', x'', y', y'' \in G_+$ elemeket, hogy $x = x' - x''$ és $y = y' - y''$. Ekkor $z := x'' + y'' \in G$ olyan elem, hogy $x + z = x' + y'' \in G_+$ és $y + z = y' + x'' \in G_+$. A hipotézis szerint az $\{x + z, y + z\}$ halmaznak létezik szuprémuma G_+-ban a $\leq_{G_+}$ megszorított rendezés szerint: jelölje u ezt a szuprémumot. Ekkor $x + z \leq u$ és $y + z \leq u$, ezért $x \leq u - z$ és $y \leq u - z$, vagyis $u - z \in G$ felső korlátja $\leq$ szerint az $\{x, y\}$ halmaznak. Legyen $v \in G$ felső korlátja $\leq$ szerint az $\{x, y\}$ halmaznak, vagyis $x \leq v$ és $y \leq v$. Ekkor $x + z \leq v + z$ és

$y+z \leq v+z$, és $0 \leq x+z$ miatt $v+z \in G_+$, ezért $u \leq_{G_+} v+z$, vagyis $u \leq v+z$, azaz $u-z \leq v$. Ez azt jelenti, hogy $u-z$ az $\{x,y\}$ halmaz legkisebb felső korlátja G-ben a $\leq$ rendezés szerint, tehát létezik az $x \vee y$ szuprémum. Ebből 25.2.2. alapján kapjuk, hogy $\leq$ hálószerű rendezés G felett.

A 25.1.2. állítás szerint a $\leq$ rendezés már azon G feletti rendezések halmazában is egyértelműen van meghatározva, amelyekre $(G,+,\leq)$ rendezett csoport és $P = G_+$. ■

25.2.9. Állítás. (Felbontási lemma.) *Legyen G hálószerűen rendezett csoport, és $(x_i)_{i\in I}$ nem üres véges G_+-ban haladó rendszer.*

a) *Ha $y \in G$ olyan, hogy $0 \leq y \leq \sum_{i\in I} x_i$, akkor létezik olyan G-ben haladó $(y_i)_{i\in I}$ rendszer, hogy $y = \sum_{i\in I} y_i$ és minden $i \in I$ esetén $0 \leq y_i \leq x_i$.*

b) *Ha $y \in G$ olyan, hogy $|y| \leq \sum_{i\in I} x_i$, akkor létezik olyan G-ben haladó $(y_i)_{i\in I}$ rendszer, hogy $y = \sum_{i\in I} y_i$ és minden $i \in I$ esetén $|y_i| \leq x_i$.*

Bizonyítás. a) Az I halmaz számossága szerinti teljes indukcióval bizonyítunk. Az állítás triviálisan igaz $\mathrm{Card}(I) = 1$ esetén. Megmutatjuk, hogy akkor is igaz, ha $I = \{0,1\}$. (Erre szükség lesz az indukciós lépés megtételénél.)

A hipotézis szerint $x_0, x_1 \in G_+$ és $y \in G$ olyan, hogy $0 \leq y \leq x_0 + x_1$. Vezessük be az

$$u := (x_0 - y)^+ \tag{$*$}$$

elemet. Meg fogjuk mutatni, hogy $y_0 := x_0 - u$ és $y_1 := y - y_0$ olyan elemek G-ben, amelyek létezését állítjuk, vagyis $y = y_0 + y_1$ (ami a definíció szerint triviális), valamint $0 \leq y_0 \leq x_0$ és $0 \leq y_1 \leq x_1$.

Világos, hogy $0 \leq u$ miatt $y_0 = x_0 - u \leq x_0$. Továbbá, $0 \leq y$ miatt $x_0 - y \leq x_0$ és a hipotézis szerint $0 \leq x_0$, ezért $u = (x_0-y)^+ \leq x_0$, tehát $0 \leq x_0 - u = y_0$.

Ugyanakkor, a definíció szerint $y_1 = y - y_0 = y - x_0 + u = y - x_0 + (x_0-y)^+ = (x_0-y)^+ - (x_0-y) \geq 0$, tehát $0 \leq y_1$. Másfelől, $0 \leq x_1$ miatt $x_0 - y \leq x_0 + x_1 - y$ és a hipotézis alapján $0 \leq x_0 + x_1 - y$, ezért $(x_0-y)^+ \leq x_0 + x_1 - y$, így $y_1 = y - x_0 + (x_0-y)^+ \leq x_1$. Ezzel igazoltuk az állítást $I = \{0,1\}$ esetén.

Tegyük most fel, hogy az állítás igaz minden olyan I véges indexhalmazra, amelyre $\mathrm{Card}(I) = n$, ahol $n \in \mathbb{N}$ és $n \geq 2$. Legyen $y \in G$ és $(x_i)_{i\in I}$ olyan G_+-ban haladó rendszer, amelyre $\mathrm{Card}(I) = n+1$ és $0 \leq y \leq \sum_{i\in I} x_i$. Rögzítsünk tetszőlegesen egy $i_* \in I$ indexet, és legyen $I_* := I \setminus \{i_*\}$. Vezessük be az $X_0 := \sum_{i\in I_*} x_i$ és $X_1 := x_{i_*}$ elemeket. Ekkor $X_0, X_1 \in G_+$ olyan elemek, hogy

$$0 \leq y \leq \sum_{i\in I} x_i = \sum_{i\in I_*} x_i + x_{i_*} = X_0 + X_1 = \sum_{i\in\{0,1\}} X_i,$$

így az előzőek szerint léteznek olyan $Y_0, Y_1 \in G$ elemek, hogy $y = Y_0 + Y_1$, valamint $0 \leq Y_0 \leq X_0$ és $0 \leq Y_1 \leq X_1$. Ekkor az X_0 elem definíciója szerint $0 \leq Y_0 \leq \sum_{i\in I_*} x_i$, és $\mathrm{Card}(I_*) = n$, így az indukciós hipotézis alapján létezik olyan G-ben haladó $(y_i)_{i\in I_*}$

rendszer, hogy $Y_0 = \sum_{i \in I_*} y_i$ és minden $i \in I_*$ esetén $0 \leq y_i \leq x_i$. Legyen $y_{i_*} := Y_1$. Ekkor $(y_i)_{i \in I}$ olyan G-ben haladó rendszer, hogy $y = Y_0 + Y_1 = \sum_{i \in I_*} y_i + y_{i_*} = \sum_{i \in I} y_i$, és minden $i \in I$ esetén, ha $i \neq i_*$, akkor $0 \leq y_i \leq x_i$, valamint $0 \leq y_{i_*} = Y_1 \leq X_1 = x_{i_*}$. Ez azt jelenti, hogy $(y_i)_{i \in I}$ olyan G-ben haladó rendszer, amelynek a létezését állítottuk.

b) Az I halmaz számossága szerinti teljes indukcióval bizonyítunk. Az állítás triviálisan igaz $\mathrm{Card}(I) = 1$ esetén. Megmutatjuk, hogy akkor is igaz, ha $I = \{0, 1\}$. (Erre szükség lesz az indukciós lépés megtételénél.)

A hipotézis szerint $x_0, x_1 \in G_+$ és $y \in G$ olyan, hogy $|y| \leq x_0 + x_1$. Vezessük be az

$$u := x_0 + (x_0 \wedge (x_1 - y)) \tag{$**$}$$

elemet. Meg fogjuk mutatni, hogy $y_0 := x_0 - u$ és $y_1 := y - y_0$ olyan elemek G-ben, amelyek létezését állítjuk, vagyis $y = y_0 + y_1$ (ami a definíció szerint triviális), valamint $|y_0| \leq x_0$ és $|y_\mathbf{1}| \leq x_1$.

Ehhez először megjegyezzük, hogy $0 \leq u$, mert

– mivel $0 \leq x_0$, így $-x_0 \leq 0$, tehát $-x_0 \leq 0 \leq x_0$, és

– mivel $y \leq |y| \leq x_0 + x_1$, így $-x_0 \leq x_1 - y$,

tehát $-x_0$ alsó korlátja az $\{x_0, x_1 - y\}$ halmaznak, ezért $-x_0 \leq x_0 \wedge (x_1 - y)$, következésképpen $0 \leq x_0 + (x_0 \wedge (x_1 - y)) = u$.

A $(**)$ definíció szerint nyilvánvaló, hogy $-y_0 = -(x_0 - u) = u - x_0 = x_0 \wedge (x_1 - y) \leq x_0$, ugyanakkor $0 \leq u$ miatt $y_0 = x_0 - u \leq x_0$, tehát x_0 felső korlátja a $\{-y_0, y_0\}$ halmaznak, vagyis $|y_0| = y_0 \vee (-y_0) \leq x_0$.

A definíciók szerint $y_1 = y - y_0 = y - (x_0 - u) = (y - x_0) + u = (y - x_0) + (x_0 + (x_0 \wedge (x_1 - y))) = y + (x_0 \wedge (x_1 - y))$. Mivel $x_0 \wedge (x_1 - y) \leq x_1 - y$, ebből következik, hogy $y_1 = y + (x_0 \wedge (x_1 - y)) \leq y + (x_1 - y) = x_1$. Továbbá,

– mivel $-y \leq |y| \leq x_0 + x_1$, így $-(y + x_1) = -y - x_1 \leq x_0$ és

– mivel $0 \leq x_1$, így $-y \leq x_1 - y$, vagyis $-(y + x_1) = -y - x_1 \leq -y \leq x_1 - y$,

tehát $-(y + x_1)$ alsó korlátja a $\{x_0, x_1 - y\}$ halmaznak, így $-y - x_1 = -(y + x_1) \leq (x_0 \wedge (x_1 - y))$, vagyis $-(x_0 \wedge (x_1 - y)) \leq y + x_1$, amiből következik, hogy $-y_1 = -y - (x_0 \wedge (x_1 - y)) \leq -y + (y + x_1) = x_1$. Tehát x_1 felső korlátja az $\{y_1, -y_1\}$ halmaznak, így $|y_1| \leq x_1$. Ezzel igazoltuk az állítást $I = \{0, 1\}$ esetén.

Tegyük most fel, hogy az állítás igaz minden olyan I véges indexhalmazra, amelyre $\mathrm{Card}(I) = n$, ahol $n \in \mathbb{N}$ és $n \geq 2$. Legyen $y \in G$ és $(x_i)_{i \in I}$ olyan G_+-ban haladó rendszer, amelyre $\mathrm{Card}(I) = n + 1$ és $|y| \leq \sum_{i \in I} x_i$. Rögzítsünk tetszőlegesen egy $i_* \in I$ indexet, és legyen $I_* := I \setminus \{i_*\}$. Vezessük be az $X_0 := \sum_{i \in I_*} x_i$ és $X_1 := x_{i_*}$ elemeket. Ekkor $X_0, X_1 \in G_+$ olyan elemek, hogy

$$|y| \leq \sum_{i \in I} x_i = \sum_{i \in I_*} x_i + x_{i_*} = X_0 + X_1 = \sum_{i \in \{0,1\}} X_i,$$

és $\mathrm{Card}(\{0, 1\}) = 2$, így az előzőek szerint léteznek olyan $Y_0, Y_1 \in G$ elemek, hogy $y = Y_0 + Y_1$, valamint $|Y_0| \leq X_0$ és $|Y_1| \leq X_1$. Ekkor az X_0 elem definíciója szerint $|Y_0| \leq \sum_{i \in I_*} x_i$, és $\mathrm{Card}(I_*) = n$, így az indukciós hipotézis alapján létezik olyan G-ben haladó

$(y_i)_{i\in I_*}$ rendszer, hogy $Y_0 = \sum_{i\in I_*} y_i$ és minden $i \in I_*$ esetén $|y_i| \leq x_i$. Legyen $y_{i_*} := Y_1$. Ekkor $(y_i)_{i\in I}$ olyan G-ben haladó rendszer, hogy $y = Y_0 + Y_1 = \sum_{i\in I_*} y_i + y_{i_*} = \sum_{i\in I} y_i$, és minden $i \in I$ esetén, ha $i \neq i_*$, akkor $|y_i| \leq x_i$, valamint $|y_{i_*}| = |Y_1| \leq X_1 = x_{i_*}$. Ez azt jelenti, hogy $(y_i)_{i\in I}$ olyan G-ben haladó rendszer, amelynek a létezését állítottuk. ■

Megjegyzés. Az $(*)$ és $(**)$ definíciók hogyan találhatóak ki?

25.2.10. Állítás. *Ha G hálószerűen rendezett csoport, $x \in G_+$ és $(x_i)_{i\in I}$ véges rendszer G_+-ban, akkor*

$$x \wedge \Big(\sum_{i\in I} x_i\Big) \leq \sum_{i\in I} (x \wedge x_i).$$

Bizonyítás. Az állítás igaz, ha $I = \emptyset$, mert ekkor a $(G, +)$ kommutatív monoidban definíció szerint $\sum_{i\in I} x_i = 0$ és $\sum_{i\in I}(x \wedge x_i) = 0$, ugyanakkor $0 \leq x$ miatt $x \wedge 0 = 0$, tehát ekkor egyenlőségről van szó. Ezért feltehető, hogy I nem üres.

Az I halmaz számossága szerinti teljes indukcióval bizonyítunk. Az állítás triviálisan igaz $\mathrm{Card}(I) = 1$ esetén. Megmutatjuk, hogy akkor is igaz, ha $I = \{0, 1\}$. (Erre szükség lesz az indukciós lépés megtételénél.)

A hipotézis szerint $x, x_0, x_1 \in G_+$. Vezessük be a $y := x \wedge (x_0 + x_1)$ jelölést, tehát azt kell igazolni, hogy $y \leq (x \wedge x_0) + (x \wedge x_1)$.

Világos, hogy $0 \leq x$ miatt $y - x \leq y = x \wedge (x_0 + x_1) \leq x$, továbbá $0 \leq x_0$ miatt $y = x \wedge (x_0 + x_1) \leq x \leq x + x_0$, tehát $y - x \leq x_0$. Ez azt jelenti, hogy $y - x$ alsó korlátja az $\{x, x_0\}$ halmaznak, ezért $y - x \leq x \wedge x_0$, következésképpen $y - (x \wedge x_0) \leq x$.

Világos, hogy $0 \leq x_1$ miatt $y - x_1 \leq y = x \wedge (x_0 + x_1) \leq x$, továbbá $y = x \wedge (x_0 + x_1) \leq x_0 + x_1$, tehát $y - x_1 \leq x_0$. Ez azt jelenti, hogy $y - x_1$ alsó korlátja az $\{x, x_0\}$ halmaznak, ezért $y - x_1 \leq x \wedge x_0$, következésképpen $y - (x \wedge x_0) \leq x_1$.

Ezzel beláttuk, hogy $y - (x \wedge x_0)$ alsó korlátja az $\{x, x_1\}$ halmaznak, következésképpen $y - (x \wedge x_0) \leq x \wedge x_1$, amiből kapjuk a bizonyítandó $x \wedge (x_0 + x_1) = y \leq (x \wedge x_0) + (x \wedge x_1)$ egyenlőtlenséget. Tehát az állítás igaz akkor, ha $I = \{0, 1\}$.

Tegyük most fel, hogy az állítás igaz minden olyan I véges indexhalmazra, amelyre $\mathrm{Card}(I) = n$, ahol $n \in \mathbb{N}$ és $n \geq 2$. Legyen $x \in G_+$ és $(x_i)_{i\in I}$ nem üres véges rendszer G_+-ban, ahol $\mathrm{Card}(I) = n + 1$. Rögzítsünk tetszőlegesen egy $i_* \in I$ indexet, és legyen $I_* := I \setminus \{i_*\}$. Ekkor

$$x \wedge \Big(\sum_{i\in I} x_i\Big) = x \wedge \Big(\Big(\sum_{i\in I_+} x_i\Big) + x_{i_*}\Big) \overset{(1)}{\leq} \Big(x \wedge \Big(\sum_{i\in I_*} x_i\Big)\Big) + (x \wedge x_{i_*}) \overset{(2)}{\leq}$$

$$\overset{(2)}{\leq} \Big(\sum_{i\in I_*} (x \wedge x_i)\Big) + (x \wedge x_{i_*}) = \sum_{i\in I} (x \wedge x_i),$$

ahol

– az $\overset{(1)}{\leq}$ egyenlőtlenségnél felhasználtuk az álltást az $x, \sum_{i\in I_*} x_i, x_{i_*} \in G_+$ elemekre;

– a $\overset{(2)}{\leq}$ egyenlőtlenségnél az indukciós hipotézist alkalmaztuk az I_* indexhalmazra, amelyre $\mathrm{Card}(I_*) = n$. ■

25.3. Rendezett vektorterek és lineáris hálók

25.3.1. Definíció. *Azt mondjuk, hogy az* $(E, +, ., \leq)$ *négyes* **rendezett vektortér**, *ha az* $(E, +, .)$ *hármas valós vektortér és az* $(E, +, \leq)$ *hármas rendezett csoport, és teljesül a következő tulajdonság.*

(EVO) *Minden* $\lambda \in \mathbb{R}_+$ *valós számra és* $x, y \in E$ *vektorra, ha* $x \leq y$, *akkor* $\lambda.x \leq \lambda.y$ *(vagyis minden* $\lambda \in \mathbb{R}_+$ *esetén az* $E \to E$; $x \to \lambda.x$ *leképezés monoton növő a* $\leq$ *rendezés szerint).*

Azt mondjuk, hogy az $(E, +, ., \leq)$ *négyes* **lineáris háló** *vagy* **vektorháló** *vagy* **Riesz-tér**, *ha* $(E, +, ., \leq)$ *olyan rendezett vektortér, hogy* $\leq$ *hálószerű rendezés az* E *halmaz felett.*

A szokásos jelölési konvenciónak megfelelően minden rendezett vektorteret és minden lineáris hálót egyetlen szimbólummal, az alaphalmaz jelével jelölünk.

25.3.2. Állítás. *Legyen* E *lineáris háló.*

a) *Minden* $x \in E_+$ *és* $\lambda, \sigma \in \mathbb{R}$ *esetén, ha* $\lambda \leq \sigma$, *akkor* $\lambda.x \leq \sigma.x$.

b) *Minden* $x \in E$ *és* $\lambda \in \mathbb{R}$ *esetén* $|\lambda.x| \leq |\lambda|.|x|$.

Bizonyítás. a) Ha $\lambda, \sigma \in \mathbb{R}$ olyanok, hogy $\lambda \leq \sigma$, akkor $\sigma - \lambda \in \mathbb{R}_+$, ezért és $x \in E$ és $0 \leq x$ esetén (EVO) szerint $(\sigma - \lambda).0 \leq (\sigma - \lambda).x$, vagyis $0 \leq \sigma.x - \lambda.x$, következésképpen $\lambda.x \leq \sigma.x$.

b) Legyen $x \in E$ és $\lambda \in \mathbb{R}$ olyan, hogy $\lambda \neq 0$. Mivel $\dfrac{\lambda}{|\lambda|} \in \{-1, 1\}$, így nyilvánvalóan $\dfrac{\lambda}{|\lambda|}.x \in \{-x, x\}$, következésképpen $\dfrac{\lambda}{|\lambda|}.x \leq |x|$, amiből (EVO) alkalmazásával kapjuk, hogy $\lambda.x = |\lambda|.\left(\dfrac{\lambda}{|\lambda|}.x\right) \leq |\lambda|.|x|$. Ez minden $x \in E$ és $\lambda \in \mathbb{R}$ esetén igaz, így λ helyett a $-\lambda$ számra felírva kapjuk, hogy $-\lambda.x = (-\lambda).x \leq |-\lambda|.|x| = |\lambda|.|x|$. Ebből következik, hogy minden $x \in E$ és $\lambda \in \mathbb{R}$ esetén $|\lambda.x| \leq |\lambda|.|x|$. ■

25.3.3. Állítás. *Legyen* E *lineáris háló. Ekkor minden* $x, y \in E$ *esetén*

$$x^+ = \frac{1}{2}.(|x| + x), \quad x^- = \frac{1}{2}.(|x| - x);$$
$$x \vee y = \frac{1}{2}.(x + y + |x - y|), \quad x \wedge y = \frac{1}{2}.(x + y - |x - y|).$$

Bizonyítás. A 25.2.4. a) állítás szerint $x = x^+ - x^-$ és $|x| = x^+ + x^-$. Ezeket az egyenlőségeket összeadva (illetve kivonva) és $\frac{1}{2}$-del szorozva kapjuk, hogy $x^+ = \dfrac{1}{2}.(|x|+x)$ (illetve $x^- = \dfrac{1}{2}.(|x| - x)$). A 25.2.4. b) állítás szerint $x \vee y = x + (y - x)^+$ (illetve $x \wedge y = x - (x - y)^+$). Ebből az előzőek és $|y - x| = |x - y|$ alkalmazásával következik, hogy

$$x \vee y = x + \frac{1}{2}.(|y - x| + y - x) = \frac{1}{2}.(x + y + |x - y|),$$

illetve

$$x \wedge y = x - \frac{1}{2}.(|x - y| + x - y) = \frac{1}{2}.(x + y - |x - y|). \blacksquare$$

25.3.4. Állítás. *Ha E rendezett vektortér, akkor a következő állítások ekvivalensek.*

(i) *E lineáris háló.*

(ii) *Minden $x, y \in E$ esetén $x \vee y$ létezik.*

(iii) *Minden $x \in E$ esetén $(-x) \vee 0$ létezik.*

(iv) *Minden $x \in E$ esetén $x \vee 0$ létezik.*

(v) *Minden $x \in E$ esetén $(-x) \vee x$ létezik.*

(vi) *Minden $x, y \in E$ esetén $x \wedge y$ létezik.*

Bizonyítás. (i)$\Rightarrow$(ii) és (ii)$\Rightarrow$(iii) Triviális.

(iii)$\Rightarrow$(iv) Ha (iii) teljesül, akkor minden $x \in E$ esetén $(-(-x)) \vee 0$, vagyis $x \vee 0$ létezik az E rendezett halmazban.

(iv)$\Rightarrow$(v) A (iv) feltétel alapján, minden $x \in E$ esetén az $x^+ := x \vee 0$ jelölést alkalmazzuk. Legyen $x \in E$ rögzítve, és vezessük be az $y := 2.x^+ - x$ elemet. Memgutatjuk, hogy y a $\{-x, x\}$ halmaz szuprémuma. Valóban, $x \leq x^+$ és (EVO) alapján $2.x \leq 2.x^+$, ezért $x \leq 2.x^+ - x = y$, továbbá $0 \leq x^+$, így (EVO) szerint $0 \leq 2.x^+$, ezért $-x \leq 2.x^+ - x = y$. Ez azt jelenti, hogy y felső korlátja a $\{-x, x\}$ halmaznak. Legyen $z \in E$ felső korlátja a $\{-x, x\}$ halmaznak. Mivel $x \leq z$, így $2.x = x + x \leq z + x$, amiből (EVO) alapján $x \leq \frac{1}{2}.(z + x)$ követlezik. Másfelől, $-x \leq z$ miatt $0 \leq z + x$, így (EVO) alapján $0 \leq \frac{1}{2}.(z + x)$. Tehát $\frac{1}{2}.(z + x)$ felső korlátja az $\{x, 0\}$ halmaznak, így $x^+ \leq \frac{1}{2}.(z + x)$, amiből ismét (EVO)-t alkalmazva $2.x^+ \leq z + x$, vagyis $y = 2.x^+ - x \leq z$ adódik. Tehát y a $\{-x, x\}$ halmaz legkisebb felső korlátja.

(v)$\Rightarrow$(vi) Az (v) feltétel alapján minden $x \in E$ esetén az $|x| := (-x) \vee x$ jelölést alkalmazzuk. Legyenek $x, y \in E$ rögzítve, és vezessük be a $z := \frac{1}{2}.(x + y - |x - y|)$ elemet. Megmutatjuk, hogy z az $\{x, y\}$ halmaz legnagyobb alsó korlátja.

A (GO) és (EVO) feltételek alapján fennállnak a következő összefüggések

$$\begin{aligned} z \leq x \;\Leftrightarrow\; \frac{1}{2}.(x + y - |x - y|) \leq x \;\Leftrightarrow\; x + y - |x - y| \leq 2.x = x + x \;\Leftrightarrow \\ \Leftrightarrow\; y - |x - y| \leq x \;\Leftrightarrow\; -(x - y) = y - x \leq |x - y|, \end{aligned}$$

és az ekvivalencia-lánc utolsó tagja definíció szerint igaz, így $z \leq x$. Hasonlóan, (GO) és (EVO) alkalmazásával kapjuk, hogy

$$\begin{aligned} z \leq y \;\Leftrightarrow\; \frac{1}{2}.(x + y - |x - y|) \leq y \;\Leftrightarrow\; \leq x + y - |x - y| \leq 2.y = y + y \;\Leftrightarrow \\ \Leftrightarrow\; x - |x - y| \leq y \;\Leftrightarrow\; x - y \leq |x - y|, \end{aligned}$$

és az ekvivalencia-lánc utolsó tagja definíció szerint igaz, így $z \leq y$. Tehát z alsó korlátja az $\{x, y\}$ halmaznak.

Legyen $z' \in E$ alsó korlátja az $\{x, y\}$ halmaznak. Ekkor (GO) és (EVO) alapján fennállnak a következő összefüggések

$$\begin{aligned} z' \leq z \;\Leftrightarrow\; z' \leq \frac{1}{2}.(x + y - |x - y|) \;\Leftrightarrow\; 2.z' \leq x + y - |x - y| \;\Leftrightarrow \\ \Leftrightarrow\; |x - y| \leq x + y - 2.z' = x + y - z' - z' = (x - z') + (y - z'). \end{aligned} \tag{$*$}$$

Mivel $z' \leq y$, vagyis $0 \leq y - z'$, így az egyenlőtlenségek összeadásának szabálya szerint $0 \leq (y - z') + (y - z')$, amiből (GO) alkalmazásával kapjuk, hogy

$$x - y \leq (x - y) + (y - z') + (y - z') = (x - z') + (y - z').$$

Mivel $z' \leq x$, vagyis $0 \leq x - z'$, így az egyenlőtlenségek összeadásának szabálya szerint $0 \leq (x - z') + (x - z')$, amiből (GO) alkalmazásával kapjuk, hogy

$$-(x - y) = y - x \leq (y - x) + (x - z') + (x - z') = (x - z') + (y - z').$$

Ezért $|x - y| \leq (x - z') + (y - z')$, tehát az $(*)$ ekvivalencia-lánc utolsó tagja igaz, így $z' \leq z$ teljesül. Ez azt jelenti, hogy z az $\{x, y\}$ halmaz legnagyobb alsó korlátja.

(vi)⇒(i) Ha $x, y \in E$, akkor (vi)-ból következik, hogy $(-x) \wedge (-y)$ létezik E-ben, ezért 25.1.4. a) szerint $-((-x) \wedge (-y))$ az $\{x, y\}$ halmaz szuprémuma, vagyis $x \vee y$ létezik. Ezért E rendezése hálószerű. ■

25.4. Teljes lineáris hálók

25.4.1. Definíció. *Azt mondjuk, hogy E* **teljes lineáris háló***, ha E olyan lineáris háló, hogy E minden nem üres felülről korlátos részhalmazának létezik szuprémuma és E minden nem üres alulról korlátos részhalmazának létezik infimuma.*

25.4.2. Állítás. *Legyen E lineáris háló. A következő állítások ekvivalensek.*

(i) E teljes lineáris háló.

(ii) Az E minden nem üres, alulról korlátos részhalmazának létezik infimuma.

(iii) Minden E_+-ban haladó, nem üres lefelé irányított rendszernek létezik infimuma.

(iv) Minden E_+-ban haladó, nem üres, felülről korlátos, felfelé irányított rendszernek létezik szuprémuma.

(v) Az E minden nem üres, felülről korlátos részhalmazának létezik szuprémuma.

Bizonyítás. (i)⇒(ii) Ha $X \subseteq E$ nem üres, alulról korlátos halmaz, és $y \in E$ alsó korlátja X-nek, akkor minden $x \in X$ esetén $y \leq x$, így $-x \leq -y$, tehát $-y$ felső korlátja a $-X := \{-x | x \in X\}$ nem üres halmaznak, következésképpen (i)-ből kapjuk, hogy $\sup(-X)$ létezik E-ben, amiből 25.1.4. b) alapján adódik, hogy $-\sup(-X)$ az X halmaz infimuma E-ben.

(ii)⇒(iii) Triviális.

(iii)⇒(iv) Legyen $(x_i)_{i \in I}$ E_+-ban haladó nem üres, felülről korlátos, felfelé irányított rendszer. Legyen $y \in E$ felső korlátja az $(x_i)_{i \in I}$ rendszernek. Ekkor az $(y - x_i)_{i \in I}$ rendszer E_+-ban halad, nem üres, és lefelé irányított, ezért (iii) alapján létezik a $z := \inf\limits_{i \in I}(y - x_i)$ infimum. Memutatjuk, hogy ekkor $y - z$ az $(x_i)_{i \in I}$ rendszer szuprémuma. Valóban, minden $i \in I$ esetén $z \leq y - x_i$, ezért $x_i \leq y - z$, tehát $y - z$ felső korlátja az $(x_i)_{i \in I}$ rendszernek. Ha $x \in E$ tetszőleges felső korlátja az $(x_i)_{i \in I}$ rendszernek, akkor minden $i \in I$ esetén $x_i \leq x$, tehát $-x \leq -x_i$, ezért $y - x \leq y - x_i$, amiből $y - x \leq z$ következik, hiszen z az $(y - x_i)_{i \in I}$ rendszer legnagyobb alsó korlátja. Ezért $y - z \leq x$, tehát $y - z$ az $(x_i)_{i \in I}$ rendszer legkisebb felső korlátja.

(iv)⇒(v) Legyen $X \subseteq E$ nem üres, felülről korlátos halmaz. Rögzítsünk egy $x_* \in X$ elemet, és készítsük el az

$$X_* := \{ \sup(H) - x_* \mid (H \subseteq X) \wedge (H \text{ véges}) \wedge (x_* \in H) \}$$

halmazt. Ekkor $X_* \subseteq E_+$ és ha $z \in E$ felső korlátja X-nek, akkor $z - x_*$ felső korlátja X_*-nak. Továbbá, X_* nyilvánvalóan felfelé irányított halmaz, mert ha $H, H' \subseteq X$ olyan véges halmazok, hogy $x_* \in H$ és $x_* \in H'$, akkor $H \cup H'$ olyan véges réeszhalmaza X-nek, hogy $x_* \in H \cup H'$ és $\sup(H) - x_* \leq \sup(H \cup H') - x_*$, és $\sup(H') - x_* \leq \sup(H \cup H') - x_*$. Ezért (iv) alapján létezik az $y := \sup(X_*)$ szuprémum. Megmutatjuk, hogy $y + x_*$ az X halmaz szuprémuma.

Legyen $x \in X$ tetszőleges. Ekkor $\{x, x_*\}$ olyan véges részhalmaza X-nek, amelynek x_* eleme, így $x \vee x_* - x_* \in X_*$, tehát $x \vee x_* - x_* \leq y$, következésképpen $x \leq x \vee x_* \leq y + x_*$. Ez azt jelenti, hogy $y + x_*$ felső korlátja X-nek.

Legyen $z \in E$ felső korlátja X-nek. Ekkor minden $H \subseteq X$ nem üres, véges halmazra $\sup(H) \leq z$, ezért $z - x_*$ felső korlátja X_*-nak. Mivel $y = \sup(X_*)$, így ekkor $y \leq z - x_*$, tehát $y + x_* \leq z$. Ezzel beláttuk, hogy $y + x_*$ a legkisebb felső korlátja X-nek.

(v)$\Rightarrow$(i) Ha $X \subseteq E$ nem üres, felülről korlátos halmaz, és $y \in E$ felső korlátja X-nek, akkor minden $x \in X$ esetén $x \leq y$, így $-y \leq -x$, tehát $-y$ alsó korlátja a $-X := \{-x | x \in X\}$ nem üres halmaznak, következésképpen (v)-ből kapjuk, hogy $\inf(-X)$ létezik E-ben, amiből 25.1.4. a) alapján adódik, hogy $-\inf(-X)$ az X halmaz szuprémuma E-ben. Ezért (v)-ből következik, hogy E minden nem üres felülről korlátos részhalmazának létezik szuprémuma és E minden nem üres alulról korlátos részhalmazának létezik infimuma. ■

25.5. Sávok és a Riesz-féle felbontási tétel

25.5.1. Definíció. *Legyen E lineáris háló. Azt mondjuk, hogy az $x \in E$ és $y \in E$ elemek* **függetlenek**, *ha $|x| \wedge |y| = 0$. Továbbá, minden $H \subseteq E$ halmazra $H^\perp$ jelöli a H halmaz minden elemétől független elemek részhalmazát E-ben, vagyis*

$$H^\perp := \{x \in E \mid (\forall y \in H)\ |x| \wedge |y| = 0\}.$$

Ha $H \subseteq E$, akkor a $H^{\perp\perp} := (H^\perp)^\perp$ jelölést alkalmazzuk.

Természetesen a $H^\perp$ jelöléssel óvatosan kell bánni, ha E egyszerre lineáris háló és valós prehilbert-tér, hiszen akkor ennek a jelnek két különböző értelme van.

Nyilvánvaló, hogy ha E lineáris háló, akkor $A \subseteq B \subseteq E$ esetén $B^\perp \subseteq A^\perp$, továbbá minden $H \subseteq E$ halmazra $H \subseteq (H^\perp)^\perp = H^{\perp\perp}$. Ebből azonnal következik, hogy ha E lineáris háló, akkor minden $H \subseteq E$ halmazra $H^\perp = ((H^\perp)^\perp)^\perp$, hiszen $H \subseteq H^{\perp\perp}$ miatt $\left(H^{\perp\perp}\right)^\perp \subseteq H^\perp$, ugyanakkor $H^\perp \subseteq \left(H^\perp\right)^{\perp\perp}$, és természetesen

$$\left(H^{\perp\perp}\right)^\perp = ((H^\perp)^\perp)^\perp = \left(H^\perp\right)^{\perp\perp}.$$

25.5.2. Definíció. *Azt mondjuk, hogy az E teljes lineáris háló M lineáris altere* **sáv** *E-ben, ha*

– *minden $x \in M$ és $y \in E$ esetén, ha $|y| \leq x$, akkor $y \in M$, és*

– *minden $B \subseteq M$ nem üres, E-ben felülről korlátos halmazra $\sup(B) \in M$.*

25.5.3. Állítás. *Ha E teljes lineáris háló, akkor minden $H \subseteq E$ halmazra $H^\perp$ sáv.*

Bizonyítás. Legyenek $x, y \in H^\perp$ és $z \in H$. Ekkor $|x+y| \leq |x|+|y|$ miatt $0 \leq |x+y| \wedge |z| \leq (|x| + |y|) \wedge |z| \leq (|x| \wedge |z|) + (|y| \wedge |z|) = 0$, ahol felhasználtuk a 25.2.10. állításban igazolt egyenlőtlenséget. Ez azt jelenti, hogy $H^\perp + H^\perp \subseteq H^\perp$.

Legyenek $x \in H^\perp$, $\lambda \in \mathbb{R}$ és $y \in H$. A 25.3.2. b) állítás szerint $|\lambda.x| \leq |\lambda|.|x|$, és ha $n \in \mathbb{N}$ olyan, hogy $|\lambda| \leq n$, akkor 25.3.2. a) szerint $|\lambda|.|x| \leq n.|x|$. Ebből következik, hogy ha $n \in \mathbb{N}$ olyan, hogy $|\lambda| \leq n$, akkor $|\lambda.x| \leq n.|x|$, ugyanakkor 25.2.10. alapján

$$|y| \wedge |\lambda.x| \leq |y| \wedge (n.|x|) = |y| \wedge \Big(\sum_{i\in n} |x|\Big) \leq \sum_{i\in n}(|y| \wedge |x|) = n.(|y| \wedge |x|) = 0,$$

tehát $\lambda.x \in H^\perp$. Ez azt jelenti, hogy $\mathbb{R}.H^\perp \subseteq H^\perp$. Ezzel beláttuk, hogy $H^\perp$ lineáris altere E-nek.

Ha $x \in H^\perp$ és $y \in E$ olyan, hogy $|y| \leq |x|$, akkor minden $z \in H$ esetén $0 \leq |y| \wedge |z| \leq |x| \wedge |z| = 0$, tehát $y \in H^\perp$.

Végül, legyen $B \subseteq H^\perp$ nem üres, E-ben felülről korlátos halmaz és $x := \sup(B)$. Azt kell igazolni, hogy $x \in H^\perp$, vagyis minden $y \in H$ esetén $|x| \wedge |y| = 0$. Ehhez legyen $y \in H$ tetszőleges. Mivel a hálószerűen rendezett csoportokra vonatkozó disztributivitás formula (25.2.6.) szerint

$$|x| \wedge |y| = (x \vee (-x)) \wedge |y| = (x \wedge |y|) \vee ((-x) \wedge |y|),$$

így az $|x| \wedge |y| = 0$ egyenlőség bizonyításához elegendő az $x \wedge |y| \leq 0$ és $(-x) \wedge |y| \leq 0$ egyenlőtlenségeket igazolni. A 25.2.6. állítás alkalmazásával

$$x \wedge |y| = \Big(\bigvee_{b\in B} b\Big) \wedge |y| = \bigvee_{b\in B} (b \wedge |y|) \leq \bigvee_{b\in B} (|b| \wedge |y|) \leq 0,$$

mert minden $b \in B$ esetén $b \in H^\perp$ és $y \in H$, tehát $|b| \wedge |y| = 0$. Továbbá, $B \neq \emptyset$ alapján rögzítve egy $b_* \in B$ elemet, 25.1.4. b) alkalmazásával kapjuk, hogy

$$(-x) \wedge |y| = \Big(-\bigvee_{b\in B} b\Big) \wedge |y| = \Big(\bigwedge_{b\in B}(-b)\Big) \wedge |y| = \bigwedge_{b\in B}((-b) \wedge |y|) \leq (-b_*) \wedge |y| \leq |b_*| \wedge |y| = 0,$$

mert $b_* \in H^\perp$ és $y \in H$, tehát $|b_*| \wedge |y| = 0$. ■

25.5.4. Lemma. *Legyen E teljes lineáris háló és $H \subseteq E_+$ olyan nem üres halmaz, hogy $H + H \subseteq H$ és minden $x \in H$ esetén $[0, x] \subseteq H$. Legyen $\overline{H}$ a H halmaz nem üres, E-ben felülről korlátos részhalmazai szuprémumainak halmaza. Ekkor minden $x \in E_+$ esetén $H \cap [0, x]$ nem üres, felülről korlátos halmaz E-ben, és az $y := \sup(H \cap [0, x])$ elemre $y \in \overline{H}$ és $x - y \in H^\perp$ teljesül.*

Bizonyítás. Legyen $x \in E_+$. Világos, hogy $0 \in H \cap [0, x]$, és x felső korlátja $H \cap [0, x]$-nek, tehát $y := \sup(H \cap [0, x]) \in \overline{H}$ és $y \leq x$. Az $x - y \in H^\perp$ összefüggés bizonyításához legyen $z \in H$. Mivel $0 \leq z$ és $0 \leq x - y$, így azt kell igazolni, hogy $u := z \wedge (x - y) = 0$. A hipotézis szerint $u \in [0, z] \subseteq H$, tehát $u \in H$, továbbá $0 \leq u + y \leq x$. De 25.1.4. c) alapján $u + y = u + \sup(H \cap [0, x]) = \sup(u + (H \cap [0, x]))$, és minden $v \in H \cap [0, x]$ esetén $u + v \in H + H \subseteq H$ és $u + v \leq u + y \leq x$, ezért $u + v \in H \cap [0, x]$, amiből y definíciója szerint következik, hogy $u + y = \sup(u + (H \cap [0, x])) \leq y$, vagyis $u \leq 0$. Mivel $0 \leq u$, ebből kapjuk, hogy $u = 0$. ■

25.5.5. Tétel. (**Riesz-féle felbontási tétel.**) *Ha E teljes lineáris háló, akkor minden $M \subseteq E$ sávra*

$$(M^\perp)^\perp = M, \qquad M \oplus M^\perp = E, \qquad (M \cap E_+) + (M^\perp \cap E_+) = E_+,$$

és minden $x \in E_+$ esetén, ha $x_M \in M$ és $x_{M^\perp} \in M^\perp$ azok a vektorok, amelyekre fennáll az $x = x_M + x_{M^\perp}$ egyenlőség, akkor $x_M = \sup(M \cap [0, x])$.

Bizonyítás. Legen $M \subseteq E$ sáv. A 25.5.4. lemmát alkalmazva a $H := M \cap E_+$ választással kapjuk, hogy $x \in E_+$ esetén $y := \sup(M \cap [0, x]) \in \overline{M \cap E_+} \subseteq M$ és $x - y \in M^\perp$, tehát $x = y + (x - y) \in M + M^\perp$. Ez azt jelenti, hogy $E_+ \subseteq (M \cap E_+) + (M^\perp \cap E_+) \subseteq M + M^\perp$, ezért $E = E_+ - E_+ \subseteq M + M^\perp$, hiszen $M + M^\perp$ lineáris altere E-nek. Tehát $E = M + M^\perp$, és ha $x \in M \cap M^\perp$, akkor $|x| = |x| \wedge |x| = 0$, tehát $x = 0$, ezért $M \cap M^\perp = \{0\}$. Ezzel igazoltuk azt, hogy $E = M \oplus M^\perp$ és $(M \cap E_+) + (M^\perp \cap E_+) = E_+$, továbbá azt is beláttuk, hogy ha $x \in E_+$, valamint $x_M \in M$ és $x_{M^\perp} \in M^\perp$ azok a vektorok, amelyekre $x = x_M + x_{M^\perp}$, akkor szükségképpen $x_M = \sup(M \cap [0, x])$.

Legyen $x \in (M^\perp)^\perp$. Mivel $E = M + M^\perp$, így léteznek olyan $y \in M$ és $z \in M^\perp$, hogy $x = y + z$. Ekkor $M \subseteq (M^\perp)^\perp$ miatt $x - y \in (M^\perp)^\perp$, ugyanakkor $z \in M^\perp$, így $x - y = z \in M^\perp \cap (M^\perp)^\perp = \{0\}$, vagyis $x = y \in M$. Ez azt jelenti, hogy $(M^\perp)^\perp \subseteq M$ is teljesül, tehát $(M^\perp)^\perp = M$. ■

25.5.6. Következmény. *Ha E teljes lineáris háló, akkor minden $H \subseteq E$ halmazra $H^{\perp\perp}$ megegyezik a H halmazt tartalmazó, tartalmazás tekintetében legkisebb E-beli sávval.*

Bizonyítás. Ha $M \subseteq E$ olyan sáv, hogy $H \subseteq M$, akkor $M^\perp \subseteq H^\perp$, ezért $H^{\perp\perp} = (H^\perp)^\perp \subseteq (M^\perp)^\perp$ és a Riesz-féle felbontási tétel szerint $M^{\perp\perp} = M$, ezért $H^{\perp\perp} \subseteq M$. Tehát $H^{\perp\perp}$ olyan sáv E-ben (25.5.3.), amely tartalmazza H-t, valamint részhalmaza minden olyan E-beli sávnak, amely tartalmazza a H halmazt. ■

25.5.7. Következmény. *Ha E teljes lineáris háló, akkor és $M \subseteq E$, akkor a következő állízások ekvivalensek.*

(i) *M sáv.*

(ii) *$M = M^{\perp\perp}$ sáv.*

(iii) *Létezik olyan $H \subseteq E$ halmaz, hogy $M = H^\perp$.*

Bizonyítás. (i)⇒(ii) A Riesz-féle felbontási tételből következik.

(ii)⇒(iii) Triviális.

(iii)⇒(i) A 25.5.3. állításból következik. ■

25.5.8. Állítás. *Legyen E teljes lineáris háló és $H \subseteq E$ tetszőleges. Vezessük be a*

$$H_* := \left\{ x \in E_+ \;\middle|\; (\exists Z \subseteq H)\Big((Z \text{ "véges"}) \wedge \Big(x \leq \sum_{z \in Z} |z|\Big)\Big) \right\},$$

$$H_{**} := \{\, \sup(B) \mid (B \subseteq H_*) \wedge (B \neq \emptyset) \wedge (B \text{ felülről korlátos } E\text{-ben}) \,\}$$

halmazokat. Ekkor

$$H^{\perp\perp} \cap E_+ = H_{**}.$$

Bizonyítás. Mivel $H^{\perp\perp}$ olyan sáv, amelyre $H \subseteq H^{\perp\perp}$, így nyilvánvaló, hogy $H_* \subseteq H^{\perp\perp}$, ezért $H_{**} \subseteq H^{\perp\perp}$ is teljesül. Ebből következik, hogy

$$H_{**} \subseteq H^{\perp\perp} \cap E_+. \tag{1}$$

Most megmutatjuk, hogy

$$H_*^\perp \subseteq H^\perp. \tag{2}$$

Ehhez legyen $y \in H_*^\perp$ és $x \in H$. Ekkor $0 \leq x^+ \leq |x|$, így $x^+ \in H_*$, és hasonlóan, $0 \leq x^- \leq |x|$, így $x^- \in H_*$. Ezért $|y| \wedge x^+ = 0$ és $|y| \wedge x^- = 0$, így 25.2.4. a) és 25.2.10. alapján $0 \leq |y| \wedge |x| = |y| \wedge (x^+ + x^-) \leq (|y| \wedge x^+) + (|y| \wedge x^-) = 0$, következésképpen

$|y| \wedge |x| = 0$.

Megjegyezzük, hogy $0 \in H_*$, még akkor is, ha $H = \emptyset$, hiszen az üres rendszer összege kommutatív monoidban egyenlő a neutrális elememmel, vagyis 0-val. Továbbá, nyilvánvaló, hogy $H_* + H_* \subseteq H_*$ és minden $x \in E$ és $y \in H_*$ esetén, ha $0 \leq x \leq y$, akkor $x \in H_*$. Ezért alkalmazható a 25.5.4. lemma a $H_* \subseteq E_+$ halmazra. Tehát, ha $x \in H^{\perp\perp} \cap E_+$, akkor léteznek olyan $y \in H_{**}$ és $z \in H_*^{\perp}$, hogy $x = y + z$. Ekkor $x - y \in H^{\perp\perp} - H_{**} \subseteq H^{\perp\perp} - H^{\perp\perp} \subseteq H^{\perp\perp}$, ugyanakkor (2) alapján $z \in H_*^{\perp} \subseteq H^{\perp}$, ezért $x - y = z \in H^{\perp\perp} \cap H^{\perp} = \{0\}$, vagyis $x = y \in H_{**}$. Ez azt jelenti, hogy $H^{\perp\perp} \cap E_+ \subseteq H_{**}$, ami az (1) összefüggéssel együtt az állítást bizonyítja. ■

25.5.9. Következmény. *Legyen E teljes lineáris háló, $y \in E$, és $M := (\{y\}^{\perp})^{\perp}$. Ha $x \in E_+$, valamint $x_M \in M$ és $x_{M^\perp} \in M^{\perp}$ azok a vektorok, amelyekre $x = x_M + x_{M^\perp}$, akkor*

$$x_M = \bigvee_{n\in\mathbb{N}} (x \wedge (n.|y|)),$$
$$x_{M^\perp} = \bigwedge_{n\in\mathbb{N}} (x - n.|y|)^+.$$

Bizonyítás. Az előző állítást alkalmazzuk a $H := \{y\}$ halmazra. Ekkor $H_* = \{x' \in E_+ | (\exists n \in \mathbb{N})\ x' \leq n.|y|\}$, tehát ha $x \in E_+$ és $x_M \in M$ és $x_{M^\perp} \in M^\perp$ azok a vektorok, amelyekre $x = x_M + x_{M^\perp}$, akkor $x_M \in M \cap E_+ = H^{\perp\perp} \cap E_+$, így az előző állítás alapján $x_M \in H_{**}$, vagyis létezik olyan $B \subseteq H_*$ nem üres, E-ben felülről korlátos halmaz, hogy $x_M = \sup(B)$. Tehát, ha $b \in B$, akkor van olyan $m \in \mathbb{N}$, hogy $b \leq m.|y|$, és $b \leq x_M \leq x$ miatt $b \leq x \wedge (m.|y|) \leq \bigvee_{n\in\mathbb{N}} (x \wedge (n.|y|))$, következésképpen $x_M \leq \bigvee_{n\in\mathbb{N}} (x \wedge (n.|y|))$. Másfelől, a Riesz-féle felbontási tétel szerint $x_M = \sup(M \cap [0, x])$, és világos, hogy minden $n \in \mathbb{N}$ esetén $x \wedge (n.|y|) \in M \cap [0, x]$, ezért $\bigvee_{n\in\mathbb{N}} (x \wedge (n.|y|)) \leq x_M$. Ezért $x_M = \bigvee_{n\in\mathbb{N}} (x \wedge (n.|y|))$, amiből következik, hogy

$$x_{M^\perp} = x - x_M = x - \bigvee_{n\in\mathbb{N}} (x \wedge (n.|y|)) \overset{(1)}{=} x + \bigwedge_{n\in\mathbb{N}} (-(x \wedge (n.|y|))) \overset{(2)}{=}$$
$$\overset{(2)}{=} \bigwedge_{n\in\mathbb{N}} (x - (x \wedge (n.|y|))) \overset{(3)}{=} \bigwedge_{n\in\mathbb{N}} (x - n.|y|)^+,$$

ahol

– az $\overset{(1)}{=}$ egyenlőségnél a 25.1.4. a) állítást,

– a $\overset{(2)}{=}$ egyenlőségnél a 25.1.4. d) állítást, és

– a $\overset{(3)}{=}$ egyenlőségnél a 25.2.4. b) állítást alkalmaztuk. ■

25.6. Relatív korlátos lineáris funkcionálok

25.6.1. Tétel. *Legyen E lineáris háló és $\mu_0 : E_+ \to \mathbb{R}_+$ függvény. Akkor és csak akkor létezik olyan E feletti lineáris funkcionál, amely kiterjesztése μ_0-nak, ha μ_0 additív, vagyis minden $x, y \in E_+$ esetén $\mu_0(x + y) = \mu_0(x) + \mu_0(y)$. Ha μ_0 additív, akkor egyetlen olyan E feletti lineáris funkcionál létezik, amely μ_0-nak kiterjesztése (és természetesen ez a kiterjesztés pozitív funkcionál).*

Bizonyítás. A szükségesség nyilvánvaló, tehát csak az elégségességet kell bizonyítani. Tehát feltesszük, hogy a $\mu_0 : E_+ \to \mathbb{R}_+$ függvény additív.

Először megjegyezzük, hogy μ_0 additivitásából és pozitivitásából következik, hogy $\mu_0(y) = \mu_0(x + (y - x)) = \mu_0(x) + \mu_0(y - x) \geq \mu_0(x)$, vagyis μ_0 *monoton növő*. Megmutatjuk, hogy μ_0 *pozitív* $\mathbb{R}$-*homogén*, vagyis minden $x \in E_+$ és $c \in \mathbb{R}_+$ esetén $\mu_0(c.x) = c\mu_0(c)$.

Ha $x \in E_+$, akkor teljes indukcióval könnyen belátható, hogy minden $n \in \mathbb{N}$ esetén $\mu_0(n.x) = n\mu_0(x)$, hiszen ez $n = 0$ esetén triviálisan igaz, és ha igaz az $n \in \mathbb{N}$ természetes számra, akkor μ_0 additivitása folytán $\mu_0((n + 1).x) = \mu_0(n.x + x) = \mu_0(n.x) + \mu_0(x) = n\mu_0(x)+\mu_0(x) = (n+1).\mu_0(x)$, tehát az állítás igaz az $n+1$ természetes számra is. Ebből következik, hogy ha $x \in E_+$ és $n \in \mathbb{N}^*$, akkor $\mu_0(x) = \mu_0\left(n.\left(1/n\right).x\right) = n\mu_0\left(\left(1/n\right).x\right)$, ezért $\left(1/n\right).\mu_0(x) = \mu_0\left(\left(1/n\right).x\right)$. Ebből kapjuk, hogy minden $r \in \mathbb{Q}_+$ számra és $x \in E_+$ vektorra $\mu_0(r.x) = r\mu_0(x)$, hiszen léteznek ilyen $m \in \mathbb{N}$ és $n \in \mathbb{N}^*$ számok, hogy $r = m/n$, és ekkor $\mu_0(r.x) = \mu_0\left(m.\left(1/n\right).x\right) = m\mu_0\left(\left(1/n\right).x\right) = m\left(1/n\right)\mu_0(x) = r\mu_0(x)$. Ez azt jelenti, hogy a μ_0 leképezés pozitív $\mathbb{Q}$-homogén. Legyen $c \in \mathbb{R}_+^*$, és vegyünk olyan $\mathbb{Q}_+$-ban haladó monoton növő $(s_n)_{n\in\mathbb{N}}$ sorozatot, hogy $\sup\limits_{n\in\mathbb{N}} s_n = c$, és vegyünk olyan $\mathbb{Q}_+$-ban haladó monoton fogyó $(d_n)_{n\in\mathbb{N}}$ sorozatot, hogy $\inf\limits_{n\in\mathbb{N}} d_n = c$. Ekkor minden $n \in \mathbb{N}$ esetén $s_n \leq c \leq d_n$, így $x \in E$ esetén $s_n.x \leq c.x \leq d_n.x$, tehát ha $x \in E_+$, akkor μ_0 monoton növése és pozitív $\mathbb{Q}$-homogenitása miatt $s_n\mu_0(x) = \mu_0(s_n.x) \leq \mu_0(c.x) \leq \mu_0(d_n.x) = d_n\mu(x)$. Ha $x \in E_+$ olyan, hogy $\mu_0(x) = 0$, akkor ebből $\mu_0(c.x) = 0 = c.\mu_0(x)$ következik. Ha $x \in E_+$ olyan, hogy $\mu_0(x) > 0$, akkor ebből következik, hogy minden $n \in \mathbb{N}$ esetén $s_n \leq \dfrac{\mu_0(c.x)}{\mu_0(x)} \leq d_n$, ezért $c = \sup\limits_{n\in\mathbb{N}} s_n \leq \dfrac{\mu_0(c.x)}{\mu_0(x)} \leq \inf\limits_{n\in\mathbb{N}} d_n = c$, tehát $\mu_0(c.x) = c.\mu_0(x)$. Ezzel beláttuk, hogy μ_0 pozitív $\mathbb{R}$-homogén.

Legyen $x \in E$ rögzítve. Mivel $E = E_+ - E_+$, így léteznek olyan $x_0, x_1 \in E_+$ elemek, hogy $x = x_0 - x_1$, így jól értelmezett a $\mu_0(x_0) - \mu_0(x_1)$ valós szám. Ha $= x_0', x_1' \in E_+$ szintén olyanok, hogy $x = x_0' - x_1'$, akkor $x_0 + x_1' = x_0' + x_1$, ezért μ_0 additivitása folytán $\mu_0(x)_0 + \mu_0(x_1') = \mu_0(x_0') + \mu_0(x_1)$, vagyis $\mu_0(x_0) - \mu_0(x_1) = \mu_0(x_0') - \mu_0(x_1')$. Ez azt jelenti, hogy egyértelműen létezik az a $\mu : E \to \mathbb{R}$ függvény, amelyre teljesül az, hogy minden $x_0, x_1 \in E_+$ esetén $\mu(x_0 - x_1) = \mu_0(x_0) - \mu_0(x_1)$. Világos, hogy ez a függvény μ_0 kiterjesztése, hiszen $x \in E_+$ esetén $\mu(x) = \mu(x - 0) = \mu_0(x) - \mu_0(0) = \mu_0(x)$. Meg fogjuk mutatni, hogy μ lineáris funkcionál E felett.

A $\mu : E \to \mathbb{R}$ leképezés additivitásának bizonyításához legyenek $x, y \in E$ és vegyünk olyan $x_0, x_1, y_0, y_1 \in E_+$ elemeket, hogy $x = x_0 - x_1$ és $y = y_0 - y_1$. Ekkor $x+y = (x_0+y_0)-(x_1+y_1)$ és $x_0+y_0, x_1+y_1 \in E_+$, ezért μ definíciója és μ_0 additivitása miatt

$$\begin{aligned}\mu(x + y) &= \mu_0(x_0 + y_0) - \mu_0(x_1 + y_1) = (\mu_0(x_0) + \mu_0(y_0)) - (\mu_0(x_1) + \mu_0(y_1)) = \\ &= (\mu_0(x_0) - \mu_0(x_1)) + (\mu_0(y_0) - \mu_0(y_1)) = \mu(x) + \mu(y),\end{aligned}$$

tehát μ additív. A $\mu : E \to \mathbb{R}$ leképezés $\mathbb{R}$-homogenitásának bizonyításához legyen $x \in E$ és $c \in \mathbb{R}$. Rögzítsünk olyan $x_0, x_1 \in E_+$ elemeket, hogy $x = x_0 - x_1$. Két eset lehetséges.

– Tegyük fel, hogy $c \geq 0$. Ekkor $c.x = c : x_0 - c.x_1$ és $c.x_0, c.x_1 \in E_+$, így μ definíciója és μ_0 pozitív $\mathbb{R}$-homogenitása miatt

$$\mu(c.x) = \mu_0(c.x_0) - \mu_0(c.x_1) = c\mu_0(x_0) - c\mu_0(x_1) = c(\mu_0(x_0) - \mu_0(x_1)) = c\mu(x).$$

– Tegyük fel, hogy $c < 0$. Ekkor $c.x = (-c).x_1 - (-c).x_0$ és $(-c).x_1, (-c).x_0 \in E_+$, így

μ definíciója és μ_0 pozitív $\mathbb{R}$-homogenitása miatt

$$\mu(c.x)=\mu_0((-c).x_1)-\mu_0((-c).x_0)=(-c)\mu_0(x_1)-(-c)\mu_0(x_0)=c(\mu_0(x_0)-\mu_0(x_1))=c\mu(x).$$

Tehát a μ leképezés $\mathbb{R}$-homogén.

Ezzel megmutattuk az előírt tulajdonságú lineáris funkcionál egzisztenciáját, amelynek unicitása nyilvánvaló, mert $E = E_+ - E_+$ miatt E_+ generátorhalmaz az E valós vektortérben, és a keresett lineáris funkcionál értékei μ_0 által elő vannak írva az E_+ halmazon. ■

25.6.2. Definíció. *Legyen E lineáris háló. Azt mondjuk, hogy a $\mu \in E^*$ lineáris funkcionál* **relatív korlátos***, ha minden $x \in E_+$ esetén*

$$\sup_{\substack{y\in E,\\ |y|\leq x}} |\mu(y)| < +\infty,$$

vagyis a $\{\mu(y)|(y \in E) \wedge (|y| \leq x)\}$ halmaz korlátos $\mathbb{R}$-ben. Az E lineáris háló feletti relatív korlátos lineáris funkcionálok halmazát $\Omega(E)$ jelöli. Az E lineáris háló feletti pozitív relatív korlátos lineáris funkcionálok halmazát $\Omega_+(E)$ jelöli.

25.6.3. Állítás. *Legyen E lineáris háló. Az E feletti relatív korlátos lineáris funkcionálok halmaza lineáris altere E^*-nak, és minden $\mu : E \to \mathbb{R}$ pozitív lineáris funkcionál relatív korlátos, és minden $y \in E$ esetén*

$$|\mu(y)| \leq \mu(|y|).$$

Bizonyítás. Legyenek $\mu, \nu \in \Omega(E)$, $c \in \mathbb{R}$ és $x \in E_+$. Ekkor minden $y \in E$ esetén, ha $|y| \leq x$, akkor

$$|(\mu+\nu)(y)| \leq |\mu(y)| + |\nu(y)| \leq \sup_{\substack{z\in E,\\ |z|\leq x}} |\mu(z)| + \sup_{\substack{z\in E,\\ |z|\leq x}} |\nu(z)|,$$

$$|(c.\mu)(y)| = |c||\mu(y)| \leq |c| \sup_{\substack{z\in E,\\ |z|\leq x}} |\mu(z)|,$$

következésképpen

$$\sup_{\substack{y\in E,\\ |y|\leq x}} |(\mu+\nu)(y)| \leq \sup_{\substack{z\in E,\\ |z|\leq x}} |\mu(z)| + \sup_{\substack{z\in E,\\ |z|\leq x}} |\nu(z)| < +\infty,$$

$$\sup_{\substack{y\in E,\\ |y|\leq x}} |(c.\mu)(y)| \leq |c| \sup_{\substack{z\in E,\\ |z|\leq x}} |\mu(z)| < +\infty,$$

tehát $\mu + \nu \in \Omega(E)$ és $c.\mu \in \Omega(E)$. Nyilvánvaló, hogy a 0 funkcionál relatív korlátos, tehát $\Omega(E) \neq \emptyset$, ezért $\Omega(E)$ lineáris altere E^*-nak.

Legyen μ pozitív lineáris funkcionál E felett. Ekkor μ monoton növő, így minden $y \in E$ esetén a $-|y| \leq y \leq |y|$ egyenlőtlenségekből $-\mu(|y|) \leq \mu(y) \leq \mu(|y|)$ következik, vagyis $|\mu(y)| \leq \mu(|y|)$. Ebből látható, hogy ha $x \in E_+$ és $y \in E$ olyan, hogy $|y| \leq x$, akkor $|\mu(y)| \leq \mu(|y|) \leq \mu(x)$, tehát

$$\sup_{\substack{y\in E,\\ |y|\leq x}} |\mu(y)| \leq \mu(x) < +\infty,$$

ami azt jelenti, hogy μ relatív korlátos. ■

25.6.4. Állítás. *Legyen E lineáris háló, és $\mu \in \Omega(E)$. Ekkor egyértelműen létezik az a $\nu : E \to \mathbb{R}$ pozitív lineáris funkcionál, amelyre minden $x \in E_+$ esetén*

$$\nu(x) = \sup_{\substack{y \in E_+, \\ y \le x}} \mu(y).$$

Továbbá, ekkor a $\nu - \mu : E \to \mathbb{R}$ lineáris funkcionál pozitív.

Bizonyítás. Először megjegyezzük, hogy $x \in E_+$ esetén

$$0 \in \{y \in E_+ | y \le x\} \subseteq \{y \in E | \, |y| \le x\},$$

ezért a μ lineáris funkcionál relatív korlátossága miatt

$$0 \le \sup_{\substack{y \in E_+, \\ y \le x}} \mu(y) \le \sup_{\substack{y \in E, \\ |y| \le x}} |\mu(y)| < +\infty,$$

Tekintsük most a

$$\nu_0 : E_+ \to \mathbb{R}_+; \quad x \mapsto \sup_{\substack{y \in E_+, \\ y \le x}} \mu(y)$$

leképezést. A 25.6.1. tétel alapján az előírt tulajdonságú ν lineáris funkcionál egyértelmű létezéséhez elegendő azt igazolni, hogy ν_0 additív. Ehhez legyenek $x_0, x_1 \in E_+$ rögzített elemek.

Legyen $y_1 \in E_+$ olyan, hogy $y_1 \le x_1$. Ekkor minden $y_0 \in E_+$ esetén, ha $y_0 \le x_0$, akkor $0 \le y_0 + y_1 \le x_0 + x_1$, ezért ν_0 definíciója és μ additivitása szerint $\mu(y_0) + \mu(y_1) = \mu(y_0 + y_1) \le \nu_0(x_0 + x_1)$, vagyis $\mu(y_0) \le \nu_0(x_0 + x_1) - \mu(y_1)$. Ezért ν_0 definíciója szerint

$$\nu_0(x_0) = \sup_{\substack{y_0 \in E_+, \\ y_0 \le x_0}} \mu(y_0) \le \nu_0(x_0 + x_1) - \mu(y_1),$$

amiből következik, hogy $\mu(y_1) \le \nu_0(x_0 + x_1) - \nu_0(x_0)$. Ez az egyenlőtlenség minden olyan $y_1 \in E_+$ elemre érvényes, amelyre $y_1 \le x_1$, így ν_0 definíciója szerint

$$\nu_0(x_1) = \sup_{\substack{y_1 \in E_+, \\ y_1 \le x_1}} \mu(y_1) \le \nu_0(x_0 + x_1) - \nu_0(x_0),$$

tehát $\nu_(x_0) + \nu_(x_1) \le \nu_0(x_0 + x_1)$.

A fordított egyenlőtlenség bizonyításához legyen $c \in \mathbb{R}$ tetszőleges olyan szám, amelyre $c < \nu(x_0 + x_1)$. Ekkor ν_0 definíciója szerint van olyan $y \in E_+$, hogy $y \le x_0 + x_1$ és $c < \mu(y)$. A 25.2.9. állítás alapján léteznek olyan $y_0, y_1 \in E$ elemek, hogy $y = y_0 + y_1$ és $0 \le y_0 \le x_0$ és $0 \le y_1 \le x_1$. Ekkor ν_0 definíciója és μ additivitása szerint

$$c < \mu(y) = \mu(y_0 + y_1) = \mu(y_0) + \mu(y_1) \le \nu_0(x_0) + \nu_0(x_1),$$

amiből következik, hogy $\nu_0(x_0 + x_1) \le \nu_0(x_0) + \nu_0(x_1)$.

Ha $x \in E_+$, akkor $0 \le x \le x$ miatt $\mu(x) \le \nu(x)$, vagyis $0 \le (\nu - \mu)(x)$, ami azt jelenti, hogy $\nu - \mu$ pozitív lineáris funkcionál. ■

25.6.5. Állítás. *Legyen E lineáris háló. Egy E feletti lineáris funkcionál pontosan akkor relatív korlátos, ha előáll E feletti pozitív lineáris funkcionálok lineáris kombinációjaként, vagyis az E feletti pozitív lineáris funkcionálok halmaza generátorhalmaz az $\Omega(E)$ vektortérben.*

Bizonyítás. Mivel az E feletti pozitív lineáris funkcionálok relatív korlátosak és $\Omega(E)$ lineáris altere E^*-nak (25.6.3.), így a feltétel elégséges. Ha $\mu \in \Omega(E)$, akkor az előző állítás szerint van olyan ν pozitív lineáris funkcionál E felett, amelyre $\nu - \mu$ is pozitív lineáris funkcionál, és természetesen $\mu = \nu - (\nu - \mu)$, így μ előáll két pozitív lineáris funkcionál különbségeként. ■

25.6.6. Tétel. *Ha E lineáris háló, akkor a*

$$\mu \leq \nu \quad \overset{\text{def}}{\Leftrightarrow} \quad (\mu \in \Omega(E)) \wedge (\nu \in \Omega(E)) \wedge ((\forall x \in E_+)\ \mu(x) \leq \nu(x))$$

reláció olyan rendezés $\Omega(E)$ felett, amellyel $\Omega(E)$ teljes lineáris háló.

Bizonyítás. (I) Először megmutatjuk, hogy a $\leq$ reláció rendezés $\Omega(E)$ felett. Az triviális, hogy a $\leq$ reláció reflexív az $\Omega(E)$ halmazon és tranzitív. Ha $\mu, \nu \in \Omega(E)$ és $\mu \leq \nu$ és $\nu \leq \mu$, akkor $\mu = \nu$ az E_+ halmazon, és mivel E_+ generátorhalmaz az E valós vektortérben (mert $E_+ - E_+ = E$), valamint μ és ν lineáris funkcionálok, így $\mu = \nu$, ami azt jelenti, hogy a $\leq$ reláció antiszimmetrikus.

(II) Megmutatjuk, hogy az $\Omega(E)$ halmaz feletti $\leq$ rendezésre teljesülnek a (GO) és (EVO) állítások.

Ehhez legyenek $\mu, \nu \in \Omega(E)$ olyanok, hogy $\mu \leq \nu$, tehát minden $x \in E_+$ elemre $\mu(x) \leq \nu(x)$. Ekkor

– minden $\varrho \in \Omega(E)$ esetén minden $x \in E_+$ elemre $(\mu+\varrho)(x) = \mu(x)+\varrho(x) \leq \nu(x)+\varrho(x) = (\nu + \varrho)(x)$, vagyis $\mu + \varrho \leq \nu + \varrho$, ami azt jelenti, hogy (GO) teljesül az $(\Omega(E), +)$ kommutatív csoportra, és

– minden $\lambda \in \mathbb{R}_+$ esetén minden $x \in E_+$ elemre $(\lambda.\mu)(x) = \lambda\mu(x) \leq \lambda\nu(x) = (\lambda.\nu)(x)$, vagyis $\lambda.\mu \leq \lambda.\nu$, ami azt jelenti, hogy (EVO) is teljesül.

Tehát az $\Omega(E)$ vektortér a $\leq$ rendezéssel ellátva rendezett vektortér, és világos, hogy ennek pozitivitástartománya egyenlő az E feletti pozitív lineáris funkcionálok halmazával.

(III) Megmutatjuk, hogy az $\Omega(E)$ rendezett vektortér lineáris háló. Ehhez 25.3.4. alapján elegendő azt igazolni, hogy minden $\mu \in \Omega(E)$ esetén létezik a $\mu \vee 0$ szuprémum. Ennek bizonyításához legyen $\mu \in \Omega(E)$ rögzítve, és a 25.6.4. állítást alkalmazva jelölje ν azt a pozitív lineáris funkcionált E felett, amelyre minden $x \in E_+$ esetén

$$\nu(x) = \sup_{\substack{y \in E_+, \\ y \leq x}} \mu(y).$$

Bebizonyítjuk, hogy ν a $\{\mu, 0\}$ halmaz szuprémuma. Valóban, minden $x \in E_+$ esetén $x \in E_+$ olyan, hogy $x \leq x$, így ν definíciója szerint $\mu(x) \leq \nu(x)$, vagyis $\mu \leq \nu$. Mivel $0 \in E_+$ olyan, hogy minden $x \in E_+$ esetén $0 \leq x$, így ν definíciója szerint $0 = \mu(0) \leq \nu(x)$, vagyis $0 \leq \nu$. Ez azt jelenti, hogy ν felső korlátja a $\{\mu, 0\}$ halmaznak. Tegyük fel, hogy $\varrho \in \Omega(E)$ felső korlátja a $\{\mu, 0\}$ halmaznak. Ha $x \in E_+$ és $y \in E_+$ olyan vektorok, hogy $y \leq x$, akkor $0 \leq x - y$, így $0 \leq \varrho$ miatt $0 \leq \varrho(x-y) = \varrho(x) - \varrho(y)$, tehát $\mu \leq \varrho$ folytán $\mu(y) \leq \varrho(y) \leq \varrho(x)$. Ezért ν definíciója szerint minden $x \in E_+$ elemre $\nu(x) \leq \varrho(x)$, vagyis $\nu \leq \varrho$. Ez azt jelenti, hogy ν a $\{\mu, 0\}$ halmaz legkisebb felső korlátja.

(IV) Végül bebizonyítjuk, hogy $\Omega(E)$ teljes lineáris háló. Ehhez 25.4.2. alapján elegendő azt igazolni, hogy ha $(\mu_i)_{i \in I}$ olyan nem üres rendszer $\Omega(E)$-ben, hogy minden $i \in I$ esetén $0 \leq \mu_i$, és a $(\mu_i)_{i \in I}$ rendszer felülről korlátos $\Omega(E)$-ben, és felfelé irányított (vagyis minden $i, j \in I$ esetén van olyan $k \in I$, hogy $\mu_i \leq \mu_k$ és $\mu_j \leq \mu_k$), akkor létezik a $\bigvee\limits_{i \in I} \mu_i$ szuprémum az $\Omega(E)$ lineáris hálóban.

Ennek bizonyításához legyen $\nu \in \Omega(E)$ olyan, amelyre minden $i \in I$ esetén $\mu_i \leq \nu$. Ekkor minden $x \in E_+$ vektorra, minden $i \in I$ esetén $\mu_i(x) \leq \nu(x)$, ezért jól értelmezett a

$$\mu_* : E_+ \to \mathbb{R}_+; \quad x \mapsto \sup_{i \in I} \mu_i(x)$$

függvény. Megmutatjuk, hogy μ_* *additív*, vagyis minden $x, x' \in E_+$ esetén $\mu_*(x + x') = \mu_*(x) + \mu_*(x')$.

Legynek $x, x' \in E_+$. Ekkor minden $i \in I$ indexre $\mu_i(x + x') = \mu_i(x) + \mu_i(x') \leq \mu_*(x) + \mu_*(x')$, ezért $\mu_*(x + x') \leq \mu_*(x) + \mu_*(x')$. Legyen $c \in \mathbb{R}$ olyan szám, hogy $c < \mu_*(x) + \mu_*(x')$. Ekkor $c - \mu_*(x') < \mu_*(x) = \sup\limits_{i \in I} \mu_i(x)$, tehát van olyan $i \in I$, hogy $c - \mu_*(x') < \mu_i(x)$. Ekkor $c - \mu_i(x) < \mu_*(x') = \sup\limits_{j \in I} \mu_j(x')$, tehát van olyan $j \in I$, hogy $c - \mu_i(x) < \mu_j(x')$, vagyis $c < \mu_i(x) + \mu_j(x')$. A $(\mu_k)_{k \in I}$ rendszer felfelé irányítottságából következik olyan $k \in I$ létezése, amelyre $\mu_i \leq \mu_k$ és $\mu_j \leq \mu_k$. Ekkor $\mu_i(x) \leq \mu_k(x)$ és $\mu_j(x') \leq \mu_k(x')$, következésképpen $c < \mu_i(x) + \mu_j(x') \leq \mu_k(x) + \mu_k(x') = \mu_k(x + x') \leq \mu_*(x + x')$. Tehát minden $c < \mu_*(x) + \mu_*(x')$ valós számra $c < \mu_*(x + x')$, amiből következik, hogy $\mu_*(x) + \mu_*(x') \leq \mu_*(x + x')$.

Tehát a $\mu_* : E_+ \to \mathbb{R}_+$ leképezés additív, így 25.6.1. alapján egyértelműen létezik az a pozitív lineáris funkcionál E felett, amely μ_*-nak kiterjesztése: jelölje μ ezt a pozitív lineáris funkcionált. Világos, hogy minden $i \in I$ és $x \in E_+$ esetén $\mu_i(x) \leq \mu_*(x) = \mu(x)$, tehát μ felső korlátja a $(\mu_i)_{i \in I}$ rendszernek. Ha $\varrho \in \Omega(E)$ szintén felső korlátja a $(\mu_i)_{i \in I}$ rendszernek, akkor $i \in I$ és $x \in E_+$ esetén $\mu_i(x) \leq \varrho(x)$, így minden $x \in E_+$ vektorra $\mu(x) = \mu_*(x) = \sup\limits_{i \in I} \mu_i(x) \leq \varrho(x)$, ezért $\mu \leq \varrho$. Tehát μ szuprémuma a $(\mu_i)_{i \in I}$ rendszernek az $\Omega(E)$ lineáris hálóban. ■

Külön említésre méltó, hogy az előző tétel bizonyításának (III) pontjában igazoltuk azt, hogy ha E lineáris háló és $\mu \in \Omega(E)$, akkor minden $x \in E_+$ esetén

$$\mu^+(x) = \sup_{\substack{y \in E_+,\\ y \leq x}} \mu(y).$$

Hasonlóan fontos, hogy az előző tétel bizonyításának (IV) pontjában igazoltuk azt, hogy ha E lineáris háló és $(\mu_i)_{i \in I}$ olyan nem üres rendszer $\Omega(E)$-ben, hogy minden $i \in I$ esetén $0 \leq \mu_i$, és a $(\mu_i)_{i \in I}$ rendszer felülről korlátos $\Omega(E)$-ben, és felfelé irányított (vagyis minden $i, j \in I$ esetén van olyan $k \in I$, hogy $\mu_i \leq \mu_k$ és $\mu_j \leq \mu_k$), akkor létezik a $\bigvee\limits_{i \in I} \mu_i$ szuprémum az $\Omega(E)$ lineáris hálóban, és minden $x \in E_+$ esetén

$$\Big(\bigvee_{i \in I} \mu_i\Big)(x) = \sup_{i \in I} \mu_i(x).$$

25.6.7. Állítás. *Ha E lineáris háló, akkor minden $\mu \in \Omega(E)$ és $x \in E$ esetén*

$$|\mu(x)| \leq |\mu|(|x|).$$

Bizonyítás. Legyen $\mu \in \Omega(E)$ és $x \in E$. Mivel $\mu \leq |\mu|$ és $-\mu \leq |\mu|$, így fennállnak a következő egyenlőtlenségek:

$$\mu(x^+) \leq |\mu|(x^+), \quad -\mu(x^+) \leq |\mu|(x^+), \quad \mu(x^-) \leq |\mu|(x^-), \quad -\mu(x^-) \leq |\mu|(x^-).$$

A két első egyenlőtlenségből $|\mu(x^+)| \leq |\mu|(x^+)$, a két utolsó egyenlőtlenségből $|\mu(x^-)| \leq |\mu|(x^-)$ következik. Ezért 25.2.4. a) alapján

$$|\mu(x)| = |\mu(x^+ - x^-)| = |\mu(x^+) - \mu(x^-)| \leq |\mu(x^+)| + |\mu(x^-)| \leq$$
$$\leq |\mu|(x^+) + |\mu|(x^-) = |\mu|(x^+ + x^-) = |\mu|(|x|). \blacksquare$$

25.6.8. Állítás. *Legyen E lineáris háló és $\mu \in \Omega(E)$. Ekkor minden $x \in E_+$ esetén*

$$|\mu|(x) = \sup_{\substack{y\in E,\\ |y|\leq x}} |\mu(y)|.$$

Bizonyítás. (I) Vezessük be a

$$\nu_0 : E_+ \to \mathbb{R}_+; \quad x \mapsto \sup_{\substack{y\in E,\\ |y|\leq x}} |\mu(y)|$$

leképezést. Megmutatjuk, hogy ν_0 additív. Ehhez legyenek $x, x' \in E_+$ rögzítve.

Ha $y \in E$ és $|y| \leq x + x'$, akkor a felbontási lemma (25.2.9.) b) pontja szerint vehetünk olyan $z, z' \in E$ elemeket, hogy $y = z + z'$ és $|z| \leq x$ és $|z'| \leq x'$. Ekkor ν_0 definíciója és μ additivitása folytán

$$|\mu(y)| = |\mu(z + z')| = |\mu(z) + \mu(z')| \leq |\mu(z)| + |\mu(z')| \leq \nu_0(x) + \nu_0(x'),$$

következésképpen $\mu_0(x + x') \leq \nu_0(x) + \nu_0(x')$.

Megfordítva, legyenek $y, y' \in E$ olyan elemek, hogy $|y| \leq x$ és $|y'| \leq x'$. Most felhasználjuk azt az esetszétválasztással könnyen igazolható elemi tényt, hogy minden $a, b \in \mathbb{R}$ esetén az

$$\varepsilon := \begin{cases} +1 & \text{, ha } a \cdot b \geq 0, \\ -1 & \text{, ha } a \cdot b < 0 \end{cases}$$

számra fennáll az $|a| + |b| = |a + \varepsilon b|$ egyenlőség. Ezt alkalmazva az $a := \mu(y)$ és $b := \mu(y')$ valós számokra kapjuk olyan $\varepsilon \in \{-1, 1\}$ létezését, amelyre $|\mu(y)| + |\mu(y')| = |\mu(y) + \varepsilon\mu(y')|$. Tehát ekkor μ additivitása és ν_0 definíciója szerint

$$|\mu(y)| + |\mu(y')| = |\mu(y) + \varepsilon\mu(y')| = |\mu(y + \varepsilon.y')| \leq \nu_0(x + x'),$$

hiszen 25.3.2. b) alapján $y + \varepsilon.y' \in E$ olyan, hogy $|y + \varepsilon.y'| \leq |y| + |\varepsilon.y'| = |y| + |\varepsilon|.|y'| = |y| + |y'| \leq x + x'$. Tehát azt kaptuk, hogy ha $y' \in E$ olyan, hogy $|y'| \leq x'$, akkor minden $y \in E$ vektorra, $|y| \leq x$ esetén $|\mu(y)| \leq \nu_0(x + x') - |\mu(y')|$, így ν_0 definíciója szerint $\nu_0(x) \leq \nu_0(x + x') - |\mu(y')|$, vagyis $|\mu(y')| \leq \nu_0(x + x') - \nu_0(x)$. Ez minden olyan $y' \in E$ vektorra igaz, amelyre $|y'| \leq x'$, így ismét ν_0 definícióját alkalmazva a $\nu_0(x') \leq \nu_0(x + x') - \nu_0(x)$ egyenlőtlenségre jutunk, vagyis $\nu_0(x) + \nu_0(x') \leq \nu_0(x + x')$ is teljesül.

Ezzel ν_0 additivitását igazoltuk, így 25.6.1. alapján vehetjük azt a ν lineáris funkcionált E felett, amely ν_0-nak kiterjesztése.

(II) Megmutatjuk, hogy ν a $\{-\mu, \mu\}$ halmaz szuprémuma az $\Omega(E)$ lineáris hálóban, tehát $\nu = |\mu|$.

Ha $x \in E_+$, akkor $x \leq x$ és ν_0 definíciója szerint $\mu(x) \leq |\mu(x)| \leq \nu_0(x) = \nu(x)$, és $(-\mu)(x) = -\mu(x) \leq |\mu(x)| \leq \nu_0(x) = \nu(x)$, tehát $\mu \leq \nu$ és $-\mu \leq \nu$. Legyen $\varrho \in \Omega(E)$ olyan, hogy $\mu \leq \varrho$ és $-\mu \leq \varrho$. Ekkor $x \in E_+$, $y \in E$ és $|y| \leq x$ esetén 25.6.7. alkalmazásával kapjuk, hogy $|\mu(y)| \leq |\mu|(|y|) \leq \varrho(|y|) \leq \varrho(x)$, így ν_0 definíciója szerint $\nu(x) = \nu_0(x) \leq \varrho(x)$, következésképpen $\nu \leq \varrho$. $\blacksquare$

25.6.9. Állítás. *Legyen E lineáris háló, és $\mu, \nu \in \Omega(E)$. Ekkor minden $x \in E_+$ vektorra*

$$(\mu \vee \nu)(x) = \sup_{\substack{(y',y)\in E_+\times E_+,\\ y+y'=x}} (\mu(y') + \nu(y)) = \sup_{\substack{y\in E_+,\\ y\le x}} (\mu(x-y) + \nu(y)),$$

$$(\mu \wedge \nu)(x) = \inf_{\substack{(y',y)\in E_+\times E_+,\\ y+y'=x}} (\mu(y') + \nu(y)) = \inf_{\substack{y\in E_+,\\ y\le x}} (\mu(x-y) + \nu(y)).$$

Bizonyítás. A 25.2.4. b) állítás szerint $\mu \vee \nu = \mu + (\nu - \mu)^+$, így a relatív korlátos lineáris funkcionálok pozitív részére vonatkozó explicit formula alkalmazásával kapjuk, hogy minden $x \in E_+$ esetén

$$(\mu \vee \nu)(x) = \left(\mu + (\nu-\mu)^+\right)(x) = \mu(x) + (\nu-\mu)^+(x) = \mu(x) + \sup_{\substack{y\in E_+,\\ y\le x}} (\nu-\mu)(y) =$$

$$= \sup_{\substack{y\in E_+,\\ y\le x}} (\mu(x) + (\nu(y) - \mu(y))) = \sup_{\substack{y\in E_+,\\ y\le x}} (\mu(x-y) + \nu(y)).$$

Mivel 25.1.4. b) alapján $\mu \wedge \nu = -((-\mu) \vee (-\nu))$, ebből következik, hogy minden $x \in E_+$ esetén

$$(\mu \wedge \nu)(x) = -((-\mu)\vee(-\nu))(x) = -\sup_{\substack{y\in E_+,\\ y\le x}} (-\mu(x-y) - \nu(y)) = \inf_{\substack{y\in E_+,\\ y\le x}} (\mu(x-y) + \nu(y)),$$

amit bizonyítani kellett. ■

25.6.10. Következmény. *Legyen E lineáris háló és $\mu, \nu \in \Omega(E)$. A μ és ν relatív korlátos lineáris funkcionálok pontosan akkor függetlenek az $\Omega(E)$ lineáris hálóban, ha*

$$(\forall x \in E_+)(\forall \varepsilon \in \mathbb{R}_+^*)(\exists y \in [0,x]) : \ |\mu|(x-y) + |\nu|(y) < \varepsilon.$$

Bizonyítás. A 25.6.9. állításban szereplő második formulából azonnal következik. ■

25.7. Lineáris funkcionálok Lebesgue-felbontása

25.7.1. Állítás. *Legyen E lineáris háló, és $\mu, \nu \in \Omega_+(E)$. Ekkor $\mu \in \{\nu\}^{\perp\perp}$ ekvivalens a következő kijelentéssel:*

$$(\forall x \in E_+)(\forall \varepsilon \in \mathbb{R}_+^*)(\exists \delta \in \mathbb{R}_+^*)(\forall y \in [0,x]) : (\nu(y) < \delta \ \Rightarrow \ \mu(y) < \varepsilon). \qquad (*)$$

(**Megjegyzés.** A $\mu \in \{\nu\}^{\perp\perp}$ összefüggést gyakran úgy fejezzük ki, hogy "μ **abszolút folytonos** ν-re nézve". Ez a terminológia a teljes lineáris hálók elméletének valós Radon-mértékekre való alkalmazásából származik (**RAD**).)

Bizonyítás. (I) Tegyük fel, hogy $\mu \in \{\nu\}^{\perp\perp}$ és $0 \le \mu$. Megmutatjuk, hogy ekkor $(*)$ teljesül. Ehhez legyenek $x \in E_+$ és $\varepsilon \in \mathbb{R}_+^*$ rögzítve.

A 25.5.9. állítást alkalmazva E helyett az $\Omega(E)$ teljes lineáris hálóra, y helyett ν-re, és x helyett μ-re kapjuk, hogy

$$\mu = \bigvee_{n\in\mathbb{N}} (\mu \wedge (n.\nu)),$$

és világos, hogy az $\Omega_+(E)$-ben haladó $(\mu \wedge (n.\nu))_{n\in\mathbb{N}}$ sorozat monoton növő $\Omega(E)$-ben, tehát felfelé irányított, így a 25.6.6. tétel után álló második megjegyzés szerint minden $y \in E_+$ esetén

$$\mu(y) = \sup_{n\in\mathbb{N}} ((\mu \wedge (n.\nu))(y)).$$

Speciálisan, ebből következik, hogy létezik olyan $n \in \mathbb{N}$, amelyre

$$\mu(x) - \frac{\varepsilon}{2} \ < \ (\mu \wedge (n.\nu))(x).$$

Rögzítsünk ilyen $n \in \mathbb{N}$ számot és tekintsük a $\mu - (\mu \wedge (n.\nu)) : E \to \mathbb{R}$ pozitív lineáris funkcionált. Ha $y \in [0, x]$, akkor

$$\mu(y) - (\mu \wedge (n.\nu))(y) = (\mu - (\mu \wedge (n.\nu)))\,(y) \leq$$
$$\leq (\mu - (\mu \wedge (n.\nu)))\,(x) = \mu(x) - (\mu \wedge (n.\nu))\,(x) < \frac{\varepsilon}{2},$$

következésképpen

$$\mu(y) \ < \ \frac{\varepsilon}{2} + (\mu \wedge (n.\nu))(y) \ \leq \ \frac{\varepsilon}{2} + n\nu(y).$$

Ez azt mutatja, hogy, ha $\delta \in \mathbb{R}^*_+$ olyan szám, hogy $n\delta < \dfrac{\varepsilon}{2}$, akkor minden $y \in [0, x]$ esetén, ha $\nu(y) < \delta$, akkor $\mu(y) < \dfrac{\varepsilon}{2} + n\delta < \varepsilon$, így teljesül a $(*)$ állítás.

(II) Tegyük fel, hogy $(*)$ teljesül. Közvetlenül azt fogjuk igazolni, hogy $\mu \in \{\nu\}^{\perp\perp}$, vagyis minden $\varrho \in \{\nu\}^{\perp}$ esetén $\mu \wedge |\varrho| = 0$. Ehhez elegendő azt belátni, hogy minden $\varrho \in \{\nu\}^{\perp} \cap \Omega_+(E)$ esetén $\mu \wedge \varrho = 0$, hiszen ha ez igaz, akkor $\varrho \in \{\nu\}^{\perp}$ esetén $|\varrho| \in \{\nu\}^{\perp} \cap \Omega_+(E)$, tehát $\mu \wedge |\varrho| = 0$.

Legyen tehát $\varrho \in \{\nu\}^{\perp} \cap \Omega_+(E)$ rögzített, és $x \in E_+$. Azt akarjuk bizonyítani, hogy $(\mu \wedge \varrho)(x) = 0$, ami 25.6.9. alapján azzal ekvivalens, hogy minden $\varepsilon \in \mathbb{R}^*_+$ számhoz létezik olyan $(y, z) \in E_+ \times E_+$ pár, amelyre $x = y + z$ és $\mu(y) + \varrho(z) < \varepsilon$. Legyen tehát $\varepsilon \in \mathbb{R}^*_+$ szintén rögzítve, és ilyen tulajdonságú (y, z) párt keresünk.

Először a $(*)$ hipotézist alkalmazva, az $\varepsilon/2$ számhoz rögzítünk olyan $\delta \in \mathbb{R}^*_+$ számot, amelyre teljesül az, hogy minden $y \in [0, x]$ esetén: ha $\nu(y) < \delta$, akkor $\mu(y) < \varepsilon/2$. Természetes feltehető, hogy $\delta \leq \varepsilon/2$. Ezután kihasználjuk azt, hogy ϱ és ν függetlenek, így a 25.6.10. állítást alkalmazva kapunk olyan $y \in [0, x]$ elemet, amelyre $\nu(y) + \varrho(x - y) < \delta$. Mivel ekkor $\nu(y) < \delta$ is teljesül, így $\mu(y) < \varepsilon/2$. Ezért

$$\mu(y) + \varrho(x - y) \leq \nu(y) + \varrho(x - y) + \mu(y) < \delta + \mu(y) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

vagyis $(y, x - z)$ olyan pár, amit kerestünk. ■

25.7.2. Definíció. *Ha E lineáris háló, és $\mu, \nu \in \Omega_+(E)$, akkor a μ pozitív lineáris funkcionál ν szerinti* **Lebesgue-felbontásának** *nevezzük a $(\mu_*, \varrho) \in \Omega_+(E) \times \Omega_+(E)$ párt, ha $\mu = \mu_* + \varrho$ és $\mu_* \in \{\nu\}^{\perp\perp}$ (vagyis μ_** **abszolút folytonos** *ν-re nézve), és $\varrho \in \{\nu\}^{\perp}$ (vagyis ϱ független ν-től, amit úgy is mondunk, hogy ϱ* **szinguláris** *ν-re nézve).*

Tehát, ha E lineáris háló, és $\mu, \nu \in \Omega_+(E)$, akkor a Riesz-féle felbontási tétel szerint egyértelműen létezik μ-nek ν szerinti (μ_*, ϱ) Lebesgue-felbontása, és a 25.6.10. állítás jellemzést ad ϱ-ra (vagyis a felbontás szinguláris részére), míg a 25.7.1. állítás μ_*-ot (vagyis a felbontás abszolút folytonos részét) jellemzi.

IV. rész

A matematikai analízis topológiai alapjai

BEVEZETÉS

Irodalomjegyzék

[1] N. Bourbaki, **Éleménts de mathématique. Topologie.** Hermann, Paris

[2] K. Kuratowski, **Topology, I-II**, Academic Press, New York-London, 1968.

[3] J. L. Kelley, **General Topology**, D. Van Vostrand Company, Inc, Princeton, New Jersey, 1957.

[4] Császár Ákos, **Bevezetés az általános topológiába**, Akadémiai Kiadó, Budapest, 1970.

26. fejezet

Topologikus terek és folytonos függvények

26.1. Topológiák

26.1.1. Definíció. *Legyen T halmaz. Egy $\mathscr{T} \subseteq \mathscr{P}(T)$ halmazt T feletti* **topológiának** *nevezünk, ha teljesülnek a következők.*

($\mathrm{O_I}$) $T \in \mathscr{T}$.

($\mathrm{O_{II}}$) *Minden $\mathscr{T}$-ben haladó nem üres véges rendszer metszete eleme $\mathscr{T}$-nek.*

($\mathrm{O_{III}}$) *Minden $\mathscr{T}$-ben haladó rendszer uniója eleme $\mathscr{T}$-nek.*

A $(T, \mathscr{T})$ párt **topologikus térnek** *nevezzük, ha $\mathscr{T}$ topológia a T halmaz felett. Ha $(T, \mathscr{T})$ topologikus tér, akkor a $\mathscr{T}$ topológia elemeit a T halmaz* **$\mathscr{T}$-nyílt** *részhalmazainak nevezzük, és egy $F \subseteq T$ halmazt* **$\mathscr{T}$-zártnak** *nevezünk, ha a $T \setminus F$ halmaz $\mathscr{T}$-nyílt.*

Ha $\mathscr{T}$ topológia a T halmaz felett, akkor ($\mathrm{O_{III}}$) miatt az üres rendszer uniója, vagyis az $\emptyset$ halmaz szintén eleme $\mathscr{T}$-nek.

A definícióból és a halmazelméleti de Morgan-egyenlőségekből következik, hogy a $(T, \mathscr{T})$ topologikus térben az $\emptyset$ és T halmazok $\mathscr{T}$-zártak, továbbá $\mathscr{T}$-zárt halmazok bármely nem üres rendszerének a metszete $\mathscr{T}$-zárt, valamint véges sok $\mathscr{T}$-zárt halmaz uniója $\mathscr{T}$-zárt.

Példák (topologikus terekre).

1) Legyen T halmaz. Ekkor az $\{\emptyset, T\}$ és a $\mathscr{P}(T)$ halmazok nyilvánvalóan topológiák T felett. A $\{\emptyset, T\}$ topológiát T feletti *antidiszkrét* topológiának nevezzük és a $\mathscr{T}_{ind}(T)$ szimbólummal jelöljük. A $\mathscr{P}(T)$ topológiát T feletti *diszkrét* topológiának nevezzük és a $\mathscr{T}_{dis}(T)$ szimbólummal jelöljük. Nyilvánvaló, hogy minden T feletti $\mathscr{T}$ topológiára $\mathscr{T}_{ind}(T) = \{\emptyset, T\} \subseteq \mathscr{T} \subseteq \mathscr{P}(T) = \mathscr{T}_{dis}(T)$.

2) Ha (M, d) metrikus tér, akkor a d által meghatározott nyílt halmazok $\mathscr{T}_d$ halmaza topológia M felett; ezt nevezzük a *d metrika által generált topológiának.* A T halmaz feletti $\mathscr{T}$ topológiát *metrizálhatónak* nevezzük, ha létezik olyan T feletti d metrika, amelyre $\mathscr{T} = \mathscr{T}_d$. A T halmaz feletti $\mathscr{T}$ topológiát *teljesen metrizálhatónak* nevezzük, ha létezik olyan T feletti d metrika, amelyre $\mathscr{T} = \mathscr{T}_d$ és (T, d) teljes metrikus tér. Világos, hogy bármely halmaz felett a diszkrét topológia teljesen metrizálható, míg az antidiszkrét topológia biztosan nem metrizálható, ha az alaphalmaz legalább két elemű.

3) Ha K test és $|\cdot|$ abszolútérték-függvény K felett, akkor a

$$d_{|\cdot|} : K \times K \to \mathbb{R}_+; \quad (x, y) \mapsto |x - y|$$

függvény metrika K felett, tehát $\mathscr{T}_{d_{|\cdot|}}$ topológia K felett; ezt nevezzük az $|\cdot|$ *abszolútérték-függvény által generált* topológiának, és erre a $\mathscr{T}_{|\cdot|}$ egyszerűsített jelölést alkalmazzuk. Speciálisan, ha $|\cdot|$ jelöli az euklideszi abszolútérték-függvényt $\mathbb{K}$ felett, akkor a $\mathscr{T}_{|\cdot|}$ topológiát $\mathbb{K}$ feletti *euklideszi topológiának* nevezzük. Az $\mathbb{R}$ (illetve $\mathbb{C}$) feletti euklideszi topológiát gyakran az $\mathscr{E}_{\mathbb{R}}$ (illetve $\mathscr{E}_{\mathbb{C}}$) szimbólummal jelöljük.

4) Ha $(E, \|\cdot\|)$ normált tér, akkor a

$$d_{\|\cdot\|} : E \times E \to \mathbb{R}_+ \quad (x, y) \mapsto \|x - y\|$$

függvény metrika E felett, tehát $\mathscr{T}_{d_{\|\cdot\|}}$ topológia E felett; ezt nevezzük a $\|\cdot\|$ *norma által generált topológiának*, és a $\mathscr{T}_{\|\cdot\|}$ szimbólummal jelöljük. A $\mathbb{K}$ feletti E vektortér alaphalmaza feletti $\mathscr{T}$ topológiát *normálhatónak* nevezzük, ha létezik olyan $\|\cdot\|$ norma E felett, amelyre $\mathscr{T} = \mathscr{T}_{\|\cdot\|}$. A $\mathbb{K}$ feletti E vektortér alaphalmaza feletti $\mathscr{T}$ topológiát *teljesen normálhatónak* nevezzük, ha létezik olyan $\|\cdot\|$ norma E felett, amelyre $\mathscr{T} = \mathscr{T}_{\|\cdot\|}$ és $(E, \|\cdot\|)$ Banach-tér.

5) Legyen E vektortér $\mathbb{K}$ felett. Két E feletti norma ekvivalenciája – a definíció szerint – azt jelenti, hogy az általuk generált topológiák egyenlőek. Ha E véges dimenziós, akkor bármely két E feletti norma ekvivalens, és létezik norma E felett, tehát létezik egyértelműen olyan E feletti topológia, amelyet bármelyik E feletti norma generál; ezt a topológiát nevezzük az E véges dimenziós valós vagy komplex vektortér *euklideszi topológiájának*.

6) (*Topológia inverz képe.*) Legyen T halmaz, $(T', \mathscr{T}')$ topologikus tér és $f : T \to T'$ függvény. Ekkor az

$$\overset{-1}{f}[\mathscr{T}'] := \{\overset{-1}{f}\langle\Omega'\rangle \mid \Omega' \in \mathscr{T}'\}$$

halmaz nyilvánvalóan topológia T felett; ezt nevezzük a $\mathscr{T}'$ topológia f függvény által létesített *inverz képének*. Speciálisan, ha $E \subseteq T$ és $\mathrm{in}_{E,T}$ jelöli az $E \to T$ kanonikus injekciót, akkor a $\mathscr{T}$ topológia $\mathrm{in}_{E,T}$ által létesített inverz képe topológia az E részhalmaz felett; ezt nevezzük a $\mathscr{T}$ topológia E-re vett *leszűkítésének* és a $\mathscr{T}|E$ szimbólummal jelöljük. A definíció alapján világos, hogy

$$\mathscr{T}|E = \{\Omega \cap E | \Omega \in \mathscr{T}\}.$$

A $(T, \mathscr{T})$ topologikus tér *topologikus alterének* nevezünk minden olyan $(T', \mathscr{T}')$ topologikus teret, amelyre $T' \subseteq T$ és $\mathscr{T}' = \mathscr{T}|T'$.

7) (*Topológia képe.*) Legyen T halmaz, $(T', \mathscr{T}')$ topologikus tér és $f : T' \to T$ függvény. Ekkor az

$$f[\mathscr{T}'] := \{\Omega \in \mathscr{P}(T) \mid \overset{-1}{f}\langle\Omega\rangle \in \mathscr{T}'\}$$

halmaz nyilvánvalóan topológia T felett; ezt nevezzük a $\mathscr{T}'$ topológia f függvény által létesített *képének*. Speciálisan, ha $(T, \mathscr{T})$ topologikus tér, R ekvivalencia-reláció T felett és $\pi_{T/R}$ jelöli a $T \to T/R$ kanonikus szürjekciót, akkor a $\mathscr{T}$ topológia $\pi_{T/R}$ által létesített képe topológia a T/R faktorhalmaz felett; ezt nevezzük a $\mathscr{T}$ topológia R ekvivalencia-reláció szerinti *faktortopológiájának* és a $\mathscr{T}/R$ szimbólummal jelöljük. A $(T, \mathscr{T})$ topologikus tér *topologikus faktorterének* nevezünk minden olyan $(T', \mathscr{T}')$ topologikus teret, amelyhez van olyan T feletti R ekvivalencia-reláció, hogy $T' = T/R$ és $\mathscr{T}' = \mathscr{T}/R$.

26.2. Környezetek, környezetbázisok, rácsok és szűrők

26.2.1. Definíció. *Legyen $(T, \mathscr{T})$ topologikus tér. Minden $t \in T$ esetén*

$$\mathscr{T}(t) := \{V \in \mathscr{P}(T) \mid (\exists\, \Omega \in \mathscr{T}) : t \in \Omega \subseteq V\},$$

és az $\mathscr{T}(t)$ halmaz elemeit a t pont **környezeteinek** *nevezzük a $\mathscr{T}$ topológia szerint. Ha $t \in T$, akkor egy $\mathfrak{R} \subseteq \mathscr{T}(t)$ halmazt a t pont* **környezetbázisának** *nevezünk a $\mathscr{T}$ topológia szerint, ha minden $V \in \mathscr{T}(t)$ esetén van olyan $U \in \mathfrak{R}$, hogy $U \subseteq V$.*

A környezetek és az altértopológia definíciója alapján nyilvánvaló, hogy ha $(T, \mathscr{T})$ topologikus tér és $E \subseteq T$, akkor $t \in E$ esetén $(\mathscr{T}|E)(t) = \{V \cap E | V \in \mathscr{T}(t)\}$.

26.2.2. Definíció. *Ha $(T, \mathscr{T})$ topologikus tér, akkor egy $\mathfrak{B} \subseteq \mathscr{T}$ halmazt a $\mathscr{T}$* **topológia bázisának** *nevezünk, ha minden $\mathscr{T} \ni \Omega$-hoz létezik olyan $\mathfrak{B}$-ben haladó $(\Omega_i)_{i \in I}$ rendszer, amelyre $\Omega = \bigcup_{i \in I} \Omega_i$.*

26.2.3. Állítás. *Ha T halmaz és $\mathfrak{B} \subseteq \mathscr{P}(T)$ olyan részhalmaz, amely befedése T-nek és minden $\Omega, \Omega' \in \mathfrak{B}$ esetén $\Omega \cap \Omega' \in \mathfrak{B}$, akkor létezik egyetlen olyan T feletti topológia, amelynek $\mathfrak{B}$ topologikus bázisa.*

Bizonyítás. Az egyértelműség nyilvánvaló, mert ha $\mathfrak{B}$ topologikus bázisa a T halmaz feletti $\mathscr{T}$ topológiának, akkor $\mathscr{T}$ azon $\Omega \subseteq T$ halmazok halmaza, amelyekhez létezik olyan $\mathfrak{B}$-ben haladó $(\Omega_i)_{i \in I}$ rendszer, hogy $\Omega = \bigcup_{i \in I} \Omega_i$, tehát $\mathscr{T}$ egyértelműen van meghatározva $\mathfrak{B}$ által.
Az egzisztencia bizonyításához legyen $\mathscr{T}$ azon $\Omega \subseteq T$ halmazok halmaza, amelyekhez létezik olyan $\mathfrak{B}$-ben haladó $(\Omega_i)_{i \in I}$ rendszer, hogy $\Omega = \bigcup_{i \in I} \Omega_i$. Megmutatjuk, hogy $\mathscr{T}$ topológia T felett.
A hipotézis szerint $\mathfrak{B}$ befedi T-t, ezért $T \in \mathscr{T}$, vagyis $\mathscr{T}$-re $(\mathrm{O_I})$ teljesül.
Legyen $(\Omega_i)_{i \in I}$ nem üres véges rendszer $\mathscr{T}$-ben. A $\mathscr{T}$ halmaz definíciója alapján minden $i \in I$ esetén vehetünk olyan $\mathfrak{B}$-ben haladó $(\Omega_{i,j})_{j \in J_i}$ rendszert, hogy $\Omega_i = \bigcup_{j \in J_i} \Omega_{i,j}$. Ekkor a metszet unióra vonatkozó általános disztributivitása szerint

$$\bigcap_{i \in I} \Omega_i = \bigcap_{i \in I} \Big(\bigcup_{j \in J_i} \Omega_{i,j} \Big) = \bigcup_{\sigma \in J} \Big(\bigcap_{i \in I} \Omega_{i,\sigma(i)} \Big),$$

ahol $J := \prod_{i \in I} J_i$. A $\mathfrak{B}$ halmazra vonatkozó hipotézis szerint minden $\mathfrak{B}$-ben haladó nem üres véges rendszer metszete eleme $\mathfrak{B}$-nek: ez az adott rendszer indexhalmazának számossága szerinti teljes indukcióval könnyen igazolható. Minden $\sigma \in J$ esetén $(\Omega_{i,\sigma(i)})_{i \in I}$ egy $\mathfrak{B}$-ben haladó nem üres véges rendszer, így $\Big(\bigcap_{i \in I} \Omega_{i,\sigma(i)} \Big)_{\sigma \in J}$ olyan $\mathfrak{B}$-ben haladó rendszer, amelynek uniója egyenlő $\bigcap_{i \in I} \Omega_i$-vel, tehát $\bigcap_{i \in I} \Omega_i \in \mathfrak{B}$. Ezért $\mathscr{T}$-re $(\mathrm{O_{II}})$ teljesül.
Végül, legyen $(\Omega_i)_{i \in I}$ tetszőleges $\mathscr{T}$-ben haladó rendszer. A $\mathfrak{B}$ halmaz definíciója alapján

kiválaszthatunk olyan $((\Omega_{i,j})_{j\in J_i})_{i\in I}$ rendszert, hogy minden $i \in I$ és $j \in J_i$ esetén $\Omega_{i,j} \in \mathfrak{B}$, és minden $i \in I$ indexre $\Omega_i = \bigcup\limits_{j\in J_i} \Omega_{i,j}$. Ekkor

$$\bigcup_{i\in I} \Omega_i = \bigcup_{i\in I} \Big(\bigcup_{j\in J_i} \Omega_{i,j} \Big) = \bigcup_{(i,j)\in K} \Omega_{i,j},$$

ahol $K := \{(i,j) | (i \in I) \wedge (j \in J_i)\}$. A $\mathscr{T}$ halmaz definíciója szerint ez azt jelenti, hogy $\bigcup\limits_{i\in I} \Omega_i \in \mathscr{T}$, így $\mathscr{T}$-re $(\mathrm{O_{III}})$ teljesül.

Tehát $\mathscr{T}$ olyan topológa T felett, amelynek $\mathfrak{B}$ topologikus bázisa. ■

Az előző állítás alkalmazásaként értelmezhetjük a *rendezéstopológiákat.*

26.2.4. Állítás. *Ha E legalább két elemű lineárisan rendezett halmaz, akkor létezik egyetlen olyan E feletti topológia, amelynek topologikus bázisát alkotják E nyílt intervallumai. Ez a topológia Hausdorff-topológia.*

Bizonyítás. A nyílt intervallumok befedését alkotják E-nek, mert E legalább két elemű, és az E rendezése lineáris. Valóban, ha $x \in E$, akkor van olyan $y \in E$, amelyre $y \neq x$, és ekkor E rendezésének linearitása miatt $x < y$ (tehát $x \in]\leftarrow, y[$) vagy $x > y$ (tehát $x \in]y, \rightarrow[$). Továbbá, szintén az E rendezésének linearitásából következik, hogy két nyílt intervallum metszete is nyílt intervallum. Ezért az első állítás azonnal következik 26.2.3.-ból.

Legyenek $x, y \in E$ és $x \neq y$. Az E rendezése lineáris, ezért $x < y$ vagy $y < x$. Tegyük fel, hogy $x < y$. Ha $]x, y[= \emptyset$, akkor $]\leftarrow, y[$ környezete x-nek és $]x, \rightarrow[$ környezete y-nak, és $]\leftarrow, y[\cap]x, \rightarrow[=]x, y[= \emptyset$. Ha $]x, y[\neq \emptyset$ és $z \in]x, y[$, akkor $]\leftarrow, z[$ környezete x-nek és $]z, \rightarrow[$ környezete y-nak, és természetesen $]\leftarrow, z[\cap]z, \rightarrow[= \emptyset$. Tehát x-nek és y-nak léteznek diszjunkt környezetei E-ben. Ha $y < x$, akkor az előzőekből kapjuk, hogy az y és x pontoknak léteznek diszjunkt környezetei E-ben, tehát az E topologikus tér Hausdorff-tér. ■

Vigyázzunk arra, hogy ha E *egy elemű* rendezett halmaz, akkor egyáltalán nem létezik E-ben nem üres nyílt intervallum, így a nyílt intervallumok *nem fedik be* E-t. Másfelől, ha az E rendezett halmaz *nem lineárisan rendezett*, akkor két E-beli nyílt intervallum metszete nem szükségképpen nyílt intervallum. Ezért az előző állításban mindkét E-re vonatkozó feltétel lényeges.

26.2.5. Definíció. *Ha E legalább két elemű lineárisan rendezett halmaz, akkor E feletti* **rendezéstopológiának** *nevezzük azt az E feletti topológiát, amelynek topologikus bázisát alkotják E nyílt intervallumai.*

Megjegyezzük, hogy a valós számok rendezett halmazának rendezéstopológiája egyenlő az euklidészi topológiával, mert minden nyílt intervallum nyílt halmaz az euklidészi topológia szerint, és minden euklidészi topológia szerinti nyílt halmaz előáll nyílt intervallumok uniójaként.

26.2.6. Definíció. *Azt mondjuk, hogy a $(T, \mathscr{T})$ topologikus tér* $\mathrm{M_1}$**-tér**, *ha T minden pontjának létezik megszámlálható környezetbázisa $\mathscr{T}$ szerint. Azt mondjuk, hogy a $(T, \mathscr{T})$ topologikus tér* $\mathrm{M_2}$**-tér**, *vagy* **megszámlálható bázisú**, *ha a $\mathscr{T}$ topológiának létezik megszámlálható bázisa.*

Ha $(T, \mathscr{T})$ topologikus tér és $\mathfrak{B}$ bázisa a $\mathscr{T}$ topológiának, akkor nyilvánvaló, hogy minden $t \in T$ esetén az $\{\Omega \in \mathfrak{B} | t \in \Omega\}$ halmaz a t pontnak környezetbázisa $\mathscr{T}$ szerint. Ebből következik, hogy minden M_2-tér M_1-tér.

Minden metrizálható topologikus tér M_1-tér, mert ha (M, d) metrikus tér és $(r_n)_{n \in \mathbb{N}}$ tetszőleges $\mathbb{R}_+^*$-ban haladó zérussorozat, akkor minden $T \ni t$-re a $\{\mathrm{B}_{r_n}(t; d) | n \in \mathbb{N}\}$ halmaz megszámlálható környezetbázisa t-nek a $\mathscr{T}_d$ topológia szerint.

Könnyű példát adni metrizálható topologikus térre, amely M_1-tér és nem M_2-tér: ilyet mutatunk majd be a 26.3.4. állítás után. A 28.5.1. tétel után majd példát látunk olyan topologikus térre, amely nem metrizálható M_1-tér és nem M_2-tér.

Létezik olyan topologikus tér, amely nem M_1-tér. Ilyenre példa minden nem félmetrizálható *topologikus vektortér.*

26.2.7. Definíció. *Legyen T halmaz.*

– *Egy $\mathfrak{F} \subseteq \mathscr{P}(T)$ halmazt* **szűrőnek** *nevezünk T felett, ha teljesülnek rá a következő állítások.*

$(\mathrm{FT_I})$ *$\mathfrak{F} \neq \emptyset$ és minden $V \in \mathfrak{F}$ esetén $V \neq \emptyset$, vagyis $\emptyset \notin \mathfrak{F}$.*

$(\mathrm{FT_{II}})$ *Minden $V, V' \in \mathfrak{F}$ esetén $V \cap V' \in \mathfrak{F}$.*

$(\mathrm{FT_{III}})$ *Minden $E \subseteq T$ halmazra, ha van olyan $V \in \mathfrak{F}$, hogy $V \subseteq E$, akkor $E \in \mathfrak{F}$.*

– *Egy $\mathfrak{R} \subseteq \mathscr{P}(T)$ halmazt* **rácsnak** *nevezünk T felett, ha teljesülnek rá a következő állítások.*

$(\mathrm{R_I})$ *$\mathfrak{R} \neq \emptyset$ és minden $R \in \mathfrak{R}$ esetén $R \neq \emptyset$, vagyis $\emptyset \notin \mathfrak{R}$.*

$(\mathrm{R_{II}})$ *Minden $R, R' \in \mathfrak{R}$ halmazhoz van olyan $S \in \mathfrak{R}$, hogy $S \subseteq R \cap R'$.*

26.2.8. Állítás. *Legyen $(T, \mathscr{T})$ topologikus tér. Ha $t \in T$, akkor $\mathscr{T}(t)$ olyan szűrő T felett, hogy minden $\mathscr{T}(t) \ni V$-re $t \in V$. Ha $t \in T$, akkor a t pont minden $\mathscr{T}$ szerinti $\mathfrak{B}$ környezetbázisa olyan rács T felett, amelyre minden $V \in \mathfrak{B}$ esetén $t \in V$.*

Bizonyítás. $(\mathrm{FT_I})$ és $(\mathrm{FT_{III}})$ a $\mathscr{T}(t)$ definíciójából következik, míg $(\mathrm{FT_{II}})$ azon múlik, hogy két $\mathscr{T}$-nyílt halmaz metszete szintén $\mathscr{T}$-nyílt. Ha $\mathfrak{B}$ környezetbázisa a $t \in T$ pontnak a $\mathscr{T}$ topológia szerint, akkor $V, V' \in \mathfrak{B}$ esetén léteznek olyan Ω és Ω' $\mathscr{T}$-nyílt halmazok, hogy $t \in \Omega \subseteq V$ és $t \in \Omega' \subseteq V'$. Ekkor $t \in \Omega \cap \Omega' \in \mathscr{T}$, tehát $\Omega \cap \Omega' \in \mathscr{T}(t)$, így van olyan $W \in \mathfrak{B}$, hogy $W \subseteq \Omega \cap \Omega'$, így $W \subseteq V \cap V'$. Ebből következik, hogy a $\mathfrak{B}$ halmaz rács. ■

Ha $(T, \mathscr{T})$ topologikus tér, akkor a definíciók alapján nyilvánvaló, hogy

$$\mathscr{T} = \{\Omega \in \mathscr{P}(T) \mid (\forall\, t \in \Omega) : \Omega \in \mathscr{T}(t)\}.$$

Valóban, ha $\Omega \in \mathscr{T}$, akkor minden $t \in \Omega$ esetén, a $\mathscr{T}(t)$ értelmezése alapján, $\Omega \in \mathscr{T}(t)$ teljesül. Megfordítva, ha $\Omega \subseteq T$ olyan halmaz, hogy minden $t \in \Omega$ esetén $\Omega \in \mathscr{T}(t)$, akkor kiválasztható olyan $(\Omega_t)_{t \in \Omega}$ rendszer, amelynek mindegyik tagja eleme $\mathscr{T}$-nek és minden $\Omega \ni t$-re $t \in \Omega_t \subseteq \Omega$; ekkor $\Omega = \bigcup_{t \in \Omega} \Omega_t$ teljesül, tehát az $(\mathrm{O_{III}})$ alapján $\Omega \in \mathscr{T}$. Ez azt jelenti, hogy a topológiát egyértelműen meghatározzák a pontok környezetei. Felvetődik a kérdés, hogy ha minden $t \in T$ ponthoz hozzárendelünk egy T feletti $\mathfrak{F}_t$ szűrőt úgy, hogy minden $t \in T$ és $V \in \mathfrak{F}_t$ esetén $t \in V$, akkor létezik-e olyan T feletti $\mathscr{T}$ topológia, hogy minden $T \ni t$-re $\mathscr{T}(t) = \mathfrak{F}_t$. Erre a kérdésre ad választ a következő állítás.

26.2.9. Állítás. *Legyen T halmaz és $(\mathfrak{F}_t)_{t\in T}$ olyan rendszer, hogy minden $t \in T$ esetén $\mathfrak{F}_t$ szűrő T felett és minden $\mathfrak{F}_t \ni V$-re $t \in V$. Akkor és csak akkor létezik olyan T feletti $\mathscr{T}$ topológia, amelyre minden $t \in T$ esetén $\mathscr{T}(t) = \mathfrak{F}_t$, ha teljesül a következő állítás:*

$$(\forall\ t \in T)(\forall\ V \in \mathfrak{F}_t)(\exists\ V' \in \mathfrak{F}_t)(\forall\ t' \in V') : V \in \mathfrak{F}_{t'}.$$

Ha ez a feltétel teljesül, akkor a

$$\mathscr{T} := \{\Omega \in \mathscr{P}(T) \mid (\forall\ t \in \Omega) : \Omega \in \mathfrak{F}_t\}$$

halmaz az egyetlen olyan T feletti topológia, amelyre minden $t \in T$ esetén $\mathscr{T}(t) = \mathfrak{F}_t$.

Bizonyítás. A feltétel *szükséges*, mert ha $\mathscr{T}$ olyan topológia T felett, hogy minden $T \ni t$-re $\mathscr{T}(t) = \mathfrak{F}_t$, akkor $t \in T$ és $V \in \mathfrak{F}_t$ esetén van olyan $\Omega \in \mathscr{T}$, hogy $t \in \Omega \subseteq V$, és ekkor minden $\Omega \ni t'$-re $\Omega \in \mathscr{T}(t') = \mathfrak{F}_{t'}$, tehát $V \in \mathfrak{F}_{t'}$, ami azt jelenti, hogy a $V' := \Omega$ halmazra $V' \in \mathfrak{F}_t$ és minden $V' \ni t'$-re $V \in \mathfrak{F}_{t'}$.
A feltétel *elégségességének* bizonyításához értelmezzük a $\mathscr{T}$ halmazt az állításban megfogalmazott módon. Világos, hogy $T \in \mathscr{T}$, mert minden $t \in T$ esetén $T \in \mathfrak{F}_t$ (a szűrők definíciója alapján). Ha $(\Omega_i)_{i\in I}$ tetszőleges rendszer $\mathscr{T}$-ben és $t \in \bigcup_{i\in I} \Omega_i$, akkor van olyan $j \in I$, hogy $t \in \Omega_j$ és $\mathfrak{F}_t$ szűrő T felett, így $\Omega_j \subseteq \bigcup_{i\in I} \Omega_i$ miatt $\bigcup_{i\in I} \Omega_i \in \mathfrak{F}_t$; ezért $\bigcup_{i\in I} \Omega_i \in \mathscr{T}$. Ha $(\Omega_i)_{i\in I}$ tetszőleges nem üres véges rendszer $\mathscr{T}$-ben és $t \in \bigcap_{i\in I} \Omega_i$, akkor minden $I \ni i$-re $\Omega_i \in \mathfrak{F}_t$, így $\bigcap_{i\in I} \Omega_i \in \mathfrak{F}_t$, hiszen $\mathfrak{F}_t$ szűrő T felett; ezért $\bigcap_{i\in I} \Omega_i \in \mathscr{T}$. Ez azt jelenti, hogy $\mathscr{T}$ topológia T felett.

A $\mathscr{T}$ topológia, valamint a környezetszűrők definíciója alapján nyilvánvaló, hogy $t \in T$ esetén $\mathscr{T}(t) \subseteq \mathfrak{F}_t$. Valóban, ha $V \in \mathscr{T}(t)$, akkor van olyan $\Omega \in \mathscr{T}$, hogy $t \in \Omega \subseteq V$, tehát $\Omega \in \mathfrak{F}_t$, így $V \in \mathfrak{F}_t$, mert $\mathfrak{F}_t$ szűrő T felett.

Megmutatjuk, hogy $t \in T$ esetén $\mathfrak{F}_t \subseteq \mathscr{T}(t)$. Legyen $V \in \mathfrak{F}_t$ és értelmezzük az $\Omega := \{t' \in T | V \in \mathfrak{F}_{t'}\}$ halmazt. Ha teljesülne az, hogy $t \in \Omega \subseteq V$ és $\Omega \in \mathscr{T}$, akkor $V \in \mathscr{T}(t)$ is igaz volna (amit bizonyítani kell). A definíció és $V \in \mathfrak{F}_t$ miatt $t \in \Omega$. Ha $t' \in \Omega$, akkor $V \in \mathfrak{F}_{t'}$, ezért $t' \in V$, vagyis $\Omega \subseteq V$. Az $\Omega \in \mathscr{T}$ összefüggés bizonyításához legyen $t' \in \Omega$ tetszőleges. Ekkor $V \in \mathfrak{F}_{t'}$, ezért a hipotézist alkalmazva a t' pontra és a V halmazra kapjuk olyan $V' \in \mathfrak{F}_{t'}$ létezését, amelyre minden $t'' \in V'$ esetén $V \in \mathfrak{F}_{t''}$, azaz $t'' \in \Omega$. Tehát $V' \in \mathfrak{F}_{t'}$ olyan, hogy $V' \subseteq \Omega$, így $\Omega \in \mathfrak{F}_{t'}$, mert $\mathfrak{F}_{t'}$ szűrő T felett. Ez azt jelenti, hogy minden $t' \in \Omega$ esetén $\Omega \in \mathfrak{F}_{t'}$, tehát $\Omega \in \mathscr{T}$.

Végül, a környezetek egyértelműen meghatározzák a topológiát, ezért legfeljebb egy olyan T feletti $\mathscr{T}$ topológia létezhet, amelyre minden $t \in T$ esetén $\mathscr{T}(t) = \mathfrak{F}_t$. ■

26.3. Halmaz belseje és lezártja

26.3.1. Állítás. *Legyen $(T, \mathscr{T})$ topologikus tér. Minden $E \subseteq T$ halmazhoz létezik olyan tartalmazás tekintetében legnagyobb (illetve legkisebb) $\mathscr{T}$-nyílt (illetve $\mathscr{T}$-zárt) halmaz, amely része E-nek (illetve tartalmazza E-t).*

Bizonyítás. Az E által tartalmazott $\mathscr{T}$-nyílt halmazok uniója $\mathscr{T}$-nyílt, és a tartalmazás tekintetében ez a legnagyobb mindazon $\mathscr{T}$-nyílt halmazok közül, amelyek részhalmazai E-nek. Az E halmazt tartalmazó $\mathscr{T}$-zárt halmazok metszete $\mathscr{T}$-zárt, és a tartalmazás tekintetében ez a legkisebb mindazon $\mathscr{T}$-zárt halmazok közül, amelyeknek E részhalmaza. ■

26.3.2. Definíció. *Legyen $(T, \mathscr{T})$ topologikus tér és $E \subseteq T$. Az E halmaz* **belsejének** (*illetve* **lezártjának**) *nevezzük a $\mathscr{T}$ topológia szerint a tartalmazás tekintetében legnagyobb (illetve legkisebb) $\mathscr{T}$-nyílt (illetve $\mathscr{T}$-zárt) halmazt, amely része E-nek (illetve tartalmazza E-t). Az E halmaz $\mathscr{T}$ szerinti belsejét (illetve lezártját) az* $\mathrm{Int}(E)$ *vagy* $\overset{\circ}{E}$ (*illetve* $\mathrm{Cl}(E)$ *vagy* $\overline{E}$) *szimbólum jelöli. Az* $\mathrm{Int}(E)$ (*illetve* $\mathrm{Cl}(E)$) *elemeit az E halmaz* **belső pontjainak** (*illetve* **érintési pontjainak**) *nevezzük a $\mathscr{T}$ topológia szerint. Az $\overline{E} \setminus \overset{\circ}{E}$ halmazt az E* **határának** *nevezzük a $\mathscr{T}$ topológia szerint, és az* $\mathrm{Fr}(E)$ *vagy* $\overset{\bullet}{E}$ *szimbólummal jelöljük. Azt mondjuk, hogy a $t \in T$ pont* **torlódási pontja** *E-nek a $\mathscr{T}$ topológia szerint, ha $t \in \overline{E \setminus \{t\}}$.*

Megjegyezzük, hogy ha $(T, \mathscr{T})$ topologikus tér és $E \subseteq T$, akkor

$$\overset{\circ}{E} = \{t \in T \mid (\exists\, V \in \mathscr{T}(t)) : V \subseteq E\},$$
$$\overline{E} = \{t \in T \mid (\forall\, V \in \mathscr{T}(t)) : V \cap E \neq \emptyset\}.$$

Ezek az egyenlőségek a környezetek értelmezése valamint az előző definíció alapján könnyen bizonyíthatók. Az is könnyen belátható, hogy ha $(T, \mathscr{T})$ topologikus tér és $E \subseteq T$, akkor

$$\overset{\circ}{E} = T \setminus \overline{T \setminus E}, \qquad \overline{E} = T \setminus (\overset{\circ}{\overbrace{T \setminus E}}),$$

továbbá, ha $(E_i)_{i \in I}$ a T részhalmazainak tetszőleges nem üres *véges* rendszere, akkor

$$\overset{\circ}{\overbrace{\bigcap_{i \in I} E_i}} = \bigcap_{i \in I} \overset{\circ}{E}_i, \qquad \overline{\bigcup_{i \in I} E_i} = \bigcup_{i \in I} \overline{E}_i,$$

és ez utóbbi összefüggés természetesen $I = \emptyset$ esetén is (triviálisan) igaz.

26.3.3. Definíció. *Ha $(T, \mathscr{T})$ topologikus tér, akkor az $E \subseteq T$ halmazt* **sűrűnek** *nevezzük a $\mathscr{T}$ topológia szerint, ha $\overline{E} = T$. A $(T, \mathscr{T})$ topologikus teret* **szeparábilisnak** *nevezzük, ha létezik T-nek megszámlálható sűrű részhalmaza.*

26.3.4. Állítás. *Metrizálható topologikus tér pontosan akkor szeparábilis, ha megszámlálható bázisú.*

Bizonyítás. Tegyük fel, hogy (M, d) szeparábilis metrikus tér, és legyen $D \subseteq M$ olyan megszámlálható halmaz, amelyre $\overline{D} = M$. Legyen $(r_n)_{n \in \mathbb{N}}$ tetszőleges olyan $\mathbb{R}_+^*$-ban haladó sorozat, amelyre $\inf_{n \in \mathbb{N}} r_n = 0$. Értelmezzük az

$$\mathfrak{S} := \{\mathrm{B}_{r_n}(\mathfrak{a}; d) | (n \in \mathbb{N}) \wedge (\mathfrak{a} \in D)\}$$

halmazt. Ekkor $\mathfrak{S} \subseteq \mathscr{T}_d$, és $\mathfrak{S}$ megszámlálható, mert az

$$\mathbb{N} \times D \to \mathfrak{S}; \quad (n, \mathfrak{a}) \mapsto \mathrm{B}_{r_n}(\mathfrak{a}; d)$$

leképezés szürjekció, és az $\mathbb{N} \times D$ halmaz megszámlálható. Könnyen látható, hogy az M minden d szerint nyílt részhalmaza előáll $\mathfrak{S}$-ben haladó rendszer uniójaként.

Valóban, legyen $\Omega \in \mathscr{T}_d$ és $x \in \Omega$. Vehetünk olyan $r > 0$ valós számot, amelyre

$\mathrm{B}_r(x;d) \subseteq \Omega$; ekkor $\inf_{n\in\mathbb{N}} r_n = 0$ miatt van olyan $n \in \mathbb{N}$, amelyre $r_n < r/2$. A D halmaz sűrű d szerint, így $\mathrm{B}_{r_n}(x;d) \cap D \neq \emptyset$; legyen $\mathfrak{a}$ eleme ennek a metszetnek. Ekkor $\mathrm{B}_{r_n}(\mathfrak{a};d) \in \mathfrak{S}$, és

$$x \in \mathrm{B}_{r_n}(\mathfrak{a};d) \subseteq \mathrm{B}_r(x;d) \subseteq \Omega,$$

hiszen $y \in \mathrm{B}_{r_n}(\mathfrak{a};d)$ esetén $d(y,x) \leq d(y,\mathfrak{a}) + d(\mathfrak{a},x) < 2\cdot r_n < r$. Ez azt jelenti, hogy ha $I := \{H \in \mathfrak{S} | H \subseteq \Omega\}$, akkor $\Omega = \bigcup_{H\in I} H$.

Megfordítva, tegyük fel, hogy $\mathfrak{S} \subseteq \mathscr{T}_d$ olyan megszámlálható halmaz, hogy az M minden d szerint nyílt részhalmaza előáll $\mathfrak{S}$-ben haladó rendszer uniójaként. Legyen $\mathfrak{S}_0 := \mathfrak{S} \setminus \{\emptyset\}$, és tekintsük az $(S)_{S\in\mathfrak{S}_0}$ halmazrendszert, amelynek minden tagja nem üres halmaz. A kiválasztási axióma szerint vehetünk egy

$$f \in \prod_{S\in\mathfrak{S}_0} S$$

kiválasztó-függvényt. Ekkor $\mathrm{Im}(f)$ megszámlálható halmaz, mert $\mathrm{Dom}(f) = \mathfrak{S}_0$ megszámlálható. Továbbá $\mathrm{Im}(f)$ sűrű d szerint, mert ha $x \in M$ és Ω az x-nek nyílt környezete, akkor a feltevés szerint van olyan $S \in \mathfrak{S}$ halmaz, amelyre $x \in S \subseteq \Omega$; ekkor $S \in \mathfrak{S}_0$ és $f(S) \in S$, vagyis $f(S) \in \mathrm{Im}(f) \cap \Omega$. ■

Könnyen látható, hogy minden megszámlálható bázisú topologikus tér szeparábilis. Valóban, ha a $(T,\mathscr{T})$ topologikus tér M_2-tér és $\mathfrak{B} \subseteq \mathscr{T}$ megszámlálható bázis, akkor a $\mathfrak{B}_0 := \mathfrak{B} \setminus \{\emptyset\}$ halmazra a kiválasztási axióma alapján $\prod_{\Omega\in\mathfrak{B}_0} \Omega \neq \emptyset$, és ha f eleme ennek a szorzathalmaznak, akkor $\mathrm{Im}(f)$ megszámlálható és sűrű részhalmaza T-nek. Ugyanis $t \in T$ és $V \in \mathscr{T}(t)$ esetén van olyan $\Omega \in \mathscr{T}$, hogy $t \in \Omega \subseteq V$, tehát van olyan $\Omega' \in \mathfrak{B}$, hogy $t \in \Omega' \subseteq \Omega$, így $\Omega' \in \mathfrak{B}_0$ és $f(\Omega') \in \Omega'$, vagyis $f(\Omega') \in V \cap \mathrm{Im}(f)$.

Megjegyezzük, hogy létezik olyan (szükségképpen nem metrizálható) topologikus tér, amely szeparábilis, de nem megszámlálható bázisú. Ilyen térre példát látunk majd a 28.5.1. tétel után.

Ha T nem megszámlálhatóan végtelen halmaz, akkor a T halmaz feletti $\mathscr{T}_{dis}(T)$ diszkrét topológia (teljesen) metrizálható, és $(T,\mathscr{T}_{dis}(T))$ nyilvánvalóan M_1-tér, de T-nek nincs olyan megszámlálható részhalmaza, amely sűrű volna $\mathscr{T}_{dis}(T)$ szerint, hiszen T minden részhalmaza $\mathscr{T}_{dis}(T)$-zárt, ezért 26.3.4. alapján $(T,\mathscr{T}_{dis}(T))$ nem M_2-tér.

26.3.5. Definíció. *Legyen $(T,\mathscr{T})$ topologikus tér és $(T_i)_{i\in I}$ a T részhalmazainak rendszere. Azt mondjuk, hogy $(T_i)_{i\in I}$* **pontonként véges**, *ha minden $T \ni t$-re az $\{i \in I | t \in T_i\}$ halmaz véges. Azt mondjuk, hogy $(T_i)_{i\in I}$* **lokálisan véges** *a $\mathscr{T}$ topológia szerint, ha minden $T \ni t$-nek van olyan V környezete $\mathscr{T}$ szerint, hogy az $\{i \in I | T_i \cap V \neq \emptyset\}$ halmaz véges.*

26.3.6. Állítás. *Ha $(T,\mathscr{T})$ topologikus tér és $(E_i)_{i\in I}$ a T halmaz részhalmazainak lokálisan véges rendszere, akkor*

$$\overline{\bigcup_{i\in I} E_i} = \bigcup_{i\in I} \overline{E_i}.$$

Bizonyítás. Minden $i \in I$ esetén $E_i \subseteq \overline{E_i}$, ezért nyilvánvaló, hogy $\bigcup_{i\in I} \overline{E_i} \subseteq \overline{\bigcup_{i\in I} E_i}$, még akkor is, ha az $(E_i)_{i\in I}$ halmazrendszer nem lokálisan véges.

Megfordítva, legyen $t \in \overline{\bigcup_{i\in I} E_i}$. Az $(E_i)_{i\in I}$ halmazrendszer lokálisan véges, ezért vehetünk olyan $V \in \mathscr{T}(t)$ környezetet, amelyre $I_* := \{i \in I | V \cap E_i \neq \emptyset\}$ véges halmaz. Ha $U \in \mathscr{T}(t)$ tetszőleges, akkor $U \cap V \in \mathscr{T}(t)$, így $t \in \overline{\bigcup_{i\in I} E_i}$ miatt

$$\emptyset \neq (U \cap V) \cap \bigcup_{i\in I} E_i = U \cap \bigcup_{i\in I} (V \cap E_i) = U \cap \bigcup_{i\in I_*} (V \cap E_i),$$

ami azt jelenti, hogy

$$t \in \overline{\bigcup_{i\in I_*} (V \cap E_i)} = \bigcup_{i\in I_*} \overline{V \cap E_i} \subseteq \bigcup_{i\in I_*} \overline{E_i} \subseteq \bigcup_{i\in I} \overline{E_i},$$

ahol az első egyenlőségnél felhasználtuk azt, hogy I_* véges. Ezért $\overline{\bigcup_{i\in I} E_i} \subseteq \bigcup_{i\in I} \overline{E_i}$ is teljesül. ■

26.3.7. Következmény. *Ha $(T, \mathscr{T})$ topologikus tér és $(F_i)_{i\in I}$ a T halmaz $\mathscr{T}$-zárt részhalmazainak lokálisan véges rendszere, akkor az $\bigcup_{i\in I} F_i$ halmaz is $\mathscr{T}$-zárt.* ■

26.3.8. Definíció. *Ha $(T, \mathscr{T})$ topologikus tér, akkor az $E \subseteq T$ halmazt* **lokálisan zártnak** *nevezzük a $\mathscr{T}$ topológia szerint, ha minden $t \in E$ esetén létezik olyan $V \in \mathscr{T}(t)$ környezet, hogy $V \cap E$ zárt halmaz V-ben a $\mathscr{T}|V$ altértopológia szerint, vagyis $\overline{V \cap E} \cap V = V \cap E$.*

A definíció alapján nyilvánvaló, hogy minden zárt halmaz és minden nyílt halmaz lokálisan zárt.

26.3.9. Állítás. *Ha $(T, \mathscr{T})$ topologikus tér, és $E \subseteq T$ lokálisan zárt halmaz a $\mathscr{T}$ topológia szerint, akkor létezik olyan $\Omega \in \mathscr{T}$, hogy $\Omega \cap \overline{E} = E$ (ezért E előáll egy $\mathscr{T}$-nyílt és egy $\mathscr{T}$-zárt halmaz metszeteként).*

Bizonyítás. Az E halmaz lokális zártsága miatt kiválaszthatunk olyan $(V_t)_{t\in E}$ halmazrendszert, hogy minden $t \in E$ esetén $V_t \in \mathscr{T}(t)$ és $\overline{V_t \cap E} \cap V_t = V_t \cap E$. Ekkor a környezetek definíciója szerint kiválaszthatunk olyan $(\Omega_t)_{t\in E}$ halmazrendszert, hogy minden $t \in E$ esetén $t \in \Omega_t \in \mathscr{T}$ és $\Omega_t \subseteq V_t$. Legyen $\Omega := \bigcup_{t\in E} \Omega_t$, és megmutatjuk, hogy $\Omega \cap \overline{E} = E$.

Legyen $t \in \Omega \cap \overline{E}$. Ekkor Ω definíciója szerint rögzíthetünk egy $s \in E$ pontot, amelyre $t \in \Omega_s$. Ha $V \in \mathscr{T}(t)$ tetszőleges környezet, akkor $V \cap \Omega_s \in \mathscr{T}(t)$ is teljesül, így $t \in \overline{E}$ miatt $\emptyset \neq (V \cap \Omega_s) \cap E = V \cap (\Omega_s \cap E)$, ezért $t \in \overline{\Omega_s \cap E}$. Ebből $\Omega_s \subseteq V_s$ miatt következik, hogy $t \in \overline{V_s \cap E} \cap V_s = V_s \cap E$, tehát $t \in E$. Ez azt jelenti, hogy $\Omega \cap \overline{E} \subseteq E$, és az $E \subseteq \Omega \cap \overline{E}$ összefüggés nyilvánvalóan igaz. ■

26.3.10. Következmény. *Topologikus térben egy halmaz pontosan akkor lokálisan zárt, ha előáll egy nyílt halmaz és egy zárt halmaz metszeteként.*

Bizonyítás. A feltétel az előző állítás szerint szükséges. Az elégségesség bizonyításához legyen $(T, \mathscr{T})$ topologikus tér, $\Omega \subseteq T$ $\mathscr{T}$-nyílt és $F \subseteq T$ $\mathscr{T}$-zárt halmaz, valamint $E := \Omega \cap F$. Legyen $t \in E$. Ekkor $t \in \Omega \in \mathscr{T}$ miatt $\Omega \in \mathscr{T}(t)$, továbbá $E \subseteq \Omega$ és $\overline{E} \subseteq F$ miatt $\overline{\Omega \cap E} \cap \Omega = \overline{E} \cap \Omega \subseteq F \cap \Omega = E = \Omega \cap E$, ezért $\overline{\Omega \cap E} \cap \Omega = \Omega \cap E$. Ez azt jelenti, hogy E lokálisan zárt halmaz a $\mathscr{T}$ topológia szerint. ■

26.4. Folytonos függvények

26.4.1. Definíció. *Legyenek* $(T, \mathscr{T})$ *és* $(T', \mathscr{T}')$ *topologikus terek. Egy* $f : T \to T'$ *függvényt* **folytonosnak** *nevezünk a* $t \in T$ *pontban a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, ha minden* $V' \in \mathscr{T}'(f(t))$ *környezethez van olyan* $V \in \mathscr{T}(t)$*, amelyre* $f\langle V\rangle \subseteq V'$ *teljesül. Azt mondjuk, hogy az* $f : T \to T'$ *függvény* **folytonos** *a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, ha* f *a* T *minden pontjában folytonos a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint. A* T*-n értelmezett,* T'*-be érkező,* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint folytonos függvények halmazát* $\mathscr{C}(T, \mathscr{T}; T', \mathscr{T}')$ *jelöli.*

Ha $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek, akkor a $\mathscr{C}(T, \mathscr{T}; T', \mathscr{T}')$ jelölés helyett az egyszerűbb $\mathscr{C}(T; T')$ jelölést is alkalmazzuk, ha világos, hogy mely topológiák szerint folytonos függvények halmazáról van szó.

26.4.2. Állítás. (A folytonosság lokalitása) *Legyenek* $(T, \mathscr{T})$ *és* $(T', \mathscr{T}')$ *topologikus terek, valamint* $f, g : T \to T'$ *függvények. Legyen* $t \in T$ *olyan pont, amelyhez van olyan* $V \in \mathscr{T}(t)$*, amelyre* $f = g$ *a* V *halmazon. Az* f *függvény pontosan akkor folytonos a* t *pontban a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, ha* g *folytonos a* t *pontban a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint.*

Bizonyítás. Tegyük fel, hogy f folytonos a t pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, és legyen $V_t \in \mathscr{T}(t)$ olyan, hogy $f = g$ a V_t halmazon. Ha $V' \in \mathscr{T}'(g(t))$, akkor $g(t) = f(t)$ miatt $V' \in \mathscr{T}'(f(t))$, tehát létezik olyan $V \in \mathscr{T}(t)$, amelyre $f\langle V\rangle \subseteq V'$; ekkor $V \cap V_t \in \mathscr{T}(t)$ és $f = g$ a $V \cap V_t$ halmazon, így $g\langle V \cap V_t\rangle = f\langle V \cap V_t\rangle \subseteq f\langle V\rangle \subseteq V'$, vagyis g folytonos a t pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint. ■

26.4.3. Állítás. *Legyenek* $(T, \mathscr{T})$, $(T', \mathscr{T}')$ *és* $(T'', \mathscr{T}'')$ *topologikus terek, valamint* $f : T \to T'$ *és* $g : T' \to T''$ *függvények. Ha* f *folytonos a* $t \in T$ *pontban a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, valamint* g *folytonos az* $f(t)$ *pontban a* $\mathscr{T}'$ *és* $\mathscr{T}''$ *topológiák szerint, akkor* $g \circ f$ *folytonos a* t *pontban a* $\mathscr{T}$ *és* $\mathscr{T}''$ *topológiák szerint. Ha* f *folytonos a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint és* g *folytonos a* $\mathscr{T}'$ *és* $\mathscr{T}''$ *topológiák szerint, akkor* $g \circ f$ *folytonos a* $\mathscr{T}$ *és* $\mathscr{T}''$ *topológiák szerint.*

Bizonyítás. A második állítás nyilvánvalóan következik az elsőből. Az első állítás bizonyításához legyen $V'' \in \mathscr{T}''((g \circ f)(t))$ tetszőleges. A g függvény folytonos az $f(t)$ pontban a $\mathscr{T}'$ és $\mathscr{T}''$ topológiák szerint, ezért van olyan $V' \in \mathscr{T}'(f(t))$, hogy $g\langle V'\rangle \subseteq V''$. Ha V' ilyen környezet, akkor van olyan $V \in \mathscr{T}(t)$, hogy $f\langle V\rangle \subseteq V'$, mert f folytonos a t pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint. Ekkor $(g \circ f)\langle V\rangle = g\langle f\langle V\rangle\rangle \subseteq g\langle V'\rangle \subseteq V''$, tehát $g \circ f$ folytonos a t pontban a $\mathscr{T}$ és $\mathscr{T}''$ topológiák szerint. ■

26.4.4. Definíció. *Ha* $(T, \mathscr{T})$ *és* $(T', \mathscr{T}')$ *topologikus terek, akkor egy* $f : T \to T'$ *függvényt* **homeomorfizmusnak** *nevezünk a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, ha* f *bijekció, és* f *folytonos a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, valamint* f^{-1} *folytonos a* $\mathscr{T}'$ *és* $\mathscr{T}$ *topológiák szerint. A* $(T, \mathscr{T})$ *és* $(T', \mathscr{T}')$ *topologikus tereket* **homeomorfaknak** *nevezzük, ha létezik olyan* $f : T \to T'$ *függvény, amely homeomorfizmus a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint.*

Könnyen látható, hogy a topologikus terek bármely halmazán a homeomorfia ekvivalencia-reláció, ugyanis

– a $(T, \mathscr{T})$ topologikus tér homeomorf önmagával, mert az $\mathrm{id}_T : T \to T$ függvény homeomorfizmus a $\mathscr{T}$ és $\mathscr{T}$ topológiák szerint (a homeomorfia *reflexív*);

– ha a $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek homeomorfak és $f : T \to T'$ homeomorfizmus a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, akkor az $f^{-1} : T' \to T$ függvény homeomorfizmus a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, így a $(T', \mathscr{T}')$ és $(T, \mathscr{T})$ topologikus terek homeomorfak (a homeomorfia *szimmetrikus*);

– ha a $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek homeomorfak, valamint a $(T', \mathscr{T}')$ és $(T'', \mathscr{T}'')$ topologikus terek homeomorfak, akkor van olyan $f : T \to T'$ függvény, amely homeomorfizmus a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, valamint van olyan $g : T' \to T''$ függvény, amely homeomorfizmus a $\mathscr{T}'$ és $\mathscr{T}''$ topológiák szerint; ekkor a $g \circ f : T \to T''$ függvény homeomorfizmus a $\mathscr{T}$ és $\mathscr{T}''$ topológiák szerint, tehát a $(T, \mathscr{T})$ és $(T'', \mathscr{T}'')$ topologikus terek homeomorfak (a homeomorfia *tranzitív*).

26.4.5. Állítás. (A folytonosság topologikus jellemzése) *Ha $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek, akkor minden $f : T \to T'$ függvényre a következő kijelentések ekvivalensek.*

(i) *f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint.*

(ii) *Minden $\Omega' \in \mathscr{T}'$ halmazra $\overset{-1}{f}\langle \Omega' \rangle \in \mathscr{T}$ teljesül (vagy ami ugyanaz: $\overset{-1}{f}[\mathscr{T}'] \subseteq \mathscr{T}$).*

(iii) *Minden $F' \subseteq T'$ $\mathscr{T}'$-zárt halmazra az $\overset{-1}{f}\langle F' \rangle \subseteq T$ halmaz $\mathscr{T}$-zárt.*

(iv) *Minden $E \subseteq T$ halmazra $f\langle \overline{E} \rangle \subseteq \overline{f\langle E \rangle}$.*

(v) *Minden $t \in T$ pontra és minden $V' \in \mathscr{T}'(f(t))$ környezetre $\overset{-1}{f}\langle V' \rangle \in \mathscr{T}(t)$.*

Bizonyítás. (i)$\Rightarrow$(ii) Tegyük fel, hogy f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, és legyen $\Omega' \in \mathscr{T}'$ tetszőleges. Ha $t \in \overset{-1}{f}\langle \Omega' \rangle$, akkor $f(t) \in \Omega'$, ezért $\Omega' \in \mathscr{T}'$ miatt $\Omega' \in \mathscr{T}'(f(t))$, így az f függvény t pontbeli folytonossága következtében létezik olyan $V \in \mathscr{T}(t)$, hogy $f\langle V \rangle \subseteq \Omega'$, vagyis $V \subseteq \overset{-1}{f}\langle \Omega' \rangle$. Ez azt jelenti, hogy az $\overset{-1}{f}\langle \Omega' \rangle$ halmaz minden pontja belső pont a $\mathscr{T}$ topológia szerint, tehát $\overset{-1}{f}\langle \Omega' \rangle \in \mathscr{T}$.

(ii)$\Rightarrow$(iii) Ha $F' \subseteq T'$ $\mathscr{T}'$-zárt halmaz, vagyis $T' \setminus F' \in \mathscr{T}'$, akkor (ii) miatt $T \setminus \overset{-1}{f}\langle F' \rangle = \overset{-1}{f}\langle T' \setminus F' \rangle \in \mathscr{T}$, vagyis az $\overset{-1}{f}\langle F' \rangle$ halmaz $\mathscr{T}$-zárt.

(iii)$\Rightarrow$(iv) Legyen $E \subseteq T$ tetszőleges halmaz. Azt kell igazolni, hogy (iii)-ból következik, hogy $\overline{E} \subseteq \overset{-1}{f}\langle \overline{f\langle E \rangle} \rangle$. Mivel $\overline{f\langle E \rangle}$ $\mathscr{T}'$-zárt részhalmaza T'-nek, így (iii) alapján $\overset{-1}{f}\langle \overline{f\langle E \rangle} \rangle$ $\mathscr{T}$-zárt halmaz. Halmaz lezártja egyenlő az azt tartalmazó zárt halmazok metszetével, ezért a bizonyítandó összefüggés ekvivalens az $E \subseteq \overset{-1}{f}\langle \overline{f\langle E \rangle} \rangle$ tartalmazással. Ez viszont nyilvánvalóan igaz, mert $f\langle E \rangle \subseteq \overline{f\langle E \rangle}$.

(iv)$\Rightarrow$(v) Legyen $t \in T$ és $V' \in \mathscr{T}'(f(t))$. Azt kell igazolni, hogy (iv) teljesülése esetén $\overset{-1}{f}\langle V' \rangle \in \mathscr{T}(t)$, vagy ami ugyanaz: $t \in \mathrm{Int}(\overset{-1}{f}\langle V' \rangle)$. Ehhez felhasználjuk azt, hogy

$$\mathrm{Int}(\overset{-1}{f}\langle V' \rangle) = T \setminus \overline{(T \setminus \overset{-1}{f}\langle V' \rangle)},$$

tehát az $t \in \mathrm{Int}(\overset{-1}{f}\langle V' \rangle)$ kijelentés ekvivalens azzal, hogy $t \notin \overline{T \setminus \overset{-1}{f}\langle V' \rangle}$. Az állítással ellentétben tegyük fel, hogy $t \in \overline{T \setminus \overset{-1}{f}\langle V' \rangle}$. Ekkor (iv) alapján

$$f(t) \in f\left\langle \overline{T \setminus \overset{-1}{f}\langle V' \rangle} \right\rangle \subseteq \overline{f\langle T \setminus \overset{-1}{f}\langle V' \rangle \rangle}.$$

A V' halmaz $f(t)$-nek környezete, ezért $V' \cap f\langle T \setminus \overset{-1}{f}\langle V'\rangle\rangle \neq \emptyset$. Ugyanakkor halmazelméleti trivialitás az, hogy ez a metszet üres, hiszen ha t' eleme ennek a halmaznak, akkor van olyan $s \in T \setminus \overset{-1}{f}\langle V'\rangle$, hogy $t' = f(s) \notin V'$ és $t' \in V'$, ami ellentmondás.

(v)⇒(i) Legyen $t \in T$ és $V' \in \mathscr{T}'(f(t))$. Ekkor (v) szerint $V := \overset{-1}{f}\langle V'\rangle \in \mathscr{T}(t)$, és nyilvánvaló, hogy $f\langle V\rangle \subseteq V'$, tehát f folytonos a t pontban. ■

26.4.6. Következmény. *Legyenek $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek és $f : T \to T'$ függvény.*

a) *Ha f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, akkor minden $E \subseteq T$ halmazra az $f|_E : E \to T'$ függvény folytonos a $\mathscr{T}|E$ és $\mathscr{T}'$ topológiák szerint.*

b) *Ha $(T_i)_{i\in I}$ a T halmaz részhalmazainak olyan rendszere, hogy a $\left(\overset{\circ}{T_i}\right)_{i\in I}$ halmazrendszer befedése T-nek (például $(T_i)_{i\in I}$ a T halmaznak $\mathscr{T}$-nyílt halmazokból álló befedése), és minden $I \ni i$-re az $f|_{T_i} : T_i \to T'$ függvény folytonos a $\mathscr{T}|T_i$ és $\mathscr{T}'$ topológiák szerint, akkor f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint.*

c) *Ha $(T_i)_{i\in I}$ a T halmaz $\mathscr{T}$-zárt részhalmazainak lokálisan véges befedése a $\mathscr{T}$ topológia szerint, és minden $I \ni i$-re az $f|_{T_i} : T_i \to T'$ függvény folytonos a $\mathscr{T}|T_i$ és $\mathscr{T}'$ topológiák szerint, akkor f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint.*

Bizonyítás. a) Tegyük fel, hogy f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, és legyen $E \subseteq T$ tetszőleges. Ha az $\Omega' \subseteq T'$ halmaz $\mathscr{T}'$-nyílt, akkor a folytonosság topologikus jellemzése alapján az $\overset{-1}{f}\langle\Omega'\rangle$ halmaz $\mathscr{T}$-nyílt, ugyanakkor nyilvánvalóan $\overset{-1}{f|_E}\langle\Omega'\rangle = E \cap \overset{-1}{f}\langle\Omega'\rangle$, tehát az altértopológia értelmezése alapján $\overset{-1}{f|_E}\langle\Omega'\rangle \in \mathscr{T}|E$. Ismét a folytonosság topologikus jellemzésére hivatkozva kapjuk, hogy az $f|_E : E \to T'$ függvény folytonos a $\mathscr{T}|E$ és $\mathscr{T}'$ topológiák szerint.

b) Tegyük fel, hogy $(T_i)_{i\in I}$ a T halmaz részhalmazainak olyan rendszere, hogy a $\left(\overset{\circ}{T_i}\right)_{i\in I}$ halmazrendszer befedése T-nek, és minden $I \ni i$-re az $f|_{T_i} : T_i \to T'$ függvény folytonos a $\mathscr{T}|T_i$ és $\mathscr{T}'$ topológiák szerint. Az a) állítás szerint minden $i \in I$ esetén az $f|_{\overset{\circ}{T_i}} : \overset{\circ}{T_i} \to T'$ függvény folytonos a $(\mathscr{T}|T_i)\,|\overset{\circ}{T_i}$ $(= \mathscr{T}|\overset{\circ}{T_i})$ és $\mathscr{T}'$ topológiák szerint. Ha az $\Omega' \subseteq T'$ halmaz $\mathscr{T}'$-nyílt, akkor a folytonosság topologikus jellemzése alapján minden $i \in I$ esetén az $\overset{-1}{f|_{\overset{\circ}{T_i}}}\langle\Omega'\rangle = \overset{\circ}{T_i} \cap \overset{-1}{f}\langle\Omega'\rangle$ halmaz $\mathscr{T}|\overset{\circ}{T_i}$-nyílt, és mivel az $\overset{\circ}{T_i}$ halmaz $\mathscr{T}$-nyílt, így $\mathscr{T}$-nyílt is. Ebből következik, hogy $\overset{-1}{f}\langle\Omega'\rangle = \bigcup_{i\in I}\left(\overset{\circ}{T_i} \cap \overset{-1}{f}\langle\Omega'\rangle\right)$ is nyílt halmaz a $\mathscr{T}$ topológia szerint, tehát a folytonosság topologikus jellemzése alapján az f függvény folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint.

c) Tegyük fel, hogy minden $I \ni i$-re az $f|_{T_i} : T_i \to T'$ függvény folytonos a $\mathscr{T}|T_i$ és $\mathscr{T}'$ topológiák szerint. Legyen $F' \subseteq T'$ tetszőleges $\mathscr{T}'$-zárt halmaz. Ekkor $\overset{-1}{f}\langle F'\rangle = \bigcup_{i\in I} \overset{-1}{f|_{T_i}}\langle F'\rangle$, és minden $i \in I$ esetén a folytonosság topologikus jellemzése alapján az $\overset{-1}{f|_{T_i}}\langle F'\rangle$ halmaz $\mathscr{T}|T_i$-zárt részhalmaza T_i-nek. De minden $I \ni i$-re T_i a T-nek $\mathscr{T}$-zárt részhalmaza, ezért az $\overset{-1}{f|_{T_i}}\langle F'\rangle$ halmaz $\mathscr{T}$-zárt is. Továbbá, a $(T_i)_{i\in I}$ rendszer lokálisan véges a $\mathscr{T}$ topológia szerint, és minden $i \in I$ esetén $\overset{-1}{f|_{T_i}}\langle F'\rangle \subseteq T_i$, így az $\left(\overset{-1}{f|_{T_i}}\langle F'\rangle\right)_{i\in I}$

halmazrendszer is lokálisan véges a $\mathscr{T}$ topológia szerint. Ezért $\bigcup_{i\in I} \overset{-1}{f|_{T_i}}\langle F'\rangle$ a T-nek $\mathscr{T}$-zárt részhalmaza, tehát a folytonosság topologikus jellemzése alapján az f függvény folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint. ■

26.4.7. Állítás. *Legyen $(T,\mathscr{T})$ topologikus tér és $(F,\|\cdot\|)$ normált tér $\mathbb{K}$ felett.*

a) *Ha az $f,g:T\to F$ függvények folytonosak a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{T}_{\|\cdot\|}$ topológiák szerint, akkor az $f+g:T\to F;\ t\mapsto f(t)+g(t)$ függvény folytonos a t_0 pontban a $\mathscr{T}$ és $\mathscr{T}_{\|\cdot\|}$ topológiák szerint.*

b) *Ha az $f:T\to F$ függvény folytonos a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{T}_{\|\cdot\|}$ topológiák szerint, valamint a $\lambda:T\to\mathbb{K}$ függvény folytonos a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{K}}$ topológiák szerint, akkor a $\lambda.f:T\to F;\ t\mapsto\lambda(t).f(t)$ függvény folytonos a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{T}_{\|\cdot\|}$ topológiák szerint.*

c) *Ha az $f:T\to F$ függvény folytonos a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{T}_{\|\cdot\|}$ topológiák szerint, akkor az $\|f\|:T\to\mathbb{R};\ t\mapsto\|f(t)\|$ függvény folytonos a t_0 pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.*

d) *Ha az $f:T\to\mathbb{K}$ függvény folytonos a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{K}}$ topológiák szerint és minden $t\in T$ esetén $f(t)\neq 0$, akkor az $1/f:T\to\mathbb{K};\ t\mapsto 1/f(t)$ függvény folytonos a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{K}}$ topológiák szerint.*

e) *Ha az $f,g:T\to\mathbb{R}$ függvények folytonosak a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, akkor a $\sup(f,g):T\to\mathbb{R};\ t\mapsto\max(f(t),g(t))$ és az $\inf(f,g):T\to\mathbb{R};\ t\mapsto\min(f(t),g(t))$ függvények folytonosak a $t_0\in T$ pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.*

Bizonyítás. Mindegyik esetre felírjuk azokat az egyenlőtlenségeket, amelyekből nyilvánvalóan következik az állítás.

a) Ha $t\in T$, akkor

$$\begin{aligned}\|(f+g)(t)-(f+g)(t_0)\| &:= \|(f(t)+g(t))-(f(t_0)+g(t_0))\|\le\\ &\le\|f(t)-f(t_0)\|+\|g(t)-g(t_0)\|.\end{aligned}$$

b) Ha $t\in T$, akkor

$$\begin{gathered}\|(\lambda.f)(t)-(\lambda.f)(t_0)\| := \|\lambda(t).f(t)-\lambda(t_0).f(t_0)\|\le\\ \le|\lambda(t)-\lambda(t_0)|\|f(t)-f(t_0)\|+|\lambda(t)-\lambda(t_0)|\|f(t_0)\|+|\lambda(t_0)|\|f(t)-f(t_0)\|.\end{gathered}$$

c) Ha $t\in T$, akkor

$$|\|f\|(t)-\|f\|(t_0)| := |\|f(t)\|-\|f(t_0)\|| \le \|f(t)-f(t_0)\|.$$

d) Ha $t\in T$, akkor

$$|(1/f)(t)-(1/f)(t_0)| := \left|\frac{1}{f(t)}-\frac{1}{f(t_0)}\right| = \frac{|f(t_0)-f(t)|}{|f(t)||f(t_0)|}.$$

Az f függvény folytonos a t_0 pontban és $|f(t_0)|>0$, ezért bármely $c\in]0,|f(t_0)|[$ rögzített számhoz létezik olyan $V\in\mathscr{T}(t_0)$, hogy minden $V\ni t$-re $|f(t_0)|-|f(t)|\le|f(t_0)-f(t)|<c$, így $|f(t)|>|f(t_0)|-c$, vagyis

$$|(1/f)(t)-(1/f)(t_0)|\le\frac{|f(t_0)-f(t)|}{(|f(t_0)|-c)\,|f(t_0)|}.$$

Tehát, ha $\varepsilon \in \mathbb{R}_+^*$ és $W \in \mathscr{T}(t_0)$ olyan, hogy minden $t \in W$ esetén $|f(t_0) - f(t)| < \varepsilon\,(|f(t_0)| - c)\,|f(t_0)|$, akkor a fenti egyenlőtlenség alapján minden $W \cap V \ni t$-re $|(1/f)(t) - (1/f)(t_0)| < \varepsilon$ és $W \cap V \in \mathscr{T}(t_0)$, tehát $1/f$ folytonos a $t_0 \in T$ pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{K}}$ topológiák szerint.

e) Ha $t \in T$, akkor

$$\begin{aligned}
|\sup(f,g)(t) - \sup(f,g)(t_0)| &:= |\max(f(t),g(t)) - \max(f(t_0),g(t_0))| \leq \\
&\leq |f(t) - f(t_0)| + |g(t) - g(t_0)|, \\
|\inf(f,g)(t) - \inf(f,g)(t_0)| &:= |\min(f(t),g(t)) - \min(f(t_0),g(t_0))| \leq \\
&\leq |f(t) - f(t_0)| + |g(t) - g(t_0)|. \ \blacksquare
\end{aligned}$$

Vigyázzunk arra, hogy nyílt (illetve zárt) halmaz folytonos függvény által létesített képe nem szükségképpen nyílt (illetve zárt). Ezért tartalmas a következő definíció.

26.4.8. Definíció. *Ha $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek, akkor egy $f : T \to T'$ függvényt* **nyíltnak** (*illetve* **zártnak**) *nevezünk, ha minden $\Omega \subseteq T$ $\mathscr{T}$-nyílt (illetve $F \subseteq T$ $\mathscr{T}$-zárt) halmazra az $f\langle\Omega\rangle \subseteq T'$ (illetve $f\langle F\rangle \subseteq T'$) halmaz $\mathscr{T}$-nyílt (illetve $\mathscr{T}$-zárt).*

A következő állítást alkalmazhatjuk két topológia egyenlőségének bizonyításához.

26.4.9. Állítás. *Legyenek $\mathscr{T}_1$ és $\mathscr{T}_2$ topológák a T halmaz felett. Ha létezik olyan $(T', \mathscr{T}')$ topologikus tér és létezik olyan $f : T \to T'$ függvény, amely homemorfizmus a $\mathscr{T}_1$ és $\mathscr{T}'$ topológiák, valamint a $\mathscr{T}_2$ és $\mathscr{T}'$ topológiák szerint, akkor $\mathscr{T}_1 = \mathscr{T}_2$.*

Bizonyítás. Legyen $(T', \mathscr{T}')$ olyan topologikus tér és legyen $f : T \to T'$ olyan függvény, amely homemorfizmus a $\mathscr{T}_1$ és $\mathscr{T}'$ topológiák, valamint a $\mathscr{T}_2$ és $\mathscr{T}'$ topológiák szerint.

Legyen $\Omega \in \mathscr{T}_1$. Mivel $f^{-1} : T' \to T$ folytonos a $\mathscr{T}'$ és $\mathscr{T}_1$ topológiák szerint, így a folytonosság topologikus jellemzése alapján $(\overset{-1}{f^{-1}})\langle\Omega\rangle \in \mathscr{T}'$, tehát $(\overset{-1}{f^{-1}})\langle\Omega\rangle = f\langle\Omega\rangle$ miatt $f\langle\Omega\rangle \in \mathscr{T}'$. Mivel $f : T \to T'$ folytonos a $\mathscr{T}_2$ és $\mathscr{T}'$ topológiák szerint, így a folytonosság topologikus jellemzése alapján $\overset{-1}{f}\langle f\langle\Omega\rangle\rangle \in \mathscr{T}_2$, tehát $\overset{-1}{f}\langle f\langle\Omega\rangle\rangle = \Omega$ miatt $\Omega \in \mathscr{T}_2$. Ez azt jelenti, hogy $\mathscr{T}_1 \subseteq \mathscr{T}_2$.

Legyen $\Omega \in \mathscr{T}_2$. Mivel $f^{-1} : T' \to T$ folytonos a $\mathscr{T}'$ és $\mathscr{T}_2$ topológiák szerint, így a folytonosság topologikus jellemzése alapján $\overset{-1}{f^{-1}}\langle\Omega\rangle \in \mathscr{T}'$, tehát $\overset{-1}{f^{-1}}\langle\Omega\rangle = f\langle\Omega\rangle$ miatt $f\langle\Omega\rangle \in \mathscr{T}'$. Mivel $f : T \to T'$ folytonos a $\mathscr{T}_1$ és $\mathscr{T}'$ topológiák szerint, így a folytonosság topologikus jellemzése alapján $\overset{-1}{f}\langle f\langle\Omega\rangle\rangle \in \mathscr{T}_1$, tehát $\overset{-1}{f}\langle f\langle\Omega\rangle\rangle = \Omega$ miatt $\Omega \in \mathscr{T}_1$. Ez azt jelenti, hogy $\mathscr{T}_2 \subseteq \mathscr{T}_1$. $\blacksquare$

26.5. Rendezés a topológiák halmazában

26.5.1. Állítás. *Ha T halmaz, akkor a T feletti topológiák halmaza a $\subseteq$ relációval ellátva olyan rendezett halmaz, amelynek a T feletti antidiszkrét topológia a legkisebb és a T feletti diszkrét topológia a legnagyobb eleme, továbbá a T feletti topológiák tetszőleges $(\mathscr{T}_i)_{i \in I}$ rendszerére létezik a $\sup_{i \in I} \mathscr{T}_i$ felső határ és az $\inf_{i \in I} \mathscr{T}_i$ alsó határ a $\subseteq$ reláció szerint.* (*Ezt úgy is megfogalmazhatjuk, hogy a T feletti topológiák halmaza a $\subseteq$ relációval ellátva* **teljes rendezett halmaz**.)

Bizonyítás. Legyen $(\mathscr{T}_i)_{i\in I}$ T feletti topológiák tetszőleges rendszere. Ha $I = \emptyset$, akkor a T feletti diszkrét topológia a $(\mathscr{T}_i)_{i\in I}$ rendszer legnagyobb alsó korlátja a $\subseteq$ rendezés szerint. Ha $I \neq \emptyset$, akkor könnyen látható, hogy $\bigcap\limits_{i\in I} \mathscr{T}_i$ olyan topológia T felett, amely alsó korlátja a $(\mathscr{T}_i)_{i\in I}$ rendszernek a $\subseteq$ rendezés szerint, és ha $\mathscr{T}$ olyan topológia T felett, hogy minden $I \ni i$-re $\mathscr{T} \subseteq \mathscr{T}_i$, akkor természetesen $\mathscr{T} \subseteq \bigcap\limits_{i\in I} \mathscr{T}_i$, ezért $\bigcap\limits_{i\in I} \mathscr{T}_i$ a $(\mathscr{T}_i)_{i\in I}$ rendszer legnagyobb alsó korlátja a $\subseteq$ rendezés szerint. Tehát a T feletti topológiák tetszőleges rendszerének létezik infimuma a $\subseteq$ rendezés szerint. Ebből már következik, hogy a $(\mathscr{T}_i)_{i\in I}$ topológia-rendszer felső korlátjai halmazának az infimuma létezik és egyenlő a $(\mathscr{T}_i)_{i\in I}$ rendszer szuprémumával a $\subseteq$ rendezés szerint. ■

Megállapodunk abban, hogy a továbbiakban minden T halmazra a T feletti topológiák halmazát a $\subseteq$ rendezéssel ellátva (teljes) rendezett halmaznak tekintjük. Az előző állítás szerint a T halmaz feletti topológiák bármely $(\mathscr{T}_i)_{i\in I}$ nem üres rendszerére $\inf\limits_{i\in I} \mathscr{T}_i = \bigcap\limits_{i\in I} \mathscr{T}_i$, ugyanakkor a $\sup\limits_{i\in I} \mathscr{T}_i$ topológiára nem adtunk ilyen explicit formulát. A következő állítás teljes jellemzést ad a topológia-szuprémumra.

26.5.2. Állítás. *Legyen T halmaz, $(\mathscr{T}_i)_{i\in I}$ T feletti topológiák tetszőleges nem üres rendszere, és értelmezzük a*

$$\prod_{i\in I}{}^{*} \mathscr{T}_i := \left\{(\Omega_i)_{i\in I} \in \prod_{i\in I} \mathscr{T}_i \;\middle|\; \{i \in I | \Omega_i \neq T\} \text{ véges halmaz}\right\}$$

halmazt. Ekkor a

$$\mathfrak{B} := \left\{ \bigcap_{i\in I} \Omega_i \;\middle|\; (\Omega_i)_{i\in I} \in \prod_{i\in I}{}^{*} \mathscr{T}_i \right\}$$

halmaz bázisa a $\sup\limits_{i\in I} \mathscr{T}_i$ topológiának.

Bizonyítás. Először megmutatjuk, hogy bármely $\mathfrak{B}$-ben haladó nem üres véges rendszer metszete eleme $\mathfrak{B}$-nek. Legyen ugyanis $((\Omega_{\alpha,i})_{i\in I})_{\alpha\in A}$ nem üres véges rendszer $\prod\limits_{i\in I}{}^{*} \mathscr{T}_i$-ben. Minden $i \in I$ esetén $\bigcap\limits_{\alpha\in A} \Omega_{\alpha,i} \in \mathscr{T}_i$, mert $\mathscr{T}_i$-re $(\mathrm{O_{II}})$ teljesül, ezért $\left(\bigcap\limits_{\alpha\in A} \Omega_{\alpha,i}\right)_{i\in I} \in \prod\limits_{i\in I} \mathscr{T}_i$. Továbbá, minden $\alpha \in A$ esetén van olyan $I_\alpha \subseteq I$ véges halmaz, hogy minden $I \ni i$-re: $\Omega_{\alpha,i} \neq T$ esetén $i \in I_\alpha$. Ha $i \in I$ és $\bigcap\limits_{\alpha\in A} \Omega_{\alpha,i} \neq T$, akkor van olyan $\alpha \in A$, hogy $\Omega_{\alpha,i} \neq T$, így $i \in I_\alpha$. Ez azt jelenti, hogy

$$\left\{ i \in I \;\middle|\; \bigcap_{\alpha\in A} \Omega_{\alpha,i} \neq T \right\} \subseteq \bigcup_{\alpha\in A} I_\alpha,$$

és itt a jobb oldalon véges halmaz áll, ezért $\left(\bigcap\limits_{\alpha\in A} \Omega_{\alpha,i}\right)_{i\in I} \in \prod\limits_{i\in I}{}^{*} \mathscr{T}_i$. Ebből következik, hogy

$$\bigcap_{\alpha\in A} \left(\bigcap_{i\in I} \Omega_{\alpha,i}\right) = \bigcap_{i\in I} \left(\bigcap_{\alpha\in A} \Omega_{\alpha,i}\right) \in \mathfrak{B}.$$

Értelmezzük a

$$\mathscr{T}' := \left\{ \bigcup_{H\in\mathfrak{B}'} H \;\middle|\; \mathfrak{B}' \subseteq \mathfrak{B} \right\}$$

halmazt, és vezessük be a $\mathscr{T} := \sup_{i \in I} \mathscr{T}_i$ jelölést. Világos, hogy a $\mathscr{T}' = \mathscr{T}$ egyenlőséget kell igazolni.

Minden $i \in I$ esetén $\mathscr{T}_i \subseteq \mathscr{T}$, ezért a $\mathscr{T}$-re vonatkozó $(\mathrm{O_{II}})$ feltétel és a $\mathfrak{B}$ értelmezése alapján $\mathfrak{B} \subseteq \mathscr{T}$, amiből azonnal következik, hogy $\mathscr{T}' \subseteq \mathscr{T}$ is teljesül, mert $\mathscr{T}$-re $(\mathrm{O_{III}})$ teljesül.

Minden $I \ni i$-re $\mathscr{T}_i \subseteq \mathfrak{B} \subseteq \mathscr{T}'$ nyilvánvalóan igaz, ezért ha $\mathscr{T}'$ topológia lenne T felett, akkor $\mathscr{T} \subseteq \mathscr{T}'$ is teljesülne, amit bizonyítani kell. A $\mathscr{T}'$-re $(\mathrm{O_I})$ és $(\mathrm{O_{III}})$ triviálisan igaz. Az $(\mathrm{O_{II}})$ bizonyításához legyen $(H_\alpha)_{\alpha \in A}$ nem üres véges rendszer $\mathscr{T}'$-ben; azt kell belátni, hogy $\bigcap_{\alpha \in A} H_\alpha \in \mathscr{T}'$. Minden $A \ni \alpha$-hoz van olyan $\mathfrak{B}_\alpha \subseteq \mathfrak{B}$ halmaz, hogy $H_\alpha = \bigcup_{H \in \mathfrak{B}_\alpha} H$. Legyen $F := \prod_{\alpha \in A} \mathfrak{B}_\alpha$; ekkor az ismert disztributivitás-formula alapján

$$\bigcap_{\alpha \in A} H_\alpha = \bigcap_{\alpha \in A} \Big(\bigcup_{H \in \mathfrak{B}_\alpha} H \Big) = \bigcup_{f \in F} \Big(\bigcap_{\alpha \in A} f(\alpha) \Big) \in \mathscr{T}',$$

mert a definíció szerint minden $f \in F$ esetén minden $A \ni \alpha$-ra $f(\alpha) \in \mathfrak{B}_\alpha \subseteq \mathfrak{B}$, ezért $\bigcap_{\alpha \in A} f(\alpha) \in \mathfrak{B}$, mert láttuk, hogy bármely $\mathfrak{B}$-ben haladó nem üres véges rendszer metszete eleme $\mathfrak{B}$-nek. ■

26.6. Projektíven előállított topológiák

26.6.1. Tétel. *Legyen T halmaz, $((T_i, \mathscr{T}_i))_{i \in I}$ topologikus terek rendszere és $(f_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T \to T_i$ függvény. Ekkor létezik T felett olyan $\mathscr{T}$ topológia, amely a legkisebb mindazon T feletti topológiák között, amelyekre minden $i \in I$ esetén az $f_i : T \to T_i$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}_i$ topológiák szerint.*

Bizonyítás. Minden $I \ni i$-re legyen $\overset{-1}{f_i}[\mathscr{T}_i] := \left\{ \overset{-1}{f_i}\langle \Omega_i \rangle \;\middle|\; \Omega_i \in \mathscr{T}_i \right\}$. Ekkor $i \in I$ esetén $\overset{-1}{f_i}[\mathscr{T}_i]$ topológia T felett; legyen $\mathscr{T} := \sup_{i \in I} \overset{-1}{f_i}[\mathscr{T}_i]$. Ha $i \in I$ és $\Omega_i \in \mathscr{T}_i$, akkor a definíció szerint $\overset{-1}{f_i}\langle \Omega_i \rangle \in \overset{-1}{f_i}[\mathscr{T}_i] \subseteq \mathscr{T}$, tehát minden $i \in I$ esetén az $f_i : T \to T_i$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}_i$ topológiák szerint. Ha $\mathscr{T}'$ olyan topológia T felett, hogy minden $i \in I$ esetén az $f_i : T \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint, akkor minden $I \ni i$-re és $\mathscr{T}_i \ni \Omega_i$-re $\overset{-1}{f_i}\langle \Omega_i \rangle \in \mathscr{T}'$, így $\overset{-1}{f_i}[\mathscr{T}_i] \subseteq \mathscr{T}'$, vagyis a $\mathscr{T}$ definíciója alapján $\mathscr{T} \subseteq \mathscr{T}'$. Ez azt jelenti, hogy $\mathscr{T}$ az a topológia, amely a legkisebb mindazon T feletti topológiák között, amelyekre minden $i \in I$ esetén az $f_i : T \to T_i$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}_i$ topológiák szerint. ■

26.6.2. Definíció. *Legyen T halmaz, $((T_i, \mathscr{T}_i))_{i \in I}$ topologikus terek rendszere és $(f_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T \to T_i$ függvény. Ekkor a $((T_i, \mathscr{T}_i), f_i)_{i \in I}$ rendszer által* **projektíven előállított** *(vagy* **iniciális***) T feletti topológiának nevezzük azt a legkisebb T feletti $\mathscr{T}$ topológiát, amelyre minden $i \in I$ esetén az $f_i : T \to T_i$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}_i$ topológiák szerint.*

Az előző tétel bizonyításából látható, hogy ha T halmaz, $((T_i, \mathscr{T}_i))_{i \in I}$ topologikus terek nem üres rendszere és $(f_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T \to T_i$

függvény, akkor a $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ rendszer által előállított T feletti $\mathscr{T}$ iniciális topológiára $\mathscr{T} = \sup_{i\in I} \overset{-1}{f}_i[\mathscr{T}_i]$ teljesül, ezért a topológiák inverz képének definíciója és a szuprémum-topológiák jellemzésére vonatkozó korábbi állításunk szerint a

$$\left\{ \bigcap_{i\in I} \overset{-1}{f}_i\langle\Omega_i\rangle \;\middle|\; \left((\Omega_i)_{i\in I} \in \prod_{i\in I} \mathscr{T}_i\right) \wedge (\{i \in I | \Omega_i \neq T_i\} \text{ véges halmaz}) \right\}$$

halmaz bázisa a $\mathscr{T}$ topológiának.

Tehát, ha T halmaz, $(T', \mathscr{T}')$ topologikus tér és $f : T \to T'$ függvény, akkor az $\overset{-1}{f}[\mathscr{T}']$ topológia megegyezik a $((T', \mathscr{T}'), f)$ rendszer által előállított T feletti iniciális topológiával. Speciálisan, ha $(T, \mathscr{T})$ topologikus tér és $E \subseteq T$, akkor a $\mathscr{T}|E$ altértopológia megegyezik a $((T, \mathscr{T}), \mathrm{in}_{E,T})$ rendszer által előállított E feletti iniciális topológiával, ahol $\mathrm{in}_{E,T}$ az $E \to T$ kanonikus injekció.

26.6.3. Állítás. *Legyen T halmaz, $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T \to T_i$ függvény.*

a) *Ha $\mathscr{T}$ a $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ rendszer által előállított T feletti iniciális topológia, akkor minden $(T', \mathscr{T}')$ topologikus térre és $f : T' \to T$ függvényre: az f pontosan akkor folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, ha minden $I \ni i$-re a $f_i \circ f : T' \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint.*

b) *Ha $\mathscr{T}$ olyan topológia T felett, hogy minden $(T', \mathscr{T}')$ topologikus térre és $f : T' \to T$ függvényre: az f pontosan akkor folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, ha minden $I \ni i$-re a $f_i \circ f : T' \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint, akkor $\mathscr{T}$ megegyezik a $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ rendszer által előállított T feletti iniciális topológiával.*

Bizonyítás. a) Ha az $f : T' \to T$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, akkor minden $i \in I$ esetén az $f_i \circ f : T' \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint, mert $f_i : T \to T_i$ folytonos a $\mathscr{T}$ és $\mathscr{T}_i$ topológiák szerint, és folytonos függvények kompozíciója folytonos.

Megfordítva, tegyük fel, hogy minden $I \ni i$-re a $f_i \circ f : T' \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint. Ha $i \in I$ és $\Omega_i \in \mathscr{T}_i$, akkor a folytonosság topologikus jellemzése alapján

$$\overset{-1}{f}\langle \overset{-1}{f_i}\langle\Omega_i\rangle\rangle = (\overset{-1}{f_i \circ f})\langle\Omega_i\rangle \in \mathscr{T}',$$

tehát $\overset{-1}{f_i}\langle\Omega_i\rangle \in f[\mathscr{T}'] := \left\{ \Omega \in \mathscr{P}(T) \;\middle|\; \overset{-1}{f}\langle\Omega\rangle \in \mathscr{T}' \right\}$. Ez azt jelenti, hogy minden $i \in I$ esetén az $f_i : T \to T_i$ függvény folytonos az $f[\mathscr{T}']$ és $\mathscr{T}_i$ topológiák szerint. Az iniciális topológia definíciója alapján $\mathscr{T} \subseteq f[\mathscr{T}']$, vagyis minden $\Omega \in \mathscr{T}$ esetén $\overset{-1}{f}\langle\Omega\rangle \in \mathscr{T}'$, tehát f folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint.

b) Legyen $\mathscr{T}$ olyan topológia T felett, hogy minden $(T', \mathscr{T}')$ topologikus térre és $f : T' \to T$ függvényre: az f pontosan akkor folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, ha minden $I \ni i$-re a $f_i \circ f : T' \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint.

Az $\mathrm{id}_T : T \to T$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}$ topológiák szerint, így a feltételt alkalmazva a $(T', \mathscr{T}') := (T, \mathscr{T})$ topologikus térre és az $f := \mathrm{id}_T$ függvényre kapjuk, hogy minden $I \ni i$-re az $f_i = f_i \circ \mathrm{id}_T : T \to T_i$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}_i$ topológiák szerint.

Megfordítva, ha $\mathscr{T}'$ olyan topológia T felett, hogy minden $I \ni i$-re az $f_i \circ \mathrm{id}_T = f_i : T \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint, akkor a feltételt alkalmazva a $(T, \mathscr{T}')$ topologikus térre és az id_T függvényre kapjuk, hogy id_T folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, ami azzal ekvivalens, hogy $\mathscr{T} \subseteq \mathscr{T}'$. Ez azt jelenti, hogy $\mathscr{T}$ a legkisebb topológia T felett, amelyre minden $i \in I$ esetén az $f_i : T \to T_i$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}_i$ topológiák szerint. ■

26.6.4. Következmény. *Ha $(T, \mathscr{T})$ topologikus tér, $E \subseteq T$ és $(T', \mathscr{T}')$ topologikus tér, akkor egy $f : T' \to E$ függvény pontosan akkor folytonos a $\mathscr{T}'$ és $\mathscr{T}|E$ topológiák szerint, ha f folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint.*

26.7. Topologikus szorzatterek

26.7.1. Definíció. *Legyen $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere, és minden $I \ni j$-re jelölje pr_j a $\prod_{i\in I} T_i \to T_j$ projekció-függvényt. A $((T_i, \mathscr{T}_i), \mathrm{pr}_i)_{i\in I}$ rendszer által előállított $\prod_{i\in I} T_i$ feletti iniciális topológiát a $(\mathscr{T}_i)_{i\in I}$* **topológia-rendszer szorzatának** *nevezzük, és a $\times_{i\in I} \mathscr{T}_i$ szimbólummal jelöljük. Ekkor a $\left(\prod_{i\in I} T_i, \times_{i\in I} \mathscr{T}_i\right)$ topologikus teret a $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus tér-rendszer szorzatának nevezzük. Ha minden $i \in I$ esetén $(T_i, \mathscr{T}_i) = (T, \mathscr{T})$ ugyanaz a topologikus tér, akkor $\prod_{i\in I} T_i = \mathscr{F}(I; T) = T^I$, és ekkor a $\times_{i\in I} \mathscr{T}_i$ topológiát a $\mathscr{T}^I$ szimbólummal jelöljük, továbbá a $\left(T^I, \mathscr{T}^I\right)$ alakú topologikus tereket* **topologikus kockáknak** *nevezzük. Speciálisan, a $\left([0,1]^I, (\mathscr{E}_{\mathbb{R}}|[0,1])^I\right)$ alakú topologikus kockákat* **euklidészi kockáknak** *nevezzük.*

Figyeljük meg, hogy a definíció szerint tetszőleges $(T, \mathscr{T})$ topologikus térre és tetszőleges I halmazra, az *összes* $I \to T$ függvények halmaza (vagyis T^I-n) felett van értelmezve a $\mathscr{T}^I$ szorzattopológia; ez a legkisebb olyan $\mathscr{F}(I; T)$ feletti topológia, amelyre teljesül az, hogy minden $i \in I$ esetén a $\mathscr{F}(I; T) \to T$; $f \mapsto f(i)$ függvény folytonos. A függvényhalmazok feletti topológiákkal csak jóval később foglalkozunk részletesebben (**MET** 25.3. pont és **EVT** 5. fejezet).

Az előzőek alapján nyilvánvaló, hogy ha $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek nem üres rendszere, akkor a

$$\left\{ \bigcap_{i\in I} \overset{-1}{\mathrm{pr}}_i\langle \Omega_i \rangle \;\middle|\; \left((\Omega_i)_{i\in I} \in \prod_{i\in I} \mathscr{T}_i\right) \wedge (\{i \in I | \Omega_i \neq T_i\} \text{ véges halmaz}) \right\}$$

halmaz bázisa a $\times_{i\in I} \mathscr{T}_i$ topológiának.

Az alábbiakban alkalmazzuk a következő jelölést: ha $(T_i)_{i\in I}$ tetszőleges rendszer, $t = (t_i)_{i\in I} \in \prod_{i\in I} T_i$ és $k \in I$, akkor $\mathrm{in}_{k,t}$ jelöli azt a $T_k \to \prod_{i\in I} T_i$ függvényt, amelynek k-adik komponens-függvénye egyenlő a $T_k \to T_k$ identikus függvénnyel, és minden $I \setminus \{k\} \ni i$-re az i-edik komponens-függvénye egyenlő a t_i értékű $T_k \to T_i$ konstansfüggvénnyel.

26.7.2. Állítás. *Ha $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere, $(T', \mathscr{T}')$ topologikus tér és $f : \prod_{i\in I} T_i \to T'$ olyan függvény, amely a $t = (t_i)_{i\in I} \in \prod_{i\in I} T_i$ pontban folytonos a $\times_{i\in I} \mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint, akkor minden $I \ni k$-ra az $f \circ \mathrm{in}_{k,t} : T_k \to T'$ függvény folytonos a t_k pontban a $\mathscr{T}_k$ és $\mathscr{T}'$ topológiák szerint.*

Bizonyítás. A folytonos függvények kompozíciójának folytonossága miatt az állítás *ekvivalens* azzal, hogy minden $t = (t_i)_{i\in I} \in \prod_{i\in I} T_i$ pontra és $I \ni k$-ra az $\mathrm{in}_{k,t} : T_k \to \prod_{i\in I} T_i$ függvény folyonos a t_k pontban a $\mathscr{T}_k$ és $\bigtimes_{i\in I} \mathscr{T}_i$ topológiák szerint. Ennek bizonyításához elég azt igazolni, hogy minden $j, k \in I$ és $t = (t_i)_{i\in I} \in \prod_{i\in I} T_i$ esetén a $\mathrm{pr}_j \circ \mathrm{in}_{k,t} : T_k \to T_j$ függvény folytonos a $\mathscr{T}_k$ és $\mathscr{T}_j$ topológiák szerint. Ez viszont igaz, mert ha $j = k$, akkor $\mathrm{pr}_j \circ \mathrm{in}_{k,t} = \mathrm{id}_{T_k}$ folytonos a $\mathscr{T}_k$ és $\mathscr{T}_j$ topológiák szerint, míg $j \neq k$ esetén $\mathrm{pr}_j \circ \mathrm{in}_{k,t}$ egyenlő a t_j értékű $T_k \to T_j$ konstansfüggvénnyel, ami szintén folytonos a $\mathscr{T}_k$ és $\mathscr{T}_j$ topológiák szerint. ■

26.7.3. Állítás. *Legyenek $((T_i, \mathscr{T}_i))_{i\in I}$ és $((T'_i, \mathscr{T}'_i))_{i\in I}$ topologikus terek rendszerei (ugyanazzal az I indexhalmazzal), és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $I \ni i$-re $f_i : T_i \to T'_i$ folytonos függvény a $\mathscr{T}_i$ és $\mathscr{T}'_i$ topológiák szerint. Ekkor a*

$$\bigtimes_{i\in I} f_i : \prod_{i\in I} T_i \to \prod_{i\in I} T'_i, \quad (t_i)_{i\in I} \mapsto (f_i(t_i))_{i\in I}$$

függvény folytonos a $\bigtimes_{i\in I} \mathscr{T}_i$ és $\bigtimes_{i\in I} \mathscr{T}'_i$ topológiák szerint.

Bizonyítás. Minden $j \in I$ esetén legyen pr_j a $\prod_{i\in I} T_i \to T_j$ projekció-függvény, és pr'_j a $\prod_{i\in I} T'_i \to T'_j$ projekció-függvény. Tudjuk, hogy a $\bigtimes_{i\in I} f_i$ függvény pontosan akkor folytonos a $\bigtimes_{i\in I} \mathscr{T}_i$ és $\bigtimes_{i\in I} \mathscr{T}'_i$ topológiák szerint, ha minden $I \ni j$-re a $\mathrm{pr}'_j \circ \left(\bigtimes_{i\in I} f_i\right) : \prod_{i\in I} T_i \to T'_j$ függvény folytonos a $\bigtimes_{i\in I} \mathscr{T}_i$ és $\mathscr{T}'_j$ topológiák szerint. A $\bigtimes_{i\in I} f_i$ függvény definíciója alapján nyilvánvaló, hogy minden $j \in I$ esetén

$$\mathrm{pr}'_j \circ \left(\bigtimes_{i\in I} f_i\right) = f_j \circ \mathrm{pr}_j,$$

továbbá a $\mathrm{pr}_j : \prod_{i\in I} T_i \to T_j$ függvény folytonos a $\bigtimes_{i\in I} \mathscr{T}_i$ és $\mathscr{T}_j$ topológiák szerint, valamint $f_j : T_j \to T'_j$ a hipotézis alapján folytonos a $\mathscr{T}_j$ és $\mathscr{T}'_j$ toplógiák szerint, ezért az $f_j \circ \mathrm{pr}_j : \prod_{i\in I} T_i \to T'_j$ függvény folytonos a $\bigtimes_{i\in I} \mathscr{T}_i$ és $\mathscr{T}'_j$ topológiák szerint, hiszen folytonos függvények kompozíciója folytonos. ■

26.7.4. Állítás. *Ha $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere, J halmaz és $\sigma : J \to I$ bijekció, akkor az*

$$f : \prod_{i\in I} T_i \to \prod_{j\in J} T_{\sigma(j)}; \quad (t_i)_{i\in I} \mapsto (t_{\sigma(j)})_{j\in J}$$

függvény homeomorfizmus a $\left(\prod_{i\in I} T_i, \bigtimes_{i\in I} \mathscr{T}_i\right)$ és $\left(\prod_{j\in J} T_{\sigma(j)}, \bigtimes_{j\in J} \mathscr{T}_{\sigma(j)}\right)$ topologikus terek között.

Bizonyítás. Vezessük be a $T := \prod_{i\in I} T_i$, $T' := \prod_{j\in J} T_{\sigma(j)}$, $\mathscr{T} := \bigtimes_{i\in I} \mathscr{T}_i$ és $\mathscr{T}' := \bigtimes_{j\in J} \mathscr{T}_{\sigma(j)}$ jelöléseket, továbbá $i \in I$ és $j \in J$ esetén legyenek $\mathrm{pr}_i : T \to T_i$ és $\mathrm{pr}'_j : T' \to T_{\sigma(j)}$ a projekció-függvények. Az f függvény pontosan akkor folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ha minden $J \ni j$-re a $\mathrm{pr}'_j \circ f : T \to T_{\sigma(j)}$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}_{\sigma(j)}$ topológiák szerint. Az f definíciójából látható, hogy $j \in J$ esetén $\mathrm{pr}'_j \circ f = \mathrm{pr}_{\sigma(j)}$, és a szorzattopológia értelmezése alapján $\mathrm{pr}_{\sigma(j)}$ folytonos a $\mathscr{T}$ és $\mathscr{T}_{\sigma(j)}$ topológiák szerint. Tehát f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint. Világos, hogy a

$$g : \prod_{j\in J} T_{\sigma(j)} \to \prod_{i\in I} T_i; \quad (t'_j)_{j\in J} \mapsto \left(t'_{\sigma^{-1}(i)}\right)_{i\in I}$$

függvény az f inverze, és g pontosan akkor folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, ha minden $I \ni i$-re a $\mathrm{pr}_i \circ g : T' \to T_i$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint. A g definíciójából látható, hogy minden $i \in I$ esetén $\mathrm{pr}_i \circ g = \mathrm{pr}'_{\sigma^{-1}(i)}$ és a szorzattopológia értelmezése alapján a $\mathrm{pr}'_{\sigma^{-1}(i)}$ projekció-függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_i$ topológiák szerint. Tehát f^{-1} folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint. ■

A következő állításban felhasználjuk azt a könnyen ellenőrizhető állítást, hogy ha d metrika az M halmaz felett, akkor a $d' : M \times M \to \mathbb{R}_+$; $(x, y) \mapsto \min(d(x, y), 1)$ függvény olyan metrika M felett, hogy $\mathscr{T}_d = \mathscr{T}_{d'}$ és $d' \leq 1$.

26.7.5. Állítás. *Metrizálható terek megszámlálható rendszerének topologikus szorzata metrizálható topologikus tér.*

Bizonyítás. Legyen $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek olyan rendszere, hogy I megszámlálható halmaz és minden $I \ni i$-re a $(T_i, \mathscr{T}_i)$ topologikus tér metrizálható. *Kiválaszthatunk* olyan $(d_i)_{i\in I}$ rendszert, hogy minden $i \in I$ esetén d_i metrika T_i felett és $\mathscr{T}_i = \mathscr{T}_{d_i}$, valamint minden $(t, t') \in T_i \times T_i$ párra $d_i(t, t') \leq 1$. Legyen $T := \prod_{i\in I} T_i$, $\mathscr{T} := \times_{i\in I} \mathscr{T}_i$, és minden $I \ni i$-re pr_i a $T \to T_i$ projekció-függvény. A $(T, \mathscr{T})$ topologikus tér metrizálhatóságát három lépésben bizonyítjuk.

(I) Először feltesszük, hogy I nem üres és *véges.* Ekkor a

$$\left(\prod_{i\in I} T_i\right) \times \left(\prod_{i\in I} T_i\right) \to \mathbb{R}_+; \quad ((t_i)_{i\in I}, (t'_i)_{i\in I}) \mapsto \max_{i\in I} d_i(t_i, t'_i)$$

leképezésről közvetlenül látható, hogy olyan metrika a $\prod_{i\in I} T_i$ szorzathalmaz felett, amely a szorzattopológiát generálja.

(II) Most feltesszük, hogy $I = \mathbb{N}$. Legyen $(c_k)_{k\in\mathbb{N}}$ olyan sorozat $\mathbb{R}_+^*$-ban, hogy a $\sum_{k\in\mathbb{N}} c_k$ sor konvergens $\mathbb{R}$-ben, és értelmezzük a

$$d : T \times T \to \mathbb{R}_+; \quad ((t_k)_{k\in\mathbb{N}}, (t'_k)_{k\in\mathbb{N}}) \mapsto \sum_{k=0}^{\infty} c_k d_k(t_k, t'_k)$$

függvényt. Könnyen látható, hogy d metrika a T szorzathalmaz felett; megmutatjuk, hogy $\mathscr{T} = \mathscr{T}_d$.

Legyen $t := (t_k)_{k\in\mathbb{N}} \in T$ és $V \in \mathscr{T}_d(t)$. Rögzítsünk olyan $\varepsilon \in \mathbb{R}_+^*$ számot, hogy $B_\varepsilon(t; d) \subseteq V$. Vegyünk olyan $N \in \mathbb{N}$ számot, hogy $\sum_{k=N+1}^{\infty} c_k < \frac{\varepsilon}{2}$, és legyen minden $k \leq N$ természetes számra $\varepsilon_k := \frac{\varepsilon/2}{(N+1)c_k}$. Minden $\mathbb{N} \ni k$-ra legyen $\Omega_k := B_{\varepsilon_k}(t_k; d_k)$, ha $k \leq N$, és $\Omega_k := T_k$, ha $k > N$. Ekkor $k \in \mathbb{N}$ esetén $\Omega_k \in \mathscr{T}_{d_k} = \mathscr{T}_k$, és $\{k \in \mathbb{N} | \Omega_k \neq T_k\} \subseteq \{k \in \mathbb{N} | k \leq N\}$ véges halmaz, tehát a szorzattopológia értelmezése alapján $\prod_{k\in\mathbb{N}} \Omega_k \in \mathscr{T}$. Ugyanakkor $t \in \prod_{k\in\mathbb{N}} \Omega_k$, tehát $\prod_{k\in\mathbb{N}} \Omega_k \in \mathscr{T}(t)$. Állítjuk, hogy $\prod_{k\in\mathbb{N}} \Omega_k \subseteq B_\varepsilon(t; d)$. Valóban, ha $(t'_k)_{k\in\mathbb{N}} \in \prod_{k\in\mathbb{N}} \Omega_k$, akkor $k \in \mathbb{N}$ és $k \leq N$ esetén $t'_k \in B_{\varepsilon_k}(t_k; d_k)$, tehát

$$d\left((t_k)_{k\in\mathbb{N}}, (t'_k)_{k\in\mathbb{N}}\right) = \sum_{k=0}^{\infty} c_k d_k(t_k, t'_k) = \sum_{k=0}^{N} c_k d_k(t_k, t'_k) + \sum_{k=N+1}^{\infty} c_k d_k(t_k, t'_k) <$$
$$< \sum_{k=0}^{N} c_k \varepsilon_k + \sum_{k=N+1}^{\infty} c_k = \sum_{k=0}^{N} c_k \frac{\varepsilon/2}{(N+1)c_k} + \sum_{k=N+1}^{\infty} c_k = \frac{\varepsilon}{2} + \sum_{k=N+1}^{\infty} c_k < \varepsilon,$$

amint állítottuk. Ebből következik, hogy $V \in \mathscr{T}(t)$. Ezért $\mathscr{T}_d \subseteq \mathscr{T}$.

Megfordítva, legyen $t := (t_k)_{k\in\mathbb{N}} \in T$ és $V \in \mathscr{T}(t)$. Létezik olyan $(\Omega_k)_{k\in\mathbb{N}}$ sorozat, hogy minden $\mathbb{N} \ni k$-ra $\Omega_k \in \mathscr{T}_k = \mathscr{T}_{d_k}$, és $\{k \in \mathbb{N} | \Omega_k \neq T_k\}$ véges halmaz, és $t \in \prod_{k\in\mathbb{N}} \Omega_k \subseteq V$. Legyen $N \in \mathbb{N}$ olyan, hogy minden $k > N$ természetes számra $\Omega_k = T_k$. Minden $k \leq N$ természetes számhoz válasszunk olyan $\varepsilon_k \in \mathbb{R}_+^*$ számot, amelyre $B_{\varepsilon_k}(t_k; d_k) \subseteq \Omega_k$, és legyen $\varepsilon := \min_{0\leq k\leq N}(c_k \varepsilon_k)$. Állítjuk, hogy $B_\varepsilon(t; d) \subseteq \prod_{k\in\mathbb{N}} \Omega_k$. Valóban, ha $(t'_k)_{k\in\mathbb{N}} \in B_\varepsilon(t; d)$, akkor minden $k \leq N$ természetes számra $d_k(t_k, t'_k) < \varepsilon_k$, hiszen ha $n \leq N$ olyan természetes szám volna, hogy $d_n(t_n, t'_n) \geq \varepsilon_n$, akkor

$$\varepsilon := \min_{0\leq k\leq N}(c_k \varepsilon_k) \leq c_n \varepsilon_n \leq c_n d_n(t_n, t'_n) \leq$$
$$\leq \sum_{k=0}^{N} c_k d_k(t_k, t'_k) \leq d\left((t_k)_{k\in\mathbb{N}}, (t'_k)_{k\in\mathbb{N}}\right) < \varepsilon$$

teljesülne, ami lehetetlen. Ebből következik, hogy $V \in \mathscr{T}_d(t)$. Ezért $\mathscr{T} \subseteq \mathscr{T}_d$.

(III) Végül feltesszük, hogy I *megszámlálhatóan végtelen* halmaz. Ekkor létezik $\sigma : \mathbb{N} \to I$ bijekció, így az előző állításból következik, hogy a $\left(\prod_{i\in I} T_i, \times_{i\in I} \mathscr{T}_i\right)$ és $\left(\prod_{k\in\mathbb{N}} T_{\sigma(k)}, \times_{k\in\mathbb{N}} \mathscr{T}_{\sigma(k)}\right)$ topologikus terek homeomorfak, ugyanakkor az utóbbi a (II) alapján metrizálható, ezért $\left(\prod_{i\in I} T_i, \times_{i\in I} \mathscr{T}_i\right)$ metrizálható topologikus tér. ■

26.8. Induktívan előállított topológiák

26.8.1. Tétel. *Legyen T halmaz, $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere, és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T_i \to T$ függvény. Ekkor létezik olyan T feletti legnagyobb $\mathscr{T}$ topológia, amelyre teljesül az, hogy minden $I \ni i$-re az $f_i : T_i \to T$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}$ topológiák szerint.*

Bizonyítás. Minden $i \in I$ esetén $f_i[\mathscr{T}_i] := \left\{ \Omega \in \mathscr{P}(T) \,\middle|\, \overset{-1}{f_i}\langle\Omega\rangle \in \mathscr{T}_i \right\}$ topológia T felett; legyen $\mathscr{T} := \inf_{i\in I} f_i[\mathscr{T}_i]$. Ha $i \in I$ és $\Omega \in \mathscr{T}$, akkor a definíció szerint $\Omega \in f_i[\mathscr{T}_i]$, vagyis $\overset{-1}{f_i}\langle\Omega\rangle \in \mathscr{T}_i$, tehát az $f_i : T_i \to T$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}$ topológiák szerint. Ha

$\mathscr{T}'$ olyan topológia T felett, hogy minden $I \ni i$-re az $f_i : T_i \to T$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}$ topológiák szerint, akkor minden $i \in I$ és $\Omega \in \mathscr{T}'$ esetén $\overset{-1}{f_i}\langle\Omega\rangle \in \mathscr{T}_i$, vagyis $\Omega \in f_i[\mathscr{T}_i]$, tehát $\Omega \in \mathscr{T}$, így $\mathscr{T}' \subseteq \mathscr{T}$. Ez azt jelenti, hogy $\mathscr{T}$ a legnagyobb T feletti topológia, amelyre minden $i \in I$ esetén az $f_i : T_i \to T$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}$ topológiák szerint. ■

26.8.2. Definíció. *Legyen T halmaz, $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere, és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T_i \to T$ függvény. Ekkor a $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ rendszer által* **induktívan előállított** (*vagy* **finális**) *T feletti topológiának nevezzük azt a legnagyobb T feletti $\mathscr{T}$ topológiát, amelyre minden $i \in I$ esetén az $f_i : T_i \to T$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}$ topológiák szerint.*

Az előző tétel bizonyításából látszik, hogy ha T halmaz, $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere, és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T_i \to T$ függvény, akkor a $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ rendszer által induktívan előállított T feletti $\mathscr{T}$ topológiára $\mathscr{T} = \inf_{i\in I} f_i[\mathscr{T}_i]$, ezért a topológiák képének definíciója szerint

$$\mathscr{T} = \{\ \Omega \in \mathscr{P}(T) \mid (\forall\, i \in I) : \overset{-1}{f}_i\langle\Omega\rangle \in \mathscr{T}_i\ \}.$$

Tehát, ha T halmaz, $(T', \mathscr{T}')$ topologikus tér és $f : T' \to T$ függvény, akkor az $f[\mathscr{T}']$ topológia megegyezik a $((T', \mathscr{T}'), f)$ rendszer által induktívan előállított T feletti topológiával. Speciálisan, ha $(T, \mathscr{T})$ topologikus tér és R ekvivalencia-reláció T felett, akkor a $\mathscr{T}/R$ faktortopológia megegyezik a $((T, \mathscr{T}), \pi_{T/R})$ rendszer által induktívan előállított T/R feletti topológiával, ahol $\pi_{T/R}$ a $T \to T/R$ kanonikus szürjekció.

26.8.3. Állítás. *Legyen T halmaz, $((T_i, \mathscr{T}_i))_{i\in I}$ topologikus terek rendszere és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T_i \to T$ függvény.*

a) *Ha $\mathscr{T}$ a $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ rendszer által induktívan előállított T feletti topológia, akkor minden $(T', \mathscr{T}')$ topologikus térre és $f : T \to T'$ függvényre: az f pontosan akkor folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ha minden $I \ni i$-re a $f \circ f_i : T_i \to T'$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint.*

b) *Ha $\mathscr{T}$ olyan topológia T felett, hogy minden $(T', \mathscr{T}')$ topologikus térre és $f : T \to T'$ függvényre: az f pontosan akkor folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ha minden $I \ni i$-re a $f \circ f_i : T_i \to T'$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint, akkor $\mathscr{T}$ megegyezik a $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ rendszer által induktívan előállított T feletti topológiával.*

Bizonyítás. a) Ha az $f : T \to T'$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, akkor minden $I \ni i$-re az $f \circ f_i : T_i \to T'$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint, mert folytonos függvények kompozíciója folytonos, és minden $i \in I$ esetén az f_i függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}$ topológiák szerint.

Megfordítva, tegyük fel, hogy minden $i \in I$ esetén az $f \circ f_i : T_i \to T'$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint. Legyen $\Omega' \in \mathscr{T}'$; ekkor a folytonosság topologikus jellemzésének ismeretében azt kell igazolni, hogy $\overset{-1}{f}\langle\Omega'\rangle \in \mathscr{T}$. Az $\overset{-1}{f}\langle\Omega'\rangle \subseteq T$ halmaz olyan, hogy minden $i \in I$ esetén

$$\overset{-1}{f_i}\langle\overset{-1}{f}\langle\Omega'\rangle\rangle = (\overset{-1}{f \circ f_i})\langle\Omega'\rangle \in \mathscr{T}_i,$$

hiszen $f \circ f_i$ folytonos a $\mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint. Ez azt jelenti, hogy minden $I \ni i$-re $\overset{-1}{f}\langle\Omega'\rangle \in f_i[\mathscr{T}_i]$, tehát az induktívan előállított topológiák értelmezése alapján

$\overset{-1}{f}\langle\Omega'\rangle \in \inf_{i\in I} f_i[\mathscr{T}_i] = \mathscr{T}$.

b) Legyen $\mathscr{T}$ olyan topológia T felett, hogy minden $(T', \mathscr{T}')$ topologikus térre és $f : T \to T'$ függvényre: az f pontosan akkor folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ha minden $I \ni i$-re a $f \circ f_i : T_i \to T'$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint. Az $\mathrm{id}_T : T \to T$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}$ topológiák szerint, ezért a feltételt alkalmazva a $(T', \mathscr{T}') := (T, \mathscr{T})$ topologikus térre és $f := \mathrm{id}_T$ függvényre kapjuk, hogy minden $I \ni i$-re az $f_i = \mathrm{id}_T \circ f_i : T_i \to T$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}$ topológiák szerint.

Ha $\mathscr{T}'$ olyan topológia T felett, hogy minden $i \in I$ esetén az $f_i = \mathrm{id}_T \circ f_i$ függvény folytonos a $\mathscr{T}_i$ és $\mathscr{T}'$ topológiák szerint, akkor a hipotézist alkalmazva a $(T, \mathscr{T}')$ topologikus térre és az id_T függvényre kapjuk, hogy id_T folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ami azzal ekvivalens, hogy $\mathscr{T}' \subseteq \mathscr{T}$. Tehát $\mathscr{T}$ a legnagyobb topológia T felett, amelyre minden $i \in I$ esetén az f_i függvény folytonos $\mathscr{T}_i$ és $\mathscr{T}$ szerint. ■

26.8.4. Következmény. *Ha $(T, \mathscr{T})$ topologikus tér, R ekvivalencia-reláció T felett, és $(T', \mathscr{T}')$ topologikus tér, akkor egy $f : T/R \to T'$ függvény pontosan akkor folytonos a $\mathscr{T}/R$ és $\mathscr{T}'$ topológiák szerint, ha az $f \circ \pi_{T/R} : T \to T'$ függvény folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint.* ■

26.8.5. Tétel. *Legyenek $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek, $f : T \to T'$ $\mathscr{T}$-$\mathscr{T}'$ folytonos függvény, $\mathrm{R}_f := \{((t, s) \in T \times T | f(t) = f(s)\}$, és jelölje $\dot{f}$ az f függvény kanonikus faktorizáltját, vagyis $\dot{f} : T/\mathrm{R}_f \to \mathrm{Im}(f)$ az a függvény, amelyre $\dot{f} \circ \pi_{T/\mathrm{R}_f} = f$, ahol $\pi_{T/\mathrm{R}_f} : T \to T/\mathrm{R}_f$ a kanonikus szürjekció.*

a) Az $\dot{f}$ függvény olyan bijekció a T/R_f faktorhalmaz és az $\mathrm{Im}(f) \subseteq T'$ részhalmaz között, amely folytonos $\mathscr{T}/\mathrm{R}_f$ faktortopológia és a $\mathscr{T}'|\mathrm{Im}(f)$ altértopológia szerint.

b) A következő állítások ekvivalensek.

(i) Az f függvény nyílt leképezés a $\mathscr{T}$ topológia és a $\mathscr{T}'|\mathrm{Im}(f)$ altértopológia szerint (vagyis minden $\Omega \in \mathscr{T}$ esetén $f\langle\Omega\rangle \in \mathscr{T}'|\mathrm{Im}(f)$).

(ii) Az $\dot{f}$ függvény homeomorfizmus a $(T/\mathrm{R}_f, \mathscr{T}/\mathrm{R}_f)$ és $(\mathrm{Im}(f), \mathscr{T}'|\mathrm{Im}(f))$ topologikus terek között, és a π_{T/R_f} kanonikus szürjekció nyílt leképezés a $\mathscr{T}$ és $\mathscr{T}/\mathrm{R}_f$ topológiák szerint (vagyis minden $\Omega \in \mathscr{T}$ esetén $\pi_{T/\mathrm{R}_f}\langle\Omega\rangle \in \mathscr{T}/\mathrm{R}_f$).

Bizonyítás. a) Mivel $\dot{f} \circ \pi_{T/\mathrm{R}_f} = f$, és f folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, így a 26.8.4. következményből kapjuk, hogy $\dot{f}$ folytonos a $\mathscr{T}/\mathrm{R}_f$ faktortopológia és $\mathscr{T}'$ szerint. Ezért 26.6.4. alapján $\dot{f}$ folytonos a $\mathscr{T}/\mathrm{R}_f$ faktortopológia és a $\mathscr{T}'|\mathrm{Im}(f)$ altértopológia szerint is.

b) (i)⇒(ii) Tegyük fel, hogy f nyílt leképezés a $\mathscr{T}$ topológia és a $\mathscr{T}'|\mathrm{Im}(f)$ altértopológia szerint. Ha $\Omega \subseteq T$ tetszőleges halmaz, akkor minden $t \in T$ esetén

$$t \in \overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\pi_{T/\mathrm{R}_f}\langle\Omega\rangle\rangle \;\Leftrightarrow\; (\exists s \in \Omega) : \pi_{T/\mathrm{R}_f}(t) = \pi_{T/\mathrm{R}_f}(s) \;\Leftrightarrow$$
$$\Leftrightarrow\; (\exists s \in \Omega) : (t, s) \in \mathrm{R}_f \;\Leftrightarrow\; (\exists s \in \Omega) : f(t) = f(s) \;\Leftrightarrow\; t \in \overset{-1}{f}\langle f\langle\Omega\rangle\rangle,$$

ami azt jelenti, hogy $\overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\pi_{T/\mathrm{R}_f}\langle\Omega\rangle\rangle = \overset{-1}{f}\langle f\langle\Omega\rangle\rangle$. Ha $\Omega \in \mathscr{T}$, akkor az f függvény $\mathscr{T}$-$\mathscr{T}'|\mathrm{Im}(f)$ nyíltsága miatt $f\langle\Omega\rangle \in \mathscr{T}'|\mathrm{Im}(f)$, így létezik olyan $\Omega' \in \mathscr{T}'$, hogy $f\langle\Omega\rangle = \Omega' \cap \mathrm{Im}(f)$, következésképpen f $\mathscr{T}$-$\mathscr{T}'$ folytonossága alapján $\overset{-1}{f}\langle f\langle\Omega\rangle\rangle = \overset{-1}{f}\langle\Omega'\rangle \in \mathscr{T}$, tehát $\overset{-1}{\pi}_{T/\mathrm{R}_f}\langle \pi_{T/\mathrm{R}_f}\langle\Omega\rangle\rangle \in \mathscr{T}$, vagyis $\pi_{T/\mathrm{R}_f}\langle\Omega\rangle \in \mathscr{T}/\mathrm{R}_f$. Ezért a π_{T/R_f} függvény nyílt a $\mathscr{T}$ és $\mathscr{T}/\mathrm{R}_f$ topológiák szerint.

Ugyanakkor az $\dot{f}$ függvény is nyílt a $\mathscr{T}/\mathrm{R}_f$ és $\mathscr{T}'|\mathrm{Im}(f)$ topológiák szerint. Valóban, legyen $\Omega' \in \mathscr{T}/\mathrm{R}_f$. A $\pi_{T/\mathrm{R}_f} : T \to T/\mathrm{R}_f$ függvény szürjektivitása miatt nyilvánvalóan $\pi_{T/\mathrm{R}_f}\langle \overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\Omega'\rangle\rangle = \Omega'$, következésképpen

$$\dot{f}\langle\Omega'\rangle = \dot{f}\langle \pi_{T/\mathrm{R}_f}\langle \overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\Omega'\rangle\rangle\rangle = \left(\dot{f}\circ\pi_{T/\mathrm{R}_f}\right)\langle \overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\Omega'\rangle\rangle = f\langle \overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\Omega'\rangle\rangle.$$

A faktortopológiák definíciója szerint a π_{T/R_f} függvény folytonos a $\mathscr{T}$ és $\mathscr{T}/\mathrm{R}_f$ topológiák szerint, így $\overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\Omega'\rangle \in \mathscr{T}$, ezért az f függvény $\mathscr{T}$ és $\mathscr{T}'|\mathrm{Im}(f)$ topológiák szerinti nyíltságából következik, hogy $f\langle \overset{-1}{\pi}_{T/\mathrm{R}_f}\langle\Omega'\rangle\rangle \in \mathscr{T}'|\mathrm{Im}(f)$, vagyis az $\dot{f}\langle\Omega'\rangle$ halmaz nyílt $\mathscr{T}/\mathrm{R}_f$ szerint. Ezért az $\dot{f}$ függvény nyílt a $\mathscr{T}/\mathrm{R}_f$ és $\mathscr{T}'|\mathrm{Im}(f)$ topológiák szerint. Ez a tény, a)-val kombinálva maga után vonja, hogy az $\dot{f}$ függvény homeomorfizmus a $(T/\mathrm{R}_f, \mathscr{T}/\mathrm{R}_f)$ és $(\mathrm{Im}(f), \mathscr{T}'|\mathrm{Im}(f))$ topologikus terek között.

(ii)$\Rightarrow$(i) Tegyük fel, hogy (ii) teljesül. Ekkor π_{T/R_f} nyílt leképezés a $\mathscr{T}$ és $\mathscr{T}/\mathrm{R}_f$ topológiák szerint, és az $\dot{f}^{-1}$ inverzfüggvény függvény folytonos a $\mathscr{T}'|\mathrm{Im}(f)$ és $\mathscr{T}/\mathrm{R}_f$ topológiák szerint, azaz $\dot{f}$ nyílt leképezés a $\mathscr{T}/\mathrm{R}_f$ és $\mathscr{T}'|\mathrm{Im}(f)$ topológiák szerint. Ezért az $f = \dot{f}\circ\pi_{T/\mathrm{R}_f}$ függvény nyílt leképezés a $\mathscr{T}$ és $\mathscr{T}'|\mathrm{Im}(f)$ topológiák szerint, vagyis (i) teljesül. ∎

26.8.6. Állítás. *Legyen $(T, \mathscr{T})$ topologikus tér, valamint R és S olyan ekvivalenciák a T halmaz felett, hogy $R \subseteq S$. Ekkor a T/S és $(T/R)/(S/R)$ faktorhalmazok közötti kanonikus bijekció homeomorfizmus a $\mathscr{T}/S$ és $(\mathscr{T}/R)/(S/R)$ faktortopológiák szerint.*

Bizonyítás. Jelölje $f : T/S \to (T/R)/(S/R)$ a T/S a kanonikus bijekciót, tehát a

$$\begin{array}{ccc}
T/S & \xrightarrow{f} & (T/R)/(S/R) \\
{\scriptstyle \pi_{T/S}}\big\uparrow & & \big\uparrow{\scriptstyle \pi_{(T/R)/(S/R)}} \\
T & \xrightarrow[\pi_{T/R}]{} & T/R
\end{array}$$

diagram kommutatív.

Legyen $\Omega \subseteq T/S$. Ekkor f bijektivitása és $f\circ\pi_{T/S} = \pi_{(T/R)/(S/R)}\circ\pi_{T/R}$ miatt

$$\Omega \in \mathscr{T}/S \Leftrightarrow \overset{-1}{\pi}_{T/S}\langle\Omega\rangle \in \mathscr{T} \Leftrightarrow \overset{-1}{\pi}_{T/S}\langle \overset{-1}{f}\langle f\langle\Omega\rangle\rangle\rangle \in \mathscr{T} \Leftrightarrow \overset{-1}{\left(f\circ\pi_{T/S}\right)}\langle f\langle\Omega\rangle\rangle \in \mathscr{T} \Leftrightarrow$$
$$\Leftrightarrow \overset{-1}{\left(\pi_{(T/R)/(S/R)}\circ\pi_{T/R}\right)}\langle f\langle\Omega\rangle\rangle \in \mathscr{T} \Leftrightarrow \overset{-1}{\pi}_{T/R}\langle \overset{-1}{\pi}_{(T/R)/(S/R)}\langle f\langle\Omega\rangle\rangle\rangle \in \mathscr{T} \Leftrightarrow$$
$$\Leftrightarrow \overset{-1}{\pi}_{(T/R)/(S/R)}\langle f\langle\Omega\rangle\rangle \in \mathscr{T}/R \Leftrightarrow f\langle\Omega\rangle \in (\mathscr{T}/R)/(S/R),$$

ezért f homeomorfizmus a $\mathscr{T}/S$ és $(\mathscr{T}/R)/(S/R)$ faktortopológiák szerint. ∎

26.8.7. Lemma. *Legyenek $(X, \mathscr{T}_X)$, $(Y, \mathscr{T}_Y)$, $(Z, \mathscr{T}_Z)$ topologikus terek, valamint $g : X \to Y$ és $f : Y \to Z$ függvények. Ha g szürjektív és folytonos a $\mathscr{T}_X$ és $\mathscr{T}_Y$ topológiák szerint, és $f\circ g$ nyílt leképezés a $\mathscr{T}_X$ és $\mathscr{T}_Z$ topológiák szerint, akkor f nyílt leképezés a $\mathscr{T}_Y$ és $\mathscr{T}_Z$ topológiák szerint.*

Bizonyítás. Legyen $\Omega \in \mathscr{T}_Y$. Ekkor a g szürjektivitása miatt $\Omega = g\langle \overset{-1}{g}\langle\Omega\rangle\rangle$, így

$$f\langle\Omega\rangle = f\langle g\langle \overset{-1}{g}\langle\Omega\rangle\rangle\rangle = (f\circ g)\langle \overset{-1}{g}\langle\Omega\rangle\rangle,$$

ugyanakkor g folytonos a $\mathscr{T}_X$ és $\mathscr{T}_Y$ topológiák szerint, ezért $\overset{-1}{g}\langle\Omega\rangle \in \mathscr{T}_X$, így az $f\circ g$ függvény $\mathscr{T}_X$ és $\mathscr{T}_Z$ topológiák szerinti nyíltsága miatt $f\langle\Omega\rangle \in \mathscr{T}_Z$, tehát f nyílt leképezés a $\mathscr{T}_Y$ és $\mathscr{T}_Z$ topológiák szerint. ■

26.8.8. Állítás. *Legyenek $(E,\mathscr{T}_E)$ és $(F,\mathscr{T}_F)$ topologikus terek, R ekvivalencia E felett, S ekvivalencia F felett, és $f : E \to F$ olyan függvény, hogy $(f\times f)\langle R\rangle \subseteq S$ (azaz minden $(x,x') \in R$ esetén $(f(x), f(x')) \in S$). Jelölje $\dot{f}_{R,S} : E/R \to F/S$ az f függvény R-S-faktorizáltját.*

a) *Ha f folytonos a $\mathscr{T}_E$ és $\mathscr{T}_F$ topológiák szerint, akkor az $\dot{f}_{R,S}$ függvény folytonos a $\mathscr{T}_E/R$ és $\mathscr{T}_F/S$ faktortopológiák szerint.*

b) *Ha f nyílt leképezés a $\mathscr{T}_E$ és $\mathscr{T}_F$ topológiák szerint és a $\pi_{F/S} : F \to F/S$ kanonikus szürjekció nyílt leképezés a $\mathscr{T}_F$ és $\mathscr{T}_F/S$ topológiák szerint, akkor az $\dot{f}_{R,S}$ függvény nyílt leképezés a $\mathscr{T}_E/R$ és $\mathscr{T}_F/S$ faktortopológiák szerint.*

c) *Ha az $f : E \to F$ függvény homeomorfizmus a $\mathscr{T}_E$ és $\mathscr{T}_F$ topológiák szerint, és a $\pi_{F/S} : F \to F/S$ kanonikus szürjekció nyílt leképezés a $\mathscr{T}_F$ és $\mathscr{T}_F/S$ topológiák szerint, és $(f\times f)\langle R\rangle = S$, akkor az $\dot{f}_{R,S}$ függvény homeomorfizmus a $\mathscr{T}_E/R$ és $\mathscr{T}_F/S$ faktortopológiák szerint.*

Bizonyítás. Az $\dot{f}_{R,S} : E/R \to F/S$ függvényre $\dot{f}_{R,S} \circ \pi_{E/R} = \pi_{F/S}\circ f$ teljesül, vagyis a következő diagram kommutatív:

$$\begin{array}{ccc} E/R & \xrightarrow{\dot{f}_{R,S}} & F/S \\ {\scriptstyle \pi_{E/R}}\uparrow & & \uparrow{\scriptstyle \pi_{F/S}} \\ E & \xrightarrow[f]{} & F \end{array}$$

a) A faktortopológiák definíciója szerint a $\pi_{F/S} : F \to F/S$ kanonikus szürjekció folytonos a $\mathscr{T}_F$ és $\mathscr{T}_F/S$ topológiák szerint, tehát ha f folytonos a $\mathscr{T}_E$ és $\mathscr{T}_F$ topológiák szerint, akkor az $\dot{f}_{R,S}\circ\pi_{E/R} = \pi_{F/S}\circ f : E \to F/S$ függvény folytonos a $\mathscr{T}_E$ és $\mathscr{T}_F/S$ topológiák szerint, ami 26.8.4. alapján azt jelenti, hogy $\dot{f}_{R,S}$ folytonos a $\mathscr{T}_E/R$ és $\mathscr{T}_F/S$ topológiák szerint.

b) Ha f nyílt leképezés a $\mathscr{T}_E$ és $\mathscr{T}_F$ topológiák szerint és a $\pi_{F/S} : F \to F/S$ kanonikus szürjekció nyílt leképezés a $\mathscr{T}_F$ és $\mathscr{T}_F/S$ topológiák szerint, akkor az $\dot{f}_{R,S}\circ\pi_{E/R} = \pi_{F/S}\circ f : E \to F/S$ függvény nyílt leképezés a $\mathscr{T}_E$ és $\mathscr{T}_F/S$ topológiák. Mivel pedig a $\pi_{E/R} : E \to E/R$ kanonikus szürjekció folytonos a $\mathscr{T}_E$ és $\mathscr{T}_E/R$ topológiák szerint, így az előző lemma alapján az $\dot{f}_{R,S}$ függvény nyílt leképezés a $\mathscr{T}_E/R$ és $\mathscr{T}_F/S$ faktortopológiák szerint.

c) Ha f bijekció és $(f\times f)\langle R\rangle = S$, akkor az $\dot{f}_{R,S} : E/R \to F/S$ függvény bijekció (6.11.8. d) pont). Ezért a c) állítás nyilvánvalóan következik a)-ból és b)-ből. ■

26.8.9. Definíció. *Legyen $((T_i,\mathscr{T}_i))_{i\in I}$ topologikus terek rendszere. Vezessük be a $T := \bigcup_{i\in I}(\{i\}\times T_i)$ halmazt, és minden $I \ni i$-re értelmezzük az $f_i : T_i \to T;\ t \mapsto (i,t)$*

függvényt. A $((T_i, \mathscr{T}_i), f_i)_{i\in I}$ *rendszer által előállított* T *feletti finális topológiát a* $(\mathscr{T}_i)_{i\in I}$ **topológia-rendszer összegének** *nevezzük, és a* $\bigsqcup_{i\in I} \mathscr{T}_i$ *szimbólummal jelöljük. Az* $\left(\bigcup_{i\in I}(\{i\}\times T_i), \bigsqcup_{i\in I}\mathscr{T}_i\right)$ *topologikus teret a* $((T_i, \mathscr{T}_i))_{i\in I}$ **topologikus tér-rendszer összegének** *nevezzük.*

Megjegyezzük, hogy ha $(T_i)_{i\in I}$ tetszőleges rendszer, akkor a $\bigcup_{i\in I}(\{i\}\times T_i)$ halmazt a $\bigsqcup_{i\in I} T_i$ szimbólummal is jelöljük, és a $(T_i)_{i\in I}$ rendszer *halmazösszegének* vagy *diszjunkt uniójának* nevezzük.

26.9. Összefüggő terek

26.9.1. Definíció. *Legyen* $(T, \mathscr{T})$ *topologikus tér. Azt mondjuk, hogy a* $C \subseteq T$ *halmaz* **összefüggő** *a* $\mathscr{T}$ *topológia szerint, ha nem léteznek olyan* $E, F \subseteq T$ *halmazok, amelyekre* $C = E \cup F$, $E \neq \emptyset \neq F$ *és* $E \cap \overline{F} = \emptyset = \overline{E} \cap F$. *Azt mondjuk, hogy a* $(T, \mathscr{T})$ *topologikus tér* **összefüggő**, *ha a* T *halmaz összefüggő a* $\mathscr{T}$ *topológia szerint.*

Könnyen belátható, hogy ha $(T, \mathscr{T})$ topologikus tér, akkor a $C \subseteq T$ halmaz pontosan akkor összefüggő a $\mathscr{T}$ topológia szerint, ha a $(C, \mathscr{T}|C)$ topologikus altér összefüggő topologikus tér.

26.9.2. Állítás. *Ha* $(T, \mathscr{T})$ *topologikus tér, akkor a következő állítások ekvivalensek.*

(i) $(T, \mathscr{T})$ *összefüggő topologikus tér.*

(ii) *Minden* $E \subseteq T$ *halmazra, ha* E *nyílt és zárt a* $\mathscr{T}$ *topológia szerint, akkor* $E = \emptyset$ *vagy* $E = T$,

(iii) *Minden* $E \subseteq T$ *halmazra, ha* $E \neq \emptyset$ *és* $E \neq T$, *akkor* $\mathrm{Fr}(E) \neq \emptyset$.

Bizonyítás. (i)⇒(ii) Tegyük fel, hogy (ii) nem igaz, és legyen $E \subseteq T$ olyan nyílt-zárt halmaz, amelyre $E \neq \emptyset$ és $E \neq T$. Ekkor az $F := T \setminus E$ halmaz olyan, hogy $F \neq \emptyset$ és $F \neq T$, továbbá $T = E \cup F$, és F is nyílt-zárt részhalmaza T-nek, így $\overline{E} \cap F = E \cap F = \emptyset$ és $E \cap \overline{F} = E \cap F = \emptyset$, tehát T nem összefüggő halmaz, így (i) nem igaz.

(ii)⇒(iii) Tegyük fel, hogy (iii) nem igaz, és legyen $E \subseteq T$ olyan halmaz, amelyre $E \neq \emptyset$, $E \neq T$, azonban $\mathrm{Fr}(E) = \emptyset$. Ekkor E nyílt-zárt halmaz, és $E \neq \emptyset$, valamint $E \neq T$, tehát (ii) nem igaz.

(iii)⇒(i) Tegyük fel, hogy (i) nem igaz, és legyenek $E, F \subseteq T$ olyan halmazok, amelyekre $T = E \cup F$, $E \neq \emptyset \neq F$ és $\overline{E} \cap F = \emptyset = E \cap \overline{F}$. Ekkor $E \neq \emptyset$ és $E \neq T$, továbbá $\overline{E} \subseteq T \setminus F = E$ miatt $\overline{E} = E$. Ugyanakkor $\overline{F} \subseteq T \setminus E = F$ miatt $\overline{F} = F$, így $\mathrm{Int}(E) = T \setminus \overline{T \setminus E} = T \setminus F = E$. Ezért $\mathrm{Fr}(E) = \emptyset$, vagyis (iii) nem igaz. ■

26.9.3. Tétel. (**Bolzano-tétel.**) *Ha* $(T, \mathscr{T})$ *és* $(T', \mathscr{T}')$ *topologikus terek, az* $f : T \to T'$ *függvény folytonos a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, és a* $C \subseteq T$ *halmaz összefüggő* $\mathscr{T}$ *szerint, akkor az* $f\langle C\rangle \subseteq T'$ *halmaz összefüggő* $\mathscr{T}'$ *szerint.*

Bizonyítás. Tegyük fel, hogy $C \subseteq T$ olyan halmaz, amelyre $f\langle C\rangle$ nem összefüggő $\mathscr{T}'$ szerint; megmutatjuk, hogy ekkor C sem összefüggő $\mathscr{T}$ szerint.

A feltevés alapján léteznek olyan $E', F' \subseteq M'$ halmazok, hogy $f\langle C\rangle = E' \cup F'$,

$E' \neq \emptyset \neq F'$ és $\overline{E'} \cap F' = \emptyset = E' \cap \overline{F'}$. Legyenek $E := C \cap \overset{-1}{f}\langle E' \rangle$ és $F := C \cap \overset{-1}{f}\langle F' \rangle$; ekkor nyilvánvalóan $C = E \cup F$. A folytonosság topologikus jellemzése szerint $\overset{-1}{f}\langle \overline{E'} \rangle$ és $\overset{-1}{f}\langle \overline{F'} \rangle$ zárt halmazok a $\mathscr{T}$ topológia szerint, ezért $\overline{\overset{-1}{f}\langle E' \rangle} \subseteq \overset{-1}{f}\langle \overline{E'} \rangle$, valamint $\overline{\overset{-1}{f}\langle F' \rangle} \subseteq \overset{-1}{f}\langle \overline{F'} \rangle$. Ebből következik, hogy

$$\overline{E} \cap F := \overline{C \cap \overset{-1}{f}\langle E' \rangle} \cap (C \cap \overset{-1}{f}\langle F' \rangle) \subseteq \overline{\overset{-1}{f}\langle E' \rangle} \cap \overset{-1}{f}\langle F' \rangle \subseteq$$
$$\subseteq \overset{-1}{f}\langle \overline{E'} \rangle \cap \overset{-1}{f}\langle F' \rangle = \overset{-1}{f}\langle \overline{E'} \cap F' \rangle = \emptyset,$$

és teljesen hasonlóan kapjuk, hogy $E \cap \overline{F} = \emptyset$, ezért $\overline{E} \cap F = \emptyset = E \cap \overline{F}$, tehát C nem összefüggő a $\mathscr{T}$ topológia szerint. ■

26.9.4. Állítás. *Legyen $(T, \mathscr{T})$ topologikus tér.*

a) *Ha $C \subseteq T$ összefüggő halmaz a $\mathscr{T}$ topológia szerint, akkor $\overline{C}$ is összefüggő a $\mathscr{T}$ topológia szerint.*

b) *Ha $(C_i)_{i \in I}$ olyan nem üres rendszer, hogy minden $i \in I$ esetén $C_i \subseteq T$ összefüggő halmaz a $\mathscr{T}$ topológia szerint és $\bigcap_{i \in I} C_i \neq \emptyset$, akkor az $\bigcup_{i \in I} C_i$ halmaz összefüggő a $\mathscr{T}$ topológia szerint.*

c) *Minden $C \subseteq T$ nem üres, $\mathscr{T}$ szerint összefüggő halmazhoz létezik olyan tartalmazás tekintetében legnagyobb $\widehat{C} \subseteq T$ halmaz, amely összefüggő a $\mathscr{T}$ topológia szerint és $C \subseteq \widehat{C}$ (ez a C halmaz* **összefüggő komponense** *a $\mathscr{T}$ topológia szerint).*

Bizonyítás. a) Tegyük fel, hogy $C \subseteq t$ olyan halmaz, amelyre $\overline{C}$ nem összefüggő; megmutatjuk, hogy ekkor C sem összefüggő.

A feltevés alapján ugyanis vehetünk olyan $E, F \subseteq T$ halmazokaz, amelyekre $\overline{C} = E \cup F$, $E \neq \emptyset \neq F$ és $\overline{E} \cap F = \emptyset = E \cap \overline{F}$. Ekkor $C = (C \cap E) \cup (C \cap F)$, továbbá $\overline{C \cap E} \cap (C \cap F) \subseteq \overline{E} \cap F = \emptyset$ és $(C \cap E) \cap \overline{C \cap F} \subseteq E \cap \overline{F} = \emptyset$, tehát a C halmaz nem összefüggő, ha $C \cap E \neq \emptyset$ *és* $C \cap F \neq \emptyset$.

Ha $C \cap E = \emptyset$ volna, akkor $C = C \cap F$, azaz $C \subseteq F$, így $\overline{C} \subseteq \overline{F}$ teljesülne. Ekkor $\overline{C} = \overline{C} \cap \overline{F} = (E \cup F) \cap \overline{F} = (E \cap \overline{F}) \cup (F \cap \overline{F}) = F$, hiszen $E \cap \overline{F} = \emptyset$. Ebből $\overline{C} = E \cup F$ miatt $E = \emptyset$ következne, holott $E \neq \emptyset$; ezért $C \cap E \neq \emptyset$.

Ha $C \cap F = \emptyset$ volna, akkor $C = C \cap E$, azaz $C \subseteq E$, így $\overline{C} \subseteq \overline{E}$ teljesülne. Ekkor $\overline{C} = \overline{C} \cap \overline{E} = (E \cup F) \cap \overline{E} = (E \cap \overline{E}) \cup (F \cap \overline{E}) = E$, hiszen $F \cap \overline{E} = \emptyset$. Ebből $\overline{C} = E \cup F$ miatt $F = \emptyset$ következne, holott $F \neq \emptyset$; ezért $C \cap F \neq \emptyset$.

Ez viszont azt jelenti, hogy C nem összefüggő.

b) Ha $I = \emptyset$, akkor $\bigcup_{i \in I} C_i = \emptyset$, tehát az állítás igaz, így feltehető, hogy $I \neq \emptyset$.

Indirekt bizonyítunk, tehát feltesszük, hogy $\bigcup_{i \in I} C_i$ nem összefüggő, és veszünk olyan $E, F \subseteq T$ halmazokat, amelyekre $\bigcup_{i \in I} C_i = E \cup F$, $E \neq \emptyset \neq F$ és $\overline{E} \cap F = \emptyset = \overline{F} \cap E$. Ha $i \in I$, akkor nyilvánvalóan $C_i = (C_i \cap E) \cup (C_i \cap F)$ és $\overline{C_i \cap E} \cap (C_i \cap F) \subseteq \overline{E} \cap F = \emptyset$, valamint $(C_i \cap E) \cap \overline{C_i \cap F} \subseteq E \cap \overline{F} = \emptyset$, így C_i összefüggősége miatt $C_i \cap E = \emptyset$ *vagy* $C_i \cap F = \emptyset$. Legyen $t \in \bigcap_{i \in I} C_i$ rögzített elem. Ekkor $t \in E \cup F$, tehát t az E és F

diszjunkt halmazok közül pontosan az egyiknek eleme. Ha $t \in E$, akkor minden $i \in I$ esetén $t \in C_i \cap E$, ezért $C_i \cap F = \emptyset$. Ekkor $F = \bigcup_{i \in I}(C_i \cap F) = \emptyset$, holott $F \neq \emptyset$. Ezért $t \in F$, következésképpen minden $i \in I$ esetén $t \in C_i \cap F$, így $C_i \cap E = \emptyset$. Ekkor viszont $E = \bigcup_{i \in I}(C_i \cap E) = \emptyset$, holott $E \neq \emptyset$, és ez ellentmondás.

c) Az előző állítás szerint a C halmazt tartalmazó T-beli összefüggő részhalmazok *uniója* összefüggő, és természetesen tartalmazza a T minden olyan összefüggő részhalmazát, amely tartalmazza C-t. ■

26.9.5. Következmény. *Ha $(T, \mathscr{T})$ topologikus tér, akkor minden $t \in T$ ponthoz létezik olyan tartalmazás tekintetében legnagyobb $C \subseteq T$ halmaz, amely összefüggő a $\mathscr{T}$ topológia szerint és $t \in C$ (ez a t pont* **összefüggő komponense** *a $\mathscr{T}$ topológia szerint).*

Bizonyítás. Nyilvánvalóan következik az előző állítás c) pontjából és abból a trivialitásból, hogy minden topologikus térben minden egy elemű halmaz összefüggő. ■

26.9.6. Következmény. *Topologikus tér nem üres összefüggő részhalmazának halmaz összefüggő komponense zárt halmaz.*

Bizonyítás. Egy C nem üres összefüggő halmaz összefüggő komponensének a lezártja összefüggő az előző állítás a) pontja szerint, valamint tartalmazza a C halmazt, ezért részhalmaza a C összefüggő komponensének. ■

Z Vigyázzunk arra, hogy topologikus térben létezhetnek nem nyílt összefüggő komponensek, sőt lehetséges, hogy egyetlen össszefüggő komponens sem nyílt.

26.9.7. Definíció. *Azt mondjuk, hogy a $(T, \mathscr{T})$ topologikus tér* **extremális**, *ha létezik T-ben $\mathscr{T}$ szerint nyílt-zárt halmazokból álló topologikus bázis. Azt mondjuk, hogy a $(T, \mathscr{T})$ topologikus tér* **teljesen összefüggéstelen**, *ha T minden $\mathscr{T}$ szerint összefüggő komponense egy elemű halmaz.*

Nyilvánvaló, hogy a $(T, \mathscr{T})$ topologikus tér pontosan akkor extremális, ha minden $t \in T$ és $V \in \mathscr{T}(t)$ esetén van olyan $\Omega \subseteq T$ halmaz, amely $\mathscr{T}$ szerint nyílt-zárt és $t \in \Omega \subseteq V$. Másként fogalmazva: topologikus tér extremalitása ekvivalens azzal, hogy a tér minden pontjának létezik nyílt-zárt halmazokból álló környezetbázisa.

Világos, hogy a diszkrét terek extremálisak is és teljesen összefüggéstelenek is. Ugyanez igaz a $(\mathbb{Q}, \mathscr{E}|\mathbb{Q})$ nem diszkrét topologikus térre is.

Később látni fogjuk, hogy az extremalitás bizonyos szétválasztási tulajdonság mellett maga után vonja a teljes összefüggéstelenséget.

26.10. Ívszerűen összefüggő terek

26.10.1. Definíció. *Ha T halmaz, akkor T-ben haladó* **görbének** *nevezünk minden olyan γ függvényt, amelyre* $\mathrm{Dom}(\gamma) \subseteq \mathbb{R}$ *intervallum és* $\mathrm{Im}(\gamma) \subseteq T$. *Ha T halmaz, akkor T-ben haladó* **ívnek** *nevezünk minden olyan T-ben haladó γ görbét, amelyre* $\mathrm{Dom}(\gamma)$ *nem üres kompakt intervallum $\mathbb{R}$-ben.*

26.10.2. Definíció. *Ha T halmaz és γ T-ben haladó ív, akkor egyértelműen léteznek olyan $a, b \in \mathbb{R}$ számok, hogy $a \leq b$ és* $\mathrm{Dom}(\gamma) = [a, b]$; *ekkor a $\gamma(a) \in M$ (illetve $\gamma(b) \in M$) pontot a γ ív* **kezdőpontjának** (*illetve* **végpontjának**) *nevezzük; továbbá azt mondjuk, hogy a γ ív* **zárt**, *ha a γ kezdőpontja egyenlő a végpontjával.*

26.10.3. Definíció. *Legyen $(T, \mathscr{T})$ topologikus tér.*

– *Egy $C \subseteq T$ halmazt* **ívszerűen összefüggőnek** *nevezzük (a $\mathscr{T}$ topológia szerint), ha minden $t, s \in C$ ponthoz létezik olyan T-ben haladó γ folytonos ív, amelyre $\mathrm{Im}(\gamma) \subseteq C$ (vagyis γ a C halmazban halad), továbbá γ kezdőpontja a t, és végpontja az s pont (amit úgy fejezünk ki, hogy γ* **összeköti** *az t és s pontokat).*

– *Az $(T, \mathscr{T})$ topologikus teret* **ívszerűen összefüggőnek** *nevezzük, ha a T halmaz ívszerűen összefüggő a $\mathscr{T}$ topológia szerint.*

– *A $(T, \mathscr{T})$ topologikus teret* **lokálisan ívszerűen összefüggőnek** *nevezzük, ha minden $t \in T$ esetén a t pont minden $V \in \mathscr{T}(t)$ környezetéhez létezik olyan $W \in \mathscr{T}(t)$ környezet, hogy W ívszerűen összefüggő halmaz a $\mathscr{T}$ topológia szerint és $W \subseteq V$ (vagyis T minden pontjának létezik ívszeűen összefüggő halmazokból álló környezetbázisa).*

26.10.4. Állítás. *Ha $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek, és $f : T \to T'$ folytonos függvény, akkor minden $C \subseteq T$, $\mathscr{T}$ topológia szerint ívszerűen összefüggő halmazra $f\langle C \rangle$ a $\mathscr{T}'$ topológia szerint ívszerűen összefüggő.*

Bizonyítás. Legyenek $t', s' \in f\langle C \rangle$ tetszőlegesek, és vegyünk olyan $t, s \in C$ pontokat, amelyekre $t' = f(t)$ és $s' = f(s)$. A C halmaz ívszerű összefüggősége miatt vehetünk olyan $a, b \in \mathbb{R}$, $a \leq b$ számokat, és olyan $\gamma : [a, b] \to T$ folytonos ívet, amelyekre $\mathrm{Im}(\gamma) \subseteq C$, $t = \gamma(a)$ és $s = \gamma(b)$. A folytonos függvények kompozíciójának folytonossága következtében $f \circ \gamma : [a, b] \to T'$ folytonos függvény, és $\mathrm{Im}(f \circ \gamma) = f\langle \mathrm{Im}(\gamma) \rangle \subseteq f\langle C \rangle$, valamint $(f \circ \gamma)(a) = t'$ és $(f \circ \gamma)(b) = s'$. Ezért t' és s' összeköthetők $f\langle C \rangle$-ben haladó folytonos ívvel. ■

Most tisztázzuk az összefüggőség és az ívszerű összefüggőség kapcsolatát. Ehhez szükségünk lesz a következő lemmára.

26.10.5. Lemma. *Egy $C \subseteq \mathbb{R}$ halmaz pontosan akkor összefüggő az euklidészi topológia szerint, ha C konvex.*

Bizonyítás. Tegyük fel, hogy C nem konvex, és legyenek $a, b \in C$ olyan pontok, hogy $a < b$, és az $[a, b]$ szakasz (ami nem más, mint az $[a, b]$ intervallum) *nem része* C-nek, vagyis van olyan $c \in [a, b]$, amelyre $c \notin C$. Ekkor az $E :=]\leftarrow, c[\cap C$ és $F :=]c, \to[\cap C$ halmazokra $a \in E$, $b \in F$, $C = E \cup F$ nyilvánvalóan teljesül, továbbá

$$\overline{E} \cap F \subseteq \overline{]\leftarrow, c[} \cap]c, \to[=]\leftarrow, c] \cap]c, \to[= \emptyset,$$

valamint

$$E \cap \overline{F} \subseteq]\leftarrow, c[\cap \overline{]c, \to[} =]\leftarrow, c[\cap [c, \to[= \emptyset,$$

is nyilvánvalóan igaz, így C nem összefüggő. Tehát ha C összefüggő, akkor konvex.

Most tegyük fel, hogy C konvex; megmutatjuk, hogy C összefüggő. Indirekt bizonyítunk, tehát feltesszük, hogy C konvex, de nem összefüggő. Legyenek $E, F \subseteq M$ olyan halmazok, amelyekre $C = E \cup F$, $E \neq \emptyset \neq F$ és $\overline{E} \cap F = \emptyset = E \cap \overline{F}$. Legyenek $a \in E$ és $b \in F$; az általánosság korlátozása nélkül feltehetjük, hogy $a < b$. Ekkor az $E' := [a, b] \cap E$ halmaz nem üres és felülről korlátos, ezért képezhető a $c := \sup(E')$ szám. Világos, hogy $c \in [a, b] \subseteq C$, mert C konvex, így $C = E \cup F$ miatt $c \in E$ vagy $c \in F$. Továbbá $c \in \overline{E'} \subseteq \overline{E}$, ezért $\overline{E} \cap F = \emptyset$ miatt $c \notin F$, vagyis $c \in E$. Ez azt jelenti, hogy $c \in E'$, vagyis c az E' halmaz *legnagyobb* eleme. Ugyanakkor $c \in E$ és $E \cap \overline{F} = \emptyset$ miatt $c \notin \overline{F}$, ezért van olyan $\delta \in \mathbb{R}_+^*$, hogy $]c - \delta, c + \delta[\cap F = \emptyset$. Világos, hogy $c < b$, hiszen

$b \in F$ és $c \notin F$, ezért δ megválasztható úgy, hogy $\delta < b - c$ teljesüljön. Ha $x \in]c, c+\delta[$, akkor $x \in [a, b]$, tehát $x \in E$ vagy $x \in F$; de $]c, c+\delta[\cap F = \emptyset$ miatt $x \notin F$, vagyis $x \in E$. Tehát a $]c, c+\delta[$ intervallum minden eleme E'-ben van és *nagyobb* c-nél, holott c az E' legnagyobb eleme; ez ellentmondás. ■

26.10.6. Állítás. *Topologikus térben minden ívszerűen összefüggő halmaz összefüggő.*

Bizonyítás. Legyen $(T, \mathscr{T})$ topologikus tér és $C \subseteq T$ ívszerűen összefüggő halmaz; megmutatjuk, hogy C összefüggő. Indirekt bizonyítunk, tehát feltesszük, hogy C nem összefüggő; legyenek $E, F \subseteq M$ olyan halmazok, amelyekre $C = E \cup F$, $E \neq \emptyset \neq F$ és $\overline{E} \cap F = \emptyset = E \cap \overline{F}$. Rögzítsünk $x \in E$ és $y \in F$ pontokat, és a C ívszerű összefüggőségét kihasználva vegyünk olyan C-ben haladó γ folytonos ívet, amely összeköti az x és y pontokat; legyen $\mathrm{Dom}(\gamma) = [a, b]$. Ekkor $[a, b] = \overset{-1}{\gamma}\langle E\rangle \cup \overset{-1}{\gamma}\langle F\rangle$, mivel $\mathrm{Im}(\gamma) \subseteq C = E \cup F$. Továbbá, $a \in \overset{-1}{\gamma}\langle E\rangle$, mert $\gamma(a) = x \in E$, és $b \in \overset{-1}{\gamma}\langle F\rangle$, mert $\gamma(b) = y \in F$. A folytonosság topologikus jellemzése alapján $\overset{-1}{\gamma}\langle \overline{E}\rangle$ és $\overset{-1}{\gamma}\langle \overline{F}\rangle$ zárt halmazok $[a, b]$-ben az euklidészi altérmetrika szerint. De az $[a, b]$ intervallum zárt halmaz $\mathbb{R}$-ben az euklidészi metrika szerint, így $\overset{-1}{\gamma}\langle \overline{E}\rangle$ és $\overset{-1}{\gamma}\langle \overline{F}\rangle$ zárt halmazok $\mathbb{R}$-ben az euklidészi szerint. Ezért $\overline{\overset{-1}{\gamma}\langle E\rangle} \subseteq \overset{-1}{\gamma}\langle \overline{E}\rangle$ és $\overline{\overset{-1}{\gamma}\langle F\rangle} \subseteq \overset{-1}{\gamma}\langle \overline{F}\rangle$ teljesül. Ebből következik, hogy

$$\overline{\overset{-1}{\gamma}\langle E\rangle} \cap \overset{-1}{\gamma}\langle F\rangle \subseteq \overset{-1}{\gamma}\langle \overline{E}\rangle \cap \overset{-1}{\gamma}\langle F\rangle = \overset{-1}{\gamma}\langle \overline{E} \cap F\rangle = \emptyset$$

$$\overset{-1}{\gamma}\langle E\rangle \cap \overline{\overset{-1}{\gamma}\langle F\rangle} \subseteq \overset{-1}{\gamma}\langle E\rangle \cap \overset{-1}{\gamma}\langle \overline{F}\rangle = \overset{-1}{\gamma}\langle E \cap \overline{F}\rangle = \emptyset.$$

Ez azt jelenti, hogy az $[a, b]$ intervallum nem összefüggő halmaz $\mathbb{R}$-ben az euklidészi metrika szerint, ami ellentmond az előző lemmának. ■

Habár az összefüggőségből általában nem következtethetünk az ívszerű összefüggőségre, létezik olyan speciális eset, amikor az összefüggőség ekvivalens az ívszerű összefüggőséggel. Erről szól a következő tétel.

26.10.7. Tétel. *Lokálisan ívszerűen összefüggő topologikus térben nyílt halmaz pontosan akkor összefüggő, ha ívszerűen összefüggő.*

Bizonyítás. Tegyük fel, hogy $(T, \mathscr{T})$ lokálisan ívszerűen összefüggő topologikus tér, és $\Omega \subseteq T$ nem üres, összefüggő nyílt halmaz. Rögzítsünk egy $c \in \Omega$ pontot, és jelölje Ω_c azon $t \in \Omega$ pontok halmazát, amelyekhez van olyan Ω-ban haladó folytonos ív, amely összeköti a c és t pontokat.

Először megmutatjuk, hogy Ω_c nyílt halmaz a $\mathscr{T}$ topológia szerint. Legyen ugyanis $t \in \Omega_c$, és az Ω nyíltsága, valamint a $(T, \mathscr{T})$ toplogikus tér lokális ívszerű összefüggősége alapján vegyünk olyan $V \in \mathscr{T}(t)$ ívszerűen összefüggő környezetet, amelyre $V \subseteq \Omega$. Állítjuk, hogy ekkor $V \subseteq \Omega_c$, ezért t belső pontja Ω_c-nek a $\mathscr{T}$ topológia szerint. Valóban, legyen $s \in V$ és V ívszerű összefüggősége alapján rögzítsünk olyan $\gamma_s : [a_s, b_s] \to M$ folytonos ívet, amelyre $\mathrm{Im}(\gamma_s) \subseteq V \subseteq \Omega$, és $\gamma_s(a_s) = t$ és $\gamma_s(b_s) = s$. Mivel $t \in \Omega_c$, így vehetünk olyan $\gamma_t : [a_t, b_t] \to M$ folytonos ívet, amelyre $\mathrm{Im}(\gamma_t) \subseteq \Omega$, és $\gamma_t(a_t) = c$ és $\gamma_t(b_t) = t$. Ekkor a

$$\gamma : [0, 1] \to M; \quad \tau \mapsto \begin{cases} \gamma_t(a_t + 2(b_t - a_t)\tau) & \text{, ha } \tau \in [0, 1/2], \\ \gamma_s(a_s + 2(b_s - a_s)(\tau - 1/2)) & \text{, ha } \tau \in]1/2, 1] \end{cases}$$

függvény jól értelmezett, mert $\gamma_t(b_t) = t = \gamma_s(a_s)$, és γ olyan Ω-ban haladó ív, amelyre $\gamma(0) = c$ és $\gamma(1) = s$, továbbá γ folytonos is (26.4.6. c) pont). Ezért $s \in \Omega$, következésképpen $V \subseteq \Omega_c$.

Megmutatjuk, hogy $\overline{\Omega_c} \cap \Omega = \Omega_c$. Legyen $t \in \overline{\Omega_c} \cap \Omega$ rögzített, és ismét az Ω nyíltsága alapján vegyünk olyan $V \in \mathscr{T}(t)$ ívszerűen összefüggő környezetet, amelyre $V \subseteq \Omega$. Ekkor $t \in \overline{\Omega_c}$ miatt $V \cap \Omega_c \neq \emptyset$; legyen s eleme ennek a halmaznak. Mivel $s \in \Omega_c$, így Ω_c definíciója alapján vehetünk olyan $\gamma_s : [a_s, b_s] \to M$ folytonos ívet, amelyre $\mathrm{Im}(\gamma_s) \subseteq \Omega$, és $\gamma_s(a_s) = c$ és $\gamma_s(b_s) = s$. A V halmaz ívszerű összefüggősége és $s, t \in V$ miatt vehetünk olyan $\gamma_t : [a_t, b_t] \to M$ folytonos ívet, amelyre $\mathrm{Im}(\gamma_t) \subseteq V \subseteq \Omega$, és $\gamma_t(a_t) = s$ és $\gamma_t(b_t) = t$. Ekkor a

$$\gamma : [0,1] \to M; \quad \tau \mapsto \begin{cases} \gamma_s(a_s + 2(b_s - a_s)\tau) & , \text{ha } \tau \in [0, 1/2], \\ \gamma_t(a_t + 2(b_t - a_t)(\tau - 1/2)) & , \text{ha } \tau \in \,]1/2, 1] \end{cases}$$

függvény jól értelmezett, mert $\gamma_s(b_s) = s = \gamma_t(a_t)$, és γ olyan Ω-ban haladó ív, amelyre $\gamma(0) = c$ és $\gamma(1) = t$, továbbá γ folytonos is (26.4.6. c) pont). Ezért $t \in \Omega_c$, következésképpen $\overline{\Omega_c} \cap \Omega \subseteq \Omega_c$. Ugyanakkor $\omega_c \subseteq \overline{\Omega_c} \cap \Omega$ triviálisan igaz, tehát $\overline{\Omega_c} \cap \Omega = \Omega_c$.

Állítjuk, hogy $\Omega = \Omega_c$. Tegyük fel, hogy nem így van, tehát Ω_c valódi részhalmaza Ω-nak, vagyis $\Omega \setminus \Omega_c \neq \emptyset$. Természetesen $c \in \Omega_c$, így $\Omega_c \neq \emptyset$. Ekkor az előző bekezdés alapján $\overline{\Omega_c} \cap (\Omega \setminus \Omega_c) = (\overline{\Omega_c} \cap \Omega) \setminus \Omega_c = \Omega_c \setminus \Omega_c = \emptyset$. Továbbá, ha $x \in \overline{\Omega \setminus \Omega_c} \cap \Omega_c$, akkor Ω_c nyílt környezete x-nek, ezért $(\Omega \setminus \Omega_c) \cap \Omega_c \neq \emptyset$, holott ez a metszethalmaz nyilvánvalóan üres. Ezért $\overline{\Omega \setminus \Omega_c} \cap \Omega_c = \emptyset$. Ez azt jelenti, hogy az $E := \Omega_c$ és $F := \Omega \setminus \Omega_c$ halmazok olyanok, hogy $\Omega = E \cup F$, $E \neq \emptyset \neq F$ és $\overline{E} \cap F = \emptyset = E \cap \overline{F}$, vagyis Ω nem összefüggő halmaz, ami ellentmondás.

Végül megmutatjuk, hogy Ω_c ívszerűen összefüggő halmaz. Valóban, legyenek $s, t \in \Omega_c$, és Ω_c definíciója alapján vegyünk olyan $\gamma_s : [a_s, b_s] \to M$ és $\gamma_t : [a_t, b_t] \to M$ folytonos ívet, hogy $\mathrm{Im}(\gamma_s) \subseteq \Omega$ és $\mathrm{Im}(\gamma_t) \subseteq \Omega$, valamint $\gamma_s(a_s) = \gamma_t(a_t) = c$ és $\gamma_s(b_s) = s$ és $\gamma_t(b_t) = t$. Ekkor a

$$\gamma : [0,1] \to M; \quad \tau \mapsto \begin{cases} \gamma_s(a_s + (b_s - a_s)(1 - 2\tau)) & , \text{ha } \tau \in [0, 1/2], \\ \gamma_t(a_t + 2(b_t - a_t)(\tau - 1/2)) & , \text{ha } \tau \in \,]1/2, 1] \end{cases}$$

függvény jól értelmezett, mert $\gamma_s(a_s) = c = \gamma_t(a_t)$, és γ olyan Ω_c-ben haladó ív, amelyre $\gamma(0) = s$ és $\gamma(1) = t$, továbbá γ folytonos is (26.4.6. c) pont). Ezért Ω_c és vele együtt Ω is ívszerűen összefüggő halmaz. ■

27. fejezet

Szétválasztási tulajdonságok

27.1. Elemi szétválasztási tulajdonságok

27.1.1. Definíció. *Azt mondjuk, hogy a* $(T, \mathscr{T})$ *topologikus tér:*

– T_0**-tér**, *ha minden* $t, t' \in T$ *pontra,* $t \neq t'$ *esetén létezik olyan* $V \in \mathscr{T}(t)$ *hogy* $t' \notin V$ *vagy létezik olyan* $V' \in \mathscr{T}(t')$*, hogy* $t \notin V'$*;*

– T_1**-tér**, *ha minden* $t, t' \in T$ *pontra,* $t \neq t'$ *esetén létezik olyan* $V \in \mathscr{T}(t)$ *hogy* $t' \notin V$ *és létezik olyan* $V' \in \mathscr{T}(t')$*, hogy* $t \notin V'$*;*

– T_2**-tér**, *ha minden* $t, t' \in T$ *pontra,* $t \neq t'$ *esetén létezik olyan* $V \in \mathscr{T}(t)$ *és* $V' \in \mathscr{T}(t')$*, hogy* $V \cap V' = \emptyset$*.*

Megemlítjük, hogy a T_0-tereket *Kolmogorov-tereknek*, míg a T_2-tereket *Hausdorff-tereknek* is nevezzük. E két elnevezés közül csak az utóbbi terjedt el széles körben. A Hausdorff-tereket még *szeparált topologikus tereknek* is nevezzük.

Logikai okok miatt nyilvánvaló, hogy minden T_1-tér T_0-tér és minden T_2-tér T_1-tér. Antidiszkrét topologikus tér nem T_0-tér, ha az alaphalmaz legalább két elemű, hiszen ilyen térben bármely két pontnak ugyanazok a környezetei.

Létezik olyan T_0-tér, amely nem T_1-tér. Legyen például $\mathscr{T}$ azon $\Omega \subseteq \mathbb{R}$ halmazok halmaza, amelyekre teljesül az, hogy minden $t \in \Omega$ esetén $[t, \rightarrow[\subseteq \Omega$. Ekkor $\mathscr{T}$ topológia $\mathbb{R}$ felett, és az $(\mathbb{R}, \mathscr{T})$ topologikus tér T_0-tér, de nem T_1-tér. Valóban, ha $t, t' \in \mathbb{R}$ és $t \neq t'$, akkor $t < t'$ vagy $t' < t$; az első esetben $[t', \rightarrow[\in \mathscr{T}(t')$ és $t \notin [t', \rightarrow[$, míg a második esetben $[t, \rightarrow[\in \mathscr{T}(t)$ és $t' \notin [t, \rightarrow[$. Ugyanakkor $t < t'$ esetén *minden* $\mathscr{T}(t) \ni V$-re $t' \in V$, és $t' < t$ esetén *minden* $\mathscr{T}(t') \ni V'$-re $t \in V'$, ezért $(\mathbb{R}, \mathscr{T})$ nem T_1-tér.

Létezik olyan T_1-tér, amely nem T_2-tér. Tekintsük például azt az R relációt a $[-1, 1] \subseteq \mathbb{R}$ intervallum felett, amelyet úgy értelmezünk, hogy $R := \{(t, t) | t \in [-1, 1]\} \cup \{(t, -t) | t \in]-1, 1[\}$. Ekkor R ekvivalencia-reláció $[-1, 1]$ felett, és könnyen ellenőrizhető, hogy a $([-1, 1]/R, (\mathscr{E}_{\mathbb{R}} | [-1, 1])/R)$ topologikus faktortér T_1-tér, de nem T_2-tér.

Nyilvánvaló, hogy minden metrizálható topologikus tér Hausdorff-tér. Ugyanakkor, ha d olyan félmetrika a T halmaz felett, amely nem metrika, akkor a $(T, \mathscr{T}_d)$ félmetrizálható topologikus tér nem T_0-tér.

27.1.2. Állítás. *Minden extremális* T_0*-tér teljesen összefüggéstelen.*

Bizonyítás. Legyen $(T, \mathscr{T})$ extremális topologikus tér (26.9.7.), és $\mathfrak{B}$ egy $\mathscr{T}$ szerint nyílt-zárt halmazokból álló topologikus bázis. Legyen $H \subseteq T$ legalább két elemű halmaz. Megmutatjuk, hogy H nem lehet összefüggő a $\mathscr{T}$ topológia szerint szerint, így a $(T, \mathscr{T})$

topologikus tér teljesen összefüggéstelen (26.9.7.).

Vegyünk olyan $t, t' \in H$ pontokat, hogy $t \neq t'$. A hipotézis szerint t-hez van olyan $V \in \mathscr{T}(t)$, hogy $t' \notin V$, vagy t'-höz van olyan $V' \in \mathscr{T}(t')$, hogy $t \notin V'$. Az általánosság korlátozása nélkül feltehető az első eset.

A $(T, \mathscr{T})$ topologikus tér extremalitása miatt van olyan $\Omega \in \mathfrak{B}$, hogy $t \in \Omega \subseteq V$. Tekintsük az $E := H \cap \Omega$ és $F := H \setminus \Omega$ halmazokat. Világos, hogy $H = E \cup F$ és $t \in E$ és $t' \in F$. Továbbá, $E \subseteq \Omega$ és Ω $\mathscr{T}$-zárt halmaz, ezért $\overline{E} \subseteq \Omega$, így $\overline{E} \cap F \subseteq \Omega \cap (H \setminus \Omega) = \emptyset$. Ugyanakkor $F \subseteq T \setminus \Omega$ és Ω $\mathscr{T}$-nyílt halmaz, tehát $T \setminus \Omega$ $\mathscr{T}$-zárt halmaz, ezért $\overline{F} \subseteq T \setminus \Omega$, így $E \cap \overline{F} \subseteq \Omega \cap (T \setminus \Omega) = \emptyset$. Ez azt jelenti, hogy H nem összefüggő a $\mathscr{T}$ topológia szerint. ■

27.1.3. Állítás. *A $(T, \mathscr{T})$ topologikus tér pontosan akkor* T_1*-tér, ha minden $t \in T$ esetén a $\{t\}$ halmaz $\mathscr{T}$-zárt.*

Bizonyítás. Legyen $(T, \mathscr{T})$ T_1-tér és $t \in T$. Ha $t' \in T \setminus \{t\}$, akkor $t \neq t'$, tehát létezik olyan $V \in \mathscr{T}(t)$, hogy $t' \notin V$, és létezik olyan $V' \in \mathscr{T}(t')$, hogy $t \notin V'$; ekkor $V' \subseteq T \setminus \{t\}$, tehát t' belső pontja a $T \setminus \{t\}$ halmaznak $\mathscr{T}$ szerint. Ez azt jelenti, hogy $T \setminus \{t\}$ nyílt a $\mathscr{T}$ topológia szerint, tehát a $\{t\}$ halmaz $\mathscr{T}$-zárt.

Megfordítva, tegyük fel, hogy minden $t \in T$ esetén a $\{t\}$ halmaz $\mathscr{T}$-zárt. Legyenek $t, t' \in T$ olyanok, hogy $t \neq t'$. A hipotézis szerint $V := T \setminus \{t'\}$ és $V' := T \setminus \{t\}$ mindketten nyílt halmazok, és $t \in V$ (tehát $V \in \mathscr{T}(t)$), $t' \in V'$ (tehát $V' \in \mathscr{T}(t')$), valamint nyilvánvalóan $t \notin V'$ és $t' \notin V$. Ez azt jelenti, hogy a $(T, \mathscr{T})$ topologikus tér T_1-tér. ■

27.1.4. Definíció. *Ha $(T, \mathscr{T})$ topologikus tér, akkor a $D \subseteq T$ halmazt* **$\mathscr{T}$-diszkrétnek** *nevezzük, ha minden $t \in D$ esetén van olyan $V \in \mathscr{T}(t)$, hogy $V \cap (D \setminus \{t\}) = \emptyset$.*

27.1.5. Állítás. *A $(T, \mathscr{T})$ topologikus tér pontosan akkor* T_1*-tér, ha T minden véges részhalmaza $\mathscr{T}$-diszkrét.*

Bizonyítás. Legyen a $(T, \mathscr{T})$ topologikus tér T_1-tér, és $H \subseteq T$ véges halmaz. Ha $H = \emptyset$ vagy H egy elemű, akkor H triviálisan $\mathscr{T}$-diszkrét, ezért feltesszük, hogy H legalább két elemű. Rögzítsünk egy $t \in H$ pontot. Mivel $(T, \mathscr{T})$ T_1-tér, így kiválaszthatunk olyan $(V_s)_{s \in H \setminus \{t\}}$ rendszert, hogy minden $s \in H \setminus \{t\}$ esetén $V_s \in \mathscr{T}(t)$ és $s \notin V_s$. Ekkor $V := \bigcap_{s \in H \setminus \{t\}} V_s \in \mathscr{T}(t)$, és $V \cap (H \setminus \{t\}) = \emptyset$. Ezért a H halmaz $\mathscr{T}$-diszkrét.

Megfordítva, tegyük fel, hogy a $(T, \mathscr{T})$ topologikus tér olyan, hogy T minden véges részhalmaza $\mathscr{T}$-diszkrét. Ha $t, t' \in T$ és $t \neq t'$, akkor a $\{t, t'\}$ halmaz $\mathscr{T}$-diszkrét, tehát van olyan $V \in \mathscr{T}(t)$ és $V' \in \mathscr{T}(t')$, hogy $V \cap (\{t, t'\} \setminus \{t\}) = \emptyset$ és $V' \cap (\{t, t'\} \setminus \{t'\}) = \emptyset$, vagyis $t' \notin V$ és $t \notin V'$. Ezért a $(T, \mathscr{T})$ topologikus tér T_1-tér. ■

27.1.6. Állítás. *Legyen $(T, \mathscr{T})$ topologikus tér és $(T', \mathscr{T}')$ Hausdorff-tér. Ha $f, g : T \to T'$ olyan függvények, amelyek folytonosak a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, akkor a $\{t \in T | f(t) = g(t)\}$ halmaz $\mathscr{T}$-zárt.*

Bizonyítás. Legyen $t_0 \in T \setminus \{t \in T | f(t) = g(t)\}$ rögzített. Ekkor $f(t_0) \neq g(t_0)$, és $(T', \mathscr{T}')$ Hausdorff-tér, tehát létezik olyan $V' \in \mathscr{T}'(f(t_0))$ és $W' \in \mathscr{T}'(g(t_0))$, hogy $V' \cap W' = \emptyset$. Az f és g függvények t_0 pontbeli folytonossága miatt van olyan $V \in \mathscr{T}(t_0)$ és $W \in \mathscr{T}(t_0)$, hogy $f\langle V \rangle \subseteq V'$ és $g\langle W \rangle \subseteq W'$. Ekkor $V \cap W \in \mathscr{T}(t_0)$, és ha $t \in V \cap W$, akkor $f(t) \in V'$ és $g(t) \in W'$, így $V' \cap W' = \emptyset$ miatt $f(t) \neq g(t)$. Ez azt jelenti, hogy $V \cap W \subseteq T \setminus \{t \in T | f(t) = g(t)\}$, tehát t_0 belső pontja a $T \setminus \{t \in T | f(t) = g(t)\}$ halmaznak $\mathscr{T}$ szerint, így a $\{t \in T | f(t) = g(t)\}$ halmaz $\mathscr{T}$-zárt. ■

27.1.7. Következmény. (Az egyenlőségek folytatásának elve.) *Legyen* $(T, \mathscr{T})$ *topologikus tér és* $(T', \mathscr{T}')$ *Hausdorff-tér. Ha* $f, g : T \to T'$ *olyan függvények, amelyek folytonosak a* $\mathscr{T}$ *és* $\mathscr{T}'$ *topológiák szerint, és* $E \subseteq T$ *olyan halmaz, hogy* $f = g$ *az* E *halmazon, akkor* $f = g$ *az* $\overline{E}$ *halmazon.*

Bizonyítás. Az előző állítás szerint a $\{t \in T | f(t) = g(t)\}$ halmaz $\mathscr{T}$-zárt, és a hipotézis alapján $E \subseteq \{t \in T | f(t) = g(t)\}$, ezért $\overline{E} \subseteq \{t \in T | f(t) = g(t)\}$. ■

27.1.8. Állítás. *Hausdorff-terek topologikus szorzata Hausdorff-tér.*

Bizonyítás. Legyen $((T_i, \mathscr{T}_i))_{i \in I}$ Hausdorff-terek tetszőleges rendszere, valamint legyenek $(t_i)_{i \in I}, (t'_i)_{i \in I} \in \prod_{i \in I} T_i$ olyan pontok, hogy $(t_i)_{i \in I} \neq (t'_i)_{i \in I}$. Legyen $k \in I$ olyan, hogy $t_k \neq t'_k$. A $(T_k, \mathscr{T}_k)$ topologikus tér Hausdorff-tér, így léteznek olyan $\Omega_k, \Omega'_k \in \mathscr{T}_k$ halmazok, hogy $\Omega_k \cap \Omega'_k = \emptyset$ és $t_k \in \Omega_k$, valamint $t'_k \in \Omega'_k$. Ekkor $(t_i)_{i \in I} \in \overset{-1}{\mathrm{pr}}_k \langle \Omega_k \rangle \in \underset{i \in I}{\times} \mathscr{T}_i$ és $(t'_i)_{i \in I} \in \overset{-1}{\mathrm{pr}}_k \langle \Omega'_k \rangle \in \underset{i \in I}{\times} \mathscr{T}_i$, továbbá $\Omega_k \cap \Omega'_k = \emptyset$ miatt $\overset{-1}{\mathrm{pr}}_k \langle \Omega_k \rangle \cap \overset{-1}{\mathrm{pr}}_k \langle \Omega'_k \rangle = \overset{-1}{\mathrm{pr}}_k \langle \Omega_k \cap \Omega'_k \rangle = \emptyset$. Ez azt jelenti, hogy $\left(\prod_{i \in I} T_i, \underset{i \in I}{\times} \mathscr{T}_i \right)$ Hausdorff-tér. ■

27.1.9. Állítás. *Ha* $(T, \mathscr{T})$ *topologikus tér és* $(T', \mathscr{T}')$ *Hausdorff-tér, akkor minden* $f : T \to T'$ $\mathscr{T}$*-*$\mathscr{T}'$ *folytonos függvényre a*

$$\mathrm{gr}(f) := \{ \ (t, f(t)) \in T \times T' \mid t \in T \ \}$$

halmaz (az f *függvény grafikonja) zárt a* $\mathscr{T} \times \mathscr{T}'$ *szorzattopológia szerint.*

Bizonyítás. Legyen $(t, t') \in (T \times T') \setminus \mathrm{gr}(f)$. Ekkor $f(t) \neq t'$ és $(T', \mathscr{T}')$ Hausdorff-tér, így léteznek olyan $V' \in \mathscr{T}'(f(t))$ és $V \in \mathscr{T}'(t')$ környezetek, hogy $V' \cap V = \emptyset$. Mivel f folytonos a t pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, így létezik olyan $U \in \mathscr{T}(t)$ környezet, hogy $f\langle U \rangle \subseteq V'$. Ekkor $(U \times V) \cap \mathrm{gr}(f) = \emptyset$, különben létezne olyan $s \in T$ pont, hogy $(s, f(s)) \in U \times V$, tehát $f(s) \in f\langle U \rangle \cap V \subseteq V' \cap V$, holott $V' \cap V = \emptyset$. Ez azt jelenti, hogy $U \times V \subseteq (T \times T') \setminus \mathrm{gr}(f)$, és a szorzattopológia definíciója szerint $U \times V$ környezete (t, t')-nek a $\mathscr{T} \times \mathscr{T}'$ topológia szerint, így (t, t') belső pontja a $(T \times T') \setminus \mathrm{gr}(f)$ halmaznak a $\mathscr{T} \times \mathscr{T}'$ topológia szerint, tehát $(T \times T') \setminus \mathrm{gr}(f)$ nyílt, és ezért $\mathrm{gr}(f)$ zárt részhalmaza $T \times T'$-nek a $\mathscr{T} \times \mathscr{T}'$ topológia szerint. ■

Tehát Hausdorff-térbe érkező folytonos függvény grafikonja zárt. Azonban Hausdorff-terek között ható, zárt grafikonú függvény nem szükségképpen folytonos. Erre példa az

$$f : \mathbb{R} \to \mathbb{R}; \quad t \mapsto \begin{cases} 1/t & , \text{ha } t \neq 0, \\ 0 & , \text{ha } t = 0 \end{cases}$$

függvény, ahol $\mathbb{R}$ felett az $\mathscr{E}_{\mathbb{R}}$ topológiát vesszük. Ez a függvény a 0 pontban nem folytonos, de a grafikonja zárt az $(\mathbb{R} \times \mathbb{R}, \mathscr{E}_{\mathbb{R}} \times \mathscr{E}_{\mathbb{R}})$ topologikus szorzattérben.

27.2. Függvény határértéke

27.2.1. Definíció. *Legyenek* $(T, \mathscr{T})$, $(T', \mathscr{T}')$ *topologikus terek,* $f : T \rightarrowtail T'$ *(nem feltétlenül mindenütt értelmezett) függvény, és* $t \in T$ *a* $\mathrm{Dom}(f)$ *halmaznak torlódási* *pontja a $\mathscr{T}$ topológia szerint. Azt mondjuk, hogy az f függvénynek* **létezik határértéke** *a t pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ha*

$$(\exists\, t' \in T')(\forall\, V' \in \mathscr{T}'(t'))(\exists\, V \in \mathscr{T}(t)):\ f\langle V \setminus \{t\}\rangle \subseteq V'.$$

27.2.2. Állítás. *Legyenek $(T, \mathscr{T})$, $(T', \mathscr{T}')$ topologikus terek, $f : T \rightarrowtail T'$ függvény, és $t \in T$ a $\mathrm{Dom}(f)$ halmaznak torlódási pontja a $\mathscr{T}$ topológia szerint. Ha $(T', \mathscr{T}')$ Hausdorff-tér, akkor legfeljebb egy olyan $t' \in T'$ létezik, amelyre*

$$(\forall\, V' \in \mathscr{T}'(t'))(\exists\, V \in \mathscr{T}(t)):\ f\langle V \setminus \{t\}\rangle \subseteq V'.$$

Bizonyítás. Indirekt bizonyítunk, tehát feltesszük, hogy $t'_1, t'_2 \in T'$ olyan pontok, amelyekre $t'_1 \neq t'_2$, de teljesülnek a következő állítások

$$(\forall\, V' \in \mathscr{T}'(t'_1))(\exists\, V \in \mathscr{T}(t)):\ f\langle V \setminus \{t\}\rangle \subseteq V',$$
$$(\forall\, V' \in \mathscr{T}'(t'_2))(\exists\, V \in \mathscr{T}(t)):\ f\langle V \setminus \{t\}\rangle \subseteq V'.$$

A $(T', \mathscr{T}')$ topologikus tér Hausdorff-tér, ezért vehetünk olyan $V'_1 \in \mathscr{T}'(t'_1)$ és $V'_2 \in \mathscr{T}'(t'_2)$ környezeteket, hogy $V'_1 \cap V'_2 = \emptyset$. A hipotézis alapján legyenek $V_1 \in \mathscr{T}(t)$ és $V_2 \in \mathscr{T}(t)$ olyan környezetek, amelyekre $f\langle V_1 \setminus \{t\}\rangle \subseteq V'_1$ és $f\langle V_2 \setminus \{t\}\rangle \subseteq V'_2$. Ekkor $V_1 \cap V_2 \in \mathscr{T}(t)$ és t torlódási pontja $\mathrm{Dom}(f)$-nek, ezért választhatunk egy $s \in ((V_1 \cap V_2) \setminus \{t\}) \cap \mathrm{Dom}(f)$ pontot. Világos, hogy $f(s) \in f\langle V_1 \setminus \{t\}\rangle \cap f\langle V_2 \setminus \{t\}\rangle \subseteq V'_1 \cap V'_2$, ami ellentmond annak, hogy $V'_1 \cap V'_2 = \emptyset$. ■

27.2.3. Definíció. *Legyenek $(T, \mathscr{T})$, $(T', \mathscr{T}')$ topologikus terek, $f : T \rightarrowtail T'$ függvény, és $t \in T$ a $\mathrm{Dom}(f)$ halmaznak torlódási pontja a $\mathscr{T}$ topológia szerint. Ha $(T', \mathscr{T}')$ Hausdorff-tér és létezik az f függvénynek határértéke a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, akkor $\lim\limits_t f$ jelöli azt az egyértelműen meghatározott pontot T'-ben, amelyre teljesül az, hogy minden $V' \in \mathscr{T}'\left(\lim\limits_t f\right)$ esetén van olyan $V \in \mathscr{T}(t)$, hogy $f\langle V \setminus \{t\}\rangle \subseteq V'$; és ezt a $\lim\limits_t f \in T'$ pontot az f függvény* **határértékének** *nevezzük a t pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint.*

A topologikus terek között ható függvények határértékére vonatkozóan könnyen igazolható az elemi analízisből ismert állítások nagy része, csak arra kell vigyázni, hogy az érkezési tér mindig Hausdorff-tér legyen. A továbbiakban nem használjuk a határérték általános fogalmát, viszont szükségünk lesz a metrikus térben haladó (általánosított) sorozatok konvergenciája fogalmának topologikus általánosítására.

27.3. Konvergens általánosított sorozatok

27.3.1. Definíció. *A reflexív és tranzitív relációkat* **előrendezéseknek** *nevezzük. Azt mondjuk, hogy I* **előrendezett halmaz**, *ha adott I felett egy előrendezés. Az I halmaz feletti $\leq$ előrendezést* **felfelé irányítottnak** *nevezzük, ha minden $i_1, i_2 \in I$ esetén van olyan $i \in I$, hogy $i_1 \leq i$ és $i_2 \leq i$.*

Például egy halmaz feletti *lineáris rendezés* nyilvánvalóan felfelé irányított rendezés. Ennek leggyakrabban előforduló speciális esete az, amikor a halmaz $\mathbb{N}$ és a lineáris rendezés az $\mathbb{N}$ feletti természetes rendezés.

Az $\mathbb{N} \times \mathbb{N}$ halmaz felett vezessük be azt a $\leq$ relációt, amelyre $(i, j), (i', j') \in \mathbb{N} \times \mathbb{N}$ esetén $(i, j) \leq (i', j')$ azt jelenti, hogy $i < i'$ (az $\mathbb{N}$ természetes rendezése szerint), vagy $i = i'$ és $j \leq j'$ (az $\mathbb{N}$ természetes rendezése szerint). Könnyen látható, hogy $\leq$ olyan felfelé irányított rendezés $\mathbb{N} \times \mathbb{N}$ felett, amely nem lineáris rendezés.

27.3.2. Definíció. **Általánosított sorozatnak** *nevezünk minden olyan* $(t_i)_{i\in I}$ *rendszert, amelynek* I *indexhalmaza nem üres, felfelé irányított előrendezett halmaz. Ha* $(T,\mathscr{T})$ *topologikus tér, akkor azt mondjuk, hogy a* T*-ben haladó* $(t_i)_{i\in I}$ *általánosított sorozat* **konvergál a** $t\in T$ **ponthoz** *a* $\mathscr{T}$ *topológia szerint, ha*

$$(\forall\ V\in\mathscr{T}(t))(\exists\ i\in I)(\forall\ j\in I):\ (i\le j)\Rightarrow(t_j\in V)$$

teljesül, és minden ilyen tulajdonságú $t\in T$ *pontot a* $(t_i)_{i\in I}$ *általánosított sorozat* $\mathscr{T}$ *szerinti* **limeszpontjának** *nevezünk. Ha* $(T,\mathscr{T})$ *topologikus tér, akkor azt mondjuk, hogy a* T*-ben haladó* $(t_i)_{i\in I}$ *általánosított sorozat* **konvergens** *a* $\mathscr{T}$ *topológia szerint, ha létezik olyan* $t\in T$*, amelyhez* $(t_i)_{i\in I}$ *konvergál* $\mathscr{T}$ *szerint.*

A definíció alapján világos, hogy ha T halmaz és $\mathscr{T}$, $\mathscr{T}'$ olyan topológiák T felett, hogy $\mathscr{T}\subseteq\mathscr{T}'$, akkor minden T-ben haladó $(t_i)_{i\in I}$ általánosított sorozatra és minden $t\in T$ pontra teljesül az, hogy ha $(t_i)_{i\in I}$ konvergál t-hez $\mathscr{T}'$ szerint, akkor $(t_i)_{i\in I}$ konvergál t-hez $\mathscr{T}$ szerint is, hiszen $\mathscr{T}(t)\subseteq\mathscr{T}'(t)$.

Vigyázzunk arra, hogy ha $(T,\mathscr{T})$ topologikus tér, akkor egy T-ben haladó általánosított sorozat *több* ponthoz is konvergálhat $\mathscr{T}$ szerint; sőt, ha $\mathscr{T}$ egyenlő a T feletti antidiszkrét topológiával, akkor *minden* T-ben haladó általánosított sorozat konvergál T *minden* pontjához $\mathscr{T}$ szerint.

27.3.3. Állítás. *A* $(T,\mathscr{T})$ *topologikus tér pontosan akkor Hausdorff-tér, ha minden* T*-ben haladó általánosított sorozathoz legfeljebb egy olyan pont létezik* T*-ben, amelyhez az adott általánosított sorozat konvergál* $\mathscr{T}$ *szerint.*

Bizonyítás. Tegyük fel, hogy $(T,\mathscr{T})$ Hausdorff-tér, és legyen $(t_i)_{i\in I}$ olyan T-ben haladó általánosított sorozat, amely konvergál a $\mathscr{T}$ topológia szerint a $t\in T$ és $t'\in T$ pontokhoz. Ha $t\ne t'$ volna, akkor léteznek olyan $V\in\mathscr{T}(t)$ és $V'\in\mathscr{T}(t')$, hogy $V\cap V'=\emptyset$. Ekkor léteznek olyan $i_V\in I$ és $i_{V'}\in I$, hogy minden $i\in I$ esetén, ha $i\ge i_V$, akkor $t_i\in V$, illetve, ha $i\ge i_{V'}$, akkor $t_i\in V'$. Az I előrendezett halmaz felfelé irányított, ezért volna olyan $i\in I$, hogy $i\ge i_V$ és $i\ge i_{V'}$ egyszerre teljesülne; ekkor $t_i\in V\cap V'$, holott $V\cap V'=\emptyset$.

Tegyük fel, hogy $(T,\mathscr{T})$ nem Hausdorff-tér; olyan T-ben haladó általánosított sorozatot keresünk, amely különböző pontokhoz konvergál a $\mathscr{T}$ topológia szerint. A hipotézis alapján vehetünk olyan $t,t'\in T$ pontokat, hogy $t\ne t'$, de minden $V\in\mathscr{T}(t)$ és minden $V'\in\mathscr{T}(t')$ esetén $V\cap V'\ne\emptyset$. A kiválasztási axióma szerint $\prod\limits_{(V,V')\in\mathscr{T}(t)\times\mathscr{T}(t')}(V\cap V')$ nem üres; legyen $(s_{V,V'})_{(V,V')\in\mathscr{T}(t)\times\mathscr{T}(t')}$ eleme ennek a szorzathalmaznak. A $\mathscr{T}(t)\times\mathscr{T}(t')$ halmaz felett bevezetjük a $\le$ relációt úgy, hogy $(V,V'),(W,W')\in\mathscr{T}(t)\times\mathscr{T}(t')$ esetén $(V,V')\le(W,W')$ pontosan akkor teljesüljön, ha $W\subseteq V$ és $W'\subseteq V'$. Ekkor $(\mathscr{T}(t)\times\mathscr{T}(t'),\le)$ olyan rendezett halmaz, amely felfelé irányított, mert $\mathscr{T}(t)$ és $\mathscr{T}(t')$ rácsok. Állítjuk, hogy a $(s_{V,V'})_{(V,V')\in\mathscr{T}(t)\times\mathscr{T}(t')}$ általánosított sorozat t-hez is és t'-höz is konvergál a $\mathscr{T}$ topológia szerint. Valóban, ha $V\in\mathscr{T}(t)$, akkor $(V,T)\in\mathscr{T}(t)\times\mathscr{T}(t')$ olyan, minden $(W,W')\in\mathscr{T}(t)\times\mathscr{T}(t')$ esetén, ha $(V,T)\le(W,W')$, akkor $W\subseteq V$, így $s_{W,W'}\in W\cap W'\subseteq W\subseteq V$; tehát $(s_{V,V'})_{(V,V')\in\mathscr{T}(t)\times\mathscr{T}(t')}$ konvergál a t ponthoz a $\mathscr{T}$ topológia szerint. Ugyanakkor $V'\in\mathscr{T}(t')$ esetén $(T,V')\in\mathscr{T}(t)\times\mathscr{T}(t')$ olyan, minden $(W,W')\in\mathscr{T}(t)\times\mathscr{T}(t')$ esetén, ha $(T,V')\le(W,W')$, akkor $W'\subseteq V'$, így $s_{W,W'}\in W\cap W'\subseteq W'\subseteq V'$; tehát $(s_{V,V'})_{(V,V')\in\mathscr{T}(t)\times\mathscr{T}(t')}$ konvergál a t' ponthoz a $\mathscr{T}$ topológia szerint. ■

27.3.4. Definíció. *Ha $(T, \mathscr{T})$ Hausdorff-tér és $(t_i)_{i\in I}$ olyan T-ben haladó általánosított sorozat, amely konvergens $\mathscr{T}$ szerint, akkor $\lim\limits_{i,\ I} t_i$ jelöli a T-nek azt az egyetlen pontját, amelyhez $(t_i)_{i\in I}$ konvergál $\mathscr{T}$-szerint, és ezt a $\lim\limits_{i,\ I} t_i \in T$ pontot a $(t_i)_{i\in I}$ általánosított sorozat* **határértékének** *nevezzük $\mathscr{T}$ szerint.*

Példa. (szummálható rendszerekre normált térben). Legyen $(E, \|\cdot\|)$ normált tér és $(x_i)_{i\in I}$ tetszőleges nem üres E-ben haladó rendszer. Jelölje $\mathscr{P}_0(I)$ az I nem üres véges részhalmazainak halmazát, és rendezzük a $\mathscr{P}_0(I)$ halmazt a $\subseteq$ relációval; ekkor felfelé irányított rendezett halmazt kapunk. Tekintsük az E-ben haladó $\left(\sum\limits_{i\in J} x_i\right)_{J\in\mathscr{P}_0(I)}$ általánosított sorozatot (azzal a konvencióval, hogy $\sum\limits_{i\in\emptyset} x_i := 0$). Ez az általánosított sorozat pontosan akkor konvergens E-ben a $\mathscr{T}_{\|\cdot\|}$ topológia szerint, ha létezik olyan $x \in E$, amelyre minden $\varepsilon \in \mathbb{R}_+^*$ esetén van olyan $J \subseteq I$ véges halmaz, hogy minden $H \subseteq I$ véges halmazra, ha $J \subseteq H$, akkor $\left\| x - \sum\limits_{i\in H} x_i \right\| < \varepsilon$. Ilyenkor azt mondjuk, hogy az $(x_i)_{i\in I}$ rendszer *szummálható* E-ben a $\|\cdot\|$ norma szerint, és ekkor a

$$\sum_{i,\ I} x_i := \lim_{J,\ \mathscr{P}_0(I)} \sum_{i\in J} x_i$$

jelölést alkalmazzuk, és ezt a vektort az $(x_i)_{i\in I}$ szummálható rendszer *összegének* nevezzük a $\|\cdot\|$ norma szerint.

Könnyen látható, hogy ha $(t_i)_{i\in I}$ olyan $\mathbb{R}$-ben haladó nem üres általánosított sorozat, amely monoton növő (tehát $i, j \in I$ és $i \le j$ esetén $t_i \le t_j$) és $\sup\limits_{i\in I} t_i < +\infty$, akkor $(t_i)_{i\in I}$ konvergens az $\mathscr{E}_{\mathbb{R}}$ topológia szerint, és $\lim\limits_{i,\ I} t_i = \sup\limits_{i\in I} t_i$.

27.3.5. Állítás. (Érintési pontok jellemzése általánosított sorozatokkal) *Ha $(T, \mathscr{T})$ topologikus tér, $E \subseteq T$ és $t \in T$, akkor $t \in \overline{E}$ ekvivalens azzal, hogy létezik olyan E-ben haladó $(t_i)_{i\in I}$ általánosított sorozat, amely konvergál t-hez a $\mathscr{T}$ topológia szerint.*

Bizonyítás. Ha $(t_i)_{i\in I}$ olyan E-ben haladó általánosított sorozat, amely t-hez konvergál a $\mathscr{T}$ topológia szerint, akkor minden $V \in \mathscr{T}(t)$ környezethez van olyan $i \in I$, hogy $t_i \in V$, tehát $V \cap E \neq \emptyset$, így $t \in \overline{E}$.

Megfordítva, legyen $t \in \overline{E}$. Ekkor minden $V \in \mathscr{T}(t)$ környezetre $V \cap E \neq \emptyset$, így a kiválasztási axióma szerint $\prod\limits_{V\in\mathscr{T}(t)} (V \cap E) \neq \emptyset$; legyen $(t_V)_{V\in\mathscr{T}(t)}$ eleme ennek a szorzathalmaznak. A $\mathscr{T}(t)$ halmazt a $\supseteq$ relációval ellátva felfelé irányított rendezett halmazt kapunk. Világos, hogy az E-ben haladó $(t_V)_{V\in\mathscr{T}(t)}$ általánosított sorozat t-hez konvergál a $\mathscr{T}$ topológia szerint, hiszen minden $\mathscr{T}(t) \ni V$-re igaz az, hogy ha $W \in \mathscr{T}$ és $V \supseteq W$, akkor $t_W \in W \subseteq V$. ■

A következő példa megmutatja, hogy az előző állításban szükségszerű az általánosított sorozatok fogalmának alkalmazása, vagyis az állítás nem feltétlenül igaz, ha benne az általánosított sorozatok helyett sorozatokról lenne szó.

Példa. Legyen $\mathfrak{B}$ az $\Omega \setminus H$ alakú halmazok halmaza, ahol $\Omega \subseteq \mathbb{R}$ nyílt halmaz az euklidészi topológia szerint és $H \subseteq \mathbb{R}$ megszámlálható (tehát véges, vagy megszámlálhatóan végtelen) halmaz. Világos, hogy $\mathbb{R} \in \mathfrak{B}$, így $\mathfrak{B}$ befedése $\mathbb{R}$-nek, továbbá ha Ω és Ω' nyílt részhalmazok $\mathbb{R}$-ben az euklidészi topológia szerint, valamint H és H' megszámlálható részhalmazok $\mathbb{R}$-ben, akkor

$$(\Omega \setminus H) \cap (\Omega' \setminus H') = (\Omega \cap \Omega') \setminus (H \cup H')$$

miatt $(\Omega \setminus H) \cap (\Omega' \setminus H') \in \mathfrak{B}$, mert $\Omega \cap \Omega'$ nyílt részhalmaza $\mathbb{R}$-nek az euklidészi topológia szerint és $H \cup H'$ megszámlálható részhalmaza $\mathbb{R}$-nek. Ezért létezik egyetlen olyan $\mathscr{E}_{\mathbb{R}}^*$ topológia $\mathbb{R}$ felett, amelynek $\mathfrak{B}$ topologikus bázisa (26.2.3.). Nyilvánvaló, hogy $\mathscr{E}_{\mathbb{R}} \subseteq \mathscr{E}_{\mathbb{R}}^*$, ezért $\mathscr{E}_{\mathbb{R}}^*$ Hausdorff-topológia $\mathbb{R}$ felett. Megmutatjuk, hogy *csak a stacionárius sorozatok konvergensek $\mathscr{E}_{\mathbb{R}}^*$ szerint*, tehát ha $(t_n)_{n\in\mathbb{N}}$ olyan valós számsorozat $\mathbb{R}$-ben és $t \in \mathbb{R}$ olyan, hogy $t = \lim\limits_{n\to\infty} t_n$ az $\mathscr{E}_{\mathbb{R}}^*$ topológia szerint, akkor van olyan $N \in \mathbb{N}$, hogy minden $n \geq N$ természetes számra $t_n = t$. Ha nem így lenne, akkor az $E := \{n \in \mathbb{N} | t_n \neq t\}$ halmaz végtelen volna, így a $H := \{t_n | n \in E\} \subseteq \mathbb{R}$ megszámlálható halmazra teljesülne az, hogy $\mathbb{R} \setminus H \in \mathscr{E}_{\mathbb{R}}^*$ és $t \in \mathbb{R} \setminus H$, vagyis $\mathbb{R} \setminus H$ nyílt környezete t-nek $\mathscr{E}_{\mathbb{R}}^*$ szerint: de ekkor létezne olyan $N \in \mathbb{N}$, hogy minden $n \geq N$ természetes számra $t_n \in \mathbb{R} \setminus H$, ami lehetetlen, mert E végtelensége folytán van olyan $n \in E$, hogy $n \geq N$, és egy ilyen n természetes számra $t_n \in \mathbb{R} \setminus H$ és $t_n \in H$ egyszerre teljesülne. Nyilvánvaló, hogy minden $t \in \mathbb{R}$ esetén a $\{t\}$ halmaz *nem nyílt $\mathscr{E}_{\mathbb{R}}^*$ szerint* hiszen minden nem üres $\mathscr{E}_{\mathbb{R}}^*$-nyílt halmaz nem megszámlálhatóan végtelen, ezért az $\mathbb{R} \setminus \{t\}$ halmaz *nem zárt $\mathscr{E}_{\mathbb{R}}^*$ szerint*. Tehát, ha $t \in \mathbb{R}$, akkor az $\mathbb{R} \setminus \{t\}$ halmaz $\mathscr{E}_{\mathbb{R}}^*$ szerinti lezártja egyenlő $\mathbb{R}$-rel, vagyis ennek a lezártnak eleme a t pont, így az előző állítás alapján létezik olyan $\mathbb{R} \setminus \{t\}$-ben haladó általánosított sorozat, amely t-hez konvergál $\mathscr{E}_{\mathbb{R}}^*$ szerint, de ilyen $\mathbb{R} \setminus \{t\}$-ben haladó sorozat nem létezik.

27.3.6. Definíció. *Legyen $(t_i)_{i\in I}$ általánosított sorozat. Ha J felfelé irányított előrendezett halmaz és $\sigma : J \to I$ olyan monoton növő függvény, hogy $\mathrm{Im}(\sigma)$ kofinális I-vel (vagyis minden $i \in I$ esetén van olyan $j \in J$, hogy $i \leq \sigma(j)$), akkor a $(t_{\sigma(j)})_{j\in J}$ általánosított sorozatot a $(t_i)_{i\in I}$ általánosított sorozat* **általánosított részsorozatának** *nevezzük. (Megjegyezzük, hogy az $\mathrm{Im}(\sigma)$ halmaz I-vel való kofinalitása és $I \neq \emptyset$ miatt $J \neq \emptyset$.)*

Nyilvánvaló, hogy az általánosított sorozat általánosított részsorozatának fogalma a sorozat részsorozata fogalmának általánosítása, mert ha $(t_n)_{n\in\mathbb{N}}$ sorozat, akkor minden $\sigma : \mathbb{N} \to \mathbb{N}$ szigorúan monoton növő függvény (azaz *indexsorozat*) értékkészlete kofinális $\mathbb{N}$-nel, hiszen minden $n \in \mathbb{N}$ esetén $n \leq \sigma(n)$; ezért a $(t_{\sigma(n)})_{n\in\mathbb{N}}$ részsorozat egyben általánosított részsorozata is a $(t_n)_{n\in\mathbb{N}}$ sorozatnak.

27.3.7. Állítás. *Ha $(T, \mathscr{T})$ topologikus tér és $(t_i)_{i\in I}$ olyan T-ben haladó általánosított sorozat, amely konvergál a $t \in T$ ponthoz $\mathscr{T}$ szerint, akkor a $(t_i)_{i\in I}$ minden általánosított részsorozata konvergál t-hez $\mathscr{T}$ szerint.*

Bizonyítás. Legyen J felfelé irányított előrendezett halmaz és $\sigma : J \to I$ olyan monoton növő függvény, amelyre $\mathrm{Im}(\sigma)$ kofinális I-vel. Legyen $V \in \mathscr{T}(t)$, és vegyünk olyan $i_V \in I$ indexet, amelyre minden $i \in I$ esetén, ha $i \geq i_V$, akkor $t_i \in V$. Az $\mathrm{Im}(\sigma)$ halmaz kofinális I-vel, ezért van olyan $j_V \in J$, hogy $i_V \leq \sigma(j_V)$. Ha $j \in J$ és $j \geq j_V$, akkor a σ monotonitása folytán $\sigma(j) \geq \sigma(j_V) \geq i_V$, így $t_{\sigma(j)} \in V$. Ez azt jelenti, hogy a $\left(t_{\sigma(j)}\right)_{j\in J}$ általánosított sorozat konvergál t-hez a $\mathscr{T}$ topológia szerint. ■

27.3.8. Állítás. (Átviteli elv) *Legyenek $(T, \mathscr{T})$ és $(T', \mathscr{T}')$ topologikus terek. Az $f : T \to T'$ függvény pontosan akkor folytonos a $t \in T$ pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ha minden T-ben haladó, $\mathscr{T}$ szerint t-hez konvergáló $(t_i)_{i \in I}$ általánosított sorozatra a T'-ben haladó $(f(t_i))_{i \in I}$ általánosított sorozat konvergál $f(t)$-hez $\mathscr{T}'$ szerint.*

Bizonyítás. Tegyük fel, hogy f folytonos a $t \in T$ pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, és legyen $(t_i)_{i \in I}$ olyan általánosított sorozat T-ben, amely t-hez konvergál a $\mathscr{T}$ topológia szerint. Legyen $V' \in \mathscr{T}'(f(t))$ tetszőleges. Ekkor van olyan $V \in \mathscr{T}(t)$, hogy $f\langle V \rangle \subseteq V'$, és a V-hez van olyan $i_V \in I$, hogy minden $I \ni i$-re, ha $i \geq i_V$, akkor $t_i \in V$, tehát $f(t_i) \in f\langle V \rangle \subseteq V'$. Ez azt jelenti, hogy a T'-ben haladó $(f(t_i))_{i \in I}$ általánosított sorozat konvergál $f(t)$-hez $\mathscr{T}'$ szerint.

Tegyük fel, hogy f nem folytonos a t pontban a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint. Ekkor létezik olyan $V' \in \mathscr{T}'(f(t))$, hogy minden $\mathscr{T}(t) \ni V$-re $f\langle V \rangle \not\subseteq V'$, vagyis $V \setminus \overset{-1}{f}\langle V' \rangle \neq \emptyset$. A kiválasztási axióma szerint $\prod\limits_{V \in \mathscr{T}(t)} \left(V \setminus \overset{-1}{f}\langle V' \rangle \right) \neq \emptyset$; legyen $(t_V)_{V \in \mathscr{T}(t)}$ eleme ennek a szorzathalmaznak. A $\mathscr{T}(t)$ halmazt a $\supseteq$ relációval ellátva felfelé irányított rendezett halmazt kapunk. Világos, hogy a T-ben haladó $(t_V)_{V \in \mathscr{T}(t)}$ általánosított sorozat t-hez konvergál a $\mathscr{T}$ topológia szerint, hiszen minden $\mathscr{T}(t) \ni V$-re igaz az, hogy ha $W \in \mathscr{T}(t)$ és $V \supseteq W$, akkor $t_W \in W \subseteq V$. Ugyanakkor minden $V \in \mathscr{T}(t)$ esetén $t_V \in V \setminus \overset{-1}{f}\langle V' \rangle$, azaz $f(t_V) \notin V'$, ezért az $(f(t_V))_{V \in \mathscr{T}(t)}$ általánosított sorozat nem konvergál $f(t)$-hez a $\mathscr{T}'$ topológia szerint. ■

A konvergens általánosított sorozatok *jellemzik* a topológiákat. Pontosabban, a következő fontos tényről van szó.

27.3.9. Állítás. *Tegyük fel, hogy $\mathscr{T}$ és $\mathscr{T}'$ topológiák a T halmaz felett. A $\mathscr{T} = \mathscr{T}'$ egyenlőség pontosan akkor teljesül, ha minden $t \in T$ pontra, és minden T-ben haladó, $(t_i)_{i \in I}$ általánosított sorozatra: a "$(t_i)_{i \in I}$ konvergál t-hez a $\mathscr{T}$ topológia szerint" kijelentés ekvivalens a "$(t_i)_{i \in I}$ konvergál t-hez a $\mathscr{T}'$ topológia szerint" kijelentéssel.*

Bizonyítás. Tegyük fel, hogy $\mathscr{T} \neq \mathscr{T}'$; ekkor van olyan $\Omega \in \mathscr{T}$, hogy $\Omega \notin \mathscr{T}'$, *vagy* van olyan $\Omega' \in \mathscr{T}'$, hogy $\Omega' \notin \mathscr{T}$. A meghatározottság kedvéért tegyük fel az utóbbit, tehát legyen $\Omega' \in \mathscr{T}'$, hogy $\Omega' \notin \mathscr{T}$. Az Ω' halmaz nem $\mathscr{T}$-nyílt, ezért vehetünk olyan $t \in \Omega'$ pontot, amely a $\mathscr{T}$ topológia szerint nem belső pontja Ω'-nek, vagyis minden $V \in \mathscr{T}(t)$ esetén $V \setminus \Omega' \neq \emptyset$. A kiválasztási axióma szerint $\prod\limits_{V \in \mathscr{T}(t)} (V \setminus \Omega') \neq \emptyset$; legyen $(t_V)_{V \in \mathscr{T}(t)}$ eleme ennek a szorzathalmaznak. A $\mathscr{T}(t)$ halmazt a $\supseteq$ relációval ellátva felfelé irányított rendezett halmazt kapunk. Világos, hogy a T-ben haladó $(t_V)_{V \in \mathscr{T}(t)}$ általánosított sorozat t-hez konvergál a $\mathscr{T}$ topológia szerint, hiszen minden $\mathscr{T}(t) \ni V$-re igaz az, hogy ha $W \in \mathscr{T}$ és $V \supseteq W$, akkor $t_W \in W \subseteq V$. Ugyanakkor a $(t_V)_{V \in \mathscr{T}(t)}$ általánosított sorozat nem konvergál t-hez a $\mathscr{T}'$ topológia szerint, hiszen $\Omega' \in \mathscr{T}'(t)$ és minden $\mathscr{T}(t) \ni V$-re $t_V \notin \Omega'$. ■

Megjegyezzük, hogy az előző állításban lényeges, hogy *általánosított sorozatokról* van szó, nem pedig természetes számokkal indexezett sorozatokról. A 27.3 példában értelmezett $\mathbb{R}$ feletti $\mathscr{E}^*_{\mathbb{R}}$ topológia szerint a konvergens sorozatok éppen a stacionárius sorozatok, és az $\mathbb{R}$ halmaz feletti diszkrét topológia szerint szintén a stacionárius sorozatok a konvergens sorozatok, ugyanakkor $\mathscr{E}^*_{\mathbb{R}}$ nem a diszkrét topológia $\mathbb{R}$ felett. Ezért létezik olyan $\mathbb{R}$-ben haladó általánosított sorozat, amely konvergens $\mathscr{E}^*_{\mathbb{R}}$ szerint, de nem konvergens az $\mathbb{R}$ halmaz feletti diszkrét topológia szerint.

27.4. Reguláris, teljesen reguláris és normális topologikus terek

Megállapodunk abban, hogy ha T halmaz, $f : T \to \overline{\mathbb{R}}$ függvény, és $c \in \overline{\mathbb{R}}$, akkor az

$$\overset{-1}{f}\langle\{c\}\rangle, \quad \overset{-1}{f}\langle\overline{\mathbb{R}} \setminus \{c\}\rangle, \quad \overset{-1}{f}\langle]\leftarrow, c[\rangle, \quad \overset{-1}{f}\langle]c, \to[\rangle, \quad \overset{-1}{f}\langle]\leftarrow, c]\rangle, \quad \overset{-1}{f}\langle[c, \to[\rangle$$

halmazokat a továbbiakban rendre a következő szimbólumokkal jelöljük

$$[f = c], \quad [f \neq c], \quad [f < c], \quad [f > c], \quad [f \leq c], \quad [f \geq c].$$

Nyilvánvaló, hogy ha $(T, \mathscr{T})$ topologikus tér és $f : T \to \mathbb{R}$ folytonos függvény a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, akkor a folytonosság topologikus jellemzése és a definíciók alapján minden $c \in \mathbb{R}$ esetén az $[f \neq c]$, $[f < c]$ és $[f > c]$ halmazok $\mathscr{T}$-nyíltak, továbbá az $[f = c]$, $[f \leq c]$ és $[f \geq c]$ halmazok $\mathscr{T}$-zártak.

27.4.1. Definíció. *Azt mondjuk, hogy a $(T, \mathscr{T})$ topologikus tér*

– **reguláris***, ha minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és $t \in T \setminus F$ ponthoz léteznek olyan $\Omega, \Omega' \subseteq T$ diszjunkt $\mathscr{T}$-nyílt halmazok, amelyekre $F \subseteq \Omega$ és $t \in \Omega'$;*

– **teljesen reguláris***, ha minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és $t \in T \setminus F$ ponthoz létezik olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint,* $0 \leq f \leq 1$, *$F \subseteq [f = 0]$ és $f(t) \neq 0$;*

– **normális***, ha bármely két $F, F' \subseteq T$ diszjunkt $\mathscr{T}$-zárt halmazhoz léteznek olyan $\Omega, \Omega' \subseteq T$ diszjunkt $\mathscr{T}$-nyílt halmazok, amelyekre $F \subseteq \Omega$ és $F' \subseteq \Omega'$.*

Nyilvánvaló, hogy a $(T, \mathscr{T})$ topologikus tér pontosan akkor teljesen reguláris, ha minden $\Omega \subseteq T$ $\mathscr{T}$-nyílt halmazhoz és $t \in \Omega$ ponthoz létezik olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, $f(t) = 1$ és $[f \neq 0] \subseteq \Omega$.

Világos továbbá, hogy minden teljesen reguláris tér reguláris, mert ha $(T, \mathscr{T})$ teljesen reguláris tér és $F \subseteq T$ $\mathscr{T}$-zárt halmaz és $t \in T \setminus F$, akkor a teljes regularitás miatt vehetünk olyan $f : T \to \mathbb{R}$ függvényt, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, $F \subseteq [f = 0]$ és $f(t) \neq 0$. Ekkor rögzítve bármilyen $\varepsilon \in]0, f(t)[$ valós számot, az $[f > \varepsilon]$ halmaz $\mathscr{T}$-nyílt és $t \in [f > \varepsilon]$, valamint az $[f < \varepsilon]$ halmaz $\mathscr{T}$-nyílt és $F \subseteq [f = 0] \subseteq [f < \varepsilon]$, és természetesen $[f > \varepsilon] \cap [f < \varepsilon] = \emptyset$.

27.4.2. Állítás. *Minden reguláris* T_0*-tér Hausdorff-tér.*

Bizonyítás. Legyen $(T, \mathscr{T})$ reguláris tér, és $t, t' \in T$ olyanok, hogy $t \neq t'$. Mivel a $(T, \mathscr{T})$ topologikus tér T_0-tér, így létezik olyan $\Omega \subseteq T$ $\mathscr{T}$-nyílt halmaz, hogy $t \in \Omega$ és $t' \notin \Omega$, *vagy* létezik olyan $\Omega' \subseteq T$ $\mathscr{T}$-nyílt halmaz, hogy $t \notin \Omega$ és $t' \in \Omega$. Az általánosság korlátozása nélkül feltehetjük, hogy az elsö eset teljesül, tehát legyen $\Omega \subseteq T$ olyan $\mathscr{T}$-nyílt halmaz, hogy $t \in \Omega$ és $t' \notin \Omega$. Ekkor a $T \setminus \Omega$ halmaz $\mathscr{T}$-zárt és $t \notin T \setminus \Omega$, így a $(T, \mathscr{T})$ topologikus tér regularitása miatt léteznek olyan $V \subseteq T$ és $V' \subseteq T$ $\mathscr{T}$-nyílt halmazok, hogy $t \in V$, $T \setminus \Omega \subseteq V'$ és $V \cap V' = \emptyset$. Ekkor $V \in \mathscr{T}(t)$ és $t' \in V'$, tehát $V' \in \mathscr{T}(t')$, vagyis V, illetve V' diszjunkt környezetei t-nek, illetve t'-nek. ■

Másként fogalmazva: ha egy reguláris tér nem Hausdorff-tér, akkor már T_0-tér sem lehet. Azonban Hausdorff-tér nem szükségképpen reguláris, ami a következő példából látható.

Példa (*nem reguláris Hausdorff-térre*). Legyen $(T, \mathscr{T})$ topologikus tér, és $Q \subseteq T$ olyan halmaz, hogy Q és $T \setminus Q$ mindketten sűrű halmazok T-ben $\mathscr{T}$ szerint. (Konkrét példa: $(T, \mathscr{T}) := (\mathbb{R}, \mathscr{E}_{\mathbb{R}})$ és $Q := \mathbb{Q}$.) Legyen $\mathscr{T}_Q := \{\Omega \cup (\Omega' \cap Q) | (\Omega \in \mathscr{T}) \wedge (\Omega' \in \mathscr{T})\}$. Könnyen ellenőrizhető, hogy $\mathscr{T}_Q$ topológia T felett (éspedig a legkisebb T feletti topológia, amely erősebb $\mathscr{T}$-nél, és amely szerint Q nyílt halmaz). Világos, hogy a $T \setminus Q$ halmaz $\mathscr{T}_Q$-zárt. Megmutatjuk, hogy minden $t \in Q$ esetén *nem léteznek* olyan disztjunkt $\mathscr{T}_Q$-nyílt halmazok, amelyek közül az egyik tartalmazza $T \setminus Q$-t, és a másiknak eleme t. Legyen ugyanis $t \in Q$ és $A, B \in \mathscr{T}_Q$ olyan halmazok, hogy $T \setminus Q \subseteq A$ és $t \in B$. Legyenek $\Omega, \Omega' \in \mathscr{T}$ olyanok, hogy $A = \Omega \cup (\Omega' \cap Q)$. Ekkor nyilvánvalóan $T \setminus Q \subseteq \Omega$, és a hipotézis szerint $T \setminus Q$ a $\mathscr{T}$ topológia szerint sűrű T-ben, így Ω is sűrű T-ben a $\mathscr{T}$ topológia szerint. A $B \in \mathscr{T}_Q$ halmazhoz legyenek $\widetilde{\Omega}, \widetilde{\Omega}' \in \mathscr{T}$ olyanok, hogy $B = \widetilde{\Omega} \cup (\widetilde{\Omega}' \cap Q)$. Mivel $t \in B$, így $t \in \widetilde{\Omega}$ vagy $t \in \widetilde{\Omega}'$. Ha $t \in \widetilde{\Omega}$, akkor $\widetilde{\Omega}$ környezete t-nek a $\mathscr{T}$ topológia szerint, ezért $\Omega \cap \widetilde{\Omega} \neq \emptyset$, így $A \cap B \neq \emptyset$, hiszen $\Omega \cap \widetilde{\Omega} \subseteq A \cap B$. Ha $t \in \widetilde{\Omega}'$, akkor $\widetilde{\Omega}'$ környezete t-nek a $\mathscr{T}$ topológia szerint, ezért $\Omega \cap \widetilde{\Omega}' \neq \emptyset$, így $\Omega \cap \widetilde{\Omega}' \cap Q \neq \emptyset$, hiszen a hipotézis szerint Q is sűrű T-ben a $\mathscr{T}$ topológia szerint. Ezért ekkor is $A \cap B \neq \emptyset$, hiszen $\Omega \cap \widetilde{\Omega}' \cap Q \subseteq A \cap B$. Tehát $(T, \mathscr{T}_Q)$ nem reguláris topologikus tér, ugyanakkor, ha $(T, \mathscr{T})$ Hausdorff-tér, akkor $(T, \mathscr{T}_Q)$ is Hausdorff-tér, mert $\mathscr{T} \subseteq \mathscr{T}_Q$.

27.4.3. Állítás. *Minden normális* T_1*-tér reguláris.*

Bizonyítás. Nyilvánvalóan következik a definíciókból és abból, hogy T_1-térben minden egy elemű halmaz zárt (27.1.3.). ■

27.4.4. Állítás. T_0*-tér* (*illetve* T_1*-tér, illetve Hausdorff-tér*) *minden topologikus altere* T_0*-tér* (*illetve* T_1*-tér, illetve Hausdorff-tér*)*. Teljesen reguláris tér* (*illetve reguláris tér*) *minden topologikus altere teljesen reguláris* (*illetve reguláris*)*. Normális tér minden zárt topologikus altere normális.*

Bizonyítás. Az első állítás nyilvánvalóan következik abból, hogy ha $(T, \mathscr{T})$ topologikus tér és $t \in E$, akkor minden $V \in \mathscr{T}(t)$ esetén $V \cap E \in (\mathscr{T}|E)(t)$.

Legyen $(T, \mathscr{T})$ teljesen reguláris tér, $E \subseteq T$, $t \in E$ és $F \subseteq E$ olyan $\mathscr{T}|E$-zárt halmaz, hogy $t \notin F$. Ekkor van olyan $G \subseteq T$ $\mathscr{T}$-zárt halmaz, hogy $F = G \cap E$, és természetesen $t \in T \setminus G$, ezért a $(T, \mathscr{T})$ topologikus tér teljes regularitása miatt van olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, $G \subseteq [f = 0]$ és $f(t) \neq 0$. Ekkor $f|_E : E \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}|E$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, valamint $F = G \cap E \subseteq [f = 0] \cap E = [f|_E = 0]$ és $(f|_E)(t) = f(t) \neq 0$, tehát $(E, \mathscr{T}|E)$ teljesen reguláris tér.

Legyen $(T, \mathscr{T})$ reguláris tér, $E \subseteq T$ tetszőleges halmaz, $t \in E$ és $F \subseteq E$ olyan $\mathscr{T}|E$-zárt halmaz, hogy $t \notin F$. Ekkor van olyan $G \subseteq T$ $\mathscr{T}$-zárt halmaz, hogy $F = G \cap E$, és természetesen $t \notin G$, különben $t \in G \cap E = F$ teljesülne. A $(T, \mathscr{T})$ topologikus tér regularitása folytán léteznek olyan $\Omega, \Omega' \subseteq T$ $\mathscr{T}$-nyílt halmazok, hogy $G \subseteq \Omega$ és $t \in \Omega'$. Ekkor $\Omega \cap E$ és $\Omega' \cap E$ diszjunkt $\mathscr{T}|E$-nyílt halmazok, és nyilvánvalóan $F = G \cap E \subseteq \Omega \cap E$, valamint $t \in \Omega' \cap E$, így $(E, \mathscr{T}|E)$ reguláris tér.

Legyen $(T, \mathscr{T})$ normális tér, $E \subseteq T$ $\mathscr{T}$-zárt halmaz, és $F, F' \subseteq E$ diszjunkt $\mathscr{T}|E$-zárt halmazok. Ekkor az F és F' halmazok $\mathscr{T}$-zártak is, így a $(T, \mathscr{T})$ topologikus tér normálissága miatt léteznek olyan $\Omega, \Omega' \subseteq T$ $\mathscr{T}$-nyílt halmazok, hogy $F \subseteq \Omega$ és $F' \subseteq \Omega'$. Világos, hogy ekkor $\Omega \cap E$ és $\Omega' \cap E$ diszjunkt $\mathscr{T}|E$-nyílt halmazok, és természetesen $F \subseteq \Omega \cap E$, valamint $F' \subseteq \Omega' \cap E$, tehát $(E, \mathscr{T}|E)$ normális tér. ■

27.4.5. Állítás. *A $(T, \mathscr{T})$ topologikus tér pontosan akkor reguláris, ha T minden pontjának létezik $\mathscr{T}$-zárt halmazokból álló környezetbázisa a $\mathscr{T}$ topológia szerint.*

Bizonyítás. Legyen $(T, \mathscr{T})$ reguláris tér, $t \in T$ és $V \in \mathscr{T}(t)$. Ekkor létezik olyan $\Omega \in \mathscr{T}$, amelyre $t \in \Omega \subseteq V$. Tehát $t \notin T \setminus \Omega$ és $T \setminus \Omega$ $\mathscr{T}$-zárt halmaz, így a $(T, \mathscr{T})$ topologikus tér regularitása miatt léteznek olyan $\Omega_t, \Omega' \subseteq T$ diszjunkt $\mathscr{T}$-nyílt halmazok, hogy $t \in \Omega_t$ és $T \setminus \Omega \subseteq \Omega'$. Ekkor $t \in \Omega_t \subseteq T \setminus \Omega' \subseteq \Omega \subseteq V$, tehát $V' := T \setminus \Omega'$ olyan $\mathscr{T}$-zárt környezete t-nek, amelyre $V' \subseteq V$. Ez azt jelenti, hogy a $\{V \in \mathscr{T}(t) | V \text{ zárt } \mathscr{T} \text{ szerint}\}$ halmaz zárt halmazokból álló környezetbázisa t-nek a $\mathscr{T}$ topológia szerint.

Megfordítva, tegyük fel, hogy T minden pontjának létezik $\mathscr{T}$-zárt halmazokból álló környezetbázisa a $\mathscr{T}$ topológia szerint. Legyen $t \in T$ és $F \subseteq T$ olyan $\mathscr{T}$-zárt halmaz, hogy $t \notin F$. Ekkor $T \setminus F$ a t-nek $\mathscr{T}$-nyílt környezete, így a hipotézis szerint van olyan $V \in \mathscr{T}(t)$, hogy $V \subseteq T \setminus F$ és a V halmaz $\mathscr{T}$-zárt. Legyen $\Omega \in \mathscr{T}$ olyan, hogy $t \in \Omega \subseteq V$, valamint legyen $\Omega' := T \setminus V$. Ekkor Ω és Ω' diszjunkt $\mathscr{T}$-nyílt halmazok, és $t \in \Omega$, valamint $F \subseteq T \setminus V =: \Omega'$, tehát $(T, \mathscr{T})$ reguláris tér. ∎

27.4.6. Állítás. *Minden félmetrizálható topologikus tér reguláris.*

Bizonyítás. Félmetrikus térben minden zárt gömb zárt halmaz, ezért az állítás nyilvánvalóan következik 27.4.5.-ből. ∎

Most megmutatjuk, hogy topologikus tér regularitása, bizonyos megszámlálhatósági feltétellel együtt, maga után vonja a normálisságot. Ehhez bevezetünk egy nevezetes topologikustér-típust.

27.4.7. Definíció. *A $(T, \mathscr{T})$ topologikus tér* $\mathscr{T}$**-nyílt befedésének** *nevezünk minden olyan $(\Omega_i)_{i \in I}$ rendszert, amelyre $T = \bigcup_{i \in I} \Omega_i$ és minden $I \ni i$-re Ω_i $\mathscr{T}$-nyílt részhalmaza T-nek. A $(T, \mathscr{T})$ topologikus teret* **Lindelöf-térnek** *nevezzük, ha a T halmaz bármely $(\Omega_i)_{i \in I}$ $\mathscr{T}$-nyílt befedéséhez létezik olyan $J \subseteq I$ megszámlálható halmaz, hogy $(\Omega_i)_{i \in J}$ is befedése T-nek.*

27.4.8. Tétel. (Lindelöf-tétel) *Minden megszámlálható bázisú topologikus tér Lindelöf-tér.*

Bizonyítás. Legyen $\mathfrak{B}$ megszámlálható bázisa a $(T, \mathscr{T})$ topologikus térnek, és legyen $(\Omega_i)_{i \in I}$ a T-nek tetszőleges $\mathscr{T}$-nyílt befedése. *Kiválasztható* olyan $(\mathfrak{B}_i)_{i \in I}$ rendszer, hogy minden $i \in I$ esetén $\mathfrak{B}_i \subseteq \mathfrak{B}$ és $\Omega_i = \bigcup_{\Omega \in \mathfrak{B}_i} \Omega$. Ekkor a $\mathfrak{B}' := \bigcup_{i \in I} \mathfrak{B}_i$ halmaz megszámlálható, mert $\mathfrak{B}' \subseteq \mathfrak{B}$, továbbá nyilvánvalóan $T = \bigcup_{\Omega \in \mathfrak{B}'} \Omega$. A $\mathfrak{B}'$ definíciója szerint minden $\Omega \in \mathfrak{B}'$ esetén van olyan $i \in I$, hogy $\Omega \in \mathfrak{B}_i$. Ezért *kiválasztható* olyan $f : \mathfrak{B}' \to I$ függvény, hogy minden $\mathfrak{B}' \ni \Omega$-ra $\Omega \in \mathfrak{B}_{f(\Omega)}$. Ekkor $\mathrm{Im}(f) \subseteq I$ megszámlálható részhalmaz és $T = \bigcup_{i \in \mathrm{Im}(f)} \Omega_i$. ∎

Később látni fogjuk, hogy minden kompakt tér is Lindelöf-tér, de létezik nem megszámlálható bázisú kompakt tér. Ezért az előző állításban található következtetés nem fordítható meg.

27.4.9. Állítás. (Tyihonov-lemma) *Minden reguláris Lindelöf-tér normális.*

Bizonyítás. Legyen $(T, \mathscr{T})$ reguláris Lindelöf-tér, és legyenek $F, F' \subseteq T$ nem üres, diszjunkt $\mathscr{T}$-zárt halmazok. Ha $t \in F$, akkor $t \in T \setminus F'$ és a $T \setminus F'$ halmaz $\mathscr{T}$-nyílt, ezért a regulartitás miatt létezik t-nek olyan V $\mathscr{T}$-nyílt környezete, hogy $\overline{V} \subseteq T \setminus F'$, azaz $\overline{V} \cap F' = \emptyset$. Ezért *kiválasztható* olyan $(V_t)_{t \in F}$ rendszer, hogy minden $F \ni t$-re $V_t \in \mathscr{T}(t)$ és a V_t halmaz $\mathscr{T}$-nyílt, valamint $\overline{V_t} \cap F' = \emptyset$. Az F és F' halmazok szerepét felcserélve hasonlóan kapjuk olyan $(V_t)_{t \in F'}$ rendszer létezését, hogy minden $F' \ni t$-re $V_t \in \mathscr{T}(t)$ és a V_t halmaz $\mathscr{T}$-nyílt, valamint $\overline{V_t} \cap F = \emptyset$. Legyen ω olyan halmaz, hogy $\omega \notin F \cup F'$, és legyen $V_\omega := T \setminus (F \cup F')$. Ekkor $(V_t)_{t \in F \cup F' \cup \{\omega\}}$ a T halmaznak $\mathscr{T}$-nyílt befedése, és $(T, \mathscr{T})$ Lindelöf-tér, ezért létezik olyan $D \subseteq F \cup F' \cup \{\omega\}$ megszámlálható halmaz, hogy $T = \bigcup_{t \in D} V_t$. Ha $t \in F$, akkor van olyan $s \in D$, hogy $t \in V_s$, és nyilvánvaló, hogy $s \notin F'$ (mert $t \in V_s \cap F$ és $s \in F'$ esetén még $\overline{V_s} \cap F = \emptyset$ is igaz), továbbá természetesen $s \neq \omega$ (mert $t \notin T \setminus (F \cup F') =: V_\omega$). Ez azt jelenti, hogy $t \in F$ esetén van olyan $s \in D \cap F$, hogy $t \in V_s$, vagyis $F \subseteq \bigcup_{s \in D \cap F} V_s$. Felcserélve az F és F' halmazok szerepét hasonlóan kapjuk, hogy $F' \subseteq \bigcup_{s \in D \cap F'} V_s$. Feltettük, hogy $F \neq \emptyset$, ezért $D \cap F$ nem üres megszámlálható halmaz, így létezik olyan $\sigma : \mathbb{N} \to D \cap F$ függvény, amely szürjekció. Hasonlóan adódik $\sigma' : \mathbb{N} \to D \cap F'$ szürjekció létezése is. Legyen minden $n \in \mathbb{N}$ esetén

$$\Omega_n := V_{\sigma(n)} \setminus \bigcup_{k=0}^{n} \overline{V_{\sigma'(k)}}, \qquad \Omega'_n := V_{\sigma'(n)} \setminus \bigcup_{k=0}^{n} \overline{V_{\sigma(k)}},$$

továbbá értelmezzük az

$$\Omega := \bigcup_{n \in \mathbb{N}} \Omega_n, \qquad \Omega' := \bigcup_{n \in \mathbb{N}} \Omega'_n$$

halmazokat. Világos, hogy minden $\mathbb{N} \ni n$-re Ω_n és Ω'_n mindketten $\mathscr{T}$-nyílt halmazok T-ben, ezért Ω és Ω' szintén $\mathscr{T}$-nyílt halmazok. Ha $m, n \in \mathbb{N}$ és $m \leq n$, akkor $\Omega_n \cap \overline{V_{\sigma'(m)}} = \emptyset$ és $\Omega'_m \subseteq V_{\sigma'(m)}$, ezért $\Omega_n \cap \Omega'_m = \emptyset$. Ha $m, n \in \mathbb{N}$ és $n \leq m$, akkor $\Omega'_m \cap \overline{V_{\sigma(n)}} = \emptyset$ és $\Omega_n \subseteq V_{\sigma(n)}$, ezért $\Omega'_m \cap \Omega_n = \emptyset$. Ez azt jelenti, hogy minden $\mathbb{N} \ni m, n$-re $\Omega_n \cap \Omega'_m = \emptyset$, amiből következik, hogy $\Omega \cap \Omega' = \emptyset$. Minden $k \in \mathbb{N}$ esetén $F \cap \overline{V_{\sigma'(k)}} = \emptyset$, ugyanakkor $F \subseteq \bigcup_{t \in D \cap F} V_t = \bigcup_{n \in \mathbb{N}} V_{\sigma(n)}$, ezért $F \subseteq \bigcup_{n \in \mathbb{N}} \Omega_n =: \Omega$. Minden $k \in \mathbb{N}$ esetén $F' \cap \overline{V_{\sigma(k)}} = \emptyset$, ugyanakkor $F' \subseteq \bigcup_{t \in D \cap F'} V_t = \bigcup_{n \in \mathbb{N}} V_{\sigma'(n)}$, ezért $F' \subseteq \bigcup_{n \in \mathbb{N}} \Omega'_n =: \Omega'$. ■

27.4.10. Következmény. *Minden megszámlálható bázisú reguláris tér normális.*

Bizonyítás. A Lindelöf-tétel és a Tyihonov-lemma összetevéséből kapjuk. ■

Legyen (M, d) félmetrikus tér. Minden nem üres $E \subseteq M$ halmazra és $x \in M$ pontra értelmezzük a

$$d(x, E) := \inf_{y \in E} d(x, y)$$

számot, amit *az x pont és az E halmaz távolságának* nevezünk. Könnyen látható, hogy ha $E \subseteq M$ nem üres halmaz, akkor az

$$d(\cdot, E) : M \to \mathbb{R}; \quad x \mapsto d(x, E)$$

leképezés folytonos a $\mathscr{T}_d$ és az $\mathscr{E}_{\mathbb{R}}$ euklidészi topológia szerint, ugyanis minden $x, y \in M$ esetén fennáll, hogy $|d(x, E) - d(y, E)| \leq d(x, y)$. Egyszerűen bizonyítható az is, hogy ha $E \subseteq M$ nem üres halmaz, akkor $\overline{E} = [d(\cdot, E) = 0]$.

27.4.11. Állítás. *Minden félmetrizálható topologikus tér normális.*

Bizonyítás. Legyen (M, d) félmetrikus tér, továbbá legyenek F és F' olyan nem üres diszjunkt zárt halmazok M-ben. A $d(\cdot, F) + d(\cdot, F') : M \to \mathbb{R}$ függvény mindenütt nullánál nagyobb értéket vesz fel, mert ha az $x \in M$ pontban az értéke nulla volna, akkor $d(x, F) = 0 = d(x, F')$, így az F és F' halmazok zártsága miatt $x \in F \cap F'$ teljesülne. Továbbá, a $d(\cdot, F) + d(\cdot, F') : M \to \mathbb{R}$ függvény folytonos is, így az

$$f := \frac{d(\cdot, F)}{d(\cdot, F) + d(\cdot, F')} : M \to \mathbb{R}$$

függvény jól értelmezett és folytonos. Nyilvánvaló, hogy

$$F = [d(\cdot, F) = 0] \subseteq [f = 0], \quad F' \subseteq [f = 1].$$

Ezért bármely $r \in]0, 1[$ valós számra az $\Omega := [f < r]$ és $\Omega' := [f > r]$ halmazok olyan diszjunkt nyílt halmazok M-ben, amelyekre $F \subseteq \Omega$ és $F' \subseteq \Omega'$. ■

27.5. Normális terek jellemzése I – Uriszon-tétel

Most először a normálisság és teljes regularitás kapcsolatát tisztázzuk. Ebből a szempontból a legfontosabb eredmény az Uriszon-tétel, amely megmutatja, hogy normális téren "elég sok" folytonos valós függvény létezik. Nemtriviális folytonos függvények létezése általában nem szükségszerű; például az antidiszkrét terekről induló, T_0-terekbe érkező folytonos függvények nyilvánvalóan mind triviálisak (vagyis állandók).

27.5.1. Tétel. (Uriszon-tétel) *Ha $(T, \mathscr{T})$ topologikus tér, akkor a következő kijelentések ekvivalensek.*

(i) *$(T, \mathscr{T})$ normális tér.*

(ii) *Minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és minden $\Omega \subseteq T$ $\mathscr{T}$-nyílt halmazhoz, $F \subseteq \Omega$ esetén létezik olyan $U \subseteq T$ $\mathscr{T}$-nyílt halmaz, hogy $F \subseteq U \subseteq \overline{U} \subseteq \Omega$.*

(iii) *Minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és minden $\Omega \subseteq T$ $\mathscr{T}$-nyílt halmazhoz, $F \subseteq \Omega$ esetén létezik olyan $(\Omega_\alpha)_{\alpha\in[0,1]}$ rendszer, hogy minden $\alpha \in [0, 1]$ számra Ω_α $\mathscr{T}$-nyílt részhalmaza T-nek, és $F \subseteq \Omega_\alpha \subseteq \overline{\Omega_\alpha} \subseteq \Omega$, továbbá minden $[0, 1] \ni \alpha, \beta$-ra, ha $\alpha < \beta$, akkor $\overline{\Omega_\alpha} \subseteq \Omega_\beta$.*

(iv) *Minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és minden $\Omega \subseteq T$ $\mathscr{T}$-nyílt halmazhoz, $F \subseteq \Omega$ esetén létezik olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, valamint $F \subseteq [f = 1] \subseteq \overline{[f \neq 0]} \subseteq \Omega$.*

(v) *Bármely két $F, F' \subseteq T$ diszjunkt $\mathscr{T}$-zárt halmazhoz létezik olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, valamint $F \subseteq [f = 1]$ és $F' \subseteq [f = 0]$.*

Bizonyítás. (i)⇒(ii) Legyen az $F \subseteq T$ halmaz $\mathscr{T}$-zárt, az $\Omega \subseteq T$ halmaz $\mathscr{T}$-nyílt, és tegyük fel, hogy $F \subseteq \Omega$. Ekkor F és $T \setminus \Omega$ diszjunkt $\mathscr{T}$-zárt halmazok, ezért az (i) miatt léteznek olyan $U, V \in \mathscr{T}$ diszjunkt halmazok, hogy $F \subseteq U$ és $T \setminus \Omega \subseteq V$. Ekkor $U \subseteq T \setminus V$ és a $T \setminus V$ halmaz $\mathscr{T}$-zárt, ezért $F \subseteq U \subseteq \overline{U} \subseteq T \setminus V \subseteq \Omega$.

(ii)⇒(iii) Legyen az $F \subseteq T$ halmaz $\mathscr{T}$-zárt, az $\Omega \subseteq T$ halmaz $\mathscr{T}$-nyílt, és tegyük fel, hogy $F \subseteq \Omega$. Minden $n \in \mathbb{N}$ esetén értelmezzük a

$$D_n := \left\{ \frac{k}{2^n} \;\middle|\; (k \in \mathbb{N}) \wedge (k \leq 2^n) \right\}$$

halmazt, és legyen $D := \bigcup_{n\in\mathbb{N}} D_n$. (A D halmaz elemeit a $[0,1]$ intervallum *diadikusan racionális* elemeinek nevezzük.) Világos, hogy minden $n \in \mathbb{N}$ esetén $D_n \subseteq D_{n+1}$, mert ha $k \in \mathbb{N}$ és $k \leq 2^n$, akkor $2k \leq 2^{n+1}$, és $\frac{k}{2^n} = \frac{2k}{2^{n+1}} \in D_{n+1}$. Továbbá, a D halmaz *megszámlálható*, és *sűrű* a $[0,1]$ intervallumban, mert $t \in [0,1]$ esetén van olyan $(c_k)_{k\in\mathbb{N}}$ sorozat, hogy minden $\mathbb{N} \ni k$-ra $c_k \in \{0,1\}$ és $t = \sum_{k=0}^{\infty} \frac{c_k}{2^k}$ (ez a t szám felírása a kettes számrendszerben), tehát, ha $\varepsilon \in \mathbb{R}_+^*$, akkor van olyan $n \in \mathbb{N}$, hogy $\left| t - \sum_{k=0}^{n} \frac{c_k}{2^k} \right| < \varepsilon$, ugyanakkor nyilvánvalóan $\sum_{k=0}^{n} \frac{c_k}{2^k} = \frac{1}{2^n} \sum_{k=0}^{n} 2^{n-k} c_k \in D_n$, hiszen $0 \leq \sum_{k=0}^{n} \frac{c_k}{2^k} \leq t \leq 1$, vagyis $0 \leq \sum_{k=0}^{n} 2^{n-k} c_k \leq 2^n$.

A kiválasztási axiómával kombinált rekurzió tételét alkalmazva megmutatjuk olyan $\left((\Omega_{n,r})_{r\in D_n}\right)_{n\in\mathbb{N}}$ sorozat létezését, amelyre minden $n \in \mathbb{N}$ esetén $(\Omega_{n,r})_{r\in D_n}$ olyan (véges) $\mathscr{T}$-ben haladó rendszer, hogy minden $D_n \ni r$-re $F \subseteq \Omega_{n,r} \subseteq \overline{\Omega_{n,r}} \subseteq \Omega$, valamint minden $r, s \in D_n$ esetén, ha $r < s$, akkor $\overline{\Omega_{n,r}} \subseteq \Omega_{n,s}$, továbbá minden $D_n \ni r$-re $\Omega_{n+1,r} = \Omega_{n,r}$.

A (ii) hipotézis alapján az F és Ω halmazokhoz létezik olyan $U \in \mathscr{T}$, hogy $F \subseteq U \subseteq \overline{U} \subseteq \Omega$. Ismét a (ii) hipotézist alkalmazva az $\overline{U}$ és Ω halmazokra kapjuk olyan $V \in \mathscr{T}$ létezését, hogy $\overline{U} \subseteq V \subseteq \overline{V} \subseteq \Omega$. Ha $\Omega_{0,0} := U$ és $\Omega_{0,1} := V$, akkor $(\Omega_{0,r})_{r\in D_0}$ olyan rendszer $\mathscr{T}$-ben, hogy minden $D_0 \ni r$-re $F \subseteq \Omega_{0,r} \subseteq \overline{\Omega_{0,r}} \subseteq \Omega$, továbbá minden $r, s \in D_0 = \{0,1\}$ esetén, ha $r < s$, akkor $\overline{\Omega_{0,r}} \subseteq \Omega_{0,s}$.

Tegyük fel, hogy $n \in \mathbb{N}^*$ és $\left((\Omega_{k,r})_{r\in D_k}\right)_{k\in n}$ olyan rendszer, hogy minden $k \in n$ esetén $(\Omega_{k,r})_{r\in D_k}$ olyan $\mathscr{T}$-ben haladó rendszer, amelyre minden $r \in D_k$ esetén $F \subseteq \Omega_{k,r} \subseteq \overline{\Omega_{k,r}} \subseteq \Omega$, valamint minden $r, s \in D_k$ esetén, ha $r < s$, akkor $\overline{\Omega}_{k,r} \subseteq \Omega_{k,s}$, továbbá minden $n \ni k$-ra, ha $k+1 < n$ és $r \in D_k$, akkor $\Omega_{k+1,r} = \Omega_{k,r}$. Minden $r \in D_{n-1}$ esetén legyen $\Omega_{n,r} := \Omega_{n-1,r}$. Legyen $r \in D_n \setminus D_{n-1}$ rögzített; ekkor egyértemű̋en létezik olyan $k \in \mathbb{N}$, hogy $2k+1 \leq 2^n$ és $r = \frac{2k+1}{2^n}$. Világos, hogy $k < 2^{n-1}$, tehát $r_0 := \frac{k}{2^{n-1}} \in D_{n-1}$ és $r_1 := \frac{k+1}{2^{n-1}} \in D_{n-1}$, továbbá $r_0 < r < r_1$, és r a D_n egyetlen eleme, amely r_0 és r_1 közé esik. Az $\left((\Omega_{k,r})_{r\in D_k}\right)_{k\in n}$ rendszer tulajdonságai alapján $\overline{\Omega_{n-1,r_0}} \subseteq \Omega_{n-1,r_1}$, így a (ii) hipotézist alkalmazva az $\overline{\Omega_{n-1,r_0}}$ és Ω_{n-1,r_1} halmazokra kapjuk olyan $\Omega_{n,r} \in \mathscr{T}$ létezését, hogy $\overline{\Omega_{n-1,r_0}} \subseteq \Omega_{n,r} \subseteq \overline{\Omega_{n,r}} \subseteq \Omega_{n-1,r_1}$. Ebből látszik, hogy a most értelmezett $\left((\Omega_{k,r})_{r\in D_k}\right)_{k\in n+1}$ rendszer teljesíti ugyanazokat a feltételeket, mint az $\left((\Omega_{k,r})_{r\in D_k}\right)_{k\in n}$ rendszer, ha az n helyére az $n+1$ számot írjuk.

Legyen tehát $\left((\Omega_{n,r})_{r\in D_n}\right)_{n\in\mathbb{N}}$ olyan sorozat, amelynek a létezését imént igazoltuk. Ha $r \in D$, akkor minden $\mathbb{N} \ni m, n$-re, $r \in D_m \cap D_n$ esetén $\Omega_{m,r} = \Omega_{n,r}$. Ezért minden $r \in D$ számra értelmezhetjük az Ω_r halmazt úgy, hogy $\Omega_r := \Omega_{n,r}$ minden olyan $\mathbb{N} \ni n$-re, amelyre $r \in D_n$. Világos, hogy minden $r \in D$ esetén $F \subseteq \Omega_r \subseteq \overline{\Omega_r} \subseteq \Omega$. Továbbá, $r, s \in D$ esetén van olyan $n \in \mathbb{N}$, hogy $r, s \in D_n$, tehát, ha $r < s$, akkor $\overline{\Omega_r} := \overline{\Omega_{n,r}} \subseteq \Omega_{n,s} =: \Omega_s$. Legyen minden $\alpha \in [0,1] \setminus D$ esetén $\Omega_\alpha := \bigcup_{\substack{r\in D\\ r\leq\alpha}} \Omega_r$. Ekkor minden $\alpha \in [0,1] \setminus D$ esetén $\Omega_\alpha \in \mathscr{T}$ és $F \subseteq \Omega_0 \subseteq \Omega_\alpha$, valamint $\overline{\Omega_\alpha} \subseteq \Omega$ is teljesül, mert $\alpha < 1$ (hiszen $1 \in D$), tehát a D sűrűsége miatt van olyan $s \in D$, hogy $\alpha < s$, így $\Omega_\alpha \subseteq \Omega_s$, vagyis $\overline{\Omega_\alpha} \subseteq \overline{\Omega_s} \subseteq \Omega$. Továbbá, ha $\alpha, \beta \in [0,1]$ és $\alpha < \beta$, akkor ismét a D sűrűségéből következik olyan $r, s \in D$ számok létezése, hogy $\alpha < r < s < \beta$, és ekkor $\overline{\Omega_\alpha} \subseteq \overline{\Omega_r} \subseteq \Omega_s \subseteq \Omega_\beta$. Ez azt jelenti, hogy $(\Omega_\alpha)_{\alpha\in[0,1]}$ olyan rendszer, amelynek a létezését (iii)-ban állítottuk.

(iii)⇒(iv) Legyen az $F \subseteq T$ halmaz $\mathscr{T}$-zárt, az $\Omega \subseteq T$ halmaz $\mathscr{T}$-nyílt, és tegyük fel, hogy $F \subseteq \Omega$. A (iii) alapján vegyünk olyan $(\Omega_\alpha)_{\alpha\in[0,1]}$ rendszert, hogy minden $\alpha \in [0,1]$ számra Ω_α $\mathscr{T}$-nyílt részhalmaza T-nek, és $F \subseteq \Omega_\alpha \subseteq \overline{\Omega_\alpha} \subseteq \Omega$, továbbá minden $[0,1] \ni \alpha, \beta$-ra, ha $\alpha < \beta$, akkor $\overline{\Omega_\alpha} \subseteq \Omega_\beta$.

Értelmezzük a $g : T \to \mathbb{R}$ függvényt úgy, hogy minden $t \in \Omega_1$ esetén

$$g(t) := \inf\{\, \gamma \in [0,1] \mid t \in \Omega_\gamma \,\},$$

és minden $T \setminus \Omega_1 \ni t$-re $g(t) := 1$. Világos, hogy $T \setminus \Omega \subseteq T \setminus \Omega_1 \subseteq [g = 1]$, és minden $t \in T$ esetén $0 \le g(t) \le 1$.

Megmutatjuk, hogy ha $\alpha, \beta \in [0,1]$ és $\alpha < \beta$, akkor

$$\overset{-1}{g}\langle]\alpha,\beta[\rangle \subseteq \Omega_\beta \setminus \overline{\Omega_\alpha} \subseteq \overset{-1}{g}\langle [\alpha,\beta] \rangle.$$

Valóban, ha $t \in \overset{-1}{g}\langle]\alpha,\beta[\rangle$, akkor $g(t) := \inf\{\gamma \in [0,1] | t \in \Omega_\gamma\} < \beta$ miatt van olyan $\gamma \in [0,1]$, hogy $t \in \Omega_\gamma$ és $\gamma < \beta$; ekkor $\Omega_\gamma \subseteq \Omega_\beta$ miatt $t \in \Omega_\beta$. Ugyanakkor $t \notin \overline{\Omega_\alpha}$, különben minden $\gamma \in [0,1]$ számra, $\alpha < \gamma$ esetén $t \in \overline{\Omega_\alpha} \subseteq \Omega_\gamma$, tehát $g(t) \le \gamma$ teljesülne, így fennállna a $g(t) \le \alpha$ egyenlőtlenség, holott $g(t) > \alpha$. Továbbá, ha $t \in \Omega_\beta \setminus \overline{\Omega_\alpha}$, akkor $t \in \Omega_\beta$, így $g(t) := \inf\{\gamma \in [0,1] | t \in \Omega_\gamma\} \le \beta$, valamint $g(t) \ge \alpha$, különben volna olyan $\gamma \in [0,1]$, hogy $\gamma < \alpha$ és $t \in \Omega_\gamma$, ami lehetetlen, mert ekkor $t \in \Omega_\gamma \subseteq \overline{\Omega_\gamma} \subseteq \Omega_\alpha \subseteq \overline{\Omega_\alpha}$ teljesülne, holott $t \notin \overline{\Omega_\alpha}$.

Megmutatjuk, hogy $\overline{\Omega_0} \subseteq [g = 0]$. Valóban, ha $t \in [g \ne 0]$ és $t \in \Omega_1$, akkor $g(t) := \inf\{\gamma \in [0,1] | t \in \Omega_\gamma\} > 0$, és ha $\beta \in]0, g(t)[$, akkor $t \notin \Omega_\beta$, így $t \notin \overline{\Omega_0}$, mert $\overline{\Omega_0} \subseteq \Omega_\beta$. Ha pedig $t \in [g \ne 0]$ és $t \notin \Omega_1$, akkor $t \notin \overline{\Omega_0}$, mert $\overline{\Omega_0} \subseteq \Omega_1$.

Most bebizonyítjuk, hogy a $g : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Ehhez legyen $t \in T$ rögzített pont; ekkor három eset lehetséges.

– Ha $t \in \overset{-1}{g}\langle]0,1[\rangle$, akkor bármely $\varepsilon \in]0, \min(g(t), 1 - g(t))]$ valós számra az előzőek alapján

$$t \in \overset{-1}{g}\langle]g(t)-\varepsilon, g(t)+\varepsilon[\rangle \subseteq \Omega_{g(t)+\varepsilon} \setminus \overline{\Omega_{g(t)-\varepsilon}} \subseteq \overset{-1}{g}\langle [g(t)-\varepsilon, g(t)+\varepsilon] \rangle,$$

tehát a $V_\varepsilon := \Omega_{g(t)+\varepsilon} \setminus \overline{\Omega_{g(t)-\varepsilon}}$ halmaz a t pontnak olyan $\mathscr{T}$-nyílt környezete, amelyre $g\langle V_\varepsilon \rangle \subseteq [g(t)-\varepsilon, g(t)+\varepsilon]$, így g folytonos a t pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.

– Ha $t \in [g = 0]$, vagyis $0 = g(t) := \inf\{\gamma \in [0,1] | t \in \Omega_\gamma\}$, akkor vegyünk tetszőleges $\varepsilon \in \mathbb{R}_+^*$ számot. Rögzítsünk olyan $\gamma \in [0,1]$ számot, amelyre $\gamma < \varepsilon$. Állítjuk, hogy Ω_γ olyan $\mathscr{T}$-nyílt környezete t-nek, hogy $g\langle \Omega_\gamma \rangle \subseteq [-\varepsilon, \varepsilon]$. Valóban, az előzőek alapján $\Omega_\gamma \setminus \overline{\Omega_0} \subseteq \overset{-1}{g}\langle [0,\gamma] \rangle \subseteq \overset{-1}{g}\langle [0,\varepsilon] \rangle$, továbbá $\Omega_\gamma \cap \overline{\Omega_0} \subseteq \overline{\Omega_0} \subseteq [g = 0] \subseteq \overset{-1}{g}\langle [0,\varepsilon] \rangle$, ezért

$$\Omega_\gamma = \left(\Omega_\gamma \setminus \overline{\Omega_0}\right) \cup \left(\Omega_\gamma \cap \overline{\Omega_0}\right) \subseteq \overset{-1}{g}\langle [0,\varepsilon] \rangle = \overset{-1}{g}\langle [-\varepsilon,\varepsilon] \rangle,$$

vagyis $g\langle \Omega_\gamma \rangle \subseteq [-\varepsilon, \varepsilon]$. Ebből következik, hogy g folytonos a t pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.

– Ha $t \in [g = 1]$, akkor két alternatíva van: $t \notin \overline{\Omega_1}$ vagy $t \in \overline{\Omega_1}$. Az első esetben $T \setminus \overline{\Omega_1}$

olyan $\mathscr{T}$-nyílt környezete t-nek, amelyen $g = 1$, ezért a folytonosság lokalitása miatt g folytonos a t pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Ezért feltehető, hogy $t \in \overline{\Omega_1}$. Legyen $\varepsilon \in]0,1[$ tetszőleges valós szám. Ekkor $t \in T \setminus \overline{\Omega_{1-\varepsilon}}$, különben véve egy $\gamma \in]1-\varepsilon, 1[$ számot kapnánk, hogy $t \in \overline{\Omega_{1-\varepsilon}} \subseteq \Omega_\gamma$, így $g(t) \leq \gamma < 1$, holott $g(t) = 1$. Tehát $T \setminus \overline{\Omega_{1-\varepsilon}}$ a t pontnak $\mathscr{T}$-nyílt környezete, és az előzőek alkalmazásával

$$g\langle T \setminus \overline{\Omega_{1-\varepsilon}} \rangle = g\langle T \setminus \Omega_1 \rangle \cup g\langle \Omega_1 \setminus \overline{\Omega_{1-\varepsilon}} \rangle \subseteq \{1\} \cup [1-\varepsilon, 1] \subseteq [1-\varepsilon, 1+\varepsilon],$$

tehát g folytonos a t pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.

Ezzel megmutattuk, hogy a $g : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq g \leq 1$, valamint $\Omega_0 \subseteq [g = 0]$ és $T \setminus \Omega_1 \subseteq [g = 1]$. Ezért az $f := 1 - g : T \to \mathbb{R}$ függvény is folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, valamint $F \subseteq \Omega_0 \subseteq [g = 0] = [f = 1]$ és $\overline{[f \neq 0]} = \overline{[g \neq 1]} \subseteq \overline{\Omega_1} \subseteq \Omega$, vagyis az f függvény eleget tesz a (iv) követelményeinek.

(iv)⇒(v) Legyenek $F, F' \subseteq T$ diszjunkt $\mathscr{T}$-zárt halmazok. Ekkor $\Omega := T \setminus F'$ olyan $\mathscr{T}$-nyílt halmaz, hogy $F \subseteq \Omega$, így a (iv) alapján van olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, valamint $F \subseteq [f = 1]$ és $\overline{[f \neq 0]} \subseteq \Omega$, vagyis $F' \subseteq [f = 0]$.

(v)⇒(i) Legyenek $F, F' \subseteq T$ diszjunkt $\mathscr{T}$-zárt halmazok, és az (v) alapján legyen $f : T \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, valamint $F \subseteq [f = 1]$ és $F' \subseteq [f = 0]$. Ekkor bármely $r \in]0,1[$ valós számra $F \subseteq [f < r]$ és $F' \subseteq [f > r]$, továbbá $[f < r] := \overset{-1}{f}\langle]\leftarrow, r[\rangle$ és $[f > r] := \overset{-1}{f}\langle]r, \to[\rangle$ diszjunkt $\mathscr{T}$-nyílt halmazok. Ezért a $(T, \mathscr{T})$ topologikus tér normális. ■

27.5.2. Következmény. *Minden normális* T_1*-tér teljesen reguláris Hausdorff-tér.*

Bizonyítás. Legyen $(T, \mathscr{T})$ normális T_1-tér, $F \subseteq T$ $\mathscr{T}$-zárt halmaz és $t \in T \setminus F$. Ekkor a $\{t\}$ halmaz $\mathscr{T}$-zárt, mert $(T, \mathscr{T})$ T_1-tér, így az Uriszon-tétel szerint van olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, valamint $\{t\} \subseteq [f = 1]$ és $F \subseteq [f = 0]$. Ez azt jelenti, hogy $(T, \mathscr{T})$ teljesen reguláris tér, és korábban láttuk, hogy minden teljesen reguláris T_1-tér szükségképpen Hausdorff-tér. ■

Megjegyezzük, hogy a teljesen reguláris T_0-tereket *Tyihonov-tereknek* is nevezik. Ezek szükségképpen Hausdorff-terek, mert minden teljesen reguáris tér reguláris, és láttuk, hogy minden reguláris T_0-tér Hausdorff-tér.

27.6. Normális terek jellemzése II – Tietze-tétel

A következő tétel előtt megjegyezzük, hogy ha $(T, \mathscr{T})$ topologikus tér, az $F \subseteq T$ halmaz $\mathscr{T}$-zárt és $f : F \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, akkor f nem szükségképpen terjeszthető ki $T \to \mathbb{R}$ függvénnyé úgy, hogy a kiterjesztés folytonos legyen a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Másként fogalmazva: topologikus tér zárt topologikus alterén folytonos valós függvény nem feltétlenül terjeszthető ki a térre folytonosan. A Tietze-tétel éppen azt mondja, hogy a zárt topologikus altereken folytonos valós függvények folytonos kiterjeszthetősége *ekvivalens* a tér normálisságával.

27.6.1. Tétel. (Tietze-tétel) *Ha* $(T, \mathscr{T})$ *topologikus tér, akkor a következő kijelentések ekvivalensek.*

(i) $(T, \mathscr{T})$ *normális tér.*

(ii) *Ha az $F \subseteq T$ halmaz $\mathscr{T}$-zárt, $f : F \to \mathbb{R}$ folytonos függvény a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, és minden $F \ni t$-re $|f(t)| \leq 1$, akkor minden $c \in]0, 1/3]$ valós számhoz létezik olyan $g : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, és minden $t \in T$ esetén $|g(t)| \leq c$, valamint minden $t \in F$ esetén $|f(t) - g(t)| \leq 1 - c$.*

(iii) *Ha az $F \subseteq T$ halmaz $\mathscr{T}$-zárt és $f : F \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, akkor létezik olyan $\widetilde{f} : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint és $f = \widetilde{f}|_F$.*

Bizonyítás. (i)⇒(ii) Legyen az $F \subseteq T$ halmaz $\mathscr{T}$-zárt és $f : F \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, valamint $-1 \leq f \leq 1$. Rögzítsünk egy $c \in]0, 1/3]$ valós számot. Az folytonosság topologikus jellemzése alapján az $\overset{-1}{f}\langle[-1, -c]\rangle$ halmaz $\mathscr{T}|F$-zárt és F a T-ben $\mathscr{T}$-zárt, ezért az $\overset{-1}{f}\langle[-1, -c]\rangle$ halmaz is $\mathscr{T}$-zárt. Ugyanígy, az $\overset{-1}{f}\langle[c, 1]\rangle$ halmaz $\mathscr{T}$-zárt T-ben, és természetesen $\overset{-1}{f}\langle[-1, -c]\rangle \cap \overset{-1}{f}\langle[c, 1]\rangle = \emptyset$. A $(T, \mathscr{T})$ topologikus tér normálissága és az Uriszon-tétel alapján létezik olyan $h : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq h \leq 1$, valamint $\overset{-1}{f}\langle[-1, -c]\rangle \subseteq [h = 1]$ és $\overset{-1}{f}\langle[c, 1]\rangle \subseteq [h = 0]$. Értelmezzük a $g := -c(2h - 1)$ függvényt, amely szintén folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, valamint $[h = 1] = [g = -c]$ és $[h = 0] = [g = c]$. Ebből következik, hogy $\overset{-1}{f}\langle[-1, -c]\rangle \subseteq [g = -c]$ és $\overset{-1}{f}\langle[c, 1]\rangle \subseteq [g = c]$. Világos, hogy $0 \leq h \leq 1$ miatt $|2h - 1| \leq 1$, ezért $|g| \leq c$. Továbbá, $t \in F$ esetén

– ha $t \in \overset{-1}{f}\langle[-1, -c]\rangle$, akkor $-1 \leq f(t) \leq -c$ és $g(t) = -c$, tehát $-1 + c \leq f(t) - g(t) \leq 0 \leq 1 - c$;

– ha $t \in \overset{-1}{f}\langle[c, 1]\rangle$, akkor $c \leq f(t) \leq 1$ és $g(t) = c$, tehát $-1 + c \leq 0 \leq f(t) - g(t) \leq 1 - c$;

– ha $t \in \overset{-1}{f}\langle] - c, c[\rangle$, akkor $-c < f(t) < c$, $-c \leq g(t) \leq c$ és $c \leq 1/3$, így $-1 + c \leq -2c < f(t) - g(t) < 2c \leq 1 - c$,

ami azt jelenti, hogy $|f(t) - g(t)| \leq 1 - c$ teljesül, tehát g olyan függvény, amelynek a létezését állítottuk.

(ii)⇒(iii) Legyen az $F \subseteq T$ halmaz $\mathscr{T}$-zárt és $f : F \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Az f megfelelő kiterjesztésének létezését három lépésben fogjuk igazolni.

(I) Először feltesszük, hogy az F halmazon $|f| \leq 1$, és megmutatjuk olyan $\widetilde{f} : T \to \mathbb{R}$ függvény létezését, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $\widetilde{f}|_F = f$, valamint a T halmazon eleget tesz a $|\widetilde{f}| \leq 1$ egyenlőtlenségnek.

Legyen $c \in]0, 1/3]$ rögzített valós szám. A kiválasztási axiómával kombinált rekurzió tételének alkalmazásával bebizonyítjuk olyan $(f_n)_{n \in \mathbb{N}}$ sorozat létezését, hogy minden $\mathbb{N} \ni n$-re $f_n : T \to \mathbb{R}$ folytonos függvény a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, továbbá a T halmazon $|f_n| \leq 1 - (1 - c)^{n+1}$ és $|f_n - f_{n+1}| \leq c \cdot (1 - c)^{n+1}$, valamint az F halmazon $|f - f_n| \leq (1 - c)^{n+1}$ teljesül.

Az $f_0 : T \to \mathbb{R}$ függvénynek olyannak kell lennie, hogy folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $|f_0| \leq c$ és az F halmazon $|f - f_0| \leq 1 - c$ teljesül. A (ii) állítás éppen ilyen tulajdonságú függvény létezését mondja ki.

Legyen $n \in \mathbb{N}^*$ és $(f_k)_{0 \leq k < n}$ olyan rendszer, hogy minden $k < n$ természetes számra $f_k : T \to \mathbb{R}$ folytonos függvény a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, továbbá a T halmazon a $|f_k| \leq 1 - (1 - c)^{k+1}$ és $k + 1 < n$ esetén $|f_k - f_{k+1}| \leq c \cdot (1 - c)^{k+1}$, valamint az

F halmazon $|f - f_k| \leq (1-c)^{k+1}$ teljesül. Ekkor az $(1-c)^{-n}(f - f_{n-1})|_F : F \to \mathbb{R}$ függvényre alkalmazva a (ii) állítást kapjuk olyan $g : T \to \mathbb{R}$ függvény létezését, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, továbbá a T halmazon $|g| \leq c$ és az F halmazon $|(1-c)^{-n}(f - f_{n-1}) - g| \leq 1 - c$ teljesül. Ekkor az $f_n := f_{n-1} + (1-c)^n.g : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, továbbá a definíció szerint az F halmazon $|f - f_n| \leq (1-c)^{n+1}$ teljesül. Továbbá, a T halmazon $|f_{n-1}| \leq 1 - (1-c)^n$ és $|g| \leq c$ is igaz, ezért

$$|f_n| \leq |f_{n-1}| + (1-c)^n |g| \leq 1 - (1-c)^n + (1-c)^n c = 1 - (1-c)^{n+1}.$$

Ugyanakkor, a definíció szerint, a T halmazon $|f_n - f_{n-1}| = (1-c)^n|g| \leq c(1-c)^n$. Ez azt jelenti, hogy az $(f_k)_{0 \leq k < n+1}$ rendszer olyan, hogy minden $k < n+1$ természetes számra $f_k : T \to \mathbb{R}$ folytonos függvény a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, továbbá a T halmazon a $|f_k| \leq 1 - (1-c)^{k+1}$ és $k+1 < n+1$ esetén $|f_k - f_{k+1}| \leq c \cdot (1-c)^{k+1}$, valamint az F halmazon $|f - f_k| \leq (1-c)^{k+1}$ teljesül. Ezért van olyan függvénysorozat, amelynek a létezését állítottuk; legyen $(f_n)_{n \in \mathbb{N}}$ ilyen sorozat.

Ha $m, n \in \mathbb{N}$ olyanok, hogy $m < n$, akkor minden $t \in T$ esetén

$$|f_n(t) - f_m(t)| \leq \sum_{k=m+1}^{n} |f_k(t) - f_{k-1}(t)| \leq \sum_{k=m+1}^{n} c(1-c)^k =$$

$$= c(1-c)^{m+1} \sum_{k=0}^{n-m-1} (1-c)^k = c(1-c)^{m+1} \frac{1 - (1-c)^{n-m}}{c} \leq (1-c)^{m+1}.$$

Ebből következik, hogy minden $T \ni t$-re az $(f_n(t))_{n \in \mathbb{N}}$ sorozat Cauchy-sorozat $\mathbb{R}$-ben, így konvergens is az $\mathscr{E}_{\mathbb{R}}$ topológia szerint, tehát jól értelmezett az

$$\widetilde{f} : T \to \mathbb{R}; \quad t \mapsto \lim_{n \to \infty} f_n(t)$$

függvény. Minden $n \in \mathbb{N}$ és $t \in F$ esetén $|f(t) - f_n(t)| \leq (1-c)^{n+1}$ és $1 - c \in]0, 1[$, ezért $\widetilde{f}(t) := \lim_{n \to \infty} f_n(t) = f(t)$, vagyis $\widetilde{f}$ az f függvény kiterjesztése. Világos továbbá, hogy minden $t \in T$ esetén $|\widetilde{f}(t)| \leq 1$, mert minden $\mathbb{N} \ni n$-re $|f_n(t)| \leq 1 - (1-c)^{n+1} \leq 1$, így $|\widetilde{f}(t)| = \lim_{n \to \infty} |f_n(t)| \leq 1$.

Megmutatjuk, hogy $\widetilde{f}$ folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Ehhez legyen $t \in T$ rögzített és $\varepsilon \in \mathbb{R}_+^*$ tetszőleges. Legyen $N \in \mathbb{N}$ olyan, hogy minden $k > N$ természetes számra $(1-c)^{k+1} < \dfrac{\varepsilon}{3}$. Az előzőek alapján minden $m, n > N$ temészetes számra és $T \ni t'$-re $|f_n(t') - f_m(t')| \leq (1-c)^{\min(m,n)+1} < \dfrac{\varepsilon}{3}$. A definíció szerint minden $n > N$ természetes számra és minden $T \ni t'$-re

$$|f_n(t') - \widetilde{f}(t')| = \lim_{m \to \infty} |f_n(t') - f_m(t')| \leq \frac{\varepsilon}{3}.$$

Ugyanakkor $\widetilde{f}(t) = \lim_{n \to \infty} f_n(t)$, ezért van olyan $n \in \mathbb{N}$, hogy $n > N$ és $|\widetilde{f}(t) - f_n(t)| < \dfrac{\varepsilon}{3}$; legyen $n \in \mathbb{N}$ ilyen szám. Ekkor az f_n függvény t pontbeli folytonosságát kihasználva kapjuk olyan $V \in \mathscr{T}(t)$ környezet létezését, hogy minden $t' \in V$ esetén $|f_n(t) - f_n(t')| < \dfrac{\varepsilon}{3}$. Ha $t' \in V$, akkor

$$|\widetilde{f}(t) - \widetilde{f}(t')| \leq |\widetilde{f}(t) - f_n(t)| + |f_n(t) - f_n(t')| + |f_n(t') - \widetilde{f}(t')| < \varepsilon$$

teljesül, ami azt jelenti, hogy $\widetilde{f}$ folytonos a t pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.

(II) Most feltesszük, hogy az $f : F \to \mathbb{R}$ függvényre minden $t \in F$ esetén teljesül az $|f(t)| < 1$ szigorú egyenlőtlenség, és megmutatjuk olyan $\widetilde{f} : T \to \mathbb{R}$ függvény létezését, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $\widetilde{f}|_F = f$ és minden $t \in T$ esetén $|\widetilde{f}(t)| < 1$.

Tekintettel arra, hogy a feltevés alapján minden $F \ni t$-re $|f(t)| \leq 1$ is teljesül, az (I) alapján van olyan $\widetilde{f_0} : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $\widetilde{f_0}|_F = f$ és minden $t \in T$ esetén $|\widetilde{f_0}(t)| \leq 1$. Ekkor az F, $[\widetilde{f_0} = -1]$ és $[\widetilde{f_0} = 1]$ halmazok páronként diszjunktak és $\mathscr{T}$-zártak T-ben, ezért az

$$f_1 : F \cup [\widetilde{f_0} = -1] \cup [\widetilde{f_0} = 1] \to \mathbb{R}; \quad t \mapsto \begin{cases} f(t) & \text{, ha } t \in F \\ 1 & \text{, ha } t \in [\widetilde{f_0} = -1], \\ -1 & \text{, ha } t \in [\widetilde{f_0} = 1] \end{cases}$$

függvény jól értelmezett és folytonos a $\mathscr{T}|(F \cup [\widetilde{f_0} = -1] \cup [\widetilde{f_0} = 1])$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, hiszen a leszűkítései a F, $[\widetilde{f_0} = -1]$ és $[\widetilde{f_0} = 1]$ halmazokra folytonosak a megfelelő altértopológia és $\mathscr{E}_{\mathbb{R}}$ szerint. Nyilvánvaló, hogy minden $t \in F \cup [\widetilde{f_0} = -1] \cup [\widetilde{f_0} = 1]$ esetén $|f_1(t)| \leq 1$, ezért ismét az (I) állítást alkalmazva az f_1 függvényre kapjuk olyan $\widetilde{f_1} : T \to \mathbb{R}$ függvény létezését, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $\widetilde{f_1}\Big|_{F\cup[\widetilde{f_0}=-1]\cup[\widetilde{f_0}=1]} = f_1$ és minden $t \in T$ esetén $|\widetilde{f_1}(t)| \leq 1$. Ekkor az

$$\widetilde{f} : T \to \mathbb{R}; \quad t \mapsto \frac{\widetilde{f_0}(t) + \widetilde{f_1}(t)}{2}$$

függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $\widetilde{f}|_F = f$ és nyilvánvaló, hogy minden $t \in T$ esetén $|\widetilde{f}(t)| < 1$.

(III) Áttérve az általános esetre; legyen $f : F \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Vegyünk egy olyan $g : \mathbb{R} \to]-1,1[$ függvényt, amely *homeomorfizmus* a $\mathscr{E}_{\mathbb{R}}$ és $\mathscr{E}_{\mathbb{R}}|]-1,1[$ topológiák szerint. Ilyen például a

$$g : \mathbb{R} \to]-1,1[; \quad x \mapsto \frac{x}{1+|x|}$$

függvény, de a továbbiakban a g konkrét alakja lényegtelen. Természetesen a $g \circ f : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, és minden $t \in F$ esetén $|(g \circ f)(t)| < 1$. A (II) alapján van olyan $h : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $h|_F = g \circ f$ és minden $t \in T$ esetén $|h(t)| < 1$. Ekkor h folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|]-1,1[$ topológiák szerint is, tehát az $\widetilde{f} := g^{-1} \circ h : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, és $\widetilde{f}|_F = g^{-1} \circ (h|_F) = g^{-1} \circ (g \circ f) = f$.

(iii)⇒(i) Legyenek $F, F' \subseteq T$ diszjunkt $\mathscr{T}$-zárt halmazok, és értelmezzük az

$$f : F \cup F' \to \mathbb{R}; \quad t \mapsto \begin{cases} 1 & \text{, ha } t \in F, \\ 0 & \text{, ha } t \in F' \end{cases}$$

függvényt. Az F halmaz $\mathscr{T}|(F \cup F')$-nyílt, mert $F = (F \cup F') \cap (T \setminus F')$ és a $T \setminus F'$ halmaz $\mathscr{T}$-nyílt. Az F és F' szerepét felcserélve kapjuk, hogy az F' halmaz $\mathscr{T}|(F \cup F')$-nyílt. Ezért a folytonosság lokalitását alkalmazva nyilvánvaló, hogy f folytonos a $\mathscr{T}|(F \cup F')$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, és az $F \cup F'$ halmaz $\mathscr{T}$-zárt, így a (iii) alapján van olyan $\widetilde{f} : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, valamint $\widetilde{f}|_{F \cup F'} = f$. Ekkor bármely $r \in]0,1[$ valós számra $F \subseteq [\widetilde{f} > r]$ és $F' \subseteq [\widetilde{f} < r]$, továbbá $[\widetilde{f} < r]$ és $[\widetilde{f} > r]$ diszjunkt $\mathscr{T}$-nyílt halmazok. Ezért a $(T, \mathscr{T})$ topologikus tér normális. ■

Megjegyezzük, hogy ha $(T, \mathscr{T})$ normális tér, az $F \subseteq T$ halmaz $\mathscr{T}$-zárt, $\alpha, \beta \in \mathbb{R}$, $\alpha \leq \beta$ és $f : F \to \mathbb{R}$ olyan függvény, amely folytonos a $\mathscr{T}|F$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint és $\alpha \leq f \leq \beta$, akkor létezik olyan $\widetilde{f} : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint és $f = \widetilde{f}|_F$, valamint $\alpha \leq \widetilde{f} \leq \beta$. Valóban, a Tietze-tétel alapján van olyan $g : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint és $g|_F = f$; ekkor az $\widetilde{f} := \sup(\alpha, \inf(g, \beta)) : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $f = \widetilde{f}|_F$, valamint $\alpha \leq \widetilde{f} \leq \beta$.

27.6.2. Következmény. *Ha $(T, \mathscr{T})$ normális tér, $F \subseteq T$ $\mathscr{T}$-zárt halmaz, E véges dimenziós normált tér és $f : F \to E$ olyan függvény, amely folytonos a $\mathscr{T}|F$ altértopológia és az E euklidészi topológiája szerint, akkor létezik olyan $\widetilde{f} : T \to E$ függvény, amely folytonos a $\mathscr{T}$ topológia és az E euklidészi topológiája szerint, és $f = \widetilde{f}|_F$.*

Bizonyítás. Ha E komplex normált tér, akkor áttérve az E alatt fekvő valós normált térre, feltehető, hogy E valós véges dimenziós normált tér. Legyen $n \in \mathbb{N}$ olyan, hogy létezik $u : E \to \mathbb{R}^n$ lineáris bijekció, továbbá minden $k < n$ természetes számra legyen pr_k az $\mathbb{R}^n \to \mathbb{R}$ kanonikus k-adik projekció. Minden $k < n$ természetes számra a $\mathrm{pr}_k \circ u \circ f : F \to \mathbb{R}$ függvény folytonos a $\mathscr{T}|F$ altértopológia és $\mathscr{E}_{\mathbb{R}}$ szerint, így a Tietze-tétel alapján vehetünk olyan $f_k : T \to \mathbb{R}$ függvényt, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, és $\mathrm{pr}_k \circ u \circ f = f_k|_F$. Ekkor a

$$\widetilde{f} : T \to E; \quad t \mapsto u^{-1}\left((f_k(t))_{0 \leq k < n}\right)$$

függvény folytonos kiterjesztése f-nek T-re. ■

27.7. Normális terek jellemzése III – Egységfelosztás-tétel

27.7.1. Definíció. *Legyen $(T, \mathscr{T})$ topologikus tér, F vektortér és $f : T \to F$ függvény. Ekkor a $\overline{\{t \in T | f(t) \neq 0\}}$ halmazt az f függvény* **tartójának** *nevezzük a $\mathscr{T}$ topológia szerint, és a $\mathrm{supp}(f)$ szimbólummal jelöljük.*

Nyilvánvaló, hogy ha $(T, \mathscr{T})$ topologikus tér, F vektortér a K test felett, és $f, g : T \to F$ függvények, valamint $\lambda \in K$, akkor

$$\mathrm{supp}(f + g) \subseteq \mathrm{supp}(f) \cup \mathrm{supp}(g), \quad \mathrm{supp}(\lambda.f) \subseteq \mathrm{supp}(f).$$

Továbbá, ha $(T, \mathscr{T})$ topologikus tér, K test és $f, g : T \to K$ függvények, akkor

$$\mathrm{supp}(f \cdot g) \subseteq \mathrm{supp}(f) \cap \mathrm{supp}(g).$$

Ha $(T, \mathscr{T})$ normális tér, az $F \subseteq T$ halmaz $\mathscr{T}$-zárt, az $\Omega \subseteq T$ halmaz $\mathscr{T}$-nyílt és $F \subseteq \Omega$, akkor az Uriszon-tétel szerint van olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, valamint $F \subseteq [f = 1]$ és $\mathrm{supp}(f) \subseteq \Omega$.

27.7.2. Definíció. *Ha $(T, \mathscr{T})$ topologikus tér és $(T_i)_{i \in I}$ a T halmaz befedése, akkor $(T_i)_{i \in I}$-nek alárendelt* **folytonos egységfelosztásnak** *nevezünk minden olyan $(f_i)_{i \in I}$ függvényrendszert, amelyre teljesül azt, hogy minden $I \ni i$-re $f_i : T \to \mathbb{R}$ folytonos* *függvény a* $\mathscr{T}$ *és* $\mathscr{E}_{\mathbb{R}}$ *topológiák szerint,* $0 \leq f_i \leq 1$, $\mathrm{supp}(f_i) \subseteq T_i$, *és a* $(\mathrm{supp}(f_i))_{i\in I}$ *halmazrendszer lokálisan véges a* $\mathscr{T}$ *topológia szerint, valamint minden* $t \in T$ *esetén* $\sum_{i\in I} f_i(t) = 1$ (*azzal a konvencióval, hogy az üres indexhalmazra vett összeg egyenlő* 0-*val*).

Megjegyezzük, hogy az előző definícióban szereplő $\sum_{i\in I} f_i(t)$ kifejezés *értelmes*, mert a feltevés alapján a $(\mathrm{supp}(f_i))_{i\in I}$ halmazrendszer lokálisan véges a $\mathscr{T}$ topológia szerint, így pontonként is véges, ezért minden $T \ni t$-re az $\{i \in I | f_i(t) \neq 0\}$ halmaz *véges*.

27.7.3. Tétel. (Egységfelosztás-tétel normális terekre) *Ha* $(T, \mathscr{T})$ *topologikus tér, akkor a következő kijelentések ekvivalensek.*

(i) $(T, \mathscr{T})$ *normális tér.*

(ii) *A* $(T, \mathscr{T})$ *topologikus tér bármely* $(\Omega_i)_{i\in I}$ *pontonként véges* $\mathscr{T}$*-nyílt befedéséhez létezik a* T*-nek olyan* $(U_i)_{i\in I}$ $\mathscr{T}$*-nyílt befedése* (*ugyanazzal az* I *indexhalmazzal*), *amelyre minden* $i \in I$ *esetén* $\overline{U_i} \subseteq \Omega_i$.

(iii) *A* $(T, \mathscr{T})$ *topologikus tér bármely lokálisan véges* $\mathscr{T}$*-nyílt befedéséhez létezik annak alárendelt folytonos egységfelosztás.*

Bizonyítás. Először azt fogjuk megmutatni, hogy az (i) és (ii) állítások *ekvivalensek* egymással.

(i)⇒(ii) Tegyük fel, hogy $(T, \mathscr{T})$ normális tér és legyen $(\Omega_i)_{i\in I}$ a T-nek pontonként véges $\mathscr{T}$-nyílt befedése. Jelölje $\mathfrak{S}$ a T azon $(U_i)_{i\in I}$ $\mathscr{T}$-nyílt befedéseinek halmazát, amelyekre minden $i \in I$ esetén $\overline{U_i} \subseteq \Omega_i$ vagy $U_i = \Omega_i$. (Megjegyezzük, hogy ha $(U_i)_{i\in I} \in \mathfrak{S}$, akkor létezhet olyan $i \in I$, hogy $\overline{U_i} \subseteq \Omega_i$ és $U_i = \Omega_i$ *egyszerre* teljesül; ekkor Ω_i egyszerre $\mathscr{T}$-nyílt és $\mathscr{T}$-zárt halmaz.) Nyilánvaló, hogy $(\Omega_i)_{i\in I} \in \mathfrak{S}$, tehát $\mathfrak{S} \neq \emptyset$. Az $\mathfrak{S}$ halmazon bevezetjük azt a $\leq$ relációt, amelyre $(U_i)_{i\in I}, (V_i)_{i\in I} \in \mathfrak{S}$ esetén $(U_i)_{i\in I} \leq (V_i)_{i\in I}$ pontosan akkor teljesül, ha minden $I \ni i$-re: ha $\overline{U_i} \subseteq \Omega_i$, akkor $U_i = V_i$. Esetszétválasztásokkal könnyen ellenőrizhető, hogy a $\leq$ reláció rendezés a $\mathfrak{S}$ halmaz felett.

Megmutatjuk, hogy $(\mathfrak{S}, \leq)$ *induktívan* rendezett halmaz. Legyen $((U_{j,i})_{i\in I})_{j\in J}$ olyan nem üres rendszer, amelyre minden $j \in J$ esetén $(U_{j,i})_{i\in I} \in \mathfrak{S}$, és minden $J \ni j_1, j_2$-re $(U_{j_1,i})_{i\in I} \leq (U_{j_2,i})_{i\in I}$ vagy $(U_{j_2,i})_{i\in I} \leq (U_{j_1,i})_{i\in I}$. Minden $I \ni i$-re legyen $U_i := \bigcap_{j\in J} U_{j,i}$.
Állítjuk, hogy $(U_i)_{i\in I} \in \mathfrak{S}$, és minden $J \ni j$-re $(U_{j,i})_{i\in I} \leq (U_i)_{i\in I}$, vagyis $(U_i)_{i\in I}$ felső korlátja az $((U_{j,i})_{i\in I})_{j\in J}$ rendszernek az $(\mathfrak{S}, \leq)$ rendezett halmazban. Legyen $i \in I$ rögzített és $J_i := \{j \in J | \overline{U_{j,i}} \subseteq \Omega_i\}$. Ha $J_i = \emptyset$, akkor minden $j \in J$ esetén $U_{j,i} = \Omega_i$ (a $\mathfrak{S}$ halmaz definíciója és $(U_{j,i})_{i\in I} \in \mathfrak{S}$ miatt), ezért $U_i = \Omega_i = U_{j,i}$. Ha $j_1, j_2 \in J_i$, akkor $\overline{U_{j_1,i}} \subseteq \Omega_i$ és $\overline{U_{j_2,i}} \subseteq \Omega_i$, ugyanakkor $(U_{j_1,i})_{i\in I} \leq (U_{j_2,i})_{i\in I}$ vagy $(U_{j_2,i})_{i\in I} \leq (U_{j_1,i})_{i\in I}$ teljesül, így szükségképpen $U_{j_1,i} = U_{j_2,i}$ (a $\leq$ rendezés értelmezése alapján). Ez azt jelenti, hogy ha $J_i \neq \emptyset$, akkor bármely $j \in J_i$ esetén $U_i = U_{j,i}$. Tehát minden $I \ni i$-re $U_i \in \mathscr{T}$, és ha $J_i = \emptyset$, akkor $U_i = \Omega_i$, míg $J_i \neq \emptyset$ esetén bármely $J_i \ni j$-re $U_i = U_{j,i}$, így $\overline{U_i} = \overline{U_{j,i}} \subseteq \Omega_i$. Ezért $(U_i)_{i\in I} \in \mathfrak{S}$ pontosan akkor teljesül, ha $(U_i)_{i\in I}$ befedése T-nek, azaz $T = \bigcup_{i\in I} U_i$. Ennek igazolásához először megjegyezzük, hogy az előzőek szerint minden $I \ni i$-hez létezik olyan $j \in J$, hogy $U_i = U_{j,i}$, hiszen $J_i = \emptyset$ esetén ez minden $j \in J$ indexre igaz, és ha $J_i \neq \emptyset$, akkor minden $j \in J_i$ indexre teljesül. Ezért a kiválasztási axióma alkalmazásával vehetünk olyan $\tau : I \to J$ függvényt, hogy minden $I \ni i$-re $U_i = U_{\tau(i),i}$. Legyen $t \in T$ rögzített pont. Az $(\Omega_i)_{i\in I}$ rendszer pontonként

véges befedése T-nek, ezért az $I_t := \{i \in I | t \in \Omega_i\}$ halmaz véges és nem üres. A $\tau\langle I_t\rangle \subseteq J$ halmaz szintén véges és nem üres, ezért az $\{(U_{j,i})_{i\in I} | j \in \tau\langle I_t\rangle\}$ halmaz $\leq$ szerinti *lineáris rendezettsége* folytán van olyan $j_0 \in \tau\langle I_t\rangle$, hogy minden $\tau\langle I_t\rangle \ni j$-re $(U_{j,i})_{i\in I} \leq (U_{j_0,i})_{i\in I}$ (8.2.3.). Az $(U_{j_0,i})_{i\in I}$ rendszer befedése T-nek, ezért van olyan $i_0 \in I$, hogy $t \in U_{j_0,i_0}$. De $U_{j_0,i_0} \subseteq \Omega_{i_0}$, ezért $t \in \Omega_{i_0}$, vagyis $i_0 \in I_t$. Tehát $\tau(i_0) \in \tau\langle I_t\rangle$, így a j_0 értelmezése alapján $(U_{\tau(i_0),i})_{i\in I} \leq (U_{j_0,i})_{i\in I}$. Ebből következik, hogy ha $\overline{U_{\tau(i_0),i_0}} \subseteq \Omega_{i_0}$, akkor $t \in U_{j_0,i_0} = U_{\tau(i_0),i_0} = U_{i_0}$, ugyanakkor $U_{\tau(i_0),i_0} = \Omega_{i_0}$ esetén $t \in \Omega_{i_0} = U_{\tau(i_0),i_0} = U_{i_0}$. Ez azt jelenti, hogy $t \in U_{i_0}$, tehát $(U_i)_{i\in I}$ befedése T-nek. Ezzel megmutattuk, hogy $(U_i)_{i\in I} \in \mathfrak{S}$; azt kell még igazolni, hogy minden $J \ni j$-re $(U_{j,i})_{i\in I} \leq (U_i)_{i\in I}$. Ez azonban nyilvánvaló, mert ha $j \in J$ és $i \in I$ olyanok, hogy $\overline{U_{j,i}} \subseteq \Omega_i$, akkor $j \in J_i$, így $U_{j,i} = U_i$.

A Zorn-lemma alapján vehetünk olyan $(U_i)_{i\in I} \in \mathfrak{S}$ elemet, amely maximális a $\leq$ rendezés szerint. Megmutatjuk, hogy minden $i \in I$ esetén $\overline{U_i} \subseteq \Omega_i$, tehát az $(U_i)_{i\in I}$ rendszer olyan $\mathscr{T}$-nyílt befedése T-nek, amelynek létezését a (ii)-ben állítottuk. Indirekt bizonyítunk, tehát feltesszük, hogy $i_0 \in I$ olyan, amelyre nem igaz az $\overline{U_{i_0}} \subseteq \Omega_{i_0}$ tartalmazás: ekkor $(U_i)_{i\in I} \in \mathfrak{S}$ és $\mathfrak{S}$ definíciója szerint $U_{i_0} = \Omega_{i_0}$, és $\overline{U_{i_0}} \neq U_{i_0}$, különben $\overline{U_{i_0}} = U_{i_0} = \Omega_{i_0}$ teljesülne, holott $\overline{U_{i_0}} \nsubseteq \Omega_{i_0}$. A $T \setminus \bigcup_{\substack{i\in I\\ i\neq i_0}} U_i$ halmaz $\mathscr{T}$-zárt és $T \setminus \bigcup_{\substack{i\in I\\ i\neq i_0}} U_i \subseteq U_{i_0}$, mert $(U_i)_{i\in I}$ befedése T-nek. A $(T, \mathscr{T})$ topologikus tér normális, ezért van olyan $U \in \mathscr{T}$, hogy $T \setminus \bigcup_{\substack{i\in I\\ i\neq i_0}} U_i \subseteq U \subseteq \overline{U} \subseteq U_{i_0} = \Omega_{i_0}$. Értelmezzük a $(V_i)_{i\in I}$ rendszert úgy, hogy minden $i \in I \setminus \{i_0\}$ esetén $V_i := U_i$, továbbá $V_{i_0} := U$. Világos, hogy $(V_i)_{i\in I} \in \mathfrak{S}$ és $(U_i)_{i\in I} \leq (V_i)_{i\in I}$, valamint $(U_i)_{i\in I} \neq (V_i)_{i\in I}$, különben $U_{i_0} = V_{i_0} = U$, így $\overline{U_{i_0}} = U_{i_0}$ teljesülne, holott $\overline{U_{i_0}} \neq U_{i_0}$. Ez azt jelenti, hogy $(V_i)_{i\in I} \in \mathfrak{S}$ olyan elem, amely nagyobb $(U_i)_{i\in I}$-nél a $\leq$ rendezés szerint; ez viszont ellentmond az $(U_i)_{i\in I}$ maximalitásának.

(ii)⇒(i) Legyenek F és F' diszjunkt $\mathscr{T}$-zárt halmazok T-ben. Legyen $I := \{0, 1\}$, $\Omega_0 := T \setminus F'$ és $\Omega_1 := T \setminus F$. Ekkor $(\Omega_i)_{i\in I}$ véges, tehát pontonként véges $\mathscr{T}$-nyílt befedése a T halmaznak. A (ii) alapján vehetjük a T-nek olyan $(U_i)_{i\in I}$ $\mathscr{T}$-nyílt befedését, amelyre minden $i \in I$ esetén $\overline{U_i} \subseteq \Omega_i$. Ekkor $\Omega := T \setminus \overline{U_1}$ és $\Omega' := T \setminus \overline{U_0}$ olyan $\mathscr{T}$-nyílt halmazok, amelyekre $F = T \setminus \Omega_1 \subseteq T \setminus \overline{U_1} =: \Omega$ és $F' = T \setminus \Omega_0 \subseteq T \setminus \overline{U_0} =: \Omega'$, valamint $\Omega \cap \Omega' = \emptyset$. Ez azt jelenti, hogy a $(T, \mathscr{T})$ topologikus tér normális.

(ii)⇒(iii) Legyen $(\Omega_i)_{i\in I}$ a $\mathscr{T}$ topológia szerint lokálisan véges és nyílt befedése a T halmaznak. Ekkor $(\Omega_i)_{i\in I}$ pontonként is véges, tehát a (ii) alapján vehetjük a a T-nek olyan $(U_i)_{i\in I}$ $\mathscr{T}$-nyílt befedését, amelyre minden $i \in I$ esetén $\overline{U_i} \subseteq \Omega_i$. (Megjegyezzük, hogy itt még csak az $(\Omega_i)_{i\in I}$ pontonkénti végességét használjuk ki, de később szükség lesz a $\mathscr{T}$ topológia szerinti lokális végességére is.) Minden $I \ni i$-re $U_i \subseteq \Omega_i$, ezért az $(\Omega_i)_{i\in I}$ rendszer pontonkénti végessége folytán az $(U_i)_{i\in I}$ rendszer is pontonként véges. Ezért ismét a (ii) állítást alkalmazva az $(U_i)_{i\in I}$ rendszerre kapjuk a T olyan $(V_i)_{i\in I}$ $\mathscr{T}$-nyílt befedését, amelyre minden $i \in I$ esetén $\overline{V_i} \subseteq U_i$. Láttuk, hogy (ii)⇒(i) teljesül, tehát a $(T, \mathscr{T})$ topologikus tér normális, így az Uriszon-tétel alapján minden $I \ni i$-hez van olyan $g : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq g \leq 1$, és $\overline{V_i} \subseteq [g = 1] \subseteq [g \neq 0] \subseteq U_i$; ekkor $\mathrm{supp}(g) := \overline{[g \neq 0]} \subseteq \overline{U_i} \subseteq \Omega_i$ is igaz. Tehát a kiválasztási axióma alkalmazásával vehetünk olyan $(g_i)_{i\in I}$ rendszert, hogy minden $I \ni i$-re $g_i : T \to \mathbb{R}$ folytonos függvény a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq g_i \leq 1$, valamint $\overline{V_i} \subseteq [g_i = 1]$ és $\mathrm{supp}(g_i) \subseteq \overline{U_i} \subseteq \Omega_i$. Világos, hogy minden $I \ni i$-re $V_i \subseteq U_i \subseteq \Omega_i$, ezért az $(\Omega_i)_{i\in I}$ rendszer $\mathscr{T}$ topológia szerinti lokális végessége miatt az $(U_i)_{i\in I}$ és $(V_i)_{i\in I}$ rendszerek szintén lokálisan végesek $\mathscr{T}$ szerint. A $(V_i)_{i\in I}$ rendszer $\mathscr{T}$ szerint lokálisan véges befedése T-nek, ezért minden $T \ni t$-hez van olyan $i \in I$, hogy $g_i(t) = 1$, így a $\{i \in I | g_i(t) \neq 0\}$ halmaz nem üres és véges. Legyen minden $I \ni i$-re

$$f_i : T \to \mathbb{R}; \quad t \mapsto \frac{g_i(t)}{\sum\limits_{\substack{j \in I \\ g_j(t) \neq 0}} g_j(t)}.$$

Nyilvánvaló, hogy $i \in I$ esetén $\mathrm{supp}(f_i) \subseteq \mathrm{supp}(g_i) \subseteq \overline{U_i} \subseteq \Omega_i$, és minden $T \ni t$-re $0 \leq f_i(t) \leq 1$, valamint $\sum\limits_{\substack{i \in I \\ f_i(t) \neq 0}} f_i(t) = 1$. Tehát, ha minden $I \ni i$-re az f_i függvény folytonos volna a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, akkor az $(f_i)_{i \in I}$ rendszer az $(\Omega_i)_{i \in I}$ befedésnek alárendelt folytonos egységfelosztás volna. A definícióból látható, hogy ha a

$$G : T \to \mathbb{R}; \quad t \mapsto \sum_{\substack{i \in I \\ g_i(t) \neq 0}} g_i(t)$$

függvény folytonos volna a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, akkor minden $I \ni i$-re f_i is folytonos lenne ugyanezen topológiák szerint.

A G függvény folytonosságának bizonyításához legyen $t \in T$ rögzített. Az $(\Omega_i)_{i \in I}$ rendszer $\mathscr{T}$ szerinti lokális végessége miatt van olyan $V \in \mathscr{T}(t)$ környezete, hogy $I_V := \{i \in I | V \cap \Omega_i \neq \emptyset\}$ véges halmaz. Ha $t' \in V$, akkor $\{i \in I | g_i(t') \neq 0\} \subseteq I_V$, tehát $G(t') = \sum\limits_{i \in I_V} g_i(t')$. Másként fogalmazva: G egyenlő a $\sum\limits_{i \in I_V} g_i$ összegfüggvénnyel a V környezeten. Tehát a folytonosság lokalitása miatt G folytonos a t pontban a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.

(iii)⇒(i) Tegyük fel, hogy a $(T, \mathscr{T})$ topologikus tér olyan, hogy a T bármely $\mathscr{T}$ szerint lokálisan véges és nyílt befedéséhez létezik annak alárendelt folytonos egységfelosztás. Legyenek F és F' diszjunkt $\mathscr{T}$-zárt halmazok T-ben. Legyen $I := \{0, 1\}$ és $\Omega_0 := T \setminus F'$, valamint $\Omega_1 := T \setminus F$. Ekkor $(\Omega_i)_{i \in I}$ véges, tehát a $\mathscr{T}$ szerint lokálisan véges $\mathscr{T}$-nyílt befedése T-nek. Legyen $(f_i)_{i \in I}$ egy $(\Omega_i)_{i \in I}$-nek alárendelt folytonos egységfelosztás. Ekkor $[f_0 \neq 0] \subseteq T \setminus F'$, tehát $F' \subseteq [f_0 = 0]$, továbbá $[f_1 \neq 0] \subseteq T \setminus F$, tehát $F \subseteq [f_1 = 0]$. Minden $t \in T$ esetén $f_0(t) + f_1(t) = 1$, így bármely $r \in]0, 1[$ valós számra az $\Omega := [f_0 > r]$ és $\Omega' := [f_0 < r]$ halmazok $\mathscr{T}$-nyíltak, diszjunktak, valamint $F \subseteq \Omega$ és $F' \subseteq \Omega'$, tehát a $(T, \mathscr{T})$ topologikus tér normális. ■

27.8. Félmetrizálható terek és teljesen reguláris terek jellemzése

27.8.1. Definíció. *A T halmaz feletti* **félmetrikának** (*vagy* **eltérésnek**) *nevezünk minden olyan $d : T \times T \to \mathbb{R}_+$ függvényt, amelyre teljesülnek a következők.*

($\mathrm{SM_I}$) *Minden $t \in T$ esetén $d(t, t) = 0$.*

($\mathrm{SM_{II}}$) *Minden $t, t' \in T$ esetén $d(t, t') = d(t', t)$* **(szimmetrikusság)**.

($\mathrm{SM_{III}}$) *Minden $t, t', t'' \in T$ esetén $d(t, t'') \leq d(t, t') + d(t', t'')$* **(háromszög-egyenlőtlenség)**.

A (T, d) párt **félmetrikus térnek** *nevezzük, ha d félmetrika a T halmaz felett. Ha (T, d)*

félmetrikus tér, akkor minden $\mathbb{R}_+^* \ni r$*-re és* $T \ni t$*-re*

$$\begin{aligned}\mathrm{B}_r(t;d) &:= \{t' \in T | d(t,t') < r\},\\ \overline{\mathrm{B}}_r(t;d) &:= \{t' \in T | d(t,t') \leq r\},\\ \mathrm{S}_r(t;d) &:= \{t' \in T | d(t,t') = r\}.\end{aligned}$$

Példák (félmetrikus terekre). 1) Ha T halmaz, akkor minden T feletti metrika félmetrika, továbbá a $T \times T \to \mathbb{R}_+$ azonosan 0 függvény olyan félmetrika T felett, amely nem metrika, ha T legalább két elemű. Minden metrikus tér félmetrikus tér.

2) Legyen T halmaz és $f : T \to \mathbb{R}$ tetszőleges függvény. Ekkor a

$$d_f : T \times T \to \mathbb{R}_+; \quad (t,t') \mapsto |f(t) - f(t')|$$

leképezés félmetrika T felett; ezt nevezzük az f *függvény által generált félmetrikának.*

3) A 2. példa általánosításaként legyen T halmaz, F normált tér és $f : T \to F$ tetszőleges függvény. Ekkor a

$$d_f : T \times T \to \mathbb{R}_+; \quad (t,t') \mapsto \|f(t) - f(t')\|$$

leképezés szintén félmetrika T felett.

4) Legyen p félnorma az E valós vagy komplex vektortér felett. Ekkor az

$$E \times E \to \mathbb{R}_+; \quad (x,x') \mapsto p(x - x')$$

leképezés félmetrika E felett. Ez a félmetrika pontosan akkor metrika, ha a p félnorma norma.

27.8.2. Állítás. *Ha* d *félmetrika a* T *halmaz felett, akkor egyértelműen létezik olyan* $\mathscr{T}$ *topológia* T *felett, amely szerint minden* $t \in T$ *esetén a* $\{\mathrm{B}_r(t;d) | r \in \mathbb{R}_+^*\}$ *halmaz környezetbázisa a* t *pontnak.*

Bizonyítás. Ha létezik ilyen $\mathscr{T}$ topológia, akkor szükségképpen

$$\mathscr{T} = \{\ \Omega \subseteq T \mid (\forall\ t \in \Omega)(\exists\ r \in \mathbb{R}_+^*) :\ \mathrm{B}_r(t;d) \subseteq \Omega\ \},$$

ezért a keresett topológia egyértelműsége nyilvánvaló, ugyanakkor a létezése azon múlik, hogy az imént felírt $\mathscr{T}$ halmaz topológia-e T felett, és ha igen, akkor igaz-e, hogy minden $t \in T$ és $r \in \mathbb{R}_+^*$ esetén a $\mathrm{B}_r(t;d)$ gömb környezete a t pontnak a $\mathscr{T}$ topológia szerint. Az előbbi könnyen ellenőrizhető, míg az utóbbi azon múlik, hogy $t \in T$ és $r \in \mathbb{R}_+^*$ esetén $\mathrm{B}_r(t;d) \in \mathscr{T}$, ami azért igaz, mert ha $t' \in \mathrm{B}_r(t;d)$ és $r' \in \mathbb{R}_+^*$ olyan, hogy $r' < r - d(t,t')$, akkor a háromszög-egyenlőtlenség alapján $\mathrm{B}_{r'}(t';d) \subseteq \mathrm{B}_r(t;d)$. ■

27.8.3. Definíció. *Ha* d *félmetrika a* T *halmaz felett, akkor* $\mathscr{T}_d$ *jelöli azt a* T *feletti topológiát, amely szerint minden* $t \in T$ *esetén a* $\{\mathrm{B}_r(t;d) | r \in \mathbb{R}_+^*\}$ *halmaz környezetbázisa a* t *pontnak; ezt a topológiát a* d **félmetrika által generált topológiának** *nevezzük. Azt mondjuk, hogy a* T *halmaz feletti* $\mathscr{T}$ *topológia* **félmetrizálható**, *ha létezik olyan* T *feletti* d *félmetrika, amelyre* $\mathscr{T}_d = \mathscr{T}$.

Megjegyezzük, hogy ha T halmaz és $d : T \times T \to \mathbb{R}_+$ az azonosan 0 függvény, akkor $\mathscr{T}_d$ egyenlő a T feletti antidiszkrét topológiával.

27.8.4. Definíció. *Ha (M,d) félmetrikus tér, akkor egy M-ben haladó $(x_n)_{n\in\mathbb{N}}$ sorozatot* **Cauchy-sorozatnak** *nevezünk a d félmetrika szerint, ha minden $\varepsilon \in \mathbb{R}_+^*$ esetén van olyan $N \in \mathbb{N}$, hogy minden $m,n > N$ természetes számra $d(x_m,x_n) < \varepsilon$. Azt mondjuk, hogy az (M,d) félmetrikus tér* **teljes**, *ha minden M-ben haladó, d szerinti Cauchy-sorozat konvergens a $\mathscr{T}_d$ topológia szerint. Azt mondjuk, hogy a $(T,\mathscr{T})$ topologikus tér* **teljesen félmetrizálható**, *ha létezik olyan T feletti d félmetrika, amelyre $\mathscr{T} = \mathscr{T}_d$ és (M,d) teljes félmetrikus tér.*

Megjegyezzük, hogy ha (M,d) félmetrikus tér, akkor minden M-ben haladó, $\mathscr{T}_d$ szerint konvergens sorozat Cauchy-sorozat a d félmetrika szerint; ez ugyanúgy igazolható, mint metrikus terek esetében.

27.8.5. Definíció. *Ha $(d_i)_{i\in I}$ a T halmaz feletti félmetrikák tetszőleges rendszere, akkor a $\sup_{i\in I} \mathscr{T}_{d_i}$ topológiát a $(d_i)_{i\in I}$* **félmetrika-rendszer által generált topológiának** *nevezzük és a $\mathscr{T}_{(d_i)_{i\in I}}$ szimbólummal jelöljük. Ha $(f_i)_{i\in I}$ a T halmazon értelmezett valós értékű függvények tetszőleges rendszere, akkor a $(d_{f_i})_{i\in I}$ félmetrika-rendszer által generált T feletti topológiát az $(f_i)_{i\in I}$* **függvényrendszer által generált topológiának** *nevezzük és a $\mathscr{T}_{(f_i)_{i\in I}}$ szimbólummal jelöljük.*

Legyen $(d_i)_{i\in I}$ a T halmaz feletti félmetrikák nem üres rendszere. A topológia-szuprémumra vonatkozó korábbi ismereteink és a $\mathscr{T}_{(d_i)_{i\in I}}$ topológia értelmezése alapján a

$$\mathfrak{B} := \left\{ \bigcap_{i\in I} \Omega_i \;\middle|\; (\Omega_i)_{i\in I} \in \prod_{i\in I}^{*} \mathscr{T}_{d_i} \right\}$$

halmaz bázisa a $\mathscr{T}_{(d_i)_{i\in I}}$ topológiának, ahol

$$\prod_{i\in I}^{*} \mathscr{T}_{d_i} := \left\{ (\Omega_i)_{i\in I} \in \prod_{i\in I} \mathscr{T}_{d_i} \;\middle|\; \{i\in I|\Omega_i \neq T\} \text{ véges halmaz} \right\}.$$

Ha $(\Omega_i)_{i\in I} \in \prod_{i\in I}^{*} \mathscr{T}_{d_i}$ és $J := \{i\in I|\Omega_i \neq T\}$, akkor $J \neq \emptyset$ esetén $\bigcap_{i\in I}\Omega_i = \bigcap_{i\in J}\Omega_i$, míg $J=\emptyset$ esetén $\bigcap_{i\in I}\Omega_i = T$. Ha $J\neq\emptyset$, akkor $t \in \bigcap_{i\in I}\Omega_i$ esetén van olyan $(r_i)_{i\in I}$ rendszer $\mathbb{R}_+^*$-ban, amelyre minden $i \in J$ esetén $\mathrm{B}_{r_i}(t;d_i) \subseteq \Omega_i$, tehát $\bigcap_{i\in J}\mathrm{B}_{r_i}(t;d_i) \subseteq \bigcap_{i\in J}\Omega_i = \bigcap_{i\in I}\Omega_i$. Ebből következik, hogy egy $\Omega \subseteq T$ halmaz pontosan akkor nyílt a $(d_i)_{i\in I}$ félmetrika-rendszer által generált topológia szerint, ha minden $t\in\Omega$ ponthoz létezik olyan $J\subseteq I$ nem üres véges halmaz, és olyan $(r_i)_{i\in J}$ rendszer $\mathbb{R}_+^*$-ban, hogy $\bigcap_{i\in J}\mathrm{B}_{r_i}(t;d_i) \subseteq \Omega$ (vagy ami ugyanaz: minden $t\in\Omega$ ponthoz létezik olyan $J\subseteq I$ nem üres véges halmaz, és olyan $r\in\mathbb{R}_+^*$, hogy $\bigcap_{i\in J}\mathrm{B}_r(t;d_i)\subseteq\Omega$). Továbbá, a $\mathscr{T}_{(d_i)_{i\in I}} := \sup_{i\in I}\mathscr{T}_{d_i}$ topológia megegyezik a $((T,\mathscr{T}_{d_i}),\mathrm{id}_T)_{i\in I}$ rendszer által projektíven előállított T feletti topológiával, ezért minden $(T',\mathscr{T}')$ topologikus térre, és minden $f : T' \to T$ függvényre, az f pontosan akkor folytonos a $\mathscr{T}'$ és $\mathscr{T}_{(d_i)_{i\in I}}$ topológiák szerint, ha minden $I \ni i$-re az f függvény folytonos a $\mathscr{T}'$ és $\mathscr{T}_{d_i}$ topológiák szerint.

Az előzőek alapján könnyen látható, hogy ha $(d_i)_{i\in I}$ a T halmaz feletti félmetrikák nem üres rendszere, akkor a $\mathscr{T}_{(d_i)_{i\in I}}$ topológia pontosan akkor Hausdorff-topológia, ha minden $t,t'\in T$ ponthoz, $t\neq t'$ esetén létezik olyan $i\in I$, hogy $d_i(t,t') > 0$.

27.8.6. Állítás. *Ha T halmaz és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $f_i : T \to \mathbb{R}$ függvény, akkor a $\mathscr{T}_{(f_i)_{i\in I}}$ topológia egyenlő az $((\mathbb{R}, \mathscr{E}_{\mathbb{R}}), f_i)_{i\in I}$ rendszer által projektíven előállított T feletti topológiával, vagyis $\mathscr{T}_{(f_i)_{i\in I}}$ az a legkisebb T feletti topológia, amelyre minden $i \in I$ esetén az $f_i : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}_{(f_i)_{i\in I}}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.*

Bizonyítás. Ha $I = \emptyset$, akkor a definíció alapján $\mathscr{T}_{(f_i)_{i\in I}}$ megegyezik az T feletti antidiszkrét topológiával; ugyanakkor minden $I \ni i$-re az f_i függvény folytonos a T feletti antidiszkrét topológia és $\mathscr{E}_{\mathbb{R}}$ szerint, tehát az $((\mathbb{R}, \mathscr{E}_{\mathbb{R}}), f_i)_{i\in I}$ rendszer által projektíven előállított T feletti topológia egyenlő a T feletti antidiszkrét topológiával. Ezért feltehető, hogy $I \neq \emptyset$.

Jelölje $\mathscr{T}$ az $((\mathbb{R}, \mathscr{E}_{\mathbb{R}}), f_i)_{i\in I}$ rendszer által projektíven előállított T feletti topológiát és $\mathscr{T}' := \mathscr{T}_{(f_i)_{i\in I}}$. Minden $i \in I$ esetén legyen $d_i := d_{f_i}$. Ha $i \in I$ és $r_i \in \mathbb{R}_+^*$, akkor minden $T \ni t$-re $\mathrm{B}_{r_i}(t; d_i) = [|f_i - f_i(t)| < r_i]$, és a jobb oldalon álló halmaz $\mathscr{T}$-nyílt, hiszen f_i folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Ebből következik, hogy ha $J \subseteq I$ nem üres véges halmaz és $(r_i)_{i\in J}$ $\mathbb{R}_+^*$-ban haladó rendszer, akkor minden $T \ni t$-re a $\bigcap\limits_{i\in J} \mathrm{B}_{r_i}(t; d_i)$ halmaz $\mathscr{T}$-nyílt. Az állítás előtt álló megjegyzés szerint ezek a halmazok topologikus bázisát alkotják a $\mathscr{T}'$ topológiának, ezért $\mathscr{T}' \subseteq \mathscr{T}$.

A fordított tartalmazás bizonyításához elég azt megmutatni, hogy minden $i \in I$ esetén az $f_i : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, hiszen a definíció szerint $\mathscr{T}$ a legkisebb ilyen tulajdonságú T feletti topológia. Legyen $i \in I$, $\varepsilon \in \mathbb{R}_+^*$ és $t \in T$. A $\mathrm{B}_\varepsilon(t; d_i)$ gömb $\mathscr{T}'$-nyílt környezete t-nek, és világos, hogy $f_i\langle \mathrm{B}_\varepsilon(t; d_i)\rangle \subseteq \mathrm{B}_\varepsilon(f_i(t); \mathbb{R})$, tehát f_i a t pontban folytonos a $\mathscr{T}'$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. ■

27.8.7. Tétel. (Teljesen reguláris terek jellemzése) *Ha $(T, \mathscr{T})$ topologikus tér, akkor a következő állítások ekvivalensek.*

(i) *$(T, \mathscr{T})$ teljesen reguláris.*

(ii) *Létezik $T \to [0, 1]$ függvényeknek olyan $(f_i)_{i\in I}$ rendszere, hogy $\mathscr{T} = \mathscr{T}_{(f_i)_{i\in I}}$.*

(iii) *Létezik T feletti félmetrikáknak olyan $(d_i)_{i\in I}$ rendszere, hogy $\mathscr{T} = \mathscr{T}_{(d_i)_{i\in I}}$.*

Továbbá, ha $(T, \mathscr{T})$ teljesen reguláris tér és $I \subseteq \mathscr{F}(T; [0, 1])$ olyan halmaz, hogy minden $f \in I$ esetén f folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|[0, 1]$ topológiák szerint, valamint minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és $T \setminus F \ni t$-hez létezik olyan $f \in I$, hogy $F \subseteq [f = 0]$ és $f(t) = 1$, akkor $\mathscr{T} = \mathscr{T}_{(f)_{f\in I}}$.

Bizonyítás. Az állítás triviálisan igaz akkor, amikor $\mathscr{T}$ a T feletti antidiszkrét topológia.

(i)⇒(ii) A $(T, \mathscr{T})$ topologikus tér teljesen reguláris, ezért van olyan $I \subseteq \mathscr{F}(T; [0, 1])$ halmaz, hogy minden $f \in I$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|[0, 1]$ topológiák szerint, valamint minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és $T \setminus F \ni t$-hez van olyan $f \in I$, hogy $f(t) = 1$ és $F \subseteq [f = 0]$. Megmutatjuk, hogy bármely ilyen tulajdonságú I halmazra az $(f)_{f\in I}$ függvényrendszer által generált T feletti topológia egyenlő $\mathscr{T}$-vel.

Jelölje $\mathscr{T}'$ az $(f)_{f\in I}$ függvényrendszer által generált T feletti topológiát, és legyen $t \in T$ rögzített pont.

Legyen $V \in \mathscr{T}(t)$; ekkor van olyan $\Omega \in \mathscr{T}$, hogy $t \in \Omega \subseteq V$. A $T \setminus \Omega$ halmaz $\mathscr{T}$-zárt és $t \notin T \setminus \Omega$, így az I függvényhalmaz választása szerint van olyan $f \in I$, hogy $f(t) = 1$ és $T \setminus \Omega \subseteq [f = 0]$. Az f függvény folytonos a $\mathscr{T}'$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, ezért bármely $r \in]0, 1[$ valós számra az $[f > r] = \overset{-1}{f}\langle]r, \to [\rangle$ halmaz $\mathscr{T}'$-nyílt és $t \in [f = 1] \subseteq [f > r] \subseteq [f \neq 0] \subseteq \Omega \subseteq V$, így $V \in \mathscr{T}'(t)$. Ez azt jelenti, hogy $\mathscr{T}(t) \subseteq \mathscr{T}'(t)$.

Megfordítva, legyen $V \in \mathscr{T}'(t)$; ekkor van olyan $\Omega \in \mathscr{T}'$, hogy $t \in \Omega' \subseteq V$. Legyen $J \subseteq I$ olyan nem üres véges halmaz és $r \in \mathbb{R}_+^*$ olyan, hogy $\bigcap_{f \in J} \mathrm{B}_r(t; d_f) \subseteq V$. Ha $f \in J$, akkor $\mathrm{B}_r(t; d_f) = [|f - f(t)| < r]$, és az f függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, így a $[|f - f(t)| < r]$ halmaz $\mathscr{T}$-nyílt. Ebből következik, hogy $\bigcap_{f \in J} \mathrm{B}_r(t; d_f) \in \mathscr{T}$, így $V \in \mathscr{T}(t)$. Ez azt jelenti, hogy $\mathscr{T}'(t) \subseteq \mathscr{T}(t)$.

Tehát minden $t \in T$ esetén $\mathscr{T}(t) = \mathscr{T}'(t)$, így $\mathscr{T} = \mathscr{T}'$. Ezzel nemcsak az (i)⇒(ii) implikációt, hanem az utolsó állításunkat is igazoltuk.

(ii)⇒(iii) Triviális.

(iii)⇒(i) Legyen $(d_i)_{i \in I}$ a T halmaz feletti félmetrikáknak olyan rendszere, hogy $\mathscr{T} = \mathscr{T}_{(d_i)_{i \in I}}$. Ha $i \in I$ és $t \in T$, akkor $d_i(\cdot, t) : T \to \mathbb{R}$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, mert a d_i-re vonatkozó háromszög-egyenlőtlenség és szimmetria alapján minden $T \ni t_1, t_2$-re fennáll a $|d_i(t_1, t) - d_i(t_2, t)| \leq d_i(t_1, t_2)$ egyenlőtlenség.

Legyen az $F \subseteq T$ halmaz $\mathscr{T}$-zárt és $t \in T \setminus F$. Ekkor a $T \setminus F$ halmaz a t pontnak $\mathscr{T}$-nyílt környezete, ezért van olyan $J \subseteq I$ nem üres véges halmaz és $r \in \mathbb{R}_+^*$, hogy $\bigcap_{i \in J} \mathrm{B}_r(t; d_i) \subseteq T \setminus F$. Ekkor az

$$f := 1 - \inf\left(1, \frac{1}{r} \sup_{i \in J} d_i(\cdot, t)\right) : T \to \mathbb{R}$$

függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, továbbá $0 \leq f \leq 1$, és $F \subseteq [f = 0]$, valamint $f(t) = 1$. A definíció alapján ez azt jelenti, hogy a $(T, \mathscr{T})$ topologikus tér teljesen reguláris. ■

Az iménti tétel bizonyításának (i)⇒(ii) részéből látható, hogy ha $(T, \mathscr{T})$ teljesen reguláris tér és $I \subseteq \mathscr{F}(T; [0,1])$ olyan halmaz, hogy minden $f \in I$ esetén f folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|[0,1]$ topológiák szerint, valamint minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és $T \setminus F \ni t$-hez létezik olyan $f \in I$, hogy $F \subseteq [f = 0]$ és $f(t) = 1$, akkor $\mathscr{T} = \mathscr{T}_{(f)_{f \in I}}$. Másfelől láttuk, hogy a $\mathscr{T}_{(f)_{f \in I}}$ topológia megegyezik az $((\mathbb{R}, \mathscr{E}_{\mathbb{R}}), f)_{f \in I}$ rendszer által előállított T feletti iniciális topológiával. Ebből azonnal következik, hogy ha I ilyen tulajdonságú függvényhalmaz, akkor minden $(T', \mathscr{T}')$ topologikus térre, és minden $g : T' \to T$ függvényre: a g pontosan akkor folytonos a $\mathscr{T}'$ és $\mathscr{T}$ topológiák szerint, ha minden $I \ni f$-re az $f \circ g : T' \to \mathbb{R}$ függvény folytonos a $\mathscr{T}'$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint.

27.9. Beágyazási tételek

27.9.1. Tétel. (Teljesen reguláris terek beágyazási tétele) *Ha $(T, \mathscr{T})$ teljesen reguláris Hausdorff-tér és $I \subseteq \mathscr{F}(T; [0,1])$ olyan halmaz, hogy minden $f \in I$ esetén f folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|[0,1]$ topológiák szerint, valamint minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és $T \setminus F \ni t$-hez létezik olyan $f \in I$, hogy $F \subseteq [f = 0]$ és $f(t) = 1$, akkor a $\left([0,1]^I, (\mathscr{E}_{\mathbb{R}}|[0,1])^I\right)$ topologikus kockának van olyan topologikus altere, amely homeomorf $(T, \mathscr{T})$-vel (amit úgy fejezünk ki, hogy a $(T, \mathscr{T})$ teljesen reguláris tér* **beágyazható** *a $\left([0,1]^I, (\mathscr{E}_{\mathbb{R}}|[0,1])^I\right)$ topologikus kockába).*

Bizonyítás. Legyen $\mathscr{T}' := (\mathscr{E}_{\mathbb{R}}|[0,1])^I$, és értelmezzük a

$$\varphi : T \to [0,1]^I; \quad t \mapsto (f \mapsto f(t))$$

leképezést, tehát $t \in T$ esetén $\varphi(t) \in [0,1]^I$ az a függvény, amely minden $f \in I$ függvényhez az $f(t)$ értéket rendeli.

Legyenek $t, t' \in T$ és $t \neq t'$; akkor $t \in T \setminus \{t'\}$ és a $\{t'\}$ halmaz $\mathscr{T}$-zárt, mert a $(T, \mathscr{T})$ topologikus tér T_1-tér. Ezért az I választása szerint van olyan $f \in I$, hogy $f(t) = 1$ és $\{t'\} \subseteq [f = 0]$, azaz $f(t') = 0$. Tehát $\varphi(t)(f) = 1 \neq 0 = f(t') = \varphi(t')(f)$, vagyis a φ függvény injektív.

Minden $f \in I$ esetén jelölje pr_f az f által meghatározott $[0,1]^I \to [0,1]$ projekciót. A szorzattopológia definíciója alapján a φ függvény pontosan akkor folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint, ha minden $I \ni f$-re a $\mathrm{pr}_f \circ \varphi : T \to [0,1]$ függvény folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|[0,1]$ topológiák szerint. De $f \in I$ esetén minden $T \ni t$-re $\left(\mathrm{pr}_f \circ \varphi\right)(t) = f(t)$, azaz $\mathrm{pr}_f \circ \varphi = f$, és f folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|[0,1]$ topológiák szerint. Ezért a $\varphi : T \to [0,1]^I$ leképezés folytonos a $\mathscr{T}$ és $\mathscr{T}'$ topológiák szerint. Tehát a $\varphi : T \to \mathrm{Im}(\varphi)$ függvény olyan bijekció, amely folytonos a $\mathscr{T}$ és $\mathscr{T}'|\mathrm{Im}(\varphi)$ topológiák szerint.

A bizonyítás utolsó lépéseként megmutatjuk, hogy a $\varphi^{-1} : \mathrm{Im}(\varphi) \to T$ függvény folytonos a $\mathscr{T}'|\mathrm{Im}(\varphi)$ és $\mathscr{T}$ topológiák szerint. Az állítás előtt álló megjegyzés alapján φ^{-1} pontosan akkor folytonos a $\mathscr{T}'|\mathrm{Im}(\varphi)$ és $\mathscr{T}$ topológiák szerint, ha minden $I \ni f$-re az $f \circ \varphi^{-1} : \mathrm{Im}(\varphi) \to \mathbb{R}$ függvény folytonos a $\mathscr{T}'|\mathrm{Im}(\varphi)$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Ha $f \in I$, akkor nyilvánvalóan $f \circ \varphi^{-1} = \mathrm{pr}_f|_{\mathrm{Im}(\varphi)}$, vagyis $f \circ \varphi^{-1}$ egyenlő a $\mathrm{pr}_f : [0,1]^I \to [0,1]$ projekció-függvény $\mathrm{Im}(\varphi)$-re vett leszűkítésével. A szorzattopológia értelmezése alapján minden $f \in I$ esetén a pr_f függvény folytonos a $\mathscr{T}'$ és $\mathscr{E}_{\mathbb{R}}|[0,1]$ topológiák szerint, így $\mathrm{pr}_f|_{\mathrm{Im}(\varphi)}$ folytonos a $\mathscr{T}'|\mathrm{Im}(\varphi)$ és $\mathscr{E}_{\mathbb{R}}|[0,1]$ topológiák szerint. Ezért minden $I \ni f$-re $f \circ \varphi^{-1}$ folytonos a $\mathscr{T}'|\mathrm{Im}(\varphi)$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. ■

27.9.2. Tétel. (Uriszon beágyazási tétele) *Minden megszámlálható bázisú reguláris* T_1*-tér homeomorf a* $\left([0,1]^{\mathbb{N}}, (\mathscr{E}_{\mathbb{R}}|[0,1])^{\mathbb{N}}\right)$ *euklidészi kocka valamelyik topologikus alterével.*

Bizonyítás. Legyen $(T, \mathscr{T})$ megszámlálható bázisú reguláris T_1-tér. A Lindelöf-tétel szerint minden megszámlálható bázisú topologikus tér Lindelöf-tér, és a Tyihonov-lemma szerint minden reguláris Lindelöf-tér normális. Ezért $(T, \mathscr{T})$ normális T_1-tér, így $(T, \mathscr{T})$ teljesen reguláris Hausdorff-tér. Ha létezne olyan $I \subseteq \mathscr{F}(T; [0,1])$ *megszámlálható* halmaz, hogy minden $f \in I$ esetén f folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}|[0,1]$ topológiák szerint, valamint minden $F \subseteq T$ $\mathscr{T}$-zárt halmazhoz és $T \setminus F \ni t$-hez létezik olyan $f \in I$, hogy $F \subseteq [f = 0]$ és $f(t) = 1$, akkor a teljesen reguláris terek beágyazási tétele (27.9.1.) szerint a $\left([0,1]^I, (\mathscr{E}_{\mathbb{R}}|[0,1])^I\right)$ topologikus kockának van olyan topologikus altere, amely homeomorf $(T, \mathscr{T})$-vel. Ekkor I véges, vagy ekvipotens $\mathbb{N}$-nel. Az első esetben $\left([0,1]^I, (\mathscr{E}_{\mathbb{R}}|[0,1])^I\right)$ homeomorf a $\left([0,1]^{\mathbb{N}}, (\mathscr{E}_{\mathbb{R}}|[0,1])^{\mathbb{N}}\right)$ euklidészi kocka valamelyik topologikus alterével, míg a második esetben $\left([0,1]^I, (\mathscr{E}_{\mathbb{R}}|[0,1])^I\right)$ és $\left([0,1]^{\mathbb{N}}, (\mathscr{E}_{\mathbb{R}}|[0,1])^{\mathbb{N}}\right)$ homeomorfak. Ezért $(T, \mathscr{T})$ is homeomorf volna a $\left([0,1]^{\mathbb{N}}, (\mathscr{E}_{\mathbb{R}}|[0,1])^{\mathbb{N}}\right)$ euklidészi kocka valamelyik topologikus alterével.

Egy ilyen tulajdonságú I függvényhalmaz előállítása céljából vegyük a $(T, \mathscr{T})$ topologikus térnek egy $\mathfrak{B}$ megszámlálható topologikus bázisát, és legyen $\mathfrak{I} := \{(U, V) \in \mathfrak{B} \times \mathfrak{B} | \overline{U} \subseteq V\}$. A $(T, \mathscr{T})$ topologikus tér normális, ezért az Uriszon-tétel alapján minden $\mathfrak{I} \ni (U, V)$-hez van olyan $f : T \to \mathbb{R}$ függvény, amely folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $0 \leq f \leq 1$, $\overline{U} \subseteq [f = 1]$ és $[f \neq 0] \subseteq V$. Ezért kiválaszthatunk olyan $\left(f_{U,V}\right)_{(U,V) \in \mathfrak{I}}$ rendszert, hogy minden $\mathfrak{I} \ni (U, V)$-re $f_{U,V} : T \to \mathbb{R}$ folytonos függvény a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint, $\overline{U} \subseteq [f_{U,V} = 1]$ és $[f_{U,V} \neq 0] \subseteq V$. Az $\mathfrak{I}$ halmaz megszámlálható, ezért $I := \left\{ f_{U,V} \;\middle|\; (U, V) \in \mathfrak{I} \right\} \subseteq \mathscr{F}(T; [0,1])$ olyan megszámlálható függvényhalmaz, amelynek minden eleme folytonos a $\mathscr{T}$ és $\mathscr{E}_{\mathbb{R}}$ topológiák szerint. Legyen az $F \subseteq T$ halmaz $\mathscr{T}$-zárt és $t \in T \setminus F$. A $\mathfrak{B}$ halmaz topologikus bázisa a $(T, \mathscr{T})$ topologikus térnek, ezért vehetünk olyan $V \in \mathfrak{B}$ halmazt, hogy $t \in V \subseteq T \setminus F$. A $(T, \mathscr{T})$ topologikus tér reguláris, ezért a $V \in \mathscr{T}(t)$ környezethez van olyan $W \in \mathscr{T}(t)$, amely $\mathscr{T}$-zárt és $W \subseteq V$. Ekkor $t \in \overset{\circ}{W} \in \mathscr{T}$, így ismét kihasználva azt, hogy $\mathfrak{B}$ topologikus bázisa $(T, \mathscr{T})$-nek kapunk olyan $U \in \mathfrak{B}$ halmazt, hogy $t \in U \subseteq \overset{\circ}{W}$. Világos, hogy $\overline{U} \subseteq W \subseteq V$, tehát $(U, V) \in \mathfrak{I}$, és $f_{U,V}(t) = 1$, valamint $F \subseteq T \setminus V \subseteq [f_{U,V} = 0]$. Ez azt jelenti, hogy I olyan függvényhalmaz, amelynek a létezését állítottuk. ■

27.9.3. Tétel. (Uriszon metrizációs tétele) *Ha* $(T, \mathscr{T})$ T_1*-tér, akkor a következő állítások ekvivalensek.*

(i) $(T, \mathscr{T})$ *reguláris és megszámlálható bázisú.*

(ii) $(T, \mathscr{T})$ *homeomorf a* $\big([0,1]^{\mathbb{N}}, (\mathscr{E}_{\mathbb{R}}|[0,1])^{\mathbb{N}}\big)$ *euklidészi kocka valamelyik topologikus alterével.*

(iii) $(T, \mathscr{T})$ *metrizálható és szeparábilis.*

Bizonyítás. (i)⇒(ii) Ez a következtetés ekvivalens Uriszon beágyazási tételével (a T_1 terek körében).

(ii)⇒(iii) A $\big([0,1]^{\mathbb{N}}, (\mathscr{E}_{\mathbb{R}}|[0,1])^{\mathbb{N}}\big)$ euklidészi kocka metrizálható, és nyilvánvaló, hogy metrizálható topologikus tér bármely topologikus altere metrizálható.

(iii)⇒(i) Láttuk, hogy szeparábilis metrizálható tér megszámlálható bázisú (26.3.4.) és normális (27.4.11.) Hausdorff-tér, ezért szükségképpen reguláris. ■

28. fejezet

Kompakt terek, lokálisan kompakt terek és parakompakt terek

28.1. A kompakt halmazok tulajdonságai

Ettől kezdve áttérünk a topologikus terek jelölésével kapcsolatos szokásos konvencióra. Tehát minden topologikus teret egyetlen szimbólummal, az alaphalmaz jelével jelölünk, ha ez nem okoz félreértést. Hasonló megállapodáshoz tartottuk magunkat a testek, a vektorterek, a metrikus terek és a normált terek esetében is. Továbbá, a $\mathbb{K}$ test minden részhalmazát az euklidészi topológia (vagyis $\mathscr{E}_{\mathbb{K}}$) leszűkítésével ellátva topologikus térnek tekintjük. Tehát a $\mathbb{K}$ részhalmazain más topológiát nem veszünk; ha arra mégis szükség volna, akkor azt külön megemlítjük.

28.1.1. Definíció. *A T topologikus teret* **kompaktnak** *nevezzük, ha a T bármely nyílt befedésének létezik véges részbefedése. A T topologikus tér E részhalmazát kompaktnak mondjuk, ha E a T topológiájának leszűkítésével ellátva kompakt tér. A T topologikus tér E részhalmazát* **relatív kompaktnak** *nevezzük, ha az $\overline{E}$ halmaz kompakt T-ben.*

Kompakt tér nem feltétlenül Hausdorff-tér. Például minden antidiszkrét tér nyilvánvalóan kompakt, de ha az alaphalmaz legalább két elemű, akkor nem Hausdorff-tér, sőt nem is T_0-tér.

28.1.2. Állítás. *Legyen T topologikus tér. Az $E \subseteq T$ halmaz pontosan akkor kompakt, ha a T nyílt részhalmazainak bármely $(\Omega_i)_{i\in I}$ rendszerére teljesül az, hogy ha $E \subseteq \bigcup_{i\in I} \Omega_i$, akkor létezik olyan $J \subseteq I$ véges halmaz, amelyre $E \subseteq \bigcup_{i\in J} \Omega_i$.*

Bizonyítás. Tegyük fel, hogy az $E \subseteq T$ halmaz kompakt, és legyen $(\Omega_i)_{i\in I}$ a T nyílt részhalmazainak olyan rendszere, hogy $E \subseteq \bigcup_{i\in I} \Omega_i$. Az altértopológia tulajdonságai szerint ekkor az $(E \cap \Omega_i)_{i\in I}$ halmazrendszer mindegyik tagja nyílt az E topologikus altérben, és $E = \bigcup_{i\in I} (E \cap \Omega_i)$. Az E kompaktsága miatt van olyan $J \subseteq I$ véges halmaz, hogy $E = \bigcup_{i\in J} (E \cap \Omega_i)$. Természetesen ekkor $E \subseteq \bigcup_{i\in J} \Omega_i$ is teljesül.

Megfordítva, tegyük fel, hogy a T nyílt részhalmazainak bármely $(\Omega_i)_{i\in I}$ rendszerére teljesül az, hogy $E \subseteq \bigcup_{i \in I} \Omega_i$ esetén van olyan $J \subseteq I$ véges halmaz, hogy $E \subseteq \bigcup_{i \in J} \Omega_i$. Legyen $(\Omega_i')_{i \in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén Ω_i' nyílt részhalmaza az E topologikus altérnek és $E = \bigcup_{i \in I} \Omega_i'$. Az altértopológia definíciója alapján kiválaszthatunk olyan $(\Omega_i)_{i \in I}$ rendszert, hogy minden $I \ni i$-re Ω_i nyílt részhalmaza T-nek és $\Omega_i' = E \cap \Omega_i$. Világos, hogy ekkor $E = \bigcup_{i \in I} \Omega_i' = \bigcup_{i \in I} (E \cap \Omega_i) \subseteq \bigcup_{i \in I} \Omega_i$, tehát a feltevés alapján van olyan $J \subseteq I$ véges halmaz, hogy $E \subseteq \bigcup_{i \in J} \Omega_i$. Ezért $E = \bigcup_{i \in J} (E \cap \Omega_i) = \bigcup_{i \in J} \Omega_i'$, így E kompakt halmaz T-ben. ■

Legyen T topologikus tér, $E \subseteq T$ kompakt halmaz, és $(V_t)_{t \in E}$ olyan rendszer, hogy minden $E \ni t$-re V_t a t-nek környezete. Ekkor van olyan $H \subseteq E$ véges halmaz, hogy $E \subseteq \bigcup_{t \in H} V_t$. Valóban, a környezetek értelmezése alapján kiválaszthatjuk a T nyílt részhalmazainak olyan $(\Omega_t)_{t \in E}$ rendszerét, amelyre minden $t \in E$ esetén $t \in \Omega_t \subseteq V_t$, tehát $E \subseteq \bigcup_{t \in E} \Omega_t$. Ez azt jelenti, hogy $(\Omega_t)_{t \in E}$ nyílt befedése E-nek, így az E kompaktsága folytán van olyan $H \subseteq E$ véges halmaz, hogy $E \subseteq \bigcup_{t \in H} \Omega_t \subseteq \bigcup_{t \in H} V_t$. Ezt az állítást a következőkben gyakran alkalmazzuk.

28.1.3. Állítás. *Legyen T topologikus tér és $T' \subseteq T$. Az $E \subseteq T'$ halmaz pontosan akkor kompakt T-ben, ha kompakt a T' topologikus altérben.*

Bizonyítás. Tegyük fel, hogy az $E \subseteq T'$ halmaz kompakt a T' topologikus altérben, és legyen $(\Omega_i)_{i \in I}$ a T nyílt részhalmazainak olyan rendszere, hogy $E \subseteq \bigcup_{i \in I} \Omega_i$. Ekkor a $(T' \cap \Omega_i)_{i \in I}$ rendszer a T' altértopológiája szerint nyílt részhalmazainak olyan rendszere, hogy $E \subseteq \bigcup_{i \in I} (T' \cap \Omega_i)$. Ezért van olyan $J \subseteq I$ véges halmaz, hogy $E \subseteq \bigcup_{i \in J} (T' \cap \Omega_i) \subseteq \bigcup_{i \in J} \Omega_i$. Ez azt jelenti, hogy E kompakt a T topologikus térben.
Megfordítva, tegyük fel, hogy az $E \subseteq T'$ halmaz kompakt a T topologikus térben, és legyen $(\Omega_i')_{i \in I}$ a T' topologikus altérben nyílt halmazok olyan rendszere, hogy $E \subseteq \bigcup_{i \in I} \Omega_i'$. Az altértopológia tulajdonságai szerint kiválasztható a T nyílt részhalmazainak olyan $(\Omega_i)_{i \in I}$ rendszere, hogy minden $i \in I$ esetén $\Omega_i' = T' \cap \Omega_i$. Ekkor $E \subseteq \bigcup_{i \in I} \Omega_i$, így létezik olyan $J \subseteq I$ véges halmaz, hogy $E \subseteq \bigcup_{i \in J} \Omega_i$. Minden $I \ni i$-re $\Omega_i' \subseteq T'$, ezért ebből következik, hogy $E \subseteq T' \cap \left(\bigcup_{i \in J} \Omega_i \right) = \bigcup_{i \in J} (T' \cap \Omega_i) = \bigcup_{i \in J} \Omega_i'$. Ez azt jelenti, hogy E kompakt a T' topologikus altérben. ■

Véges sok véges halmaz uniója véges, ezért nyilvánvaló, hogy topologikus tér véges sok kompakt részhalmazának uniója kompakt. Továbbá, topologikus tér bármely véges részhalmaza nyilvánvalóan kompakt halmaz.

28.1.4. Állítás. *Hausdorff-tér minden kompakt részhalmaza zárt. Kompakt tér minden zárt részhalmaza kompakt. Kompakt Hausdorff-térben egy halmaz pontosan akkor kompakt, ha zárt.*

Bizonyítás. A harmadik állítás nyilvánvalóan következik az első kettőből.

Legyen E nem üres kompakt halmaz a T Hausdorff-térben, és $t_0 \in T \setminus E$ rögzített pont. Minden $t \in E$ esetén $t \neq t_0$, ezért létezik t-nek olyan V környezete és t_0-nak olyan U környezete, hogy $V \cap U = \emptyset$. Tehát kiválaszthatunk olyan $(V_t)_{t\in E}$ és $(U_t)_{t\in E}$ rendszereket, hogy minden $E \ni t$-re V_t a t-nek és U_t a t_0-nak olyan környezete T-ben, hogy $V_t \cap U_t = \emptyset$. Az E kompaktsága miatt létezik olyan $H \subseteq E$ véges halmaz, hogy $E \subseteq \bigcup\limits_{t\in H} V_t$. Az $E \neq \emptyset$ feltétel alapján $H \neq \emptyset$, így az $U := \bigcap\limits_{t\in H} U_t$ halmaz a t_0-nak olyan környezete T-ben, hogy $U \cap \left(\bigcup\limits_{t\in H} V_t\right) = \emptyset$, következésképpen $U \cap E = \emptyset$, azaz $U \subseteq T \setminus E$. Ez azt jelenti, a $T \setminus E$ halmaz minden pontja belső pont, tehát E zárt halmaz T-ben.

Legyen T kompakt tér és $E \subseteq T$ zárt halmaz. Legyen $(\Omega_i)_{i\in I}$ a T nyílt részhalmazainak olyan rendszere, amelyre $E \subseteq \bigcup\limits_{i\in I} \Omega_i$. Legyen α olyan halmaz, hogy $\alpha \notin I$, és $\Omega_\alpha := T \setminus E$, tehát az E zártsága miatt Ω_α nyílt részhalmaza T-nek. Ekkor $(\Omega_i)_{i\in I\cup\{\alpha\}}$ a T nyílt befedése, így a T kompaktsága folytán létezik olyan $J \subseteq I \cup \{\alpha\}$ véges halmaz, amelyre $T = \bigcup\limits_{i\in J} \Omega_i$. Világos, hogy $E \cap \Omega_\alpha = \emptyset$, ezért $E = \bigcup\limits_{i\in J} (E \cap \Omega_i) = \bigcup\limits_{i\in J\setminus\{\alpha\}} (E \cap \Omega_i) \subseteq \bigcup\limits_{i\in J\setminus\{\alpha\}} \Omega_i$. Tehát $J \setminus \{\alpha\} \subseteq I$ olyan véges halmaz, hogy $E \subseteq \bigcup\limits_{i\in J\setminus\{\alpha\}} \Omega_i$. Ez azt jelenti, hogy E kompakt halmaz T-ben. ■

Vigyázzunk arra, hogy kompakt térben létezhet nem zárt kompakt részhalmaz; például ha T kompakt, de nem T_1-tér, akkor van olyan $t \in T$, hogy a $\{t\}$ halmaz nem zárt, de kompakt. Z

28.1.5. Következmény. *Ha T topologikus tér, $E \subseteq T$ kompakt halmaz és $F \subseteq T$ zárt halmaz, akkor $E \cap F$ kompakt halmaz T-ben.*

Bizonyítás. Az altértopológiák tulajdonságai alapján az $E \cap F$ halmaz zárt az E kompakt topologikus altérben, így az előző állítás szerint $E \cap F$ kompakt az E altértopológiája szerint. Ezért $E \cap F$ kompakt T-ben is. ■

28.1.6. Állítás. *Reguláris topologikus térben minden kompakt halmaz relatív kompakt.*

Bizonyítás. Legyen T reguláris topologikus tér és $K \subseteq T$ kompakt halmaz. Legyen $(\Omega_i)_{i\in I}$ nyílt befedése $\overline{K}$-nak T-ben. Ha $t \in K$, akkor van olyan $i \in I$, hogy $t \in \Omega_i$, tehát a T regularitása miatt van olyan V *zárt* környezete t-nek, hogy $V \subseteq \Omega_i$. Tehát kiválasztható olyan $(V_t)_{t\in K}$ rendszer, hogy minden $t \in K$ esetén V_t zárt környezete t-nek és van olyan $i \in I$, amelyre $V_t \subseteq \Omega_i$. Ekkor $(V_t)_{t\in K}$ környezetekkel való befedése a K kompakt halmaznak, ezért van olyan $H \subseteq K$ véges halmaz, hogy $K \subseteq \bigcup\limits_{t\in H} V_t$. Itt a jobb oldalon zárt halmaz áll, ezért $\overline{K} \subseteq \bigcup\limits_{t\in H} V_t$. Ha $f : H \to I$ olyan függvény, hogy minden $t \in H$ esetén $V_t \subseteq \Omega_{f(t)}$, akkor $\mathrm{Im}(f)$ olyan véges részhalmaza I-nek, hogy $\overline{K} \subseteq \bigcup\limits_{i\in \mathrm{Im}(f)} \Omega_i$, tehát $\overline{K}$ kompakt halmaz T-ben. ■

28.1.7. Állítás. *Minden kompakt Hausdorff-tér normális.*

Bizonyítás. Először megmutatjuk, hogy minden kompakt Hausdorff-tér *reguláris.* Legyen ugyanis T kompakt Hausdorff-tér, $F \subseteq T$ nem üres zárt halmaz, valamint $t \in T \setminus F$. Minden $s \in F$ esetén $t \neq s$, ezért van olyan U nyílt környezete t-nek és olyan V nyílt környezete s-nek, hogy $U \cap V = \emptyset$. Kiválaszthatunk tehát olyan $(U_s)_{s \in F}$ és $(V_s)_{s \in F}$ rendszereket, hogy minden $F \ni s$-re U_s a t-nek nyílt környezete és V_s az s-nek nyílt környezete és $U_s \cap V_s = \emptyset$. Az F halmaz zárt a T kompakt térben, tehát F kompakt halmaz, így van olyan $S \subseteq F$ véges halmaz, hogy $F \subseteq \bigcup_{s \in S} V_s$. Az $F \neq \emptyset$ feltétel alapján $S \neq \emptyset$, ezért $U := \bigcap_{s \in S} U_s$ a t-nek nyílt környezete T-ben. Világos, hogy $\Omega := U$ és $\Omega' := \bigcup_{s \in S} V_s$ olyan diszjunk nyílt halmazok T-ben, amelyekre $t \in \Omega$ és $F \subseteq \Omega'$. Ez azt jelenti, hogy T reguláris tér.

Legyen T kompakt Hausdorff-tér, és legyenek $F, F' \subseteq T$ nem üres diszjunkt zárt halmazok T-ben. A T regularitása miatt minden $t \in F$ esetén van olyan U nyílt környezete t-nek és olyan $\Omega' \subseteq T$ nyílt halmaz, hogy $F' \subseteq \Omega'$ és $U \cap \Omega' = \emptyset$. Kiválaszthatunk tehát olyan $(U_t)_{t \in F}$ és $(\Omega'_t)_{t \in F}$ rendszereket, hogy minden $F \ni t$-re U_t nyílt környezete t-nek, Ω'_t nyílt halmaz T-ben, valamint $F' \subseteq \Omega'_t$ és $U_t \cap \Omega'_t = \emptyset$. Az F halmaz zárt a T kompakt térben, ezért F kompakt halmaz, így van olyan $H \subseteq F$ véges halmaz, hogy $F \subseteq \bigcup_{t \in H} U_t$. Az $F \neq \emptyset$ feltétel alapján $H \neq \emptyset$. Ekkor $\Omega := \bigcup_{t \in H} U_t$ és $\Omega' := \bigcap_{t \in H} \Omega'_t$ olyan nyílt halmazok, hogy $F \subseteq \Omega$, $F' \subseteq \Omega'$ és $\Omega \cap \Omega' = \emptyset$. Ez azt jelenti, hogy T normális tér. ■

Megjegyezzük, hogy kompakt tér triviálisan Lindelöf-tér (27.4.7.), és a Tyihonov-lemma (27.4.9.) szerint reguláris Lindelöf-tér normális. Ezért az iménti bizonyítás első részéből a Tyihonov-lemma alapján is következik az állítás. Azonban a fenti bizonyítás nem követeli meg sem a Lindelöf-terek fogalmának, sem a Tyihonov-lemmának az ismeretét.

Tehát láttuk, hogy kompakt Hausdorff-tér szükségképpen reguláris is. Azonban létezik olyan kompakt T_1-tér, amely nem Hausdorff-tér (és akkor még kevésbé reguláris, hiszen reguláris T_1-tér szükségképpen Hausdorff-tér). Később konkrét példát adunk ilyen térre.

28.1.8. Állítás. *Ha T, T' topologikus terek, $f : T \to T'$ folytonos függvény és $K \subseteq T$ kompakt halmaz, akkor $f\langle K \rangle \subseteq T'$ kompakt halmaz.*

Bizonyítás. Legyen $(\Omega'_i)_{i \in I}$ az T' nyílt részhalmazainak olyan rendszere, amelyre $f\langle K \rangle \subseteq \bigcup_{i \in I} \Omega'_i$. Ekkor $K \subseteq \bigcup_{i \in I} \overset{-1}{f} \langle \Omega'_i \rangle$, tehát K kompaktsága miatt vehetünk olyan $J \subseteq I$ véges halmazt, amelyre $K \subseteq \bigcup_{i \in J} \overset{-1}{f} \langle \Omega'_i \rangle$. Világos, hogy ekkor $f\langle K \rangle \subseteq \bigcup_{i \in J} f\langle \overset{-1}{f} \langle \Omega'_i \rangle \rangle \subseteq \bigcup_{i \in J} \Omega'_i$, ezért $f\langle K \rangle$ kompakt halmaz T'-ben. ■

28.1.9. Következmény. *Legyen T kompakt tér, T' Hausdorff-tér és $f : T \to T'$ folytonos bijekció. Ekkor T Hausdorff-tér, T' kompakt tér és f homeomorfizmus T és T' között.*

Bizonyítás. Ha $F \subseteq T$ zárt halmaz, akkor F kompakt, tehát $f\langle F \rangle \subseteq T'$ szintén kompakt, így zárt is, mert T' Hausdorff-tér. Ez azt jelenti, hogy minden $F \subseteq T$ zárt halmazra az $\overset{-1}{(f^{-1})}\langle F\rangle = f\langle F\rangle$ halmaz zárt T'-ben. Tehát a folytonosság topologikus jellemzése alapján az f^{-1} függvény folytonos. ■

Megjegyezzük, hogy a nem Hausdorff-féle kompakt terek elmélete különös jelentőséggel bír az általános topológia algebrai topológiai alkalmazásaiban. Azonban az analízisben, majdnem minden természetes módon megjelenő kompakt tér Hausdorff-tér. Ezért az analízisben szokásos az a konvenció, hogy egy topologikus tér kompaktsága azt jelenti, hogy a tér kompakt Hausdorff-tér. Azonban ebben a fejezetben a kompaktság fogalmába nem értjük bele azt, hogy a tér Hausdorff-féle.

Most jellemzést adunk a rendezéstopológiák (26.2.5.) kompaktságára.

28.1.10. Állítás. *Legyen E legalább két elemű lineárisan rendezett halmaz, és lássuk el E-t a rendezéstopológiával. Ekkor az E Hausdorff-tér pontosan akkor kompakt, ha E-nek létezik legkisebb és legnagyobb eleme, és az E rendezése teljes (vagyis E minden részhalmazának létezik szuprémuma).*

Bizonyítás. Ha E-nek nincs legkisebb (illetve legnagyobb) eleme, akkor $(]x,\to[)_{x\in E}$ (illetve $(]\leftarrow,x[)_{x\in E}$) olyan nyílt befedése E-nek, amelynek nincs véges részbefedése, így E nem kompakt. Valóban, ez befedés, mert $y\in E$ esetén van olyan $x\in E$, hogy $x<y$ (illetve $y<x$) különben y az E halmaz legkisebb (illetve legnagyobb) eleme volna, tehát $y\in\bigcup\limits_{x\in E}]x,\to[$ (illetve $y\in\bigcup\limits_{x\in E}]\leftarrow,x[$). Ha $H\subseteq E$ olyan véges halmaz, hogy $E=\bigcup\limits_{x\in H}]x,\to[$ (illetve $E=\bigcup\limits_{x\in H}]\leftarrow,x[$), akkor $E\neq\emptyset$ miatt $H\neq\emptyset$, tehát E lineáris rendezettsége miatt vehetjük az $a:=\min(H)$ (illetve $b:=\max(H)$) elemet. Ekkor a-hoz (illetve b-hez) van olyan $x\in H$, hogy $a\in]x,\to[$ (illetve $b\in]\leftarrow,x[$), ezért $x<a=\min(H)$ (illetve $x>b=\max(H)$), ami lehetetlen.

Tegyük fel, hogy E rendezése nem teljes, és $A\subseteq E$ olyan felülről korlátos részhalmaz, amelynek nincs szuprémuma. Jelölje A' az A halmaz felső korlátjainak halmazát. Világos, hogy $A\cap A'=\emptyset$, mert ha $a\in A\cap A'$, akkor a az A halmaz legnagyobb eleme, ezért $a=\sup(A)$ teljesülne. Minden $x\in A\cup A'$ esetén legyen

$$\Omega_x := \begin{cases}]\leftarrow,x[& \text{, ha } x\in A;\\ ]x,\to[& \text{, ha } x\in A'. \end{cases}$$

Ekkor az $(\Omega_x)_{x\in A\cup A'}$ nyílt halmazokból álló rendszer befedése E-nek, mert $y\in E$ esetén, ha $y\notin A'$, vagyis y nem felső korlátja A-nak, akkor van olyan $x\in A$, hogy $y<x$, tehát $y\in]\leftarrow,x[=\Omega_x$; ha pedig $y\in A'$, akkor $\sup(A)$ nem létezése miatt van olyan $x\in A'$, hogy $x<y$, tehát $y\in]x\to[=\Omega_x$. Továbbá nyilvánvaló, hogy $\bigcup\limits_{x\in A'}\Omega_x\subseteq A'$, és megfordítva, ha $y\in A'$, akkor $\sup(A)$ nem létezése miatt van olyan $x\in A'$, hogy $x<y$, tehát $y\in]x\to[=\Omega_x$, ami azt jelenti, hogy $A'\subseteq\bigcup\limits_{x\in A'}\Omega_x$. Tehát fennáll az $\bigcup\limits_{x\in A'}\Omega_x=A'$ egyenlőség, és világos, hogy $\left(\bigcup\limits_{x\in A}\Omega_x\right)\cap\left(\bigcup\limits_{x\in A'}\Omega_x\right)=\emptyset$, mert ha y eleme a metszetnek, akkor $y\in A'$ és van olyan $x\in A$, hogy $y\in\Omega_x=]\leftarrow,x[$, vagyis $y<x\in A$, ami lehetetlen, mert y felső korlátja A-nak.

Megmutatjuk, hogy az $(\Omega_x)_{x\in A\cup A'}$ nyílt befedésnek nem létezik véges részbefedése, ezért

E nem kompakt. Indirekt, tegyük fel, hogy a $H \subseteq A \cup A'$ véges halmazra $(\Omega_x)_{x\in H}$ befedi E-t. Ekkor

$$E = \Big(\bigcup_{x\in H\cap A} \Omega_x \Big) \cup \Big(\bigcup_{x\in H\cap A'} \Omega_x \Big),$$

és az előzőek szerint a $\bigcup_{x\in H\cap A} \Omega_x$ és $\bigcup_{x\in H\cap A'} \Omega_x$ halmazok nem metszik egymást. Ha $H \cap A' = \emptyset$, akkor minden $y \in E$ esetén van olyan $x \in H \cap A$, hogy $x \in \Omega_x =]\leftarrow, x[$, ezért y nem felső korlátja A-nak, tehát ekkor A nem volna felülről korlátos. Ezért $H \cap A' \neq \emptyset$ véges halmaz, így képezhetjük az $y := \min(H \cap A')$ elemet. Ekkor $y \notin \bigcup_{x\in H\cap A'} \Omega_x$, különben létezne olyan $x \in H \cap A'$, hogy $y \in \Omega_x =]x, \rightarrow[$, vagyis $x < y$, ami lehetetlen, mert y a $H \cap A'$ halmaz legkisebb eleme. Ezért $y \in \bigcup_{x\in H\cap A} \Omega_x$, tehát létezik olyan $x \in H \cap A$, amelyre $y \in \Omega_x =]\leftarrow, x[$, vagyis $y < x \in A$. Ekkor viszont y nem felső korlátja A-nak, holott $y \in A'$, ami ellentmondás.

Ezzel bebizonyítottuk, hogy ha E kompakt, akkor E-nek létezik legkisebb és legnagyobb eleme, és E rendezése teljes.

(III) Tegyük fel, hogy E-nek létezik legkisebb és legnagyobb eleme, és E rendezése teljes. Jelölje $\mathbf{0}$ az E legkisebb és $\mathbf{1}$ az E legnagyobb elemét, és legyen $(\Omega_i)_{i\in I}$ nyílt befedése E-nek. Megmutatjuk, hogy létezik olyan $J \subseteq I$ véges halmaz, amelyre $(\Omega_i)_{i\in J}$ befedése E-nek, tehát E kompakt.

Legyen A azon $x \in E$ elemek halmaza, amelyekhez létezik olyan $J \subseteq I$ véges halmaz, hogy $[\mathbf{0}, x] \subseteq \bigcup_{i\in J} \Omega_i$. Világos, hogy $\mathbf{0} \in A$. Legyen $c := \sup(A)$, és rögzítsünk olyan $i_c \in I$ indexet, amelyre $c \in \Omega_{i_c}$. Mivel Ω_{i_c} nyílt halmaz E-ben, és a nyílt intervallumok az E topológiájának topologikus bázisát alkotják, így létezik olyan $\mathscr{I}$ nyílt intervallum E -ben, hogy $c \in \mathscr{I} \subseteq \Omega_{i_c}$. Az $\mathscr{I}$ intervallum alakja szerint három eset lehetséges:

1) van olyan $x \in E$, hogy $\mathscr{I} =]\leftarrow, x[$;

2) léteznek olyan $x, y \in E$, hogy $\mathscr{I} =]x, y[$;

3) van olyan $x \in E$, hogy $\mathscr{I} =]x, \rightarrow[$.

Először megmutatjuk, hogy az 1), 2) és 3) esetek mindegyikében $c \in A$.

Ha 1) teljesül, és $x \in E$ olyan, hogy $\mathscr{I} =]\leftarrow, x[$, akkor $[\mathbf{0}, c] \subseteq]\leftarrow, x[= \mathscr{I} \subseteq \Omega_{i_c} = \bigcup_{i\in\{i_c\}} \Omega_i$, tehát $c \in A$.

Ha 2) teljesül, és $x, y \in E$ olyanok, hogy $\mathscr{I} =]x, y[$, akkor $x < c = \sup(A)$ miatt létezik olyan $z \in A$, hogy $x < z \leq c < y$. Legyen $J_z \subseteq I$ olyan véges halmaz, hogy $[0, z] \subseteq \bigcup_{i\in J_z} \Omega_i$. Ekkor $]z, c] \subseteq]x, y[= \mathscr{I} \subseteq \Omega_{i_c}$, következésképpen

$$[\mathbf{0}, c] = [\mathbf{0}, z] \cup]z, c] \subseteq [\mathbf{0}, z] \cup]x, y[\subseteq \bigcup_{i\in J_z\cup\{i_c\}} \Omega_i,$$

tehát $c \in A$.

Ha 3) teljesül, és $x \in E$ olyan, hogy $\mathscr{I} =]x, \rightarrow[$, akkor $x < c = \sup(A)$ miatt létezik olyan $z \in A$, hogy $x < z \leq c$. Legyen $J_z \subseteq I$ olyan véges halmaz, hogy $[\mathbf{0}, z] \subseteq \bigcup_{i\in J_z} \Omega_i$.

Ekkor $]z,c] \subseteq]x,\to[= \mathscr{I} \subseteq \Omega_{i_c}$, következésképpen

$$[\mathbf{0},c] = [\mathbf{0},z] \cup]z,c] \subseteq [\mathbf{0},z] \cup]x,\to[\subseteq \bigcup_{i \in J_z \cup \{i_c\}} \Omega_i,$$

tehát $c \in A$.

Ezzel igazoltuk, hogy $c \in A$. Legyen $J_c \subseteq I$ olyan véges halmaz, hogy $[\mathbf{0},c] \subseteq \bigcup_{i \in J_c} \Omega_i$.

Most megmutatjuk az 1) és 2) esetek *nem lehetségesek.*

Tegyük fel, hogy $x \in E$ olyan, amelyre $c \in \mathscr{I} =]\leftarrow, x[\subseteq \Omega_{i_c}$. Ekkor $c < x$ és $]c,x[= \emptyset$, különben létezne $y \in]c,x[\subseteq]\leftarrow,x[$, tehát $[\mathbf{0},y] \subseteq]\leftarrow,x[\subseteq \Omega_{i_c}$, így $y \in A$ teljesülne (hiszen $[\mathbf{0},y] \subseteq \bigcup_{i \in \{i_c\}} \Omega_i$), ami lehetetlen, mert ekkor $y \leq c$ teljesülne, ugyanis c felső korlátja A-nak, ugyanakkor $c < y$. Tehát $]c,x[= \emptyset$, ezért

$$[\mathbf{0},x] = [\mathbf{0},c] \cup]c,x[\cup \{x\} = [\mathbf{0},c] \cup \{x\}.$$

Legyen $i_x \in I$ olyan, hogy $x \in \Omega_{i_x}$. Az előző egyenlőség alapján $[\mathbf{0},x] \subseteq \bigcup_{i \in J_c \cup \{i_x\}} \Omega_i$, tehát $x \in A$, ami lehetetlen, mert ekkor $x \leq c$ teljesülne, holott $c < x$. Ezért az 1) eset lehetetlen.

Tegyük fel, hogy $x, y \in E$ olyanok, amelyekre $\mathscr{I} =]x,y[$. Ekkor $]c,y[\subseteq]x,y[\subseteq \Omega_{i_c}$, tehát ha $i_y \in I$ olyan index, hogy $y \in \Omega_{i_y}$, akkor

$$[\mathbf{0},y] = [\mathbf{0},c] \cup]c,y[\cup \{y\} \subseteq \bigcup_{i \in J_c \cup \{i_c, i_y\}} \Omega_i,$$

tehát $y \in A$, ami lehetetlen, mert ekkor $y \leq c$ teljesülne, holott $c < y$. Ezért a 2) eset lehetetlen.

Tehát azt kaptuk, hogy a 3) eset teljesül, vagyis vehetünk olyan $x \in E$ elemet, amelyre $\mathscr{I} =]x,\to[$. Ekkor $]c,\to[\subseteq]x,\to[\subseteq \Omega_{i_c}$, következésképpen

$$[\mathbf{0},\mathbf{1}] = [\mathbf{0},c] \cup]c,\to[\subseteq [\mathbf{0},c] \cup]x,\to[\subseteq \bigcup_{i \in J_c \cup \{i_c\}} \Omega_i,$$

tehát $\mathbf{1} \in A$. Ez azt jelenti, hogy van olyan $J \subseteq I$ véges halmaz, hogy $E = [\mathbf{0},\mathbf{1}] \subseteq \bigcup_{i \in J} \Omega_i$, vagyis $(\Omega_i)_{i \in J}$ véges részbefedése $(\Omega_i)_{i \in I}$-nek. ■

28.1.11. Következmény. *Ha $\alpha \neq 0$ rendszám, akkor az α^+ szukcesszor a rendezéstopológiával ellátva kompakt Hausdorff-tér.*

Bizonyítás. Az α^+ rendezett halmaznak 0 a legkisebb és α a legnagyobb eleme, és ha $A \subseteq \alpha^+$ tetszőleges halmaz, akkor $\bigcup A \subseteq \alpha$ és $\bigcup A$ rendszám, így $\bigcup A \in \alpha^+$, ezért $\bigcup A$ az A halmaznak szuprémuma α^+-ban. ■

28.2. A kompaktság jellemzései

28.2.1. Definíció. *Azt mondjuk, hogy $\mathfrak{C}$* **centrált halmaz***, ha $\mathfrak{C}$ olyan nem üres halmaz, hogy minden $\mathfrak{C}' \subseteq \mathfrak{C}$ nem üres véges halmazra $\bigcap_{C \in \mathfrak{C}'} C \neq \emptyset$. Azt mondjuk, hogy $(E_i)_{i \in I}$* **centrált halmazrendszer***, ha $(E_i)_{i \in I}$ olyan halmazrendszer, hogy $\{E_i | i \in I\}$ centrált halmaz.*

Tehát az $(E_i)_{i\in I}$ halmazrendszer pontosan akkor centrált, ha $I \neq \emptyset$ és minden $J \subseteq I$ nem üres véges halmazra $\bigcap_{j\in J} E_j \neq \emptyset$.

28.2.2. Állítás. *Ha T topologikus tér, akkor a következő állítások ekvivalensek.*

(i) *T kompakt tér.*

(ii) *Minden $\mathfrak{C} \subseteq \mathscr{P}(T)$ centrált halmazra $\bigcap_{C\in\mathfrak{C}} \overline{C} \neq \emptyset$.*

(iii) *Minden $\mathfrak{R} \subseteq \mathscr{P}(T)$ rácsra $\bigcap_{R\in\mathfrak{R}} \overline{R} \neq \emptyset$.*

(iv) *Ha $(F_i)_{i\in I}$ a T zárt részhalmazainak nem üres lefelé irányított rendszere (vagyis minden $j,k \in I$ esetén van olyan $i \in I$, hogy $F_i \subseteq F_j \cap F_k$) és $\bigcap_{i\in I} F_i = \emptyset$, akkor van olyan $i \in I$, hogy $F_i = \emptyset$.*

(v) *Ha $(\Omega_i)_{i\in I}$ a T nyílt részhalmazainak felfelé irányított rendszere (vagyis minden $j,k \in I$ esetén van olyan $i \in I$, hogy $\Omega_j \cup \Omega_k \subseteq \Omega_i$) és $\bigcup_{i\in I} \Omega_i = T$, akkor van olyan $i \in I$, hogy $\Omega_i = T$.*

Bizonyítás. (i)$\Rightarrow$(ii) Tegyük fel, hogy T kompakt tér és $\mathfrak{C} \subseteq \mathscr{P}(T)$ centrált halmaz. Indirekt bizonyítunk, tehát feltesszük, hogy $\bigcap_{C\in\mathfrak{C}} \overline{C} = \emptyset$. Ekkor $T \neq \emptyset$ és a $(T \setminus \overline{C})_{C\in\mathfrak{C}}$ rendszer nyílt befedése T-nek, ezért van olyan $\mathfrak{C}' \subseteq \mathfrak{C}$ véges halmaz, amelyre $T = \bigcup_{C\in\mathfrak{C}'} (T \setminus \overline{C})$. De $T \neq \emptyset$, ezért $\mathfrak{C}' \neq \emptyset$, így $T = \bigcup_{C\in\mathfrak{C}'} (T \setminus \overline{C}) = T \setminus \left(\bigcap_{C\in\mathfrak{C}'} \overline{C} \right)$, vagyis $\bigcap_{C\in\mathfrak{C}'} \overline{C} = \emptyset$. Ugyanakkor $\bigcap_{C\in\mathfrak{C}'} C \subseteq \bigcap_{C\in\mathfrak{C}'} \overline{C}$, ezért $\bigcap_{C\in\mathfrak{C}'} C = \emptyset$ is teljesül, ami ellentmond annak, hogy $\mathfrak{C}$ centrált. Tehát, ha T kompakt tér és $\mathfrak{C} \subseteq \mathscr{P}(T)$ centrált halmaz, akkor $\bigcap_{C\in\mathfrak{C}} \overline{C} \neq \emptyset$.

(ii)$\Rightarrow$(iii) Nyilvánvaló, mert minden rács centrált halmaz.

(iii)$\Rightarrow$(iv) Indirekt bizonyítunk, tehát feltesszük, hogy az $(F_i)_{i\in I}$ halmazrendszerre teljesülnek a (iv) állítás feltételei, de minden $I \ni i$-re $F_i \neq \emptyset$. Ekkor az $\{F_i | i \in I\}$ halmaz a T zárt részhalmazaiból álló rács, tehát a (iii) alapján $\bigcap_{i\in I} F_i \neq \emptyset$, ami ellentmond a $\bigcap_{i\in I} F_i = \emptyset$ hipotézisnek.

(iv)$\Rightarrow$(v) Indirekt bizonyítunk, tehát feltesszük, hogy az $(\Omega_i)_{i\in I}$ halmazrendszerre teljesülnek az (v) állítás feltételei, de minden $I \ni i$-re $\Omega_i \neq T$. Ekkor a $(T \setminus \Omega_i)_{i\in I}$ nem üres halmazrendszer nyilvánvalóan lefelé irányított, és mindegyik tagja nem üres zárt halmaz T-ben. Ezért a (iv) alapján $\bigcap_{i\in I}(T \setminus \Omega_i) = \emptyset$ lehetetlen, így a de Morgan egyenlőség szerint $\bigcup_{i\in I} \Omega_i \neq T$, ami ellentmond a $\bigcup_{i\in I} \Omega_i = T$ feltételnek.

(v)$\Rightarrow$(i) Legyen $(\Omega_i)_{i\in I}$ nyílt befedése T-nek és A az I nem üres véges részhalmazainak halmaza (ami nem üres, mert $\emptyset \in A$). Minden $A \ni \alpha$-ra legyen $U_\alpha := \bigcup_{i\in\alpha} \Omega_i$. Ekkor $\alpha, \beta \in A$ esetén a $\gamma := \alpha \cup \beta$ halmazra $\gamma \in A$ és $U_\alpha \cup U_\beta = U_\gamma$ teljesül, tehát az $(U_\alpha)_{\alpha\in A}$

halmazrendszer felfelé irányított. Ugyanakkor $\bigcup_{\alpha\in A} U_\alpha := \bigcup_{\alpha\in A}\left(\bigcup_{i\in\alpha}\Omega_i\right) = \bigcup_{i\in I}\Omega_i = T$. Tehát az $(U_\alpha)_{\alpha\in A}$ halmazrendszer nem üres, felfelé irányított és nyílt befedése T-nek. Ezért az (v) alapján van olyan $\alpha\in A$, hogy $T = U_\alpha := \bigcup_{i\in\alpha}\Omega_i$, vagyis $(\Omega_i)_{i\in\alpha}$ véges részbefedés. Ez azt jelenti, hogy T kompakt tér. ■

Példa. Legyen T tetszőleges halmaz és

$$\mathscr{T} := \{\emptyset\}\cup\{\ \Omega\in\mathscr{P}(T) \mid T\setminus\Omega \text{ véges halmaz }\}.$$

Ekkor $\mathscr{T}$ topológia T felett, és $(T,\mathscr{T})$ kompakt tér. Valóban, $\mathscr{T}$-re $(\mathrm{O_I})$ teljesül, és ha $(\Omega_i)_{i\in I}$ nem üres véges rendszer $\mathscr{T}$-ben, és minden $I\ni i$-re $\Omega_i\neq\emptyset$, akkor $T\setminus\left(\bigcap_{i\in I}\Omega_i\right) = \bigcup_{i\in I}(T\setminus\Omega_i)$ véges halmaz T-ben, tehát $\bigcap_{i\in I}\Omega_i\in\mathscr{T}$, hiszen véges sok véges halmaz uniója véges, így $\mathscr{T}$-re $(\mathrm{O_{II}})$ is teljesül. Ha $(\Omega_i)_{i\in I}$ tetszőleges nem üres rendszer $\mathscr{T}$-ben és van olyan $i\in I$, hogy $\Omega_i\neq\emptyset$, akkor $T\setminus\left(\bigcup_{i\in I}\Omega_i\right) = \bigcap_{i\in I}(T\setminus\Omega_i)$, tehát $\bigcup_{i\in I}\Omega_i\in\mathscr{T}$, hiszen véges halmaz minden részhalmaza véges, így $\mathscr{T}$-re $(\mathrm{O_{III}})$ is teljesül. Tehát $\mathscr{T}$ topológia T felett, és könnyen látható, hogy egy $F\subseteq T$ halmaz pontosan akkor $\mathscr{T}$-zárt, ha $F = T$ vagy F véges. A $(T,\mathscr{T})$ topologikus tér kompaktságának bizonyításához legyen $(F_i)_{i\in I}$ a T nem üres $\mathscr{T}$-zárt halmazainak tetszőleges lefelé irányított nem üres rendszere; azt kell igazolni, hogy $\bigcap_{i\in I}F_i\neq\emptyset$. Legyen $I_0 := \{i\in I|F_i\neq T\}$. Ha $I_0=\emptyset$, akkor $\bigcap_{i\in I}F_i = T\neq\emptyset$, ezért feltehető, hogy $I_0\neq\emptyset$. Természetesen ekkor $\bigcap_{i\in I}F_i = \bigcap_{i\in I_0}F_i$ teljesül, és minden $I_0\ni i$-re F_i véges halmaz. A $\{\mathrm{Card}(F_i)|i\in I\}\subseteq\mathbb{N}$ halmaz nem üres, ezért van olyan $i_0\in I_0$, hogy minden $I_0\ni i$-re $\mathrm{Card}(F_{i_0})\leq\mathrm{Card}(F_i)$. Ha $i\in I_0$, akkor van olyan $j\in I$, hogy $F_j\subseteq F_{i_0}\cap F_i$, így $F_j\subseteq F_{i_0}$, tehát $\mathrm{Card}(F_j)=\mathrm{Card}(F_{i_0})$, vagyis $F_{i_0}=F_j\subseteq F_i$. Ebből következik, hogy $\bigcap_{i\in I_0}F_i = F_{i_0}\neq\emptyset$, így $(T,\mathscr{T})$ kompakt tér. Világos, hogy a $(T,\mathscr{T})$ topologikus tér $\mathrm{T_1}$-tér, mert a T minden egy elemű (sőt véges) részhalmaza zárt $\mathscr{T}$ szerint. Ha T véges, akkor $\mathscr{T}$ egyenlő a T feletti diszkrét topológiával. Azonban végtelen T esetében a $(T,\mathscr{T})$ topologikus tér nem Hausdorff-tér (de kompakt $\mathrm{T_1}$-tér). Legyenek ugyanis $t,t'\in T$ olyan pontok, hogy $t\neq t'$. Tegyük fel olyan diszjunkt $\Omega,\Omega'\in\mathscr{T}$ halmazok létezését, amelyekre $t\in\Omega$ és $t'\in\Omega'$. Ekkor $\Omega\neq T$, mert $t'\notin\Omega$, így $T\setminus\Omega$ véges halmaz és $\Omega'\subseteq T\setminus\Omega$, ezért Ω' véges. Hasonlóan, $\Omega'\neq T$, mert $t\notin\Omega'$, így $T\setminus\Omega'$ véges halmaz és $\Omega\subseteq T\setminus\Omega'$, ezért Ω véges. Ebből következik, hogy a $T=\Omega\cup(T\setminus\Omega)$ halmaz is véges. Tehát, ha T végtelen, akkor T nem Hausdorff-tér.

28.2.3. Tétel. (Cantor-féle közösrész-tétel) *Legyen T topologikus tér és $(K_\alpha)_{\alpha\in A}$ a T nem üres, zárt és kompakt részhalmazainak lefelé irányított nem üres rendszere. Ekkor $\bigcap_{\alpha\in A}K_\alpha\neq\emptyset$.*

Bizonyítás. Legyen $\alpha_*\in A$ rögzített. Ha $A'\subseteq A$ nem üres véges halmaz, akkor a $(K_\alpha)_{\alpha\in A}$ halmazrendszer lefelé irányítottsága miatt van olyan $\beta\in A$, hogy $K_\beta\subseteq\bigcap_{\alpha\in A'}K_\alpha$, tehát $\emptyset\neq K_\beta\cap K_{\alpha_*}\subseteq\bigcap_{\alpha\in A'}(K_\alpha\cap K_{\alpha_*})$. Ezért a $\{K_\alpha\cap K_{\alpha_*}|\alpha\in A\}$ halmaz *centrált.* Minden $A\ni\alpha$-ra a $K_\alpha\cap K_{\alpha_*}$ halmaz kompakt és zárt T-ben (mert K_α és K_{α_*} mindketten zártak és kompaktak), ezért $K_\alpha \cap K_{\alpha_*}$ kompakt a K_{α_*} kompakt topologikus altérben is, így az 28.2.2. állítás (ii) pontja szerint $\emptyset \neq \bigcap\limits_{\alpha\in A} \overline{K_\alpha \cap K_{\alpha_*}} = \bigcap\limits_{\alpha\in A} (K_\alpha \cap K_{\alpha_*}) \subseteq \bigcap\limits_{\alpha\in A} K_\alpha$. ■

28.2.4. Tétel. (Bolzano–Weierstrass-tétel) *A T topologikus tér pontosan akkor kompakt, ha minden T-ben haladó általánosított sorozatnak létezik olyan általánosított részsorozata, amely konvergens T-ben.*

Bizonyítás. Tegyük fel, hogy T kompakt, és legyen $(t_i)_{i\in I}$ tetszőleges T-ben haladó általánosított sorozat. Minden $I \ni i$-re legyen $F_i := \overline{\{t_j|(j\in I)\wedge(j\geq i)\}}$. Ekkor az $(F_i)_{i\in I}$ halmazrendszer minden tagja nem üres zárt halmaz T-ben, és az I halmaz felfelé irányítottsága miatt minden $i_1, i_2 \in I$ esetén van olyan $i \in I$, hogy $F_i \subseteq F_{i_1}$ és $F_i \subseteq F_{i_2}$; vagyis az $(F_i)_{i\in I}$ rendszer a tartalmazás tekintetében lefelé irányított. Minden $i \in I$ esetén F_i kompakt T-ben, mert zárt és T kompakt. A Cantor-féle közösrész-tétel alapján $\bigcap\limits_{i\in I} F_i \neq \emptyset$. Megmutatjuk, hogy bármely $t \in \bigcap\limits_{i\in I} F_i$ ponthoz létezik a $(t_i)_{i\in I}$-nek olyan általánosított részsorozata, amely t-hez konvergál.

Valóban, legyen $t \in \bigcap\limits_{i\in I} F_i$ rögzített, $\mathfrak{F}$ a t pont környezeteinek halmaza T-ben, és $J := \{(i,V)|(V\in\mathfrak{F})\wedge(t_i\in V)\}$. A J halmazon bevezetjük a $\leq$ relációt úgy, hogy $(i_1,V_1),(i_2,V_2) \in J$ esetén $(i_1,V_1) \leq (i_2,V_2)$ definíció szerint jelentse azt, hogy $i_1 \leq i_2$ és $V_1 \supseteq V_2$. Az I felfelé irányítottsága és az $\mathfrak{F}$ szűrő tartalmazás szerinti lefelé irányítottsága miatt J a $\leq$ relációval ellátva felfelé irányított előrendezett halmaz. Értelmezzük most a $\sigma : J \to I$; $(i,V) \mapsto i$ leképezést; ez nyilvánvalóan monoton növő függvény. Az $\mathrm{Im}(\sigma)$ halmaz nyilvánvalóan kofinális I-vel, mert $i \in I$ esetén $(i,T) \in J$ olyan, hogy $\sigma((i,T)) := i$ (tehát még $\mathrm{Im}(\sigma) = I$ is igaz). Ezért $\left(t_{\sigma(j)}\right)_{j\in J}$ általánosított részsorozata $(t_i)_{i\in I}$-nek. Megmutatjuk, hogy a $\left(t_{\sigma(j)}\right)_{j\in J}$ általánosított sorozat konvergál t-hez T-ben. Valóban, ha V a t-nek környezete T-ben, azaz $V \in \mathfrak{F}$, akkor van olyan $i_V \in I$, hogy $(i_V,V) \in J$, mert $I \neq \emptyset$, és ha $i_0 \in I$ rögzített, akkor $t \in F_{i_0} := \overline{\{t_i|(i\in I)\wedge(i\geq i_0)\}}$ miatt $V \cap \{t_i|(i\in I)\wedge(i\geq i_0)\} \neq \emptyset$, így van olyan $i \in I$, hogy $t_i \in V$, azaz $(i,V) \in J$. Ha $(i_V,V) \in J$, akkor $(i,W) \in J$ és $(i_V,V) \leq (i,W)$ esetén $t_{\sigma(i,W)} = t_i \in W \subseteq V$. Ez azt jelenti, hogy a $\left(t_{\sigma(j)}\right)_{j\in J}$ általánosított sorozat konvergál t-hez T-ben.

Megfordítva, tegyük fel, hogy minden T-ben haladó általánosított sorozatnak létezik konvergens általánosított részsorozata. Legyen $(F_i)_{i\in I}$ a T nem üres zárt részhalmazainak nem üres, tartalmazás tekintetében lefelé irányított rendszere; megmutatjuk, hogy ekkor $\bigcap\limits_{i\in I} F_i \neq \emptyset$. Ehhez először a kiválasztási axióma alkalmazásával veszünk egy $(t_i)_{i\in I} \in \prod\limits_{i\in I} F_i$ rendszert, és az I halmazon bevezetjük a $\leq$ relációt úgy, hogy $i_1, i_2 \in I$ esetén $i_1 \leq i_2$ azt jelentse, hogy $F_{i_1} \supseteq F_{i_2}$. Természetesen ekkor I a $\leq$ relációval ellátva felfelé irányított előrendezett halmaz (amelyen a $\leq$ előrendezés nem szükségképpen antiszimmetrikus), tehát $(t_i)_{i\in I}$ általánosított sorozat T-ben. A feltevés alapján létezik olyan J felfelé irányított előrendezett halmaz és olyan $\sigma : J \to I$ monoton növő függvény, hogy az $\mathrm{Im}(\sigma)$ halmaz kofinális I-vel, és a $(t_{\sigma(j)})_{j\in J}$ általánosított sorozat konvergál T-ben egy t ponthoz. Állítjuk, hogy bármely ilyen t pontra $t \in \bigcap\limits_{i\in I} F_i$ teljesül, vagyis minden $I \ni i$-re $t \in F_i$, ami az F_i halmaz zártsága miatt azzal ekvivalens, hogy a t minden V környezetére $V \cap F_i \neq \emptyset$. Legyen ugyanis V környezete t-nek és $i \in I$. A hipotézis szerint a $(t_{\sigma(j)})_{j\in J}$ általánosított sorozat konvergál T-ben t-hez, ezért létezik olyan $j_1 \in J$, hogy minden $j \in J$ esetén, ha $j \geq j_1$, akkor $t_{\sigma(j)} \in V$. Az $\mathrm{Im}(\sigma)$ halmaz kofinális I-vel, ezért az i-hez van olyan $j_2 \in J$, hogy $\sigma(j_2) \geq i$. A J halmaz előrendezése felfelé irányított, ezért van olyan $j_0 \in J$, hogy $j_0 \geq j_1$ és $j_0 \geq j_2$. Ekkor $j \in J$ és $j \geq j_0$ esetén $j \geq j_1$, tehát $t_{\sigma(j)} \in V$, és a σ monoton növése miatt $\sigma(j) \geq \sigma(j_2) \geq i$, következésképpen az I halmazon adott előrendezés definíciója alapján $t_{\sigma(j)} \in F_{\sigma(j)} \subseteq F_i$, így $t_{\sigma(j)} \in V \cap F_i$. ■

28.2.5. Következmény. *Legyen T topologikus tér és $K \subseteq T$.*

a) *A K halmaz pontosan akkor kompakt, ha minden K-ban haladó általánosított sorozatnak van olyan konvergens általánosított részsorozata, amelynek létezik K-ba eső limeszpontja.*

b) *A K halmaz pontosan akkor zárt és kompakt, ha minden K-ban haladó általánosított sorozatnak van olyan konvergens általánosított részsorozata, amelynek minden limeszpontja K-ba esik.*

Bizonyítás. a) Ha $\mathscr{T}$ jelöli a T topológiáját, akkor a $K \subseteq T$ halmaz $\mathscr{T}$ szerinti kompaktsága azt jelenti, hogy a $(K, \mathscr{T}|K)$ topologikus altér kompakt. Ugyanakkor a "minden K-ban haladó általánosított sorozatnak van olyan $\mathscr{T}$ szerint konvergens általánosított részsorozata, amelynek létezik K-ba eső limeszpontja" kijelentés ekvivalens azzal, hogy minden K-ban haladó általánosított sorozatnak létezik $\mathscr{T}|K$ szerint konvergens általánosított részsorozata. Ezért a 28.2.4. tételt alkalmazva $(T, \mathscr{T})$ helyett a $(K, \mathscr{T}|K)$ topologikus altérre azonnal kapjuk a)-t.

b) Legyen K zárt és kompakt halmaz, és $(t_i)_{i\in I}$ tetszőleges K-ban haladó általánosított sorozat. Ekkor a) alapján van olyan $(t'_j)_{j\in J}$ általánosított részsorozata $(t_i)_{i\in I}$-nek, amelynek valamelyik limeszpontja K-nak eleme. De a $(t'_j)_{j\in J}$ általánosított sorozat minden limeszpontja eleme $\overline{K}$-nak, vagyis K-nak. Tehát $(t_i)_{i\in I}$-nek van olyan konvergens általánosított részsorozata, amelynek minden limeszpontja K-ba esik.

Megfordítva, tegyük fel, hogy minden K-ban haladó általánosított sorozatnak van olyan konvergens általánosított részsorozata, amelynek minden limeszpontja K-ba esik. Az a) állítás alapján K kompakt, ezért csak K zártságát kell igazolni. Legyen $t \in \overline{K}$, és vegyünk olyan K-ban haladó $(t_i)_{i\in I}$ általánosított sorozatot, amely t-hez konvergál. Azt kell megmutatni, hogy $t \in K$. A hipotézis alapján vehetünk olyan $(t'_j)_{j\in J}$ általánosított részsorozata $(t_i)_{i\in I}$-nek, amelynek minden limeszpontja eleme K-nak. De $(t_i)_{i\in I}$ minden limeszpontja (így t is) limeszpontja $(t'_j)_{j\in J}$-nek is, ezért $t \in K$. ■

28.2.6. Állítás. *Ha T M_1-tér és $K \subseteq T$ zárt kompakt halmaz, akkor minden K-ban haladó sorozatnak létezik konvergens részsorozata.*

Bizonyítás. Legyen $(t_n)_{n\in\mathbb{N}}$ egy K-ban haladó sorozat, és minden $n \in \mathbb{N}$ számra legyen $K_n := \overline{\{t_k | k > n\}}$. Világos, hogy $(K_n)_{n\in\mathbb{N}}$ nem üres, zárt és kompakt halmazok monoton fogyó sorozata (28.1.4.), így a Cantor-féle közösrész-tétel (28.2.3.) szerint $\bigcap_{n\in\mathbb{N}} K_n \neq \emptyset$.

Legyen $t \in \bigcap_{n\in\mathbb{N}} K_n$ és vegyük t környezeteinek olyan $(V_n)_{n\in\mathbb{N}}$ sorozatát, amely tartalmazás tekintetében monoton fogyó és $\{V_n | n \in \mathbb{N}\}$ környezetbázisa t-nek. Ekkor minden $n \in \mathbb{N}$ esetén $t \in K_n = \overline{\{t_k | k > n\}}$ és V_n környezete t-nek, így $V_n \cap \{t_k | k > n\} \neq \emptyset$, tehát létezik olyan $k \in \mathbb{N}$, hogy $k > n$ és $t_k \in V_n$. Vezessük be az

$$f : \mathbb{N} \to \mathbb{N}; \quad n \mapsto \min\{k \in \mathbb{N} | (k > n) \wedge (t_k \in V_n)\}$$

leképezést, és jelölje σ a 0 kezdőpont és f által meghatározott iterációs sorozatot. Ekkor $\sigma : \mathbb{N} \to \mathbb{N}$ olyan függvény, hogy minden $n \in \mathbb{N}$ esetén $\sigma(n + 1) = f(\sigma(n)) \in \{k \in$

$\mathbb{N}|(k > \sigma(n)) \wedge (t_k \in V_{\sigma(n)})\}$, tehát $\sigma(n+1) > \sigma(n)$ és $t_{\sigma(n+1)} \in V_{\sigma(n)}$. Ezért $\sigma : \mathbb{N} \to \mathbb{N}$ szigorúan monoton növő függvény. Megmutatjuk, hogy a $\left(t_{\sigma(n+1)}\right)_{n\in\mathbb{N}}$ sorozat konvergál t-hez T-ben. Valóban, legyen V tetszőleges környezete t-nek T-ben. Mivel $\{V_n|n \in \mathbb{N}\}$ környezetbázisa t-nek, így vehetünk olyan $N \in \mathbb{N}$ számot, amelyre $V_N \subseteq V$. Ha $n \in \mathbb{N}$ és $n \geq N$, akkor $\sigma(n) \geq n$ miatt $t_{\sigma(n+1)} \in V_{\sigma(n)} \subseteq V_n \subseteq V_N \subseteq V$. Ez azt jelenti, hogy $\left(t_{\sigma(n+1)}\right)_{n\in\mathbb{N}}$ olyan részsorozata $(t_n)_{n\in\mathbb{N}}$-nek, amely t-hez konvergál T-ben. ■

28.3. Kompakt terek szorzata – Tyihonov-tétel

28.3.1. Lemma. *Ha T halmaz és $\mathfrak{C} \subseteq \mathscr{P}(T)$ centrált halmaz, akkor létezik olyan T feletti $\mathfrak{F}$ szűrő, amely tartalmazza $\mathfrak{C}$-t és egyetlen olyan T feletti szűrőnek sem valódi része, amely tartalmazza $\mathfrak{C}$-t (vagyis $\mathfrak{F}$ tartalmazás tekintében maximális $\mathfrak{C}$-t tartalmazó T feletti szűrő).*

Bizonyítás. Jelölje $\mathfrak{F}_{\mathfrak{C}}$ azon $E \subseteq T$ halmazok halmazát, amelyekhez van olyan $\mathfrak{C}' \subseteq \mathfrak{C}$ nem üres véges halmaz, hogy $\bigcap_{C\in\mathfrak{C}'} C \subseteq E$. Könnyen látható, hogy $\mathfrak{F}_{\mathfrak{C}}$ szűrő T felett és $\mathfrak{C} \subseteq \mathfrak{F}_{\mathfrak{C}}$, sőt az is nyilvánvaló, hogy $\mathfrak{F}_{\mathfrak{C}}$ a tartalmazás tekintetében legkisebb T feletti szűrő, amely $\mathfrak{C}$-t tartalmazza. Tehát *létezik* T feletti szűrő, amely $\mathfrak{C}$-t tartalmazza, vagyis $\mathfrak{S} := \{\mathfrak{F}|\mathfrak{F}$ szűrő T felett és $\mathfrak{C} \subseteq \mathfrak{F}\}$ nem üres halmaz. Az $\mathfrak{S}$ halmazt a $\subseteq$ relációval rendezzük, és megmutatjuk, hogy ez a rendezett halmaz *induktívan* rendezett; ekkor a Zorn-lemma alapján létezik $\mathfrak{S}$-nek maximális eleme, ami olyan szűrő lesz T felett, amelynek a létezését állítottuk.

Legyen $(\mathfrak{F}_i)_{i\in I}$ olyan $\mathfrak{S}$-ben haladó nem üres rendszer, amelyre minden $i, j \in I$ esetén $\mathfrak{F}_i \subseteq \mathfrak{F}_j$ vagy $\mathfrak{F}_j \subseteq \mathfrak{F}_i$. Értelmezzük az $\mathfrak{F} := \bigcup_{i\in I} \mathfrak{F}_i$ halmazt; megmutatjuk, hogy $\mathfrak{F} \in \mathfrak{S}$. Ha $F_1, F_2 \in \mathfrak{F}$, akkor van olyan $i_1 \in I$ és $i_2 \in I$, hogy $F_1 \in \mathfrak{F}_{i_1}$ és $F_2 \in \mathfrak{F}_{i_2}$; ekkor $\mathfrak{F}_{i_1} \subseteq \mathfrak{F}_{i_2}$ esetén $F_1, F_2 \in \mathfrak{F}_{i_2}$, így $F_1 \cap F_2 \in \mathfrak{F}_{i_2} \subseteq \mathfrak{F}$, illetve $\mathfrak{F}_{i_2} \subseteq \mathfrak{F}_{i_1}$ esetén $F_1, F_2 \in \mathfrak{F}_{i_1}$, így $F_1 \cap F_2 \in \mathfrak{F}_{i_1} \subseteq \mathfrak{F}$. Továbbá, ha $E \subseteq T$ olyan halmaz, amelyhez van olyan $F \in \mathfrak{F}$, hogy $F \subseteq E$, akkor van olyan $i \in I$, hogy $F \in \mathfrak{F}_i$, így $E \in \mathfrak{F}_i \subseteq \mathfrak{F}$, hiszen $\mathfrak{F}_i$ szűrő T felett. Minden $I \ni i$-re $\emptyset \notin \mathfrak{F}_i$, ezért $\emptyset \notin \mathfrak{F}$. Végül, $I \neq \emptyset$ miatt $\mathfrak{C} \subseteq \mathfrak{F}$. Nyilvánvaló, hogy ekkor az $\mathfrak{F}$ szűrő a tartalmazás tekintetében felső korlátja az $(\mathfrak{F}_i)_{i\in I}$ rendszernek az $\mathfrak{S}$ rendezett halmazban. ■

28.3.2. Tétel. (Tyihonov-tétel) *Kompakt terek topologikus szorzata kompakt tér.*

Bizonyítás. Legyen $(T_i)_{i\in I}$ kompakt terek tetszőleges rendszere, $T := \prod_{i\in I} T_i$, és $\mathfrak{C} \subseteq \mathscr{P}(T)$ centrált halmaz. Bebizonyítjuk, hogy $\bigcap_{C\in\mathfrak{C}} \overline{C} \neq \emptyset$, ami azt jelenti, hogy a T topologikus szorzattér kompakt.

Az előző lemma alapján vehetünk olyan T feletti $\mathfrak{F}$ szűrőt, hogy $\mathfrak{C} \subseteq \mathfrak{F}$ és $\mathfrak{F}$ egyetlen $\mathfrak{C}$-t tartalmazó T feletti szűrőnek sem valódi része. Ha $E \subseteq T$ olyan halmaz, hogy minden $\mathfrak{F} \ni F$-re $E \cap F \neq \emptyset$, akkor $E \in \mathfrak{F}$, hiszen ekkor $\{E\} \cup \mathfrak{F} \subseteq \mathscr{P}(T)$ centrált halmaz, tehát létezik olyan T feletti $\mathfrak{F}'$ szűrő, hogy $\{E\} \cup \mathfrak{F} \subseteq \mathfrak{F}'$; ekkor az $\mathfrak{F}$ maximalitása folytán $\mathfrak{F}' = \mathfrak{F}$, tehát $E \in \mathfrak{F}$, mert $E \in \mathfrak{F}'$ nyilvánvalóan igaz.

Megmutatjuk, hogy

$$\prod_{i\in I} \Big(\bigcap_{F\in\mathfrak{F}} \overline{\mathrm{pr}_i\langle F\rangle} \Big) \subseteq \bigcap_{F\in\mathfrak{F}} \overline{F} \subseteq \bigcap_{C\in\mathfrak{C}} \overline{C}.$$

Legyen $t \in \prod_{i\in I}\left(\bigcap_{F\in\mathfrak{F}} \overline{\mathrm{pr}_i\langle F\rangle}\right)$ rögzített pont, $F \in \mathfrak{F}$ és V a t-nek környezete a T topologikus szorzattérben; azt kell igazolni, hogy $V \cap F \neq \emptyset$. A szorzattopológia definíciója szerint van olyan $J \subseteq I$ nem üres véges halmaz és olyan $(V_i)_{i\in J}$ rendszer, hogy minden $J \ni i$-re V_i környezete $\mathrm{pr}_i(t)$-nek T_i-ben és $\bigcap_{i\in J} \overset{-1}{\mathrm{pr}_i}\langle V_i\rangle \subseteq V$. Ha $i \in J$, akkor minden $E \in \mathfrak{F}$ esetén $\mathrm{pr}_i(t) \in \overline{\mathrm{pr}_i\langle E\rangle}$, ezért $V_i \cap \mathrm{pr}_i\langle E\rangle \neq \emptyset$. Ez azt jelenti, hogy $i \in J$ esetén minden $\mathfrak{F} \ni E$-re $E \cap \overset{-1}{\mathrm{pr}_i}\langle V_i\rangle \neq \emptyset$, így $\overset{-1}{\mathrm{pr}_i}\langle V_i\rangle \in \mathfrak{F}$, ezért a J végessége folytán $\bigcap_{i\in J} \overset{-1}{\mathrm{pr}_i}\langle V_i\rangle \in \mathfrak{F}$. Ebből következik, hogy $V \in \mathfrak{F}$, mert $\mathfrak{F}$ szűrő T felett, így $V \cap F \neq \emptyset$.

Végül igazoljuk, hogy $\prod_{i\in I}\left(\bigcap_{F\in\mathfrak{F}} \overline{\mathrm{pr}_i\langle F\rangle}\right) \neq \emptyset$. Minden $I \ni i$-re a $\{\mathrm{pr}_i\langle F\rangle | F \in \mathfrak{F}\}$ halmaz centrált részhalmaza $\mathscr{P}(T_i)$-nek, mert minden $\mathfrak{F}$-ben haladó $(F_j)_{j\in J}$ nem üres véges rendszerre $F := \bigcap_{j\in J} F_j \in \mathfrak{F}$, tehát $F \neq \emptyset$, így $\emptyset \neq \mathrm{pr}_i\langle F\rangle \subseteq \bigcap_{j\in J} \mathrm{pr}_i\langle F_j\rangle$. Tehát $i \in I$ esetén a T_i kompaktsága miatt $\bigcap_{F\in\mathfrak{F}} \overline{\mathrm{pr}_i\langle F\rangle} \neq \emptyset$. Ebből a kiválasztási axióma alkalmazásával kapjuk, hogy $\prod_{i\in I}\left(\bigcap_{F\in\mathfrak{F}} \overline{\mathrm{pr}_i\langle F\rangle}\right) \neq \emptyset$. ■

28.3.3. Következmény. *Ha T kompakt tér és I halmaz, akkor a T^I topologikus kocka kompakt tér. Ha T metrizálható kompakt tér és I megszámlálható halmaz, akkor a T^I topologikus kocka szintén metrizálható kompakt tér. A $[0,1]^{\mathbb{N}}$ euklidészi kocka metrizálható kompakt tér.*

Bizonyítás. Az első állítás a Tyihonov-tételből és a topologikus kockák értelmezéséből következik. Metrizálható terek megszámlálható rendszerének a topologikus szorzata metrizálható, ezért a második állítás következik az elsőből. A harmadik állítás következik a másodikból és abból, hogy a $[0,1] \subseteq \mathbb{R}$ intervallum (az euklidészi topológiával) metrizálható kompakt tér. ■

28.4. Félig folytonos függvények – Weierstrass-féle maximum-minimum elv

28.4.1. Tétel. (Weierstrass-féle maximum-minimum elv) *Ha T topologikus tér, $f : T \to \mathbb{R}$ folytonos függvény és $K \subseteq T$ nem üres kompakt halmaz, akkor* $\inf(f\langle K\rangle) \in f\langle K\rangle$ *és* $\sup(f\langle K\rangle) \in f\langle K\rangle$, *vagyis f a K halmazban minimális és maximális értéket is felvesz.*

Bizonyítás. A 28.1.8. állításból következik, hogy $f\langle K\rangle$ kompakt halmaz $\mathbb{R}$-ben az $\mathscr{E}_{\mathbb{R}}$ topológia szerint, és $(\mathbb{R}, \mathscr{E}_{\mathbb{R}})$ Hausdorff-tér, tehát 28.1.4. alapján $f\langle K\rangle$ zárt halmaz $\mathbb{R}$-ben, így $\overline{f\langle K\rangle} = f\langle K\rangle$. Az infimum és szuprémum definíciója, valamint az $\mathscr{E}_{\mathbb{R}}$ topológia értelmezése alapján $\inf(f\langle K\rangle) \in \overline{f\langle K\rangle}$ és $\sup(f\langle K\rangle) \in \overline{f\langle K\rangle}$. ■

Most általánosítani fogjuk a Weierstrass-féle maximum-minimum elvet. Ehhez bevezetjük az alulról- és a felülről félig folytonos függvények fogalmát. Látni fogjuk majd, hogy az alulról félig folytonos függvények fontos szerepet játszanak a topologikus integrálelméletben (**RAD**).

28.4.2. Definíció. *Ha T topologikus tér és $f : T \to \overline{\mathbb{R}}$ függvény, akkor azt mondjuk, hogy f* **alulról** (*illetve* **felülről**) **félig folytonos**, *ha minden $c \in \mathbb{R}$ esetén az $[f > c]$ (illetve $[f < c]$) halmaz nyílt T-ben. A pozitív $T \to \overline{\mathbb{R}}$ alulról félig folytonos függvények halmazát $\mathscr{I}_+(T)$ jelöli.*

Megjegyzések. 1) A definíció alapján nyilvánvaló, hogy ha T topologikus tér, akkor az $f : T \to \overline{\mathbb{R}}$ függvény pontosan akkor alulról (illetve felülről) félig folytonos, ha a $-f$ függvény felülről (illetve alulról) félig folytonos, hiszen minden $c \in \mathbb{R}$ esetén $[f > c] = [-f < -c]$.

2) Könnyen látható, hogy ha T topologikus tér, akkor az $f : T \to \mathbb{R}$ függvény pontosan akkor folytonos, ha alulról is és felülről is félig folytonos. Valóban, a feltétel szükségessége a folytonosság topologikus jellemzéséből következik, míg az elégségesség azért igaz, mert ha f alulról is és felülről is félig folytonos, akkor minden $a, b \in \mathbb{R}$ esetén $\overset{-1}{f}\langle]a, b[\rangle = [f > a] \cap [f < b]$ nyílt halmaz T-ben, ezért minden $\Omega \subseteq \mathbb{R}$ nyílt halmazra $\overset{-1}{f}\langle \Omega \rangle$ nyílt halmaz T-ben, hiszen $\mathbb{R}$-ben minden nyílt halmaz előáll korlátos nyílt intervallumok uniójaként.

3) Ha T topologikus tér és $E \subseteq T$, akkor a $\chi_E : T \to \mathbb{R}$ karakterisztikus függvény pontosan akkor alulról (illetve felülről) félig folytonos, ha E nyílt (illetve zárt) halmaz T-ben. Speciálisan, a $\chi_E : T \to \mathbb{R}$ karakterisztikus függvény pontosan akkor folytonos, ha E nyílt-zárt halmaz T-ben.

4) Ha T topologikus tér és $(f_i)_{i \in I}$ olyan nem üres függvényrendszer, hogy minden $i \in I$ esetén $f_i : T \to \overline{\mathbb{R}}$ alulról (illetve felülről) félig folytonos függvény, akkor a $\sup\limits_{i \in I} f_i : T \to \overline{\mathbb{R}}$ felső burkoló (illetve az $\inf\limits_{i \in I} f_i : T \to \overline{\mathbb{R}}$ alsó burkoló) szintén alulról (illetve felülről) félig folyonos. Ez nyilvánvalóan következik abból, hogy minden $c \in \mathbb{R}$ esetén $\left[\sup\limits_{i \in I} f_i > c\right] = \bigcup\limits_{i \in I} [f_i > c]$ és $\left[\inf\limits_{i \in I} f_i < c\right] = \bigcup\limits_{i \in I} [f_i < c]$, valamint nyílt halmazok uniója nyílt.

5) Ha T topologikus tér és $(f_i)_{i \in I}$ olyan nem üres *véges* függvényrendszer, hogy minden $i \in I$ esetén $f_i : T \to \overline{\mathbb{R}}$ alulról (illetve felülről) félig folytonos függvény, akkor az $\inf\limits_{i \in I} f_i : T \to \overline{\mathbb{R}}$ alsó burkoló (illetve az $\sup\limits_{i \in I} f_i : T \to \overline{\mathbb{R}}$ felső burkoló) szintén alulról (illetve felülről) félig folyonos. Ez nyilvánvalóan következik abból, hogy I végessége miatt minden $c \in \mathbb{R}$ esetén $\left[\inf\limits_{i \in I} f_i > c\right] = \bigcap\limits_{i \in I} [f_i > c]$ és $\left[\sup\limits_{i \in I} f_i < c\right] = \bigcap\limits_{i \in I} [f_i < c]$, valamint nyílt halmazok nem üres véges rendszerének metszete nyílt.

6) Ha T topologikus tér és $f : T \to \overline{\mathbb{R}}$ alulról (illetve felülről) félig folytonos függvény, akkor minden $\lambda \in \mathbb{R}_+^*$ számra $\lambda.f$ is alulról (illetve felülről) félig folytonos függvény, mert minden $c \in \mathbb{R}$ esetén $[\lambda.f > c] = [f > c\lambda^{-1}]$ és $[\lambda.f < c] = [f < c\lambda^{-1}]$.

7) Legyen T topologikus tér és Q sűrű halmaz $\mathbb{R}$-ben az euklidészi topológia szerint. Ha $f, g : T \to \mathbb{R}$ tetszőleges függvények, akkor az $f + g$ függvényre teljesül az, hogy minden $c \in \mathbb{R}$ esetén

$$[f + g > c] = \bigcup_{\substack{(r,s) \in Q \times Q \\ r+s>c}} \left([f > r] \cap [g > s]\right), \tag{1}$$

$$[f + g < c] = \bigcup_{\substack{(r,s) \in Q \times Q \\ r+s<c}} \left([f < r] \cap [g < s]\right), \tag{2}$$

ezért ha f és g alulról (illetve felülről) félig folytonos függvények, akkor $f+g$ is alulról (illetve felülről) félig folytonos függvény. Az (1) egyenlőség bizonyításához legyen először $t \in T$ olyan, hogy $t \in [f+g>c]$, vagyis $f(t)+g(t)>c$. Ekkor $f(t)>c-g(t)$, így Q sűrűsége miatt van olyan $r \in Q$, hogy $f(t)>r>c-g(t)$. Ebből kapjuk, hogy $g(t)>c-r$, tehát ismét Q sűrűségét alkalmazva vehetünk olyan $s \in Q$ számot, amelyre $g(t)>s>c-r$. Ekkor $(r,s) \in Q \times Q$ olyan pár, hogy $r+s>c$, valamint $f(t)>r$ és $g(t)>s$, vagyis $t \in [f>r] \cap [g>s]$. Ez azt jelenti, hogy $[f+g>c] \subseteq \bigcup\limits_{\substack{(r,s)\in Q\times Q\\ r+s>c}} ([f>r]\cap[g>s])$, ugyanakkor a fordított irányú tartalmazás nyilvánvaló. Tehát (1) teljesül minden $Q \subseteq \mathbb{R}$ sűrű halmazra, $f,g : T \to \mathbb{R}$ függvényre és $c \in \mathbb{R}$ számra. Tehát ha $Q \subseteq \mathbb{R}$ sűrű halmaz, $f,g : T \to \mathbb{R}$ függvények és $c \in \mathbb{R}$, akkor (1) teljesül a $-Q \subseteq \mathbb{R}$ sűrű halmazra, a $-f$ és $-g$ függvényekre és a $-c \in \mathbb{R}$ számra, ami azt jelenti, hogy

$$[f+g<c] = [(-f)+(-g)>-c] = \bigcup_{\substack{(r',s')\in(-Q)\times(-Q)\\ r'+s'>-c}} ([-f>r']\cap[-g>s']) \overset{(*)}{=}$$

$$\overset{(*)}{=} \bigcup_{\substack{(r,s)\in Q\times Q\\ r+s<c}} ([f<r]\cap[g<s]),$$

ahol a $(*)$ egyenlőségnél azt használtuk fel hogy az

$$\{(r,s)\in Q\times Q | r+s<c\} \to \{(r',s')\in(-Q)\times(-Q) | r'+s'>-c\}; \quad (r,s)\mapsto(-r,-s)$$

leképezés bijekció. Ezért (2) is teljesül.

8) A 7) megjegyzésből következik, hogy ha T topologikus tér és $(f_i)_{i\in I}$ olyan $T \to \mathbb{R}$ függvényekből álló nem üres véges rendszer, amelyre minden $i \in I$ esetén f_i alulról (illetve felülről) félig folytonos függvény, akkor a $\sum\limits_{i\in I} f_i : T \to \mathbb{R}$ függvény is alulról (illetve felülről) félig folytonos. Ez az I indexhalmaz számossága szerinti teljes indukcióval bizonyítható, ahol az indukciós lépésnél a 7) megjegyzésben foglalt állításokra lehet hivatkozni.

28.4.3. Tétel. *Legyen T topologikus tér, $K \subseteq T$ kompakt halmaz és $f : T \to \overline{\mathbb{R}}$ olyan alulról* (*illetve felülről*) *félig folytonos függvény, amelyre $-\infty \notin \mathrm{Im}(f)$* (*illetve $+\infty \notin \mathrm{Im}(f)$*)*. Ekkor f alulról* (*illetve felülről*) *korlátos a K halmazon, és ha $K \neq \emptyset$ és zárt, akkor $\inf(f\langle K\rangle) \in f\langle K\rangle$* (*illetve $\sup(f\langle K\rangle) \in f\langle K\rangle$*)*, vagyis f a K halmazban felvesz minimális* (*illetve maximális*) *értéket.*

Bizonyítás. Legyen $f : T \to \overline{\mathbb{R}}$ olyan alulról félig folytonos függvény, amelyre $-\infty \notin \mathrm{Im}(f)$. Minden $n \in \mathbb{N}$ esetén az $\Omega_n := [f>-n]$ halmaz nyílt, mert f alulról félig folytonos, és $T = \bigcup\limits_{n\in\mathbb{N}} \Omega_n$, mert $-\infty \notin \mathrm{Im}(f)$. Ugyanakkor világos, hogy az $(\Omega_n)_{n\in\mathbb{N}}$ halmazsorozat monoton növő. A K halmaz kompaktsága miatt van olyan $n \in \mathbb{N}$, hogy $K \subseteq \Omega_n$, ezért $f\langle K\rangle$ alulról korlátos halmazt $\mathbb{R}$-ben. Tegyük fel, hogy K zárt is és nem üres. Legyen $c := \inf(f\langle K\rangle)$ és vegyünk tetszőleges $\mathbb{R}_+^*$-ban haladó $(\varepsilon_n)_{n\in\mathbb{N}}$ monoton fogyó zérussorozatot. Legyen minden $\mathbb{N} \ni n$-re $K_n := [f \le c+\varepsilon_n] \cap K$. Minden $n \in \mathbb{N}$ esetén $[f \le c+\varepsilon_n]$ zárt halmaz, mert f alulról félig folytonos, így K_n kompakt halmaz T-ben, és $K_{n+1} \subseteq K_n$, valamint $K_n \neq \emptyset$. Továbbá, minden $\mathbb{N} \ni n$-re K_n

zárt, mert a K zárt. A Cantor-féle közösrész-tételből következik, hogy $\bigcap_{n\in\mathbb{N}} K_n \neq \emptyset$. Ha $t \in \bigcap_{n\in\mathbb{N}} K_n$, akkor minden $\mathbb{N} \ni n$-re $c \leq f(t) \leq c + \varepsilon_n$, ezért $\lim_{n\to\infty} \varepsilon_n = 0$ miatt $c = f(t)$, így $\inf(f\langle K\rangle) \in f\langle K\rangle$. Ebből már következik a felülről félig folytonos függvényekre vonatkozó állítás is (áttérve f-ről a $-f$ függvényre). ■

28.4.4. Definíció. *Legyen T topologikus tér. Egy $E \subseteq T$ halmazt* G_δ**-halmaznak** *(illetve* F_σ**-halmaznak***) nevezünk, ha E előáll megszámlálható sok T-beli nyílt halmaz metszeteként (illetve megszámlálható sok T-beli zárt halmaz uniójaként).*

Metrizálható topologikus térben minden zárt halmaz G_δ-halmaz és minden nyílt halmaz F_σ-halmaz. Valóban, legyen T metrizálható topologikus tér és d olyan metrika, amely a tér topológiáját generálja. Ha $F \subseteq T$ zárt halmaz, akkor bármely $\mathbb{R}_+^*$-ban haladó $(\varepsilon_n)_{n\in\mathbb{N}}$ zérussorozatra

$$F = [d(\cdot, F) = 0] = \bigcap_{n\in\mathbb{N}} [d(\cdot, F) < \varepsilon_n],$$

és a $d(\cdot, F) : T \to \mathbb{R}$ függvény folytonossága miatt minden $n \in \mathbb{N}$ esetén $[d(\cdot, F) < \varepsilon_n]$ nyílt részhalmaza T-nek. A halmazelméleti de Morgan-egyenlőségből ez már maga után vonja, hogy T minden nyílt részhalmaza F_σ-halmaz.

28.4.5. Állítás. *Legyen T metrizálható topologikus tér és $f : T \to \overline{\mathbb{R}}$ alulról félig folytonos függvény. Ekkor létezik olyan $(f_n)_{n\in\mathbb{N}}$ függvénysorozat, hogy minden $n \in \mathbb{N}$ esetén $f_n : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $f_n(t) \leq f_{n+1}(t)$ és $f = \sup_{n\in\mathbb{N}} f_n$.*

Bizonyítás. Jelöljön d egy olyan metrikát a T halmaz felett, amely a T topológiáját generálja.

(I) Először tegyük fel, hogy $\Omega \subseteq T$ nyílt halmaz, és $f = \chi_\Omega$. A Ω halmaz F_σ-halmaz, tehát létezik a T zárt részhalmazainak olyan $(F_n)_{n\in\mathbb{N}}$ sorozata, hogy $\Omega = \bigcup_{n\in\mathbb{N}} F_n$, és feltehető, hogy minden $n \in \mathbb{N}$ esetén $F_n \subseteq F_{n+1}$. Metrizálható tér normális (27.4.11.), ezért az Uriszon-tétel alapján minden $n \in \mathbb{N}$ esetén az F_n zárt halmazhoz, és az ezt tartalmazó Ω nyílt halmazhoz van olyan $g : T \to \mathbb{R}$ folytonos függvény, hogy minden $t \in T$ esetén $0 \leq g(t) \leq 1$, és $\mathrm{supp}(g) \subseteq \Omega$, valamint $F_n \subseteq [g = 1]$. Tehát kiválaszthatunk olyan $(g_n)_{n\in\mathbb{N}}$ függvénysorozatot, hogy minden $n \in \mathbb{N}$ esetén $g_n : T \to \mathbb{R}$ folytonos függvény, és minden $t \in T$ esetén $0 \leq g_n(t) \leq 1$, és $\mathrm{supp}(g_n) \subseteq \Omega$, valamint $F_n \subseteq [g_n = 1]$. Minden $n \in \mathbb{N}$ esetén legyen $f_n := \sup_{0\leq k\leq n} g_k$. Ekkor nyilvánvaló, hogy $(f_n)_{n\in\mathbb{N}}$ olyan függvénysorozat, hogy minden $n \in \mathbb{N}$ esetén $f_n : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $0 \leq f_n(t) \leq f_{n+1}(t) \leq 1$, valamint $\chi_\Omega = \sup_{n\in\mathbb{N}} f_n$.

(II) Most tegyük fel, hogy $f : T \to \mathbb{R}$ olyan alulról félig folytonos függvény, hogy minden $t \in T$ esetén $0 \leq f(t) \leq 1$. Minden $\mathbb{N}^* \ni n$-re és $1 \leq k \leq n$ természetes számra legyen $\Omega_{n,k} := \left[f > \frac{k}{n}\right]$ és

$$g_n := \frac{1}{n}\sum_{k=1}^{n} \chi_{\Omega_{n,k}}.$$

Megmutatjuk, hogy minden $\mathbb{N}^* \ni n$-re és $T \ni t$-re $0 \leq f(t) - g_n(t) \leq \frac{1}{n}$. Ehhez legyen $n \in \mathbb{N}^*$ és $t \in T$ rögzített. Ha $0 \leq f(t) \leq \frac{1}{n}$, akkor minden $1 \leq k \leq n$

természetes számra $t \notin \Omega_{n,k}$, így $g_n(t) = 0$, vagyis $0 \leq f(t) = f(t) - g_n(t) \leq \frac{1}{n}$. Ha $\frac{1}{n} < f(t) \leq 1$, akkor $j := -[1 - nf(t)] \in \mathbb{Z}$ (itt $[\cdot]$ az egészrész-képzés függvény) olyan hogy $-j \leq 1 - nf(t) < -j + 1$, vagyis $\frac{j}{n} < f(t) \leq \frac{j+1}{n}$. Ebből, és az $\frac{1}{n} < f(t) \leq 1$ egyenlőtlenségből következik, hogy $1 \leq j < n$, ezért a definíció alapján

– ha $1 \leq k \leq j$, akkor $t \in \Omega_{n,k}$, és

– ha $j + 1 \leq k \leq n$, akkor $t \notin \Omega_{n,k}$,

így g_n definíciója szerint

$$g_n(t) = \frac{1}{n} \sum_{k=1}^{n} \chi_{\Omega_{n,k}}(t) = \frac{1}{n} \sum_{k=1}^{j} \chi_{\Omega_{n,k}}(t) = \frac{j}{n},$$

tehát

$$0 < f(t) - \frac{j}{n} = f(t) - g_n(t) \leq \frac{1}{n}.$$

Ebből következik, hogy $f = \sup\limits_{n\in\mathbb{N}} g_n$, ahol a $g_0 := 0$ definíciót alkalmaztuk. Az f függvény alulról félig folytonossága miatt minden $\mathbb{N}^* \ni n$-re és $1 \leq k \leq n$ természetes számra $\Omega_{n,k}$ nyílt halmaz T-ben, így (I) alapján vehetünk olyan $(h_{n,k,m})_{m\in\mathbb{N}}$ sorozatot, hogy minden $m \in \mathbb{N}$ esetén $h_{n,k,m} : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $0 \leq h_{n,k,m}(t) \leq h_{n,k,m+1}(t) \leq 1$, és $\chi_{\Omega_{n,k}} = \sup\limits_{m\in\mathbb{N}} h_{n,k,m}$. Minden $n \in \mathbb{N}^*$ és $m \in \mathbb{N}$ esetén legyen

$$\overline{h}_{n,m} := \frac{1}{n} \sum_{k=1}^{n} h_{n,k,m},$$

továbbá $\overline{h}_{0,m} := 0$. Ekkor minden $n \in \mathbb{N}$ számra a $\left(\overline{h}_{n,m}\right)_{m\in\mathbb{N}}$ függvénysorozat olyan, hogy minden $m \in \mathbb{N}$ esetén $\overline{h}_{n,m} : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $0 \leq \overline{h}_{n,m}(t) \leq \overline{h}_{n,m+1}(t) \leq 1$, és $g_n = \sup\limits_{m\in\mathbb{N}} \overline{h}_{n,m}$. Minden $n \in \mathbb{N}$ esetén legyen $f_k := \sup\limits_{\substack{m\leq k\\ n\leq k}} h_{n,m}$: ekkor $(f_k)_{k\in\mathbb{N}}$ olyan függvénysorozat, hogy minden $k \in \mathbb{N}$ esetén $f_k : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $0 \leq f_k(t) \leq f_{k+1}(t) \leq 1$, és $f = \sup\limits_{k\in\mathbb{N}} f_k$.

(III) Most tegyük fel, hogy $f : T \to \mathbb{R}$ *korlátos* alulról félig folytonos függvény, és legyenek $a, b \in \mathbb{R}$ olyanok, hogy $a < b$ és minden $t \in T$ esetén $a \leq f(t) \leq b$. Legyen $g := \frac{f-a}{b-a}$; ekkor $g : T \to \mathbb{R}$ olyan alulról félig folytonos függvény, hogy minden $t \in T$ esetén $0 \leq g(t) \leq 1$, így a (II) alapján van olyan $(g_n)_{n\in\mathbb{N}}$ függvénysorozat, hogy minden $n \in \mathbb{N}$ esetén $g_n : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $0 \leq g_n(t) \leq g_{n+1}(t) \leq 1$, és $g = \sup\limits_{n\in\mathbb{N}} g_n$. Legyen minden $\mathbb{N} \ni n$-re $f_n := a + (b-a)g_n$; ekkor $f_n : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $a \leq f_n(t) \leq f_{n+1}(t) \leq b$, és $f = \sup\limits_{n\in\mathbb{N}} f_n$.

(IV) Végül, legyen $f : T \to \overline{\mathbb{R}}$ *tetszőleges* alulról félig folytonos függvény. Minden $n \in \mathbb{N}$ esetén $g_n := \inf(n, \sup(f, -n)) : T \to \mathbb{R}$ korlátos alulról félig folytonos függvény, ezért (III) szerint van olyan $(g_{n,m})_{m\in\mathbb{N}}$ sorozat, hogy minden $\mathbb{N} \ni m$-re $g_{n,m} : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $-n \leq g_{n,m}(t) \leq g_{n,m+1}(t) \leq n$, valamint $g_n = \sup\limits_{m\in\mathbb{N}} g_{n,m}$. Világos, hogy minden $n \in \mathbb{N}$ és $t \in T$ esetén $g_n(t) \leq g_{n+1}(t)$ és

$f = \sup_{n\in\mathbb{N}} g_n$. Ebből következik, hogy ha minden $\mathbb{N} \ni k$-ra $f_k := \sup_{\substack{n\le k\\ m\le k}} g_{n,m}$, akkor $(f_k)_{k\in\mathbb{N}}$ olyan függvénysorozat, hogy minden $k \in \mathbb{N}$ esetén $f_k : T \to \mathbb{R}$ folytonos függvény, és minden $T \ni t$-re $f_k(t) \le f_{k+1}(t)$, és $f = \sup_{k\in\mathbb{N}} f_k$. ■

28.5. Kompakt terek metrizálhatósága

28.5.1. Tétel. (Kompakt terek metrizálhatósága) *Ha T kompakt Hausdorff-tér, akkor a következő állítások ekvivalensek.*

(i) *T megszámlálható bázisú.*

(ii) *T homeomorf a $\big([0,1]^{\mathbb{N}}, (\mathscr{E}_{\mathbb{R}}|[0,1])^{\mathbb{N}}\big)$ euklidészi kocka valamelyik zárt topologikus alterével.*

(iii) *T metrizálható.*

Bizonyítás. (i)⇒(ii) Kompakt Hausdorff-tér reguláris T_1-tér, tehát, ha (i) teljesül, akkor T megszámlálható bázisú reguláris T_1-tér. Ezért Uriszon beágyazási tétele alapján T homeomorf a $[0,1]^{\mathbb{N}}$ euklidészi kocka valamelyik K topologikus alterével. Ekkor K szükségképpen kompakt, tehát zárt is a $[0,1]^{\mathbb{N}}$ Hausdorff-térben.

(ii)⇒(iii) A $[0,1]^{\mathbb{N}}$ euklidészi kocka metrizálható, és metrizálható topologikus tér bármely topologikus altere metrizálható, ezért (ii)-ből nyilvánvalóan következik (iii).

(iii)⇒(i) Legyen d olyan metrika T felett, amely a T topológiát generálja, és $(\varepsilon_n)_{n\in\mathbb{N}}$ tetszőleges $\mathbb{R}_+^*$-ban haladó zérussorozat. Világos, hogy minden $\mathbb{N} \ni n$-re a $\big(\mathrm{B}_{\varepsilon_n}(t;d)\big)_{t\in T}$ gömb-rendszer nyílt befedése T-nek, ezért T kompaktsága folytán létezik olyan $D \subseteq T$ véges halmaz, hogy $T = \bigcup_{t\in D} \mathrm{B}_{\varepsilon_n}(t;d)$. Kiválaszthatunk tehát a T véges részhalmazainak olyan $(D_n)_{n\in\mathbb{N}}$ sorozatát, amelyre minden $n \in \mathbb{N}$ esetén $T = \bigcup_{t\in D_n} \mathrm{B}_{\varepsilon_n}(t;d)$. Legyen $D := \bigcup_{n\in\mathbb{N}} D_n$ és $\mathfrak{B} := \{\mathrm{B}_{\varepsilon_n}(t;d) | (n \in \mathbb{N}) \wedge (t \in D_n)\}$. Világos, hogy $\mathfrak{B}$ olyan megszámlálható halmaz, amelynek minden eleme nyílt részhalmaz T-ben.

Megmutatjuk, hogy $\mathfrak{B}$ a T-nek topologikus bázisa, tehát T megszámlálható bázisú. Ehhez legyen Ω nyílt halmaz T-ben és $t \in \Omega$. Olyan $n \in \mathbb{N}$ számot és $t' \in D_n$ pontot keresünk, hogy $t \in \mathrm{B}_{\varepsilon_n}(t';d) \subseteq \Omega$. Ehhez először veszünk olyan $\varepsilon \in \mathbb{R}_+^*$ számot, amelyre $\mathrm{B}_\varepsilon(t;d) \subseteq \Omega$, majd választunk olyan $n \in \mathbb{N}$ számot, hogy $\varepsilon_n \le \frac{\varepsilon}{2}$. Ekkor $t \in T = \bigcup_{t'\in D_n} \mathrm{B}_{\varepsilon_n}(t';d)$ miatt van olyan $t' \in D_n$, hogy $t \in \mathrm{B}_{\varepsilon_n}(t';d)$. Könnyen látható, hogy ekkor $\mathrm{B}_{\varepsilon_n}(t';d) \subseteq \Omega$, mert ha $t'' \in \mathrm{B}_{\varepsilon_n}(t';d)$, akkor $d(t'',t) \le d(t'',t') + d(t',t) < \varepsilon_n + \varepsilon_n \le \varepsilon$, vagyis $t'' \in \mathrm{B}_\varepsilon(t;d) \subseteq \Omega$. ■

Azonban létezik olyan kompakt Hausdorff-tér, amely szeparábilis M_1-tér, de nem metrizálható (mert nem megszámlálható bázisú). Legyen például

$$\mathscr{T} := \{\ \Omega \in \mathscr{P}(\mathbb{R}) \mid (\forall\, t \in \Omega)(\exists\, \varepsilon \in \mathbb{R}_+^*) :]-t-\varepsilon, -t[\cup [t, t+\varepsilon[\subseteq \Omega\ \}.$$

Ekkor $\mathscr{T}$ topológia $\mathbb{R}$ felett és a $([-1,1], \mathscr{T}|[-1,1])$ topologikus altér kompakt szeparábilis M_1-tér, de nem M_2-tér.

Megjegyezzük, hogy az előző metrizációs tétel szerint a $[0,1]^{\mathbb{N}}$ euklidészi kocka olyan metrizálható kompakt tér, amely abban az értelemben *univerzális* a metrizálható kompakt terek számára, hogy a zárt topologikus alterei (homeomorfia erejéig) az összes metrizálható kompakt teret megadják.

28.6. Lokálisan kompakt terek alaptulajdonságai

28.6.1. Definíció. *Egy topologikus teret* **lokálisan kompaktnak** *nevezünk, ha Hausdorff-tér és minden pontjának létezik kompakt környezete. Egy T topologikus tér E részhalmazát lokálisan kompaktnak mondjuk, ha az E topologikus altér lokálisan kompakt tér.*

Nyilvánvaló, hogy minden kompakt Hausdorff-tér lokálisan kompakt. Ennek megfordítása természetesen nem igaz. Például a valós számok halmaza az euklidészi topológiával ellátva nem kompakt, lokálisan kompakt tér.

28.6.2. Állítás. *Minden lokálisan kompakt tér reguláris. Lokálisan kompakt térben minden pontnak létezik kompakt halmazokból álló környezetbázisa.*

Bizonyítás. Legyen T lokálisan kompakt tér, $F \subseteq T$ zárt halmaz és $t \in T \setminus F$. Legyen V a t-nek kompakt környezete. Ha $V \cap F = \emptyset$, akkor $\Omega := \overset{\circ}{V}$ és $\Omega' := T \setminus V$ olyan diszjunkt nyílt halmazok T-ben, hogy $t \in \Omega$ és $F \subseteq \Omega'$. (Itt kihasználtuk, hogy a V kompakt halmaz zárt, mert T Hausdorff-tér.) Tegyük fel, hogy $V \cap F \neq \emptyset$; ekkor $V \cap F$ nem üres kompakt halmaz T-ben és $t \in T \setminus (V \cap F)$. A T topologikus tér Hausdorff-tér, ezért kiválaszthatunk olyan $(\Omega_s)_{s \in V \cap F}$ és $(V_s)_{s \in V \cap F}$ rendszereket, hogy minden $V \cap F \ni s$-re V_s nyílt környezete s-nek, Ω_s nyílt környezete t-nek és $\Omega_s \cap V_s = \emptyset$. Ekkor $V \cap F \subseteq \bigcup\limits_{s \in V \cap F} V_s$, tehát a $V \cap F$ kompaktsága folytán van olyan $S \subseteq V \cap F$ véges halmaz, amelyre $V \cap F \subseteq \bigcup\limits_{s \in S} V_s$. A $V \cap F \neq \emptyset$ feltétel alapján $S \neq \emptyset$. Értelmezzük az $\Omega := \overset{\circ}{V} \cap \left(\bigcap\limits_{s \in S} \Omega_s \right)$ és $\Omega' := (T \setminus V) \cup \left(\bigcup\limits_{s \in S} V_s \right)$ halmazokat. Az Ω halmaz véges sok nyílt halmaz metszete, tehát nyílt, és világos, hogy $t \in \Omega$. A V halmaz kompakt, így zárt a T Hausdorff-térben, így Ω' nyílt halmazok (véges) rendszerének az uniója, tehát nyílt. Nyilvánvaló, hogy $F \subseteq \Omega'$, mert ha $t' \in F$ és $t' \in V$, akkor $t' \in V \cap F \subseteq \bigcup\limits_{s \in S} V_s \subseteq \Omega'$, míg $t' \in F$ és $t' \notin V$ esetén $t' \in T \setminus V \subseteq \Omega'$. Végül, $\Omega \cap \Omega' = \emptyset$ is teljesül, mert ha $t' \in \Omega$, akkor $t' \in \overset{\circ}{V} \subseteq V$, tehát $t' \notin T \setminus V$, valamint $t' \notin \bigcup\limits_{s \in S} V_s$ is igaz, mert $t' \in \bigcap\limits_{s \in S} \Omega_s$, és a $\bigcap\limits_{s \in S} \Omega_s$ és $\bigcup\limits_{s \in S} V_s$ halmazok diszjunktak, ezért $t' \notin \Omega'$. Ezzel megmutattuk, hogy T reguláris tér.

Legyen $t \in T$ és V a t tetszőleges környezete. Legyen V' a t-nek kompakt környezete. Láttuk, hogy T reguláris, ezért létezik t-nek olyan V'' környezete, amely zárt és $V'' \subseteq V$. Ekkor $V' \cap V''$ olyan kompakt környezete t-nek, amely részhalmaza V-nek, tehát a t kompakt környezeteinek halmaza a t-nek környezetbázisa T-ben. ■

28.6.3. Következmény. *Ha T lokálisan kompakt tér és $\mathfrak{B}$ topologikus bázisa T-nek, akkor a $\mathfrak{B}_c := \{U \in \mathfrak{B} | U$ relatív kompakt$\}$ halmaz is topologikus bázisa T-nek.*

Bizonyítás. Legyen Ω nyílt halmaz T-ben és $t \in \Omega$. A $\mathfrak{B}$ halmaz topologikus bázis T-ben, ezért van olyan $V \in \mathfrak{B}$, hogy $t \in V \subseteq \Omega$. A V halmaz nyílt, tehát környezete t-nek, így a T lokális kompaktsága és az előző állítás szerint van olyan W kompakt környezete t-nek, hogy $W \subseteq V$. Ekkor $\overset{\circ}{W}$ a t-nek nyílt környezete, ezért van olyan $U \in \mathfrak{B}$, hogy $t \in U \subseteq \overset{\circ}{W}$. A W halmaz zárt, mert T Hausdorff-tér, következésképpen $\overline{U} \subseteq W$, tehát $\overline{U}$ kompakt halmaz. Ezért $U \in \mathfrak{B}$ relatív kompakt halmaz és $t \in U \subseteq \Omega$. ■

28.6.4. Következmény. *Ha T lokálisan kompakt tér, $K \subseteq T$ kompakt halmaz és $\Omega \subseteq T$ olyan nyílt halmaz, hogy $K \subseteq \Omega$, akkor létezik olyan $U \subseteq T$ relatív kompakt nyílt halmaz, amelyre $K \subseteq U \subseteq \overline{U} \subseteq \Omega$.*

Bizonyítás. Ha $t \in K$, akkor Ω nyílt környezete t-nek, ezért létezik a t-nek olyan V kompakt környezete, hogy $V \subseteq \Omega$; ekkor $\overset{\circ}{V}$ olyan relatív kompakt nyílt halmaz, amelyre $t \in \overset{\circ}{V}$ és $\overline{\overset{\circ}{V}} \subseteq \Omega$. Ezért kiválaszthatunk olyan $(U_t)_{t\in K}$ rendszert, amelyre minden $t \in K$ esetén U_t relatív kompakt nyílt környezete t-nek és $\overline{U_t} \subseteq \Omega$. Ekkor $(U_t)_{t\in K}$ nyílt befedése K-nak, így a K kompaktsága miatt létezik olyan $H \subseteq K$ véges halmaz, hogy $K \subseteq \bigcup_{t\in H} U_t$. Az $U := \bigcup_{t\in H} U_t$ halmaz nyílt, $K \subseteq U$, és $\overline{U} = \bigcup_{t\in H} \overline{U_t}$, tehát $\overline{U}$ kompakt (mert véges sok kompakt halmaz uniója kompakt), így $\overline{U} \subseteq \Omega$ is teljesül. ■

28.6.5. Állítás. *Ha T Hausdorff-tér és $E \subseteq T$ lokálisan kompakt halmaz, akkor van olyan $\Omega \subseteq T$ nyílt halmaz, hogy $E = \overline{E} \cap \Omega$. Ha T lokálisan kompakt tér, akkor egy $E \subseteq T$ halmaz pontosan akkor lokálisan kompakt, ha létezik olyan $\Omega \subseteq T$ nyílt és $F \subseteq T$ zárt halmaz, hogy $E = \Omega \cap F$.*

Bizonyítás. Legyen T Hausdorff-tér és $E \subseteq T$ lokálisan kompakt halmaz. Kiválasztható olyan $(V_t)_{t\in E}$ rendszer, hogy minden $E \ni t$-re V_t a t-nek kompakt környezete az E topologikus altérben. Az altértopológia és a környezetek definíciója szerint kiválasztható olyan $(\Omega_t)_{t\in E}$ rendszer, hogy minden $E \ni t$-re Ω_t nyílt halmaz T-ben és $t \in E \cap \Omega_t \subseteq V_t$. Legyen $\Omega := \bigcup_{t\in E} \Omega_t$; ez olyan nyílt halmaz T-ben, amelyre megmutatjuk, hogy $E = \overline{E} \cap \Omega$. Valóban, legyen $t \in \overline{E} \cap \Omega$ tetszőleges. Létezik olyan $s \in E$, hogy $t \in \Omega_s$. Ha a V halmaz környezete t-nek T-ben, akkor $V \cap \Omega_s$ is környezete t-nek T-ben, tehát $t \in \overline{E}$ miatt $E \cap (V \cap \Omega_s) \neq \emptyset$, vagyis $V \cap (E \cap \Omega_s) \neq \emptyset$. Ez azt jelenti, hogy t eleme az $E \cap \Omega_s$ halmaz T-beli lezártjának, tehát $E \cap \Omega_s \subseteq V_s$ miatt $t \in \overline{V_s}$. De V_s kompakt az E topologikus altérben, így T-ben is kompakt, tehát zárt T-ben, mert T Hausdorff-tér. Ezért $t \in V_s$ és $V_s \subseteq E$, vagyis $t \in E$. Ez azt jelenti, hogy $\overline{E} \cap \Omega \subseteq E$. A fordított tartalmazás triviálisan igaz.

Tegyük fel, hogy T lokálisan kompakt tér, $\Omega \subseteq T$ nyílt halmaz és $F \subseteq T$ zárt halmaz. Megmutatjuk, hogy $F \cap \Omega$ lokálisan kompakt halmaz T-ben. Legyen ugyanis $t \in F \cap \Omega$ tetszőleges; ekkor Ω környezete t-nek T-ben, tehát létezik t-nek olyan V kompakt környezete T-ben, amelyre $V \subseteq \Omega$. Az F halmaz zártsága miatt az $F \cap V$ halmaz kompakt T-ben és $F \cap V = F \cap (V \cap \Omega) = (F \cap \Omega) \cap V$, vagyis $F \cap V$ olyan környezete t-nek az $F \cap \Omega$ topologikus altérben, amely T-ben kompakt. De $F \cap V \subseteq F \cap \Omega$, így $F \cap V$ kompakt az $F \cap \Omega$ topologikus altérben is. Ezért az $F \cap \Omega$ topologikus altér lokálisan kompakt. ■

28.6.6. Következmény. *Hausdorff-térben minden lokálisan kompakt halmaz lokálisan zárt. Lokálisan kompakt térben egy halmaz pontosan akkor lokálisan kompakt, ha lokálisan zárt.*

Bizonyítás. A 28.6.5. és 26.3.10. állítások alapján nyilvánvaló. ■

28.6.7. Következmény. *Hausdorff-tér lokálisan kompakt sűrű részhalmaza nyílt.*

Bizonyítás. Ha T Hausdorff-tér és $E \subseteq T$ lokálisan kompakt sűrű halmaz T-ben, akkor a 28.6.5. állítás szerint van olyan $\Omega \subseteq T$ nyílt halmaz, hogy $E = \overline{E} \cap \Omega = T \cap \Omega = \Omega$, tehát E nyílt halmaz T-ben. ■

Az előző állításból következik, hogy $\mathbb{Q}$ nem lokálisan kompakt halmaz $\mathbb{R}$-ben.

28.6.8. Állítás. *Legyen T lokálisan kompakt tér, T' Hausdorff-tér és $\pi : T \to T'$ folytonos és nyílt szürjekció. Ekkor minden $K' \subseteq T'$ kompakt halmazhoz van olyan $K \subseteq T$ kompakt halmaz, amelyre $\pi\langle K\rangle = K'$.*

Bizonyítás. Legyen $K' \subseteq T'$ kompakt halmaz. A T lokális kompaktsága miatt van olyan $(V_t)_{t\in T}$ rendszer, hogy minden $T \ni t$-re V_t kompakt környezete a t pontnak. A π függvény nyílt szürjekció, ezért a $(\pi\langle \overset{\circ}{V_t}\rangle)_{t\in T}$ halmazrendszer nyílt befedése T'-nek. A K' kompaktsága folytán van olyan $H \subseteq T$ véges halmaz, hogy $K' \subseteq \bigcup_{t\in H} \pi\langle \overset{\circ}{V_t}\rangle$. Legyen $K := \overset{-1}{\pi}\langle K'\rangle \cap \left(\bigcup_{t\in H} V_t\right)$. A K' halmaz zárt T'-ben, mert kompakt és T' Hausdorff-tér. A π függvény folytonos, ezért $\overset{-1}{\pi}\langle K'\rangle \subseteq T$ zárt halmaz, ugyanakkor $\bigcup_{t\in H} V_t$ kompakt halmaz T-ben, így $K \subseteq T$ kompakt halmaz. Állítjuk, hogy $\pi\langle K\rangle = K'$. Valóban, $\pi\langle K\rangle \subseteq \pi\langle \overset{-1}{\pi}\langle K'\rangle\rangle \subseteq K'$; továbbá $t' \in K' \subseteq \bigcup_{t\in H} \pi\langle \overset{\circ}{V_t}\rangle$ esetén van olyan $t \in H$, hogy $t' \in \pi\langle \overset{\circ}{V_t}\rangle$; ekkor létezik olyan $s \in V_t$, hogy $\pi(s) = t' \in K'$, tehát $s \in \overset{-1}{\pi}\langle K'\rangle \cap V_t \subseteq K$, vagyis $t' = \pi(s) \in \pi\langle K\rangle$, ami azt jelenti, hogy $K' \subseteq \pi\langle K\rangle$ is teljesül. ■

28.7. Nem normális lokálisan kompakt terek

A továbbiakban be szeretnénk bizonyítani a normális terekre már igazolt Uriszon-tétel (27.5.1.), Tietze-tétel (27.6.1.) és egységfelosztás tétel (27.7.3.) lokálisan kompakt terekre érvényes alakját. Kiderül, hogy ezeket a tételeket változatlan formában biztosan nem lehetséges lokálisan kompakt terekre átvinni, mert ezek a normálisság *jellemzései*, vagyis olyan tulajdonságokat fogalmaznak meg, amelyek a normálissággal *ekvivalensek*, ugyanakkor lokálisan kompakt tér nem szükségképpen normális. Azonban egyáltalán nem nyilvánvaló nem normális lokálisan kompakt tér létezése.

Ebben a pontban két konkrét példát adunk nem normális lokálisan kompakt térre: az első ilyen az ún. *csonka Tyihonov-deszka* lesz.

28.7.1. Definíció. *Az ω^+ és ω_1^+ rendszámokat ellátjuk a rendezéstopológiával* (26.2.5.), *és az $\omega_1^+ \times \omega^+$ szorzathalmazt a szorzattopológiával. Ezt a topologikus teret* **Tyihonov-deszkának** *nevezzük. A $T := \left(\omega_1^+ \times \omega^+\right) \setminus \{(\omega_1, \omega)\}$ halmazt az altértopológiával ellátva* **csonka Tyihonov-deszkának** *nevezzük.*

Világos, hogy a Tyihonov-deszka 26.2.4. és 28.1.10. szerint kompakt Hausdorff-tér, továbbá a csonka Tyihonov-deszka lokálisan kompakt tér, mert nyílt altere egy kompakt Hausdorff-térnek (28.6.5.).

28.7.2. Állítás. *A csonka Tyihonov-deszka nem normális lokálisan kompakt tér.*

Bizonyítás. Jelölje T a csonka Tyihonov-deszkát, és legyenek

$$F := \omega_1 \times \{\omega\}, \quad F' := \{\omega_1\} \times \omega.$$

Ekkor $F \cap F' = \emptyset$ és mindketten zárt halmazok T-ben, mert $F = (\omega_1^+ \times \{\omega\}) \cap T$ és $\omega_1^+ \times \{\omega\}$ zárt az $\omega_1^+ \times \omega^+$ szorzattérben, továbbá $F' = (\{\omega_1\} \times \omega^+) \cap T$ és $\{\omega_1\} \times \omega^+$ zárt az $\omega_1^+ \times \omega^+$ szorzattérben. Megmutatjuk, hogy ha Ω és Ω' olyan nyílt halmazok T-ben, amelyekre $F \subseteq \Omega$ és $F' \subseteq \Omega'$, akkor $\Omega \cap \Omega' \neq \emptyset$, ezért T nem normális lokálisan kompakt tér.

Ehhez először megjegyezzük, hogy az Ω és Ω' halmazok T-beli nyíltsága és az altértopológia definíciója alapján vehetünk olyan $\tilde{\Omega}$ és $\tilde{\Omega}'$ nyílt halmazokat az $\omega_1^+ \times \omega^+$ szorzattérben, hogy $\Omega = \tilde{\Omega} \cap (\omega_1^+ \times \omega^+)$ és $\Omega' = \tilde{\Omega}' \cap (\omega_1^+ \times \omega^+)$.

Legyen $n \in \omega$. Ekkor $(\omega_1, n) \in F' \subseteq \Omega' \subseteq \tilde{\Omega}'$, ezért a szorzattopológia és a rendezéstopológia értelmezése alapján léteznek olyan $\mathscr{I}_1 \subseteq \omega_1^+$ és $\mathscr{I}_2 \subseteq \omega^+$ nyílt intervallumok, amelyekre $(\omega_1, n) \in \mathscr{I}_1 \times \mathscr{I}_2 \subseteq \tilde{\Omega}'$. Az $\mathscr{I}_1$ intervallum vagy $]\leftarrow, \alpha[$ alakú valamely $\alpha \in \omega_1^+$ elemre, vagy $]\alpha, \beta[$ alakú valamely $\alpha, \beta \in \omega_1^+$ elemekre, vagy $]\alpha, \rightarrow[$ alakú valamely $\alpha \in \omega_1^+$ elemre. De az első két esetben ω_1 nem lenne eleme $\mathscr{I}_1$-nek, hiszen ω_1 az ω_1^+ rendezett halmaz legnagyobb eleme, ezért szükségképpen van olyan $\alpha \in \omega_1^+$, hogy $\mathscr{I}_1 =]\alpha, \rightarrow[$. Ha $\alpha = \omega_1$ volna, akkor $]\alpha, \rightarrow[= \emptyset$, holott $\omega_1 \in]\alpha, \rightarrow[$. Ezért $\alpha \in \omega_1$. Ezzel megmutattuk, hogy minden $n \in \omega$ esetén van olyan $\alpha \in \omega_1$, hogy $]\alpha, \rightarrow[\times \{n\} \subseteq \Omega'$. Ezért *kiválaszthatunk* olyan $(\alpha_n)_{n \in \omega}$ sorozatot, hogy minden $n \in \omega$ esetén $]\alpha_n, \rightarrow[\times \{n\} \subseteq \Omega'$.

Legyen $\alpha := \sup_{n \in \omega} \alpha_n$, vagyis $\alpha = \bigcup_{n \in \mathbb{N}} \alpha_n$. Ekkor α megszámlálható halmazok megszámlálható rendszerének uniója, ezért megszámlálható rendszám, így $\alpha \in \omega_1$, hiszen ω_1 a legkisebb nem megszámlálható rendszám.

Legyen $\beta \in \omega_1$. Ekkor $(\beta, \omega) \in F \subseteq \Omega \subseteq \tilde{\Omega}$, ezért a szorzattopológia és a rendezéstopológia értelmezése alapján léteznek olyan $\mathscr{I}_1 \subseteq \omega_1^+$ és $\mathscr{I}_2 \subseteq \omega^+$ nyílt intervallumok, amelyekre $(\beta, \omega) \in \mathscr{I}_1 \times \mathscr{I}_2 \subseteq \tilde{\Omega}$. Az $\mathscr{I}_2$ intervallum vagy $]\leftarrow, \gamma[$ alakú valamely $\gamma \in \omega^+$ elemre, vagy $]\gamma, \delta[$ alakú valamely $\gamma, \delta \in \omega^+$ elemekre, vagy $]\gamma, \rightarrow[$ alakú valamely $\gamma \in \omega^+$ elemre. De az első két esetben ω nem lenne eleme $\mathscr{I}_2$-nek, hiszen ω az ω^+ rendezett halmaz legnagyobb eleme, ezért szükségképpen van olyan $\gamma \in \omega^+$, hogy $\mathscr{I}_2 =]\gamma, \rightarrow[$. Ha $\gamma = \omega$ volna, akkor $]\gamma, \rightarrow[= \emptyset$, holott $\omega \in]\gamma, \rightarrow[$. Ezért $\gamma \in \omega$. Ezzel megmutattuk, hogy minden $\beta \in \omega_1$ esetén van olyan $\gamma \in \omega$, hogy $(\beta, \omega) \in \{\beta\} \times]\gamma, \rightarrow[\subseteq \Omega$.

Végül, legyen $\beta \in \omega_1$ olyan, hogy $\alpha < \beta$. Vegyünk olyan $\gamma \in \omega$ rendszámot, amelyre $\{\beta\} \times]\gamma, \rightarrow[\subseteq \Omega$. Ha $n \in]\gamma, \rightarrow[$, akkor $(\beta, n) \in \Omega$, ugyanakkor $\alpha_n \leq \alpha < \beta$, tehát $(\beta, n) \in]\alpha_n, \rightarrow[\times \{n\} \subseteq \Omega'$, vagyis $(\beta, n) \in \Omega \cap \Omega'$, így $\Omega \cap \Omega' \neq \emptyset$. ■

A második példához felhasználjuk a következő lemmát.

28.7.3. Lemma. *Ha $n \in \mathbb{N}^*$ és $y, y' \in \mathbb{R}$ olyanok, hogy $|y' - y| \leq \dfrac{2n-1}{n^2}$, akkor létezik olyan $k \in \mathbb{Z}$, amelyre*

$$\left| y - \frac{k}{n^2} \right| \leq \frac{1}{n} \quad \textit{és} \quad \left| y' - \frac{k}{n^2} \right| \leq \frac{1}{n}$$

egyszerre teljesül.

Bizonyítás. A bizonyításban nyilvánvalóan feltehetjük, hogy $y \leq y'$. Olyan $k \in \mathbb{Z}$ számot keresünk, amelyre

$$n^2 y - n \leq k \leq n^2 y + n \quad \text{és} \quad n^2 y' - n \leq k \leq n^2 y' + n$$

egyszerre teljesül, ha $y' - y = |y' - y| \leq \dfrac{2n-1}{n^2}$. Ebből az egyenlőtlenségből következik, hogy

$$(n^2y + n) - (n^2y' - n) = 2n - n^2(y' - y) \geq 2n - n^2\left(\frac{2n-1}{n^2}\right) = 1,$$

ezért van olyan $k \in \mathbb{Z}$, hogy $n^2y' - n \leq k \leq n^2y + n$, hiszen $n^2y' - n \in \mathbb{Z}$ esetén $k := [n^2y' - n]$ ilyen, és $n^2y' - n \notin \mathbb{Z}$ esetén $k := [n^2y' - n] + 1$. Ha $k \in \mathbb{Z}$ és $n^2y' - n \leq k \leq n^2y + n$, akkor $y \leq y'$ miatt

$$y - \frac{1}{n} \leq y' - \frac{1}{n} \leq \frac{k}{n^2} \leq y + \frac{1}{n} \leq y' + \frac{1}{n},$$

tehát a k szám rendelkezik az elvárt tulajdonságokkal. ∎

28.7.4. Állítás. *Legyen $D := \{0\} \times \mathbb{R}$ és $T := D \cup \{(1/n, k/n^2) | (n \in \mathbb{N}^*) \wedge (k \in \mathbb{Z})\}$. Minden $n \in \mathbb{N}^*$ és $y \in \mathbb{R}$ esetén legyen $V_n(y) := \{(u,v) \in T | (u \leq 1/n) \wedge (|y - v| \leq u)\}$. Ekkor létezik egyetlen olyan $\mathscr{T}$ topológia T felett, amely szerint minden $t \in T \setminus D$ pontnak környezete a $\{t\}$ halmaz, és minden $y \in \mathbb{R}$ esetén a $(0, y)$ pontnak környezetbázisa a $\{V_n(y) | n \in \mathbb{N}^*\}$ halmaz. A T halmaz ezzel a $\mathscr{T}$ topológiával ellátva nem normális lokálisan kompakt tér.*

Bizonyítás. Minden $t \in T \setminus D$ esetén legyen $\mathfrak{F}_t := \{V \subseteq T | t \in V\}$, és minden $y \in \mathbb{R}$ esetén legyen $\mathfrak{F}_{(0,y)} := \{V \subseteq T | (\exists n \in \mathbb{N}^*) : V_n(y) \subseteq V\}$. Nyilvánvaló, hogy minden $t \in T \setminus D$ pontra $\mathfrak{F}_t$ szűrő T felett (ez a t ponthoz tartozó *alapszűrő* T felett). Ha $y \in \mathbb{R}$ és $m, n \in \mathbb{N}^*$, akkor $m \leq n$ esetén nyilvánvalóan $V_n(y) \subseteq V_m(y)$, és $(0, y) \in V_n(y)$, ezért $\{V_n(y) | n \in \mathbb{N}^*\}$ olyan rács, amelynek minden tagja részhalmaza T-nek és elemként tartalmazza $(0, y)$-t. Ezért minden $y \in \mathbb{R}$ esetén $\mathfrak{F}_{(0,y)}$ szűrő T felett (ez a $\{V_n(y) | n \in \mathbb{N}^*\}$ *rács által generált* T feletti szűrő).

Tehát $(\mathfrak{F}_t)_{t \in T}$ olyan rendszer, hogy minden $t \in T$ esetén $\mathfrak{F}_t$ szűrő T felett, és minden $V \in \mathfrak{F}_t$ halmazra $t \in V$. A 26.2.9. állítás szerint akkor és csak akkor létezik olyan T feletti $\mathscr{T}$ topológia, amelyre minden $t \in T$ esetén $\mathscr{T}(t) = \mathfrak{F}_t$, ha teljesül a következő állítás:

$$(\forall\, t \in T)(\forall\, V \in \mathfrak{F}_t)(\exists\, V' \in \mathfrak{F}_t)(\forall\, t' \in V') : V \in \mathfrak{F}_{t'}.$$

Most igazoljuk ezt az állítást. Ha $t \in T \setminus D$ és $V \in \mathfrak{F}_t$, akkor $V \subseteq T$ és $t \in V$, továbbá $V' := \{t\} \in \mathfrak{F}_t$ és minden $t' \in V'$ esetén $t' = t \in V$, vagyis $V \in \mathfrak{F}_{t'}$. Legyen $y \in \mathbb{R}$, $t := (0, y)$ és $V \in \mathfrak{F}_t$. A definíció alapján vehetünk olyan $n \in \mathbb{N}^*$ számot, hogy $V_n(y) \subseteq V$. Ekkor $V' := V_n(y) \in \mathfrak{F}_t$ és $t' \in V'$ esetén

– ha $t' \in T \setminus D$, akkor $V' \in \mathfrak{F}_{t'}$, hiszen $V' \subseteq T$ olyan halmaz, hogy $t' \in V'$;

– ha $t' \in D$, akkor létezik olyan $y' \in \mathbb{R}$, hogy $t' = (0, y')$: ekkor $(0, y') \in V_n(y)$, tehát a $V_n(y)$ halmaz definíciója szerint $y' = y$, vagyis $t' = t$, amiből $V' \in \mathfrak{F}_{t'}$ következik.

Tehát egyértelműen létezik olyan T feletti $\mathscr{T}$ topológia, amelyre minden $t \in T$ esetén $\mathscr{T}(t) = \mathfrak{F}_t$. Ez éppen az a T feletti topológia, amely szerint minden $t \in T \setminus D$ pontnak környezete a $\{t\}$ halmaz, és minden $y \in \mathbb{N}$ esetén a $(0, y)$ pontnak környezetbázisa a $\{V_n(y) | n \in \mathbb{N}^*\}$ halmaz.

Könnyen látható, hogy $\mathscr{T}$ Hausdorff-topológia. Valóban, különböző $T \setminus D$-beli pontoknak nyilvánvalóan léteznek diszjunkt környezetei. Legyen $t \in D$ és $y \in \mathbb{R}$ olyan, hogy $t = (0, y)$, valamint $t' \in T \setminus D$ és $n \in \mathbb{N}^*$ olyan, hogy $t' = (1/n, k/n^2)$. Ekkor $N \in \mathbb{N}^*$ és $N > n$ esetén $V_N(y) \cap \{t'\} = \emptyset$, mert $(u, v) \in V_N(y)$ esetén $u \leq 1/N < 1/n$, így $(u, v) \neq (1/n, k/n^2) = t'$. Végül, ha $y, y' \in \mathbb{R}$, $n \in \mathbb{N}$ és $(u, v) \in V_n(y) \cap V_n(y')$, akkor $u \leq 1/n$ és $|y-v| \leq u \leq 1/n$ és $|y'-v| \leq u \leq 1/n$, következésképpen $|y'-y| \leq |y'-v|+|y-v| \leq 2/n$. Ebből következik, hogy ha $y, y' \in \mathbb{R}$ és $y \neq y'$, és $n \in \mathbb{N}^*$ olyan, hogy $2/n < |y'-y|$, akkor $V_n(y) \cap V_n(y') = \emptyset$, és természetesen $V_n(y)$ a $(0,y)$ pontnak, és $V_n(y')$ a $(0,y')$ pontnak környezete $\mathscr{T}$ szerint. Ezért $\mathscr{T}$ Hausdorff-topológia.

Bebizonyítjuk, hogy T a $\mathscr{T}$ topológiával ellátva *lokálisan kompakt* tér. Ha $t \in T \setminus D$, akkor $\{t\}$ kompakt környezete t-nek $\mathscr{T}$ szerint. Legyen $t \in D$ és $y \in \mathbb{R}$ olyan, hogy $t=(0,y)$. Megmutatjuk, hogy minden $n \in \mathbb{N}^*$ esetén a $V_n(y)$ halmaz *kompakt* $\mathscr{T}$ szerint, és mivel ez környezete is t-nek $\mathscr{T}$ szerint, így $\mathscr{T}$ lokálisan kompakt topológia T felett. Legyen tehát $y \in \mathbb{R}$ és $n \in \mathbb{N}^*$ rögzítve, és vegyük $V_n(y)$-nak egy $(\Omega_i)_{i \in I}$ $\mathscr{T}$-nyílt befedését. Van olyan $i_y \in I$, hogy $(0,y) \in \Omega_{i_y}$. Az Ω_{i_y} halmaz $\mathscr{T}$ szerinti nyíltsága miatt van olyan $m \in \mathbb{N}$, hogy $V_m(y) \subseteq \Omega_{i_y}$. Legyen $p \in \mathbb{N}^*$ olyan szám, hogy $p > \max(m,n)$. Ekkor $V_p(y) \subseteq \Omega_{i_y}$, mert $p > m$ miatt $V_p(y) \subseteq V_m(y)$. Ugyanakkor $p > n$ miatt $V_p(y) \subseteq V_n(y)$ is igaz és a $V_n(y) \setminus V_p(y)$ halmaz *véges*, ugyanis $(u,v) \in V_n(y) \setminus V_p(y)$ esetén $u \leq 1/n$ és $|y-v| \leq u$ és $u > 1/p$, vagyis $(u,v) \in T \setminus D$, így létezik olyan $q \in \mathbb{N}^*$ és $k \in \mathbb{Z}$, amelyekre $(u,v) = (1/q, k/q^2)$: ekkor $n \leq q < p$ és $|y-v| \leq u = 1/q$ miatt $q^2y - q \leq k \leq q^2y+q$, vagyis ha bevezetjük az

$$a := \min_{\substack{r \in \mathbb{N}^* \\ n \leq r < p}} (r^2y - r), \quad b := \max_{\substack{r \in \mathbb{N}^* \\ n \leq r < p}} (r^2y + r)$$

számokat, akkor

$$(u,v) \in \{\ (1/q, k/q^2) \mid (q \in \mathbb{N}^*) \wedge (k \in \mathbb{Z}) \wedge (n \leq q < p) \wedge (a \leq k \leq b)\ \},$$

és nyilvánvaló, hogy itt a jobb oldalon véges halmaz áll. Ezért létezik olyan $J \subseteq I$ véges halmaz hogy $V_n(y) \setminus V_p(y) \subseteq \bigcup_{i \in J} \Omega_i$, következésképpen $(\Omega_i)_{i \in J \cup \{i_y\}}$ véges részbefedése $(\Omega_i)_{i \in I}$-nek, vagyis $V_n(y)$ kompakt $\mathscr{T}$ szerint.

Megmutatjuk, hogy minden $H \subseteq \mathbb{R}$ halmazra $\{0\} \times H$ *zárt* halmaz T-ben $\mathscr{T}$ szerint. Legyen ugyanis $t \in T \setminus (\{0\} \times H)$ tetszőleges pont. Ha $t \in T \setminus D$, akkor $\{t\}$ olyan környezete t-nek $\mathscr{T}$ szerint, amely nem metszi D-t, így a $\{0\} \times H \subseteq D$ halmazt sem. Ha $t \in D$ és $y \in \mathbb{R}$ olyan, hogy $t=(0,y)$, akkor $y \notin H$, ezért *bármely* $n \in \mathbb{N}^*$ esetén $V_n(y) \cap (\{0\} \times H) = \emptyset$, hiszen $(u,v) \in V_n(y) \cap (\{0\} \times H)$ esetén $u=0$ és $|y-v| \leq u = 0$, vagyis $v=y$, így $v \in H$ miatt $y \in H$, holott $y \notin H$. Tehát t-nek van olyan V környezete $\mathscr{T}$ szerint, amelyre $V \subseteq T \setminus (\{0\} \times H)$, vagyis a $T \setminus (\{0\} \times H)$ halmaz a $\mathscr{T}$ topológia szerint nyílt.

Vezessük most be az $F := \{0\} \times (\mathbb{R} \setminus \mathbb{Q})$ és $F' := \{0\} \times \mathbb{Q}$ halmazokat, amelyek diszjunktak, és az előzőek alapján $\mathscr{T}$-zártak. Legyenek Ω és Ω' olyan $\mathscr{T}$-nyílt halmazok, hogy $F \subseteq \Omega$ és $F' \subseteq \Omega'$. Megmutatjuk, hogy $\Omega \cap \Omega' \neq \emptyset$, ezért a $\mathscr{T}$ topológia *nem normális*. Ehhez legyen minden $n \in \mathbb{N}^*$ esetén $H_n := \{y \in \mathbb{R} \setminus \mathbb{Q} | V_n(y) \subseteq \Omega\}$. Az $F \subseteq \Omega$ feltétel és az Ω halmaz $\mathscr{T}$ szerinti nyíltsága alapján világos, hogy $\mathbb{R} \setminus \mathbb{Q} = \bigcup_{n \in \mathbb{N}^*} H_n$. Tudjuk, hogy $\mathbb{R} \setminus \mathbb{Q}$ az euklidészi topológia szerint második kategóriájú halmaz, így vehetünk olyan $n \in \mathbb{N}^*$ számot, amelyre $\overset{\circ}{\overline{H_n}} \neq \emptyset$, ahol a belsőrész és lezárás képzést az $\mathbb{R}$ halmaz euklidészi topológiájára vonatkoztatjuk. Ez azt jelenti, hogy van olyan I nem üres nyílt intervallum $\mathbb{R}$-ben, hogy $I \subseteq \overline{H_n}$. Legyen $y \in \mathbb{Q} \cap I$ rögzített racionális szám, és vegyünk olyan $(\varepsilon_m)_{m \in \mathbb{N}}$ sorozatot $\mathbb{R}_+^*$-ban, hogy $\lim_{m \to \infty} \varepsilon_m = 0$ az $\mathbb{R}$ euklidészi topológiája szerint. Ekkor $y \in \overline{H_n}$ miatt minden $m \in \mathbb{N}$ esetén $]y-\varepsilon_m, y+\varepsilon_m[\cap H_n \neq \emptyset$, ezért *kiválaszthatunk* olyan H_n-ben haladó $(y_m)_{m\in\mathbb{N}}$ sorozatot, amelyre minden $\mathbb{N}\ni m$-re $|y-y_m|<\varepsilon_m$, ezért $\lim_{m\to\infty} y_m = y$ az $\mathbb{R}$ euklidészi topológiája szerint. Mivel $y\in\mathbb{Q}$, így $(0,y)\in F'\subseteq\Omega'$, tehát létezik olyan $p\in\mathbb{N}$, hogy $V_p(y)\subseteq\Omega'$. Legyen $q\geq\max(n,p)$ rögzített természetes szám, és vegyünk olyan $m\in\mathbb{N}$ számot, amelyre $|y-y_m|<(2q-1)/q^2$. Az előző lemma szerint ekkor van olyan $k\in\mathbb{Z}$, hogy az $(u,v):=(1/q,k/q^2)$ pontra $(u,v)\in V_q(y)\cap V_q(y_m)$ teljesül, tehát $V:=V_q(y)\cap V_q(y_m)\neq\emptyset$. Ekkor $q\geq n$ és $y_m\in H_n$ miatt $V\subseteq V_q(y_m)\subseteq V_n(y_m)\subseteq\Omega$, és $q\geq p$ miatt $V\subseteq V_q(y)\subseteq V_p(y)\subseteq\Omega'$, ezért $V\subseteq\Omega\cap\Omega'$, vagyis $\Omega\cap\Omega'\neq\emptyset$. ■

Csak érdekességként megemlítjük, hogy az előző állításban értelmezett $\mathscr{T}$ topológiára teljesül az, hogy $\mathscr{E}^2_{\mathbb{R}}|T\leq\mathscr{T}$ és a $\mathscr{T}$ topológia leszűkítése mind D-re, mind $T\setminus D$-re diszkrét topológia. Ezek az állítások könnyen igazolhatók, csak azért nem foglalkoztunk velük, mert nem érintik a $\mathscr{T}$ topológia normálisságának problémáját.

28.8. Egypontú kompaktifikáció

Láttuk, hogy nem minden lokálisan kompakt tér normális (28.7.2. és 28.7.4.), mégis lehetséges a normális tereket jellemző alapvető tételek átvitele lokálisan kompakt terekre egy nagyon egyszerű konstrukció: az egypontú kompaktifikáció alkalmazásával.

28.8.1. Tétel. (Egypontú kompaktifikáció létezése és egyértelműsége) *Legyen T lokálisan kompakt tér.*

a) *Létezik olyan T' kompakt Hausdorff-tér, hogy T topologikus altere T'-nek és $T'\setminus T$ egy elemű halmaz.*

b) *Ha T' és T'' olyan kompakt Hausdorff-terek, amelyeknek T topologikus altere, és amelyekre $T'\setminus T$ és $T''\setminus T$ egy elemű halmazok, akkor létezik egyetlen olyan $f:T'\to T''$ homeomorfizmus, amelyre $f|_T=\mathrm{id}_T$.*

Bizonyítás. a) Legyen ω olyan halmaz, hogy $\omega\notin T$ (ilyen létezik, különben T az összes halmazok halmaza volna), és $T':=T\cup\{\omega\}$. Jelölje $\mathscr{T}$ a T topológiáját és $\mathscr{T}_\omega:=\{T'\setminus K|K \text{ kompakt halmaz } T\text{-ben}\}$. Megmutatjuk, hogy $\mathscr{T}':=\mathscr{T}\cup\mathscr{T}_\omega$ olyan topológia T' felett, hogy $(T',\mathscr{T}')$ kompakt Hausdorff-tér és $\mathscr{T}'|T=\mathscr{T}$.

Vilgos, hogy $T'=T'\setminus\emptyset\in\mathscr{T}_\omega\subseteq\mathscr{T}'$, tehát $\mathscr{T}'$-re $(\mathrm{O_I})$ teljesül. Két $\mathscr{T}$-beli halmaz metszete eleme $\mathscr{T}$-nek, mert $\mathscr{T}$-re $(\mathrm{O_{II}})$ teljesül. Két $\mathscr{T}_\omega$-beli halmaz metszete eleme $\mathscr{T}_\omega$-nak, mert a T bármely két kompakt részhalmazának az uniója kompakt T-ben. Ha $\Omega\in\mathscr{T}$ és $K\subseteq T$ kompakt halmaz, akkor $\Omega\cap(T'\setminus K)=\Omega\cap(T\setminus K)\in\mathscr{T}$, mert Ω nyílt T-ben és K zárt T-ben, hiszen K kompakt és T Hausdorff-tér. Ezért $\mathscr{T}'$-re teljesül az $(\mathrm{O_{II}})$ tulajdonság. A $\mathscr{T}$-re teljesül $(\mathrm{O_{III}})$, továbbá a T kompakt részhalmazai tetszőleges nem üres rendszerének a metszete kompakt T-ben, így bármely $\mathscr{T}_\omega$-ban haladó nem üres rendszer uniója eleme $\mathscr{T}_\omega$-nak. Ha $\Omega\subseteq T$ nyílt halmaz és $K\subseteq T$ kompakt halmaz, akkor $\Omega\cup(T'\setminus K)=\{\omega\}\cup(\Omega\cup(T\setminus K))=\{\omega\}\cup(T\setminus(K\setminus\Omega))\in\mathscr{T}_\omega$, mert $K\setminus\Omega$ kompakt halmaz T-ben. Ezért $\mathscr{T}'$-re $(\mathrm{O_{III}})$ is teljesül, vagyis $\mathscr{T}'$ topológia T felett.

Ha $\Omega\in\mathscr{T}$, akkor $\Omega=\Omega\cap T\in\mathscr{T}'|T$, hiszen $\Omega\in\mathscr{T}'$. Megfordítva, legyen $\Omega\in\mathscr{T}'|T$; ekkor van olyan $\Omega'\in\mathscr{T}'$, hogy $\Omega=\Omega'\cap T$. Ha $\Omega'\in\mathscr{T}$, akkor $\Omega=\Omega'\in\mathscr{T}$. Ha $\Omega'\in\mathscr{T}_\omega$, akkor van olyan $K\subseteq T$ kompakt halmaz, hogy $\Omega'=T'\setminus K$; ekkor $\Omega=(T'\setminus K)\cap T=T\setminus K\in\mathscr{T}$. Ez azt jelenti, hogy $\mathscr{T}=\mathscr{T}'|T$.

Megmutatjuk, hogy $(T',\mathscr{T}')$ kompakt Hausdorff-tér. Legyen $(\Omega'_i)_{i\in I}$ olyan halmazrendszer, hogy minden $i \in I$ esetén az $\Omega'_i \subseteq T'$ halmaz $\mathscr{T}'$-nyílt és $T' = \bigcup_{i\in I} \Omega'_i$. Létezik olyan $i(\omega) \in I$, amelyre $\omega \in \Omega'_{i(\omega)}$. Természetesen ekkor $\Omega'_{i(\omega)} \in \mathscr{T}_\omega$, így van olyan $K \subseteq T$ kompakt halmaz, hogy $\Omega'_{i(\omega)} = T' \setminus K$. A K halmaz a $\mathscr{T}'$ topológia szerint is kompakt, mert $\mathscr{T}'|T = \mathscr{T}$ és K kompakt a $\mathscr{T}$ topológia szerint. Ezért van olyan $J \subseteq I$ véges halmaz, hogy $K \subseteq \bigcup_{i\in J} \Omega'_i$. Világos, hogy az $(\Omega'_i)_{i\in\{i(\omega)\}\cup J}$ halmaz véges részbefedés, ami azt jelenti, hogy $(T', \mathscr{T}')$ kompakt tér. Ha $t \in T$, akkor a T lokális kompaktsága folytán van olyan $V \in \mathscr{T}(t) \subseteq \mathscr{T}'(t)$ környezet, amely kompakt a $\mathscr{T}$ szerint; ekkor $\omega \in T' \setminus V \in \mathscr{T}_\omega$, így $T' \setminus V \in \mathscr{T}'(\omega)$ és $V \in \mathscr{T}'(t)$, és ezek diszjunkt halmazok. Ezért $(T', \mathscr{T}')$ Hausdorff-tér.

b) Legyenek T' és T'' olyan kompakt Hausdorff-terek, hogy T topologikus altere T'-nek és T''-nek, valamint a $T' \setminus T$ és $T'' \setminus T$ halmazok egy eleműek. Legyen $\{\omega'\} = T' \setminus T$ és $\{\omega''\} = T'' \setminus T$, továbbá értelmezzük azt az $f : T' \to T''$ függvényt, amelyre $f(\omega') := \omega''$ és minden $t \in T$ esetén $f(t) := t$. Ez az egyetlen olyan $T' \to T''$ függvény, amely kiterjesztése az id_T identikus függvénynek. Minden $t \in T$ esetén a T halmaz nyílt környezete t-nek T'-ben, ezért a folytonosság lokalitása alapján f folytonos t-ben. Tehát azt kell igazolni, hogy f az ω' pontban folytonos. Legyen V környezete az $f(\omega') = \omega''$ pontnak T''-ben. Létezik olyan $\Omega \subseteq T''$ nyílt halmaz, hogy $\omega'' \in \Omega \subseteq V$. A $K := T'' \setminus \Omega$ halmaz zárt, tehát kompakt a T'' kompakt térben, és $\omega'' \in \Omega$ miatt $K \subseteq T$, így K kompakt T-ben is, hiszen T topologikus altere T''-nek. Ezért K kompakt T'-ben, mert T topologikus altere T'-nek is, következésképpen K zárt T'-ben, mert T' Hausdorff-tér. Tehát $T' \setminus K$ nyílt környezete ω'-nek T'-ben, és $\omega' \in T' \setminus K = T' \setminus \overset{-1}{f}\langle K\rangle = \overset{-1}{f}\langle T'' \setminus K\rangle = \overset{-1}{f}\langle \Omega\rangle \subseteq \overset{-1}{f}\langle V\rangle$, tehát $\overset{-1}{f}\langle V\rangle$ az ω' pontnak környezete T'-ben, így f folytonos az ω' pontban. Tehát az $f : T' \to T''$ függvény folytonos bijekció, így homeomorfizmus a T' és T'' kompakt terek között. ■

28.8.2. Definíció. *A T lokálisan kompakt tér* **egypontú** (*vagy* **Alekszandrov-féle**) **kompaktifikációjának** *nevezünk minden olyan T' kompakt Hausdorff-teret, amelynek T topologikus altere, és amelyre $T' \setminus T$ egy elemű halmaz. Ha T' egypontú kompaktifikációja a T lokálisan kompakt térnek, akkor a $T' \setminus T$ halmaz elemét a* **végtelen távoli pontnak** *nevezzük T'-ben.*

Tehát minden lokálisan kompakt térnek *létezik* egypontú kompaktifikációja és bármely két egypontú kompaktifikációja kitüntetett módon, topologikusan azonosítható egymással, tehát az egypontú kompaktifikáció (ilyen értelemben) *egyértelmű.* Az egypontú kompaktifikáció fogalmának alkalmazásaként azonnal bizonyítható a következő állítás.

28.8.3. Állítás. *Minden lokálisan kompakt tér teljesen reguláris.*

Bizonyítás. Minden lokálisan kompakt tér homeomorf bármely egypontú kompaktifikációjának egyik topologikus alterével. Ugyanakkor kompakt Hausdorff-tér normális T_1-tér, tehát teljesen reguláris, továbbá teljesen reguláris tér minden topologikus altere teljesen reguláris. ■

28.9. Uriszon-tétel, Tietze-tétel és egységfelosztás-tétel lokálisan kompakt térre

Láttuk, hogy a kompakt Hausdorff-terek normálisak (28.1.7.), ezért alkalmazható rájuk az Uriszon-tétel, a Tietze-tétel, és az egységfelosztás-tétel. Azonban a lokálisan kompakt terek nem szükségképpen normálisak (28.7.2.), ezért az imént említett tételekben megfogalmazott tulajdonságok csak korlátozott formában teljesülhetnek rájuk. Az egypontú kompaktifikáció fogalmának alkalmazásával most könnyen bebizonyíthatjuk ezeknek a tételeknek lokálisan kompakt terekre vonatkozó változatát.

28.9.1. Tétel. (Uriszon-tétel lokálisan kompakt terekre) *Ha T lokálisan kompakt tér, $K \subseteq T$ kompakt halmaz és $\Omega \subseteq T$ olyan nyílt halmaz, hogy $K \subseteq \Omega$, akkor létezik olyan $f : T \to \mathbb{R}$ kompakt tartójú folytonos függvény, hogy $0 \leq f \leq 1$, $K \subseteq [f = 1]$ és $\mathrm{supp}(f) \subseteq \Omega$.*

Bizonyítás. Legyen $U \subseteq T$ olyan relatív kompakt nyílt halmaz, amelyre $K \subseteq U \subseteq \overline{U} \subseteq \Omega$. Legyen T' egypontú kompaktifikációja T-nek. A K halmaz kompakt T'-ben, tehát zárt is T'-ben, mert T' Hausdorff-tér. Az U halmaz nyílt T'-ben, mert T nyílt topologikus altere T'-nek. A T' kompakt Hausdorff-tér normális, ezért az Uriszon-tétel alapján van olyan $f' : T' \to \mathbb{R}$ folytonos függvény, hogy $0 \leq f' \leq 1$, $K \subseteq [f' = 1]$ és $[f' \neq 0] \subseteq U$. Ekkor az $f := f'|_T : T \to \mathbb{R}$ függvény folytonos, $0 \leq f \leq 1$, $K \subseteq [f = 1]$ és $[f \neq 0] = [f' \neq 0] \cap T \subseteq U$, így $\mathrm{supp}(f) := \overline{[f \neq 0]} \subseteq \overline{U}$, tehát f kompakt tartójú és $\overline{U} \subseteq \Omega$ miatt $\mathrm{supp}(f) \subseteq \Omega$. ■

28.9.2. Tétel. (Tietze-tétel lokálisan kompakt terekre) *Legyen T lokálisan kompakt tér, $K \subseteq T$ kompakt halmaz és $\Omega \subseteq T$ olyan nyílt halmaz, hogy $K \subseteq \Omega$. Ha az $f : K \to \mathbb{R}$ függvény folytonos a K altértopológiája szerint, akkor létezik olyan $g : T \to \mathbb{R}$ kompakt tartójú folytonos függvény, amelyre $g|_K = f$ és $\mathrm{supp}(g) \subseteq \Omega$.*

Bizonyítás. Legyen T' egypontú kompaktifikációja T-nek. A lokálisan kompakt terekre vonatkozó Uriszon-tétel alapján rögzítünk olyan $\varphi : T \to \mathbb{R}$ kompakt tartójú folytonos függvényt, hogy $0 \leq \varphi \leq 1$, $K \subseteq [\varphi = 1]$ és $\mathrm{supp}(\varphi) \subseteq \Omega$. A K halmaz kompakt T'-ben is, ezért zárt, mert T' Hausdorff-tér. Alkalmazva a Tietze-tételt a T' normális térre, a $K \subseteq T'$ zárt halmazra, és az $f : K \to \mathbb{R}$ altéren folytonos függvényre kapjuk olyan $f' : T \to \mathbb{R}$ folytonos függvény létezését, amelyre $f'|_K = f$. Ekkor a $g := \varphi.(f'|_T) : T \to \mathbb{R}$ függvény folytonos kiterjesztése f-nek és $\mathrm{supp}(g) \subseteq \mathrm{supp}(\varphi) \subseteq \Omega$, tehát g kompakt tartójú. ■

Legyen T lokálisan kompakt tér, $K \subseteq T$ kompakt halmaz, $\Omega \subseteq T$ olyan nyílt halmaz, hogy $K \subseteq \Omega$, és $f : K \to \mathbb{R}$ olyan függvény, amely folytonos a K altértopológiája szerint, valamint $\alpha \leq f \leq \beta$, ahol $\alpha, \beta \in \mathbb{R}$ olyan számok, hogy $\alpha \leq \beta$. Ekkor van olyan $g : T \to \mathbb{R}$ folytonos kompakt tartójú függvény, amely f-nek kiterjesztése, $\mathrm{supp}(g) \subseteq \Omega$ és $\alpha \leq g \leq \beta$. Valóban, a lokálisan kompakt terekre vonatkozó Tietze-tétel szerint van olyan $g' : T \to \mathbb{R}$ kompakt tartójú folytonos függvény, amely kiterjesztése f-nek és $\mathrm{supp}(g') \subseteq \Omega$. Ekkor a $g := \inf(\beta, \sup(\alpha, g'))$ függvény szintén folytonos kiterjesztése f-nek, $\mathrm{supp}(g) \subseteq \mathrm{supp}(g') \subseteq \Omega$, és $\alpha \leq g \leq \beta$ nyilvánvalóan teljesül.

28.9.3. Tétel. (Dieudonné-féle egységfelosztás-tétel lokálisan kompakt terekre) *Legyen T lokálisan kompakt tér, $K \subseteq T$ kompakt halmaz és $(\Omega_i)_{i \in I}$ a T nyílt részhalmazainak olyan véges rendszere, hogy $K \subseteq \bigcup_{i \in I} \Omega_i$. Ekkor létezik olyan $(f_i)_{i \in I}$ rendszer,* *hogy minden $I \ni i$-re $f_i : T \to \mathbb{R}$ kompakt tartójú folyonos függvény,* $0 \leq f_i \leq 1$, $\operatorname{supp}(f_i) \subseteq \Omega_i$, *és* $K \subseteq \left[\sum_{i\in I} f_i = 1\right]$, *valamint* $\sum_{i\in I} f_i \leq 1$ *a T halmazon mindenütt.*

Bizonyítás. Először megmutatjuk olyan $(U_i)_{i\in I}$ halmazrendszer létezését, hogy minden $I \ni i$-re U_i relatív kompakt nyílt részhalmaza T-nek, $\overline{U_i} \subseteq \Omega_i$, és $K \subseteq \bigcup_{i\in I} U_i$. Valóban, kiválaszthatunk olyan $(V_t)_{t\in K}$ halmazrendszert, hogy minden $K \ni t$-re V_t olyan relatív kompakt nyílt környezete t-nek, amelyhez létezik olyan $i \in I$, hogy $\overline{V_t} \subseteq \Omega_i$. A K kompaktsága miatt van olyan $H \subseteq K$ véges halmaz, hogy $K \subseteq \bigcup_{t\in H} V_t$. Minden $i \in I$ esetén legyen $H_i := \{t \in H | \overline{V_t} \subseteq \Omega_i\}$, és értelmezzük az $U_i := \bigcup_{t\in H_i} V_t$ halmazt. Nyilvánvaló, hogy minden $i \in I$ esetén U_i olyan nyílt halmaz, hogy $\overline{U_i} = \bigcup_{t\in H_i} \overline{V_t} \subseteq \Omega_i$, és láthatóan U_i relatív kompakt, mert minden $H_i \ni t$-re $\overline{V_t}$ kompakt halmaz. Ha $t \in K$, akkor van olyan $s \in H$, hogy $t \in V_s$, és létezik olyan $i \in I$, hogy $\overline{V_s} \subseteq \Omega_i$; ekkor $s \in H_i$ és $t \in V_s \subseteq U_i$. Ez azt jelenti, hogy $K \subseteq \bigcup_{i\in I} U_i$, tehát $(U_i)_{i\in I}$ olyan halmazrendszer, amelynek a létezését állítottuk.

Minden $I \ni i$-re alkalmazzuk a lokálisan kompakt terekre vonatkozó Uriszon-tétel az $\overline{U_i}$ kompakt halmazra és Ω_i nyílt halmazra; tehát kiválasztunk olyan $g_i : T \to \mathbb{R}$ folytonos függvényt, hogy $0 \leq g_i \leq 1$, $\overline{U_i} \subseteq [g_i = 1]$ és $\operatorname{supp}(g_i) \subseteq \Omega_i$. Újra alkalmazzuk az Uriszon-tételt a K kompakt halmazra és az $\bigcup_{i\in I} U_i$ nyílt halmazra; tehát veszünk olyan $g : T \to \mathbb{R}$ kompakt tartójú folytonos függvényt, hogy $0 \leq g \leq 1$, $K \subseteq [g = 1]$ és $\operatorname{supp}(g) \subseteq \bigcup_{i\in I} U_i$. Ezután minden $I \ni i$-re értelmezzük az

$$f_i : T \to \mathbb{R}; \quad t \mapsto \begin{cases} \dfrac{g(t)g_i(t)}{\sum_{j\in I} g_j(t)} & \text{, ha } t \in \bigcup_{j\in I} U_j; \\ 0 & \text{, ha } t \in T \setminus \bigcup_{j\in I} U_j \end{cases}$$

függvényt, amelyre $0 \leq f_i \leq 1$ és $\operatorname{supp}(f_i) \subseteq \operatorname{supp}(g_i) \subseteq \Omega_i$ nyilvánvalóan teljesül, továbbá

$$K = K \cap [g = 1] \subseteq \left(\bigcup_{i\in I} U_i\right) \cap [g = 1] \subseteq \left[\sum_{i\in I} f_i = 1\right],$$

és természetesen $\sum_{i\in I} f_i \leq g \leq 1$. Ezért elég azt igazolni, hogy minden $i \in I$ esetén f_i *folytonos* függvény. Legyen $i \in I$ rögzített. A folytonosság lokalitása alapján nyilvánvaló, hogy f_i folytonos az $\bigcup_{j\in I} U_j$ nyílt halmaz minden pontjában. Továbbá, $f_i = 0$ a $T \setminus \operatorname{supp}(g_i)$ halmazon, ami a $T \setminus \bigcup_{j\in I} U_j$ halmaz minden pontjának nyílt környezete, ezért ismét a folytonosság lokalitása miatt f_i folytonos a $T \setminus \bigcup_{j\in I} U_j$ halmaz minden pontjában. Tehát $T = (T \setminus \operatorname{supp}(g)) \cup \left(\bigcup_{j\in I} U_j\right)$ miatt f_i folytonos függvény. ■

28.10. Félig folytonos függvények lokálisan kompakt tér felett

28.10.1. Állítás. *Legyen T lokálisan kompakt tér és jelölje $\mathscr{K}(T;\mathbb{R})$ a $T \to \mathbb{R}$ kompakt tartójú folytonos függvények halmazát.*

a) *Ha $f : T \to \overline{\mathbb{R}}_+$ alulról félig folytonos függvény, akkor*

$$f = \sup_{\substack{\varphi \in \mathscr{K}(T;\mathbb{R}) \\ 0 \le \varphi \le f}} \varphi.$$

b) *Ha $f : T \to \mathbb{R}_+$ kompakt tartójú felülről félig folytonos függvény, akkor*

$$f = \inf_{\substack{\varphi \in \mathscr{K}(T;\mathbb{R}) \\ f \le \varphi}} \varphi.$$

Bizonyítás. a) Legyenek $t \in T$ és $c \in \mathbb{R}$ olyanok, hogy $c < f(t)$. Elegendő olyan $\varphi \in \mathscr{K}(T;\mathbb{R})$ függvényt találni, amelyre $0 \le \varphi \le f$ és $c \le \varphi(t)$. Az f alulról félig folytonossága miatt a $[c < f]$ halmaz nyílt környezete t-nek. A lokálisan terekre vonatkozó Uriszon-tételt alkalmazzuk a $\{t\}$ kompakt halmazra és $[c < f]$ nyílt halmazra. Létezik tehát olyan $\psi \in \mathscr{K}(T;\mathbb{R})$, hogy $0 \le \psi \le 1$, $\psi(t) = 1$ és $\mathrm{supp}(\psi) \subseteq [c < f]$. Ekkor a $\varphi := c\psi$ függvény kompakt tartójú, folytonos, és $\varphi(t) = c$. Ha $s \in [c < f]$, akkor nyilvánvaló, hogy $0 \le \varphi(s) := c\psi(s) \le c < f(s)$, ugyanakkor $s \in T \setminus [c < f]$ esetén $\varphi(s) = 0 \le f(s)$, tehát $0 \le \varphi \le f$.

b) Először megjegyezzük, hogy f *felülről korlátos*, mert az f felülről félig folytonossága miatt az $([f < n])_{n\in\mathbb{N}}$ monoton növő halmazsorozat mindegyik tagja nyílt halmaz, és $+\infty \notin \mathrm{Im}(f)$ miatt $T = \bigcup_{n\in\mathbb{N}} [f < n]$, így a $\mathrm{supp}(f)$ kompakt halmazhoz van olyan $n \in \mathbb{N}$, amelyre $\mathrm{Im}(f) \subseteq [f < n]$, tehát minden $T \ni t$-re $f(t) < n$. A lokálisan kompakt terekre vonatkozó Uriszon-tételt alkalmazva a $\mathrm{supp}(f)$ kompakt halmazra és T nyílt halmazra kapjuk olyan $\psi_0 \in \mathscr{K}(T;\mathbb{R})$ létezését, amelyre $0 \le \psi \le 1$ és $\mathrm{supp}(f) \subseteq [\psi_0 = 1]$. Ha $C \in \mathbb{R}_+$ olyan, hogy $f \le C$, akkor a $\psi := C\psi_0 \in \mathscr{K}(T;\mathbb{R})$ függvényre $f \le \psi$ nyilvánvalóan teljesül.

Rögzítsünk olyan $\psi \in \mathscr{K}(T;\mathbb{R})$ függvényt, amelyre $f \le \psi$. Ekkor $\psi - f : T \to \mathbb{R}_+$ alulról félig folytonos függvény, tehát az a) alapján írható, hogy

$$f = \psi - (\psi - f) = \psi - \sup_{\substack{\varphi \in \mathscr{K}(T;\mathbb{R}) \\ 0 \le \varphi \le \psi - f}} \varphi = \inf_{\substack{\varphi \in \mathscr{K}(T;\mathbb{R}) \\ 0 \le \varphi \le \psi - f}} (\psi - \varphi) = \inf_{\substack{\varphi \in \mathscr{K}(T;\mathbb{R}) \\ 0 \le \varphi \\ f \le \psi - \varphi}} (\psi - \varphi) = \inf_{\substack{\varphi' \in \mathscr{K}(T;\mathbb{R}) \\ f \le \varphi' \le \psi}} \varphi',$$

ahol kihasználtuk azt a nyilvánvaló tényt, hogy

$$\{\psi - \varphi | (\varphi \in \mathscr{K}(T;\mathbb{R})) \wedge (0 \le \varphi) \wedge (f \le \psi - \varphi)\} = \{\varphi' | (\varphi' \in \mathscr{K}(T;\mathbb{R})) \wedge (f \le \varphi' \le \psi)\}.$$

Ugyanakkor

$$\inf_{\substack{\varphi \in \mathscr{K}(T;\mathbb{R}) \\ f \le \varphi}} \varphi \le \inf_{\substack{\varphi' \in \mathscr{K}(T;\mathbb{R}) \\ f \le \varphi' \le \psi}} \varphi'$$

nyilvánvalóan igaz, ezért

$$\inf_{\substack{\varphi \in \mathscr{K}(T;\mathbb{R}) \\ f \le \varphi}} \varphi \le f.$$

A fordított egyenlőtlenség triviális, ezért itt egyenlőség áll. ■

28.11. Baire-terek és a kategóriatétel

28.11.1. Definíció. *Legyen T topologikus tér. Azt mondjuk, hogy az $E \subseteq T$ halmaz*

– **sehol sem sűrű**, *ha* $\overset{\circ}{\overline{E}} = \emptyset$;

– **első kategóriájú**, *ha E előállítható megszámlálható sok sehol sem sűrű halmaz uniójaként;*

– **második kategóriájú**, *ha nem első kategóriájú.*

28.11.2. Definíció. *Azt mondjuk, hogy a T topologikus tér* **Baire-tér**, *ha a T minden nem üres nyílt részhalmaza második kategóriájú.*

Megjegyzések. 1) Sehol sem sűrű (illetve első kategóriájú) halmaz minden részhalmaza sehol sem sűrű (illetve első kategóriájú). Egy halmaz pontosan akkor sehol sem sűrű, ha a lezártja sehol sem sűrű. Első kategóriájú halmazok *megszámlálható* rendszerének az uniója szintén első kategóriájú. Ezek az állítások a definícióból nyilvánvalóan következnek.

2) Ha T topologikus tér, akkor egy $E \subseteq T$ halmaz pontosan akkor sehol sem sűrű, ha az $T \setminus \overline{E}$ halmaz sűrű T-ben. Ez azonnal látható az $\overset{\circ}{\overline{E}} = T \setminus \overline{(T \setminus \overline{E})}$ egyenlőségből.

3) *Véges* sok sehol sem sűrű halmaz uniója sehol sem sűrű. Ezt elegendő két sehol sem sűrű halmaz uniójára igazolni. Legyen T topologikus tér és legyenek $E, E' \subseteq T$ sehol sem sűrű halmazok. Azt kell megmutatni, hogy az $T \setminus \overline{E \cup E'}$ halmaz sűrű T-ben, vagyis $\overline{E \cup E'} = \overline{E} \cup \overline{E'}$ és a de Morgan egyenlőség alapján azt, hogy $(T \setminus \overline{E}) \cap (T \setminus \overline{E'})$ sűrű halmaz. Ennek bizonyításához legyen $t \in T$ és V nyílt környezete T-nek. A E halmaz sehol sem sűrű, ezért $T \setminus \overline{E}$ sűrű T-ben, tehát $(T \setminus \overline{E}) \cap V \neq \emptyset$; legyen $t' \in (T \setminus \overline{E}) \cap V$. Az $(T \setminus \overline{E}) \cap V$ halmaz nyílt környezete t'-nek, ugyanakkor E' sehol sem sűrű, tehát $T \setminus \overline{E'}$ sűrű T-ben, így $(T \setminus \overline{E'}) \cap (T \setminus \overline{E}) \cap V \neq \emptyset$. Ez azt jelenti, hogy $(T \setminus \overline{E \cup E'}) \cap V \neq \emptyset$, így $T \setminus \overline{E \cup E'}$ sűrű halmaz, vagyis $E \cup E'$ sehol sem sűrű.

4) *Megszámlálhatóan végtelen* sok sehol sem sűrű halmaz uniója nem szükségképpen sehol sem sűrű (csak első kategóriájú). Például $\mathbb{R}$-ben az euklidészi metrika szerint minden egy elemű halmaz sehol sem sűrű, így $\mathbb{Q}$ első kategóriájú halmaz, de természetesen $\mathbb{Q}$ nem sehol sem sűrű $\mathbb{R}$-ben.

5) Ha T topologikus tér, akkor egy $E \subseteq T$ halmaz pontosan akkor első kategóriájú, ha létezik az T *zárt* sehol sem sűrű részhalmazainak olyan $(F_n)_{n\in\mathbb{N}}$ sorozata, hogy $E \subseteq \bigcup\limits_{n\in\mathbb{N}} F_n$. Valóban, ha E első kategóriájú, és $(E_n)_{n\in\mathbb{N}}$ sehol sem sűrű halmazok olyan sorozata, hogy $E = \bigcup\limits_{n\in\mathbb{N}} E_n$, akkor a $(\overline{E_n})_{n\in\mathbb{N}}$ halmazsorozat mindegyik tagja sehol sem sűrű zárt halmaz, továbbá $E \subseteq \bigcup\limits_{n\in\mathbb{N}} \overline{E_n}$. Megfordítva, ha $(F_n)_{n\in\mathbb{N}}$ az T zárt sem sűrű részhalmazainak olyan sorozata, hogy $E \subseteq \bigcup\limits_{n\in\mathbb{N}} F_n$, akkor $E = \bigcup\limits_{n\in\mathbb{N}} (E \cap F_n)$, és minden $n \in \mathbb{N}$ esetén $F_n \cap E$ sehol sem sűrű halmaz, tehát E első kategóriájú.

28.11.3. Állítás. *Legyen T topologikus tér, $S \subseteq T$ és $E \subseteq S$. Ha az E halmaz sehol sem sűrű az S topologikus altérben, akkor sehol sem sűrű T-ben is. Ha S nyílt halmaz T-ben és az E halmaz sehol sem sűrű T-ben, akkor E sehol sem sűrű az S topologikus altérben is.*

Bizonyítás. (I) Tegyük fel, hogy E nem sehol sem sűrű T-ben, és vegyünk egy $t \in \overset{\circ}{\overline{E}}$ pontot. Ekkor $\overset{\circ}{\overline{E}} \subseteq \overline{E}$ miatt $t \in \overline{E}$ és $\overset{\circ}{\overline{E}}$ nyílt környezete t-nek T-ben, ezért $\overset{\circ}{\overline{E}} \cap E \neq \emptyset$. Ugyanakkor $\overset{\circ}{\overline{E}} \cap E \subseteq \overset{\circ}{\overline{E}} \cap S \subseteq \overline{E} \cap S$, és $\overline{E} \cap S$ az E halmaz lezártja az S topologikus altérben. Mivel pedig a $\overset{\circ}{\overline{E}} \cap S$ halmaz nyílt is az S topologikus altérben és nem üres, így az E halmaz S topologikus altérben vett lezártja tartalmaz ebben az altérben nyílt, nem üres halmazt, vagyis E nem sehol sem sűrű az S topologikus altérben. Ezzel az első állítást igazoltuk.

(II) Tegyük fel, hogy S nyílt részhalmaza T-nek, és az $E \subseteq S$ halmaz nem sehol sem sűrű az S topologikus altérben. Ekkor $\overline{E} \cap S$-nek, vagyis az E halmaz S altérbeli lezártjának az altérbeli belseje nem üres, tehát létezik olyan $\Omega \subseteq T$ nyílt halmaz, hogy $\emptyset \neq \Omega \cap S \subseteq \overline{E} \cap S$. Ekkor $\Omega \cap S$ nem üres nyílt halmaz T-ben, hiszen S is nyílt T-ben, és $\Omega \cap S \subseteq \overline{E}$, így E nem sehol sem sűrű T-ben. Ezzel a második állítást igazoltuk. ■

28.11.4. Következmény. *Legyen T topologikus tér, $S \subseteq T$, és $E \subseteq S$. Ha az E halmaz I. kategóriájú az S topologikus altérben, akkor I. kategóriájú T-ben is. Ha S nyílt halmaz T-ben és az E halmaz I. kategóriájú T-ben, akkor E I. kategóriájú az S topologikus altérben is.*

Bizonyítás. (I) Legyen az E halmaz I. kategóriájú az S topologikus altérben, és vegyünk olyan $(H_n)_{n\in\mathbb{N}}$ halmazsorozatot, hogy minden $n \in \mathbb{N}$ esetén $H_n \subseteq S$ sehol sem sűrű az S topologikus altérben, és $E = \bigcup\limits_{n\in\mathbb{N}} H_n$. Az előző állítás szerint minden $n \in \mathbb{N}$ esetén a H_n halmaz T-ben is sehol sem sűrű, ezért az E halmaz I. kategóriájú T-ben.

(II) Legyen az E halmaz I. kategóriájú T-ben, és vegyünk olyan $(H_n)_{n\in\mathbb{N}}$ halmazsorozatot, hogy minden $n \in \mathbb{N}$ esetén $H_n \subseteq T$ sehol sem sűrű T-ben, és $E = \bigcup\limits_{n\in\mathbb{N}} H_n$. Ekkor minden $n \in \mathbb{N}$ esetén a $H_n \subseteq S$ halmaz is sehol sem sűrű T-ben, és S nyílt T-ben, így az előző állítás szerint H_n sehol sem sűrű az S topologikus altérben. Ezért az E halmaz I. kategóriájú az S topologikus altérben. ■

Tehát ha S nyílt részhalmaz a T topologikus térben, akkor egy $E \subseteq S$ halmaz pontosan akkor I. kategóriájú (illetve II. kategóriájú) T-ben, ha I. kategóriájú (illetve II. kategóriájú) az S topologikus altérben.

28.11.5. Állítás. *Baire-tér minden nyílt topologikus altere Baire-tér.*

Bizonyítás. Legyen T Baire-tér, $S \subseteq T$ nyílt halmaz és $\Omega \subseteq S$ olyan nem üres halmaz, amely nyílt az S topologikus altérben. Ekkor az S halmaz T-beli nyíltsága miatt Ω nyílt T-ben is, és nem üres. Mivel T Baire-tér, így az Ω halmaz II. kategóriájú T-ben, vagyis nem I. kategóriájú T-ben. Az előző következmény szerint Ω nem I. kategóriájú az S topologikus altérben sem. Ez azt jelenti, hogy az S topologikus altér Baire-tér. ■

28.11.6. Állítás. *Topologikus tér pontosan akkor Baire-tér, ha minden pontjának van olyan környezete, amely az altértopológiával ellátva Baire-tér.*

Bizonyítás. A feltétel triviálisan szükséges. Az elégségesség bizonyításához legyen T olyan topologikus tér, hogy T minden pontjának van olyan környezete, amely az altértopológiával ellátva Baire-tér, és legyen $\Omega \subseteq T$ nem üres nyílt halmaz. Legyen $t \in \Omega$ rögzített pont, és legyen V a t pontnak olyan környezete, amely az altértopológiával ellátva Baire-tér. Ekkor $\overset{\circ}{V}$ a V topologikus altérben nyílt halmaz, így az előző állítás alapján $\overset{\circ}{V}$ az altértopológiával ellátva szintén Baire-tér. Ugyanakkor $\Omega \cap \overset{\circ}{V}$ nem üres nyílt részhalmaza az $\overset{\circ}{V}$ nyílt topologikus altérnek, tehát az $\Omega \cap \overset{\circ}{V}$ halmaz II. kategóriájú az $\overset{\circ}{V}$ nyílt topologikus altérben. Ezért az $\Omega \cap \overset{\circ}{V}$ halmaz II. kategóriájú T-ben is, így az ezt tartalmazó Ω halmaz még inkább II. kategóriájú T-ben. ■

28.11.7. Tétel. (Baire-féle kategóriatétel) *Minden teljesen félmetrizálható és minden lokálisan kompakt tér Baire-tér.*

Bizonyítás. (I) Legyen T teljesen félmetrizálható topologikus metrikus tér, és d olyan félmetrika T felett, amely a T topológiáját generálja. Legyen $\Omega \subseteq T$ nem üres nyílt halmaz, és $(F_n)_{n\in\mathbb{N}}$ az T zárt sehol sem sűrű részhalmazainak tetszőleges sorozata. Megmutatjuk, hogy ekkor $\Omega \setminus \bigcup_{n\in\mathbb{N}} F_n \neq \emptyset$, így az 5) megjegyzés alapján Ω nem lehet első kategóriájú.

Először megjegyezzük, hogy 3) megjegyzés szerint minden $n \in \mathbb{N}$ esetén $\bigcup_{k=0}^{n} F_k$ sehol sem sűrű zárt halmaz, vagyis $\mathrm{Int}\left(\bigcup_{k=0}^{n} F_k\right) = \emptyset$, így $\Omega \setminus \bigcup_{k=0}^{n} F_k \neq \emptyset$, különben $\emptyset \neq \Omega \subseteq \bigcup_{k=0}^{n} F_k$ teljesülne, tehát $\mathrm{Int}\left(\bigcup_{k=0}^{n} F_k\right) \neq \emptyset$ igaz volna.

Most a kiválasztási axiómával kombinált rekurzió tételét alkalmazva igazoljuk olyan $T \times \mathbb{R}_+^*$-ban haladó $((t_n, r_n))_{n\in\mathbb{N}}$ sorozat létezését, amelyre

$$\overline{\mathrm{B}}_{r_0}(t_0; d) \subseteq \Omega \setminus F_0,$$

és minden $n \in \mathbb{N}$ esetén

$$\overline{\mathrm{B}}_{r_{n+1}}(t_{n+1}; d) \subseteq \mathrm{B}_{r_n}(t_n; d) \setminus \bigcup_{k=0}^{n+1} F_k,$$

valamint $r_{n+1} < \dfrac{r_n}{2}$.

Az $\Omega \setminus F_0$ halmaz nyílt és nem üres, így van olyan $t_0 \in T$ és $r_0 \in \mathbb{R}_+^*$, hogy $\overline{\mathrm{B}}_{r_0}(t_0; d) \subseteq \Omega \setminus F_0$. Legyen $n \in \mathbb{N}$ és $((t_m, r_m))_{0\leq m\leq n}$ olyan rendszer $T \times \mathbb{R}_+^*$-ban, hogy $\overline{\mathrm{B}}_{r_0}(t_0; d) \subseteq \Omega \setminus F_0$, és minden $0<m<n$ természetes számra $\overline{\mathrm{B}}_{r_{m+1}}(t_{m+1}; d) \subseteq \mathrm{B}_{r_m}(t_m; d) \setminus \bigcup_{k=0}^{m+1} F_k$, valamint minden $m < n$ természetes számra $r_{m+1} < \dfrac{r_m}{2}$. Az $\bigcup_{k=0}^{n+1} F_k$ halmaz sehol sem sűrű és zárt, így $\mathrm{B}_{r_n}(t_n; d) \setminus \bigcup_{k=0}^{n+1} F_k \neq \emptyset$, és ez nyílt halmaz, így van olyan $t \in T$ és $r \in \mathbb{R}_+^*$, hogy $\overline{\mathrm{B}}_r(t; d) \subseteq \mathrm{B}_{r_n}(t_n; d) \setminus \bigcup_{k=0}^{n+1} F_k$. Legyen $t_{n+1} := t$ és $r_{n+1} \in \mathbb{R}_+^*$ tetszőleges olyan szám, amelyre $r_{n+1} < \min(r, r_n/2)$. Ekkor az $((t_m, r_m))_{0\leq m\leq n+1}$ rendszer $T \times \mathbb{R}_+^*$-ben halad, és minden $m < n + 1$ természetes számra $\overline{\mathrm{B}}_{r_{m+1}}(t_{m+1}; d) \subseteq \mathrm{B}_{r_m}(t_m; d) \setminus \bigcup_{k=0}^{m+1} F_k$, valamint minden $m < n + 1$ természetes számra $r_{m+1} < \dfrac{r_m}{2}$. Ezért a kiválasztási axiómával kombinált rekurzió tétele szerint vehetünk olyan $T \times \mathbb{R}_+^*$-ban haladó $((t_n, r_n))_{n\in\mathbb{N}}$ sorozatot, amely rendelkezik az előírt tulajdonságokkal.

Könnyen látható, hogy $m, n \in \mathbb{N}$ és $m \leq n$ esetén $t_n \in \overline{\mathrm{B}}_{r_n}(t_n; d) \subseteq \overline{\mathrm{B}}_{r_m}(t_m; d)$, így $d(t_m, t_n) \leq r_m$. Ebből látszik, hogy minden $\mathbb{N} \ni m, n$-re $d(t_m, t_n) \leq r_{\min(m,n)}$. Ugyanakkor minden $n \in \mathbb{N}^*$ esetén $r_n < \dfrac{r_0}{2^n}$, vagyis az $(r_n)_{n\in\mathbb{N}}$ számsorozat 0-hoz tart $\mathbb{R}$-ben. Ezért $(t_n)_{n\in\mathbb{N}}$ Cauchy-sorozat T-ben, így vehetjünk *egy olyan* $t \in T$ pontot, amelyhez a $(t_n)_{n\in\mathbb{N}}$ sorozat konvergál. Ha $m \in \mathbb{N}$, akkor az $(t_{m+n})_{n\in\mathbb{N}}$ részsorozat az $\overline{\mathrm{B}}_{r_m}(t_m; d)$ zárt halmazban halad, és szintén konvergál t-hez, ezért $t \in \overline{\mathrm{B}}_{r_m}(t_m; d)$. Tehát minden $\mathbb{N} \ni m$-re $t \in \overline{\mathrm{B}}_{r_m}(t_m; d)$, ugyanakkor $\overline{\mathrm{B}}_{r_m}(t_m; d) \cap \bigcup_{k=0}^{m} F_k = \emptyset$. Ez azt jelenti, hogy $t \in \Omega \setminus \bigcup_{k\in\mathbb{N}} F_k$.

(II) Legyen T lokálisan kompakt tér, és indirekt feltesszük, hogy $\Omega \subseteq T$ nem üres, első kategóriájú nyílt halmaz. Legyen $(F_n)_{n\in\mathbb{N}}$ olyan halmazsorozat, amelynek mindegyik tagja sehol sem sűrű zárt halmaz T-ben és $\Omega \subseteq \bigcup_{n\in\mathbb{N}} F_n$.

A kiválasztási axiómával kombinált rekurzió tételét alkalmazva igazoljuk olyan $(K_n)_{n\in\mathbb{N}}$ halmazsorozat létezését, hogy $K_0 \subseteq \Omega \setminus F_0$, és minden $\mathbb{N} \ni n$-re $K_n \subseteq T$ kompakt halmaz, $\overset{\circ}{K}_n \neq \emptyset$, valamint $K_{n+1} \subseteq \overset{\circ}{K}_n \setminus \left(\bigcup_{k=0}^{n+1} F_k\right)$.

A F_0 halmaz sehol sem sűrű és zárt, így $\overset{\circ}{F_0} = \emptyset$, tehát $\Omega \neq \emptyset$ miatt $\Omega \setminus F_0 \neq \emptyset$. Ha $t \in \Omega \setminus F_0$, akkor $\Omega \setminus F_0$ nyílt környezete t-nek, tehát létezik olyan $U \subseteq T$ relatív kompakt nyílt halmaz, hogy $t \in U \subseteq \overline{U} \subseteq \Omega \setminus F_0$. Legyen $K_0 := \overline{U}$; ekkor K_0 kompakt halmaz T-ben, $K_0 \subseteq \Omega \setminus F_0$ és $\overset{\circ}{K_0} \supseteq U \neq \emptyset$.

Legyen $n \in \mathbb{N}^*$, és tegyük fel, hogy $(K_j)_{j\in n}$ olyan rendszer, hogy $K_0 \subseteq \Omega \setminus F_0$, és minden $n \ni j$-re $K_j \subseteq T$ kompakt halmaz, $\overset{\circ}{K}_j \neq \emptyset$, valamint $j+1 < n$ esetén $K_{j+1} \subseteq \overset{\circ}{K}_j \setminus \left(\bigcup_{k=0}^{j+1} F_k\right)$. Az $\overset{\circ}{K}_{n-1}$ halmaz nyílt és nem üres, továbbá $\bigcup_{k=0}^{n} F_k$ sehol sem sűrű zárt halmaz, ezért $\overset{\circ}{K}_{n-1} \setminus \left(\bigcup_{k=0}^{n} F_k\right) \neq \emptyset$. Ha t eleme ennek a halmaznak, akkor létezik olyan $U \subseteq T$ relatív kompakt nyílt halmaz, amelyre $t \in U \subseteq \overline{U} \subseteq \overset{\circ}{K}_{n-1} \setminus \left(\bigcup_{k=0}^{n} F_k\right)$. Legyen $K_n := \overline{U}$; ekkor K_n kompakt részhalmaza T-nek, $K_n \subseteq \overset{\circ}{K}_{n-1} \setminus \left(\bigcup_{k=0}^{n} F_k\right)$ és $\overset{\circ}{K}_n \supseteq U \neq \emptyset$. Tehát a $(K_j)_{j\in n+1}$ rendszer olyan, hogy $K_0 \subseteq \Omega \setminus F_0$, és minden $n+1 \ni j$-re $K_j \subseteq T$ kompakt halmaz, $\overset{\circ}{K}_j \neq \emptyset$, valamint $j+1 < n+1$ esetén $K_{j+1} \subseteq \overset{\circ}{K}_j \setminus \left(\bigcup_{k=0}^{j+1} F_k\right)$.

Rögzítsünk egy olyan $(K_n)_{n\in\mathbb{N}}$ halmazsorozatot, amelynek létezését igazoltuk az imént. Minden $\mathbb{N} \ni n$-re $K_{n+1} \subseteq K_n$ és $K_n \neq \emptyset$ kompakt halmaz, ezért a Cantor-féle közösrész-tétel alapján $\bigcap_{n\in\mathbb{N}} K_n \neq \emptyset$; legyen $t \in \bigcap_{n\in\mathbb{N}} K_n$. Ekkor $t \in K_0 \subseteq \Omega$, ugyanakkor minden

$n \in \mathbb{N}^*$ esetén $t \in K_n \subseteq \overset{\circ}{K}_{n-1} \setminus \left(\bigcup_{k=0}^{n} F_k \right)$, tehát $t \notin \bigcup_{k=0}^{n} F_k$. Ezért $t \notin \bigcup_{n \in \mathbb{N}} F_n$, vagyis $t \in \Omega \setminus \left(\bigcup_{n \in \mathbb{N}} F_n \right)$, ami ellentmond az $\Omega \subseteq \bigcup_{n \in \mathbb{N}} F_n$ feltételnek. ■

28.12. Parakompakt terek

28.12.1. Definíció. *Ha $(U_i)_{i \in I}$ és $(V_j)_{j \in J}$ halmazrendszerek, akkor azt mondjuk, hogy $(V_j)_{j \in J}$ finomítása $(U_i)_{i \in I}$-nek, ha minden $j \in J$ esetén van olyan $i \in I$, hogy $V_j \subseteq U_i$. Azt mondjuk, hogy a T topologikus tér* **parakompakt**, *ha a T bármely nyílt befedésének létezik olyan finomítása, amely lokálisan véges nyílt befedése T-nek. A T topologikus tér E részhalmazát parakompaktnak mondjuk, ha az E topologikus altér parakompakt tér.*

Például, ha $(U_i)_{i \in I}$ tetszőleges halmazrendszer, akkor minden $J \subseteq I$ halmazra $(U_i)_{i \in J}$ finomítása $(U_i)_{i \in I}$-nek. Ugyanakkor topologikus tér részhalmazainak bármely véges rendszere nyilvánvalóan lokálisan véges. Ezért minden kompakt tér parakompakt, vagyis a parakompaktság a kompaktság fogalmának általánosítása.

Ha $(U_i)_{i \in I}$, $(V_j)_{j \in J}$ és $(W_k)_{k \in K}$ halmazrendszerek, és $(W_k)_{k \in K}$ finomítása $(V_j)_{j \in J}$-nek, valamint $(V_j)_{j \in J}$ finomítása $(U_i)_{i \in I}$-nek, akkor $(W_k)_{k \in K}$ finomítása $(U_i)_{i \in I}$-nek, hiszen $k \in K$ esetén van olyan $j \in J$, hogy $W_k \subseteq V_j$ és a j indexhez van olyan $i \in I$, hogy $V_j \subseteq U_i$, tehát ekkor $W_k \subseteq V_j \subseteq U_i$. Erre a tulajdonságra úgy fogunk hivatkozni, mint *a finomítás tranzitivitása.*

Vigyázzunk arra, hogy ha T topologikus tér és $(U_i)_{i \in I}$ lokálisan véges halmazrendszer T-ben, akkor $(U_i)_{i \in I}$ finomításai már nem szükségképpen lokálisan végesek. De ha $(V_j)_{j \in J}$ olyan finomítása az $(U_i)_{i \in I}$ lokálisan véges halmazrendszernek, hogy $J \subseteq I$ és minden $j \in J$ esetén $V_j \subseteq U_j$, akkor $(V_j)_{j \in J}$ is lokálisan véges, hiszen $t \in T$ esetén létezik t-nek olyan U környezete, hogy $\{i \in I | U \cap U_i \neq \emptyset\}$ véges halmaz, és ekkor $\{j \in J | U \cap V_j \neq \emptyset\} \subseteq \{i \in I | U \cap U_i \neq \emptyset\}$, így $\{j \in J | U \cap V_j \neq \emptyset\}$ is véges halmaz.

28.12.2. Állítás. *Ha T parakompakt tér, akkor T bármely $(\Omega_i)_{i \in I}$ nyílt befedéséhez létezik olyan $(V_i)_{i \in I}$ (ugyanolyan indexhalmazú) lokálisan véges nyílt befedése T-nek, hogy minden $i \in T$ esetén $V_i \subseteq \Omega_i$.*

Bizonyítás. A T topologikus tér parakompaktsága alapján vegyünk olyan $(W_j)_{j \in J}$ lokálisan véges finomítását $(\Omega_i)_{i \in I}$-nek, amely nyílt befedése T-nek. Minden $j \in J$ esetén $\{i \in I | W_j \subseteq \Omega_i\} \neq \emptyset$, ezért kiválaszthatunk egy $\sigma \in \prod_{j \in J} \{i \in I | W_j \subseteq \Omega_i\}$ függvényt; tehát $\sigma : J \to I$ olyan függvény, amelyre minden $j \in J$ esetén $W_j \subseteq \Omega_{\sigma(j)}$. Minden $i \in I$ esetén legyen

$$V_i := \bigcup_{j \in \overset{-1}{\sigma}\langle\{i\}\rangle} W_j.$$

Ekkor minden $i \in I$ esetén V_i nyílt részhalmaza T-nek, és $(V_i)_{i \in I}$ befedése T-nek, mert $t \in T$ esetén van olyan $j \in J$, hogy $t \in W_j$, és ekkor $i := \sigma(j) \in I$ olyan index, hogy $j \in \overset{-1}{\sigma}\langle\{i\}\rangle$, így $t \in W_j \subseteq V_i$. Nyilvánvaló, hogy minden $i \in I$ esetén $V_i \subseteq \Omega_i$, mert ha $j \in \overset{-1}{\sigma}\langle\{i\}\rangle$, akkor $W_j \subseteq \Omega_{\sigma(j)} = \Omega_i$, tehát $V_i = \bigcup_{j \in \overset{-1}{\sigma}\langle\{i\}\rangle} W_j \subseteq \Omega_i$. Végül megmutatjuk, hogy a $(V_i)_{i \in I}$ halmazrendszer lokálisan véges. Legyen $t \in T$ rögzítve, és a $(W_j)_{j \in J}$

halmazrendszer lokálisan végessége szerint vegyünk olyan V környezetét t-nek T-ben, amelyre a $J_V := \{j \in J | V \cap W_j \neq \emptyset\}$ halmaz véges. Ha $i \in I$ olyan hogy $V \cap V_i \neq \emptyset$, akkor $V \cap V_i = \bigcup_{j \in \overset{-1}{\sigma}\langle\{i\}\rangle} (V \cap W_j)$ miatt van olyan $j \in \overset{-1}{\sigma}\langle\{i\}\rangle$, hogy $V \cap W_j \neq \emptyset$, tehát $j \in J_V$, következésképpen $i = \sigma(j) \in \sigma\langle J_V\rangle$. Tehát $\{i \in I | V \cap V_i \neq \emptyset\} \subseteq \sigma\langle J_V\rangle$, és $\sigma\langle J_V\rangle$ véges halmaz, így a $(V_i)_{i \in I}$ halmazrendszer lokálisan véges. Ez azt jelenti, hogy a $(V_i)_{i \in I}$ halmazrendszer olyan, amelynek a létezését állítottuk. ■

28.12.3. Lemma. *Legyen T parakompakt tér és $F, F' \subseteq T$ olyan zárt halmazok, hogy minden $t \in F$ pontnak van olyan V környezete és van olyan $\Omega' \subseteq T$ nyílt halmaz, hogy $F' \subseteq \Omega'$ és $V \cap \Omega' = \emptyset$. Ekkor léteznek olyan $\Omega, \Omega' \subseteq T$ nyílt halmazok, hogy $F \subseteq \Omega$, $F' \subseteq \Omega'$ és $\Omega \cap \Omega' = \emptyset$.*

Bizonyítás. A hipotézis alapján kiválaszthatunk olyan $(V_t)_{t \in F}$ és $(\Omega'_t)_{t \in F}$ rendszereket, hogy minden $t \in F$ esetén V_t nyílt környezete t-nek és $\Omega'_t \subseteq T$ olyan nyílt halmaz, hogy $F' \subseteq \Omega'_t$ és $V_t \cap \Omega'_t = \emptyset$. Legyen ω olyan halmaz, hogy $\omega \notin F$ és $V_\omega := T \setminus F$. Ekkor $(V_t)_{t \in \{\omega\} \cup F}$ nyílt befedése T-nek tehát a T parakompaktsága miatt vehetjük a T-nek olyan $(\Omega_i)_{i \in I}$ lokálisan véges nyílt befedését, amely finomítása a $(V_t)_{t \in \{\omega\} \cup F}$ halmazrendszernek. Ha $i \in I$, akkor van olyan $t \in \{\omega\} \cup F$, hogy $\Omega_i \subseteq V_t$, és ha $F \cap \Omega_i \neq \emptyset$, akkor $t \neq \omega$, különben $\Omega_i \subseteq V_\omega = T \setminus F$, vagyis $F \cap \Omega_i = \emptyset$ teljesülne. Legyen $J := \{i \in I | F \cap \Omega_i \neq \emptyset\}$ és $\Omega := \bigcup_{i \in J} \Omega_i$. A J definíciója szerint $F \subseteq \Omega$, mert $(\Omega_i)_{i \in I}$ befedése T-nek. Kiválasztunk olyan $\tau : J \to F$ függvényt, hogy minden $i \in J$ esetén $\Omega_i \subseteq V_{\tau(i)}$.

Bebizonyítjuk olyan $\Omega' \subseteq T$ nyílt halmaz létezését, amelyre $F' \subseteq \Omega'$ és $\Omega \cap \Omega' = \emptyset$. Az $(\Omega_i)_{i \in I}$ halmazrendszer lokális végessége miatt kiválaszthatunk olyan $(V_{t'})_{t' \in F'}$ rendszert, hogy minden $F' \ni t'$-re $V_{t'}$ olyan nyílt környezete t'-nek, hogy az $\{i \in I | V_{t'} \cap \Omega_i \neq \emptyset\}$ halmaz véges. Minden $t' \in F'$ esetén legyen $I(t') := J \cap \{i \in I | V_{t'} \cap \Omega_i \neq \emptyset\}$; ez is véges halmaz. Ha $t' \in F'$ olyan, hogy $I(t') = \emptyset$, akkor minden $J \ni i$-re $V_{t'} \cap \Omega_i = \emptyset$; legyen ekkor $U_{t'} := V_{t'}$. Ha $t' \in F'$ olyan, hogy $I(t') \neq \emptyset$, akkor minden $J \ni i$-re az $U_{t'} := V_{t'} \cap \bigcap_{j \in I(t')} \Omega'_{\tau(j)}$ halmaz nem metszi Ω_i-t. Valóban, $\Omega_i \subseteq V_{\tau(i)}$ miatt

$$\Omega_i \cap V_{t'} \cap \bigcap_{j \in I(t')} \Omega'_{\tau(j)} = \big(\Omega_i \cap V_{\tau(i)}\big) \cap V_{t'} \cap \bigcap_{j \in I(t')} \Omega'_{\tau(j)} =$$

$$= (\Omega_i \cap V_{t'}) \cap \bigcap_{j \in I(t')} \left(\Omega'_{\tau(j)} \cap V_{\tau(i)}\right),$$

és ha ez nem volna üres, akkor $\Omega_i \cap V_{t'} \neq \emptyset$, így $i \in I(t')$, tehát $\Omega'_{\tau(i)} \cap V_{\tau(i)} \neq \emptyset$ is teljesülne, holott minden $F \ni t$-re (így a $t := \tau(t)$ pontra is) $V_t \cap \Omega'_t = \emptyset$. Ugyanakkor $t' \in F'$ és $I(t') \neq \emptyset$ esetén minden $I(t') \ni j$-re $F' \subseteq \Omega'_{\tau(j)}$, ezért a $V_{t'} \cap \bigcap_{j \in I(t')} \Omega'_{\tau(j)}$ halmaz nyílt környezete t'-nek; legyen ekkor $U_{t'} := V_{t'} \cap \bigcap_{j \in I(t')} \Omega'_{\tau(j)}$. Tehát $(U_{t'})_{t' \in F'}$ olyan halmazrendszer, hogy minden $F' \ni t'$-re $U_{t'}$ nyílt környezete t'-nek, és minden $i \in J$ esetén $\Omega_i \cap U_{t'} = \emptyset$. Ezért $t' \in F'$ esetén $\Omega \cap U_{t'} = \emptyset$ is teljesül, így az $\Omega' := \bigcup_{t' \in F'} U_{t'}$ halmaz nyílt, $F' \subseteq \Omega'$ és $\Omega \cap \Omega' = \emptyset$. ■

28.12.4. Állítás. *Minden parakompakt Hausdorff-tér normális.*

Bizonyítás. Legyen T parakompakt Hausdorff-tér és $F, F' \subseteq T$ diszjunkt zárt halmazok. Ha $t' \in F'$, akkor az előző lemmát alkalmazhatjuk az F és $\{t'\}$ zárt halmazokra, mert T Hausdorff-tér. Tehát minden $t' \in F'$ ponthoz léteznek olyan $\Omega, \Omega' \subseteq T$ diszjunkt nyílt halmazok, hogy $F \subseteq \Omega$ és $t' \in \Omega'$. Ezért ismét alkalmazhatjuk az előző lemmát az F és F' diszjunkt zárt halmazokra, amiből következik az állítás. ■

Most parakompakt Hausdorff-terekre megadjuk a 28.12.2. állítás erősebb formáját.

28.12.5. Állítás. *Ha T parakompakt Hausdorff-tér, akkor T bármely $(\Omega_i)_{i\in I}$ nyílt befedéséhez létezik olyan $(U_i)_{i\in I}$ (ugyanolyan indexhalmazú) lokálisan véges nyílt befedése T-nek, hogy minden $i \in T$ esetén $\overline{U_i} \subseteq \Omega_i$.*

Bizonyítás. 28.12.2. szerint vehetjük T-nek olyan $(V_i)_{i\in I}$ (ugyanolyan indexhalmazú) lokálisan véges nyílt befedését, amelyre minden $i \in I$ esetén $V_i \subseteq \Omega_i$. Ekkor $(V_i)_{i\in I}$ pontonként véges nyílt befedése a T normális térnek (28.12.4.), így a normális terekre vonatkozó egységfelosztás-tétel (27.7.3.) alapján van olyan $(U_i)_{i\in I}$ nyílt befedése T-nek, hogy minden $i \in I$ indexre $\overline{U_i} \subseteq V_i$. Mivel a $(V_i)_{i\in I}$ halmazrendszer lokálisan véges, így $(U_i)_{i\in I}$ is lokálisan véges, és minden $i \in I$ esetén $\overline{U_i} \subseteq V_i \subseteq \Omega_i$. ■

Korábban láttuk, hogy normális terekre érvényes az egységfelosztás-tétel (iii) pontjában megfogalmazott állítás (27.7.3.). A parakompakt Hausdorff-terek speciális normális terek (28.12.4.), ezért várható, hogy ezekre erősebb egységfelosztás-tétel is igaz. A pontos állítás a következő.

28.12.6. Tétel. (Egységfelosztás-tétel parakompakt terekre) *Parakompakt Hausdorff-tér bármely nyílt befedéséhez létezik annak alárendelt folytonos egységfelosztás.*

Bizonyítás. Legyen $(\Omega_i)_{i\in I}$ nyílt befedése a T parakompakt Hausdorff-térnek, és vegyük a T-nek olyan $(U_\alpha)_{\alpha\in A}$ lokálisan véges nyílt befedését, amely finomítása $(\Omega_i)_{i\in I}$-nek. Mivel T normális tér (28.12.4.), így a normális terekre vonatkozó egységfelosztás-tétel (27.7.3.) alapján létezik $(U_\alpha)_{\alpha\in A}$-nak alárendelt folytonos egységfelosztás; legyen $(g_\alpha)_{\alpha\in A}$ ilyen függvényrendszer. Tehát minden $A \ni \alpha$-ra $g_\alpha : T \to \mathbb{R}$ folytonos függvény, $0 \leq g_\alpha \leq 1$, $\operatorname{supp}(g_\alpha) \subseteq U_\alpha$, és minden $t \in T$ esetén $\displaystyle\sum_{\substack{\alpha\in A\\ g_\alpha(t)\neq 0}} g_\alpha(t) = 1$. Kiválasztunk olyan $\sigma : A \to I$ függvényt, hogy minden $A \ni \alpha$-ra $U_\alpha \subseteq \Omega_{\sigma(\alpha)}$. Minden $i \in I \setminus \operatorname{Im}(\sigma)$ esetén legyen f_i a $T \to \mathbb{R}$ azonosan nulla függvény, továbbá minden $\operatorname{Im}(\sigma) \ni i$-re legyen $f_i : T \to \mathbb{R}$ az a függvény, amely minden $t \in T$ ponthoz az

$$f_i(t) := \sum_{\substack{\alpha\in A\\ g_\alpha(t)\neq 0\\ \sigma(\alpha)=i}} g_\alpha(t)$$

értéket rendeli. Megmutatjuk, hogy az $(f_i)_{i\in I}$ függvényrendszer $(\Omega_i)_{i\in I}$-nek alárendelt folytonos egységfelosztás.

Ha $i \in \operatorname{Im}(\sigma)$, $t \in T$ és V olyan környezete t-nek, hogy az $A_V := \{\alpha \in A | V \cap U_\alpha \neq \emptyset\}$ halmaz véges, akkor $f_i = \displaystyle\sum_{\alpha\in A_V;\ \sigma(\alpha)=i} g_\alpha$ teljesül a V halmazon, ezért a folytonosság lokalitása miatt f_i folytonos a t pontban. Ebből látható, hogy minden $I \ni i$-re az $f_i : T \to \mathbb{R}$ függvény folytonos.

Ha $i \in \operatorname{Im}(\sigma)$, akkor

$$[f_i \neq 0] \subseteq \bigcup_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} [g_\alpha \neq 0] \subseteq \bigcup_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} \operatorname{supp}(g_\alpha) \subseteq \bigcup_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} U_\alpha \subseteq \Omega_i,$$

továbbá a $(\mathrm{supp}(g_\alpha))_{\alpha\in A;\ \sigma(\alpha)=i}$ halmazrendszer lokálisan véges, és mindegyik tagja zárt, így $\bigcup\limits_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} \mathrm{supp}(g_\alpha)$ is zárt halmaz T-ben, következésképpen fennállnak a $\mathrm{supp}(f_i) := \overline{[f_i \neq 0]} \subseteq \bigcup\limits_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} \mathrm{supp}(g_\alpha) \subseteq \Omega_i$ összefüggések. Ez azt jelenti, hogy minden $I \ni i$-re $\mathrm{supp}(f_i) \subseteq \Omega_i$.

Az $\Big(\bigcup\limits_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} \mathrm{supp}(g_\alpha)\Big)_{i\in I}$ halmazrendszer lokálisan véges. Valóban, ha $t \in T$ és V olyan környezete t-nek, hogy az $A_V := \{\alpha \in A | V \cap U_\alpha \neq \emptyset\}$ halmaz véges, akkor $i \in I$ és $V \cap \bigcup\limits_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} \mathrm{supp}(g_\alpha) \neq \emptyset$ esetén van olyan $\alpha \in A$, hogy $\sigma(\alpha) = i$ és $\emptyset \neq V \cap \mathrm{supp}(g_\alpha) \subseteq V \cap U_\alpha$, így $\alpha \in A_V$, vagyis

$$\Big\{i \in I \mid V \cap \bigcup_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} \mathrm{supp}(g_\alpha) \neq \emptyset\Big\} \subseteq \sigma\langle A_V\rangle,$$

és persze $\sigma\langle A_V\rangle$ véges halmaz. Ebből következik, hogy a $(\mathrm{supp}(f_i))_{i\in I}$ halmazrendszer is lokálisan véges, hiszen láttuk, hogy minden $i \in I$ esetén $\mathrm{supp}(f_i) \subseteq \bigcup\limits_{\substack{\alpha\in A\\ \sigma(\alpha)=i}} \mathrm{supp}(g_\alpha)$.

Végül, ha $t \in T$, akkor könnyen látható, hogy

$$1 = \sum_{\substack{\alpha\in A\\ g_\alpha(t)\neq 0}} g_\alpha(t) = \sum_{\substack{i\in I\\ f_i(t)\neq 0}} \sum_{\substack{\alpha\in A\\ g_\alpha(t)\neq 0\\ \sigma(\alpha)=i}} g_\alpha(t) = \sum_{\substack{i\in I\\ f_i(t)\neq 0}} f_i(t)$$

teljesül. ■

28.12.7. Állítás. *Ha $(T_\alpha)_{\alpha\in A}$ olyan pontonként véges (például diszjunkt) befedése a T topologikus térnek, hogy minden $\alpha \in A$ esetén T_α parakompakt nyílt részhalmaza T-nek, akkor T is parakompakt.*

Bizonyítás. Legyen $(\Omega_i)_{i\in I}$ tetszőleges nyílt befedése T-nek. Minden $\alpha \in A$ esetén $(T_\alpha \cap \Omega_i)_{i\in I}$ nyílt befedése a T_α topologikus altérnek, ezért a T_α halmaz parakompaktsága folytán kiválaszthatunk olyan $((\Omega_{\alpha,j})_{j\in J_\alpha})_{\alpha\in A}$ rendszert, hogy minden $A \ni \alpha$-ra $(\Omega_{\alpha,j})_{j\in J_\alpha}$ olyan lokálisan véges nyílt befedés a T_α topologikus altérben, amely finomítása a $(T_\alpha \cap \Omega_i)_{i\in I}$ halmazrendszernek.

Minden $A \ni \alpha$-ra T_α nyílt T-ben, ezért az $(\Omega_{\alpha,j})_{j\in J_\alpha}$ halmazrendszer mindegyik tagja T-ben is nyílt, így az $(\Omega_{\alpha,j})_{\alpha\in A,\ j\in J_\alpha}$ halmazrendszer nyílt befedése T-nek. Továbbá, minden $\alpha \in A$ és $j \in J_\alpha$ esetén van olyan $i \in I$, hogy $\Omega_{\alpha,j} \subseteq T_\alpha \cap \Omega_i \subseteq \Omega_i$, tehát az $(\Omega_{\alpha,j})_{\alpha\in A,\ j\in J_\alpha}$ halmazrendszer finomítása az $(\Omega_i)_{i\in I}$ halmazrendszernek.

Megmutatjuk, hogy az $(\Omega_{\alpha,j})_{\alpha\in A,\ j\in J_\alpha}$ halmazrendszer lokálisan véges. Legyen ugyanis $t \in T$ rögzített pont. A $(T_\alpha)_{\alpha\in A}$ halmazrendszer pontonkénti végessége folytán az $A(t) := \{\alpha \in A | t \in T_\alpha\}$ halmaz véges és persze nem üres, hiszen $(T_\alpha)_{\alpha\in A}$ befedése T-nek. Ha $\alpha \in A(t)$, akkor az $(\Omega_{\alpha,j})_{j\in J_\alpha}$ halmazrendszer lokális végessége miatt létezik t-nek olyan U_α környezete T_α-ban, hogy $J'_\alpha := \{j \in J_\alpha | U_\alpha \cap \Omega_{\alpha,j} \neq \emptyset\}$ véges halmaz.

Ekkor $U := \bigcap_{\alpha \in A(t)} U_\alpha$ környezete t-nek T-ben. Ha $\alpha \in A$ és $j \in J_\alpha$ olyanok, hogy $U \cap \Omega_{\alpha,j} \neq \emptyset$, akkor $\Omega_{\alpha,j} \cap U_\alpha \neq \emptyset$, tehát $j \in J'_\alpha$, vagyis

$$\{(\alpha, j) | (\alpha \in A) \wedge (j \in J_\alpha) \wedge (U \cap \Omega_{\alpha,j} \neq \emptyset)\} \subseteq \bigcup_{\alpha \in A(t)} (\{\alpha\} \times J'_\alpha)$$

teljesül, és itt a jobb oldalon véges halmaz áll. ■

28.13. Lokálisan kompakt tér parakompaktságának jellemzése

Nem minden lokálisan kompakt tér parakompakt, mert 28.12.4. szerint minden parakompakt Hausdorff-tér normális, és léteznek nem normális lokálisan kompakt terek (28.7.2. és 28.7.4.). Tehát a csonka Tyihonov-deszka és a 28.7.4. állításban értelmezett lokálisan kompakt tér nem parakompakt.

28.13.1. Definíció. *A T topologikus teret* σ**-kompaktnak** *nevezzük, ha létezik a T kompakt részhalmazainak olyan $(K_n)_{n \in \mathbb{N}}$ sorozata, amelyre $T = \bigcup_{n \in \mathbb{N}} K_n$. A T topologikus tér E részhalmazát σ-kompaktnak mondjuk, ha az E topologikus altér σ-kompakt tér.*

Ha T nem megszámlálhatóan végtelen halmaz, akkor T a diszkrét topológiával ellátva lokálisan kompakt, de nem σ-kompakt topologikus tér, tehát lokálisan kompakt tér nem feltétlenül σ-kompakt. Nyilvánvaló, hogy minden kompakt tér σ-kompakt, tehát a σ-kompaktság a kompaktság fogalmának általánosítása. Vigyázzunk arra, hogy σ-kompakt Hausdorff-tér nem szükségképpen lokálisan kompakt.

Ha T topologikus tér és $E \subseteq T$, akkor az E egy részhalmaza pontosan akkor kompakt T-ben, ha kompakt az E topologikus altérben; ezért E pontosan akkor σ-kompakt halmaz T-ben, ha előáll a T megszámlálható sok kompakt részhalmazának uniójaként.

28.13.2. Lemma. *Ha T σ-kompakt lokálisan kompakt tér, akkor létezik a T relatív kompakt nyílt részhalmazainak olyan $(\Omega_n)_{n \in \mathbb{N}}$ sorozata, amelyre $T = \bigcup_{n \in \mathbb{N}} \Omega_n$ és minden $\mathbb{N} \ni n$-re $\overline{\Omega_n} \subseteq \Omega_{n+1}$.*

Bizonyítás. Legyen $(K_n)_{n \in \mathbb{N}}$ a T kompakt részhalmazainak olyan sorozata, hogy $T = \bigcup_{n \in \mathbb{N}} K_n$. A kiválasztási axiómával kombinált rekurzió tételét alkalmazva megmutatjuk olyan $(\Omega_n)_{n \in \mathbb{N}}$ halmazsorozat létezését, hogy minden $\mathbb{N} \ni n$-re Ω_n relatív kompakt nyílt halmaz T-ben és $\overline{\Omega_n} \cup K_n \subseteq \Omega_{n+1}$; egy ilyen halmazsorozat nyilvánvalóan eleget tesz a követelményeknek.

Az Ω_0 halmaz a T tetszőleges relatív kompakt nyílt részhalmaza lehet, például $\Omega_0 := \emptyset$ is megfelel. Tegyük fel, hogy $n \in \mathbb{N}^*$, és legyen $(\Omega_i)_{0 \leq i < n}$ olyan rendszer, hogy minden $i < n$ természetes számra Ω_i relatív kompakt nyílt halmaz T-ben és $i + 1 < n$ esetén $\overline{\Omega_i} \cup K_i \subseteq \Omega_{i+1}$. Ekkor $\overline{\Omega_{n-1}} \cup K_{n-1}$ kompakt részhalmaza T-nek, tehát van olyan $\Omega_n \subseteq T$ relatív kompakt nyílt halmaz, hogy $\overline{\Omega_{n-1}} \cup K_{n-1} \subseteq \Omega_n$. Ekkor az $(\Omega_i)_{0 \leq i \leq n}$ rendszer olyan, hogy minden $i \leq n$ természetes számra Ω_i relatív kompakt nyílt halmaz

T-ben és $i+1 < n+1$ esetén $\overline{\Omega_i} \cup K_i \subseteq \Omega_{i+1}$. ■

Megjegyezzük, hogy az előző lemmát gyakran a következő ekvivalens megfogalmazásban használjuk: Ha T σ-kompakt lokálisan kompakt tér, akkor létezik a T kompakt részhalmazainak olyan $(K_n)_{n\in\mathbb{N}}$ sorozata, amelyre $T = \bigcup_{n\in\mathbb{N}} K_n$ és minden $\mathbb{N} \ni n$-re $K_n \subseteq \mathrm{Int}(K_{n+1})$.

28.13.3. Állítás. *Minden σ-kompakt lokálisan kompakt tér parakompakt.*

Bizonyítás. Legyen T σ-kompakt lokálisan kompakt tér, és $(U_i)_{i\in I}$ nyílt befedése T-nek; megmutatjuk, hogy $(U_i)_{i\in I}$-nek létezik olyan finomítása, amely lokálisan véges nyílt befedése T-nek.

Először vegyük a T relatív kompakt nyílt részhalmazainak olyan $(\Omega_n)_{n\in\mathbb{N}}$ sorozatát, amely befedése T-nek és minden $\mathbb{N} \ni n$-re $\overline{\Omega_n} \subseteq \Omega_{n+1}$. Legyen minden $m \in \mathbb{Z}$ *negatív* egész számra $\Omega_m := \emptyset$. Természetesen ekkor minden $\mathbb{Z} \ni m$-re $\overline{\Omega_m} \subseteq \Omega_{m+1}$.

Legyen $n \in \mathbb{N}$ rögzített és $K_n := \overline{\Omega_n} \setminus \Omega_{n-1}$. A K_n halmaz kompakt T-ben és $K_n \subseteq \Omega_{n+1} \setminus \overline{\Omega_{n-2}}$. Ha $t \in K_n$, akkor van olyan $i \in I$, hogy $t \in U_i$, tehát $U_i \cap \left(\Omega_{n+1} \setminus \overline{\Omega_{n-2}}\right)$ olyan nyílt környezete t-nek, amely részhalmaza $\Omega_{n+1} \setminus \overline{\Omega_{n-2}}$-nek. Ezért kiválaszthatunk olyan $(W_t)_{t\in K_n}$ rendszert, hogy minden $t \in K_n$ pontra W_t nyílt környezete t-nek és $W_t \subseteq \Omega_{n+1} \setminus \overline{\Omega_{n-2}}$, és van olyan $i \in I$, hogy $W_t \subseteq U_i$. Ekkor K_n kompaktsága miatt van olyan $H \subseteq K_n$ véges halmaz, hogy $K_n \subseteq \bigcup_{t\in H} W_t$.

Az előzőek alapján kiválaszthatunk olyan $(H_n)_{n\in\mathbb{N}}$ és $((V_{n,t})_{t\in H_n})_{n\in\mathbb{N}}$ sorozatokat, hogy minden $\mathbb{N} \ni n$-re $H_n \subseteq K_n$ véges halmaz, és $(V_{n,t})_{t\in H_n}$ a T nyílt részhalmazainak olyan rendszere, hogy $K_n \subseteq \bigcup_{t\in H_n} V_{n,t}$, valamint minden $H_n \ni t$-re $t \in V_{n,t} \subseteq \Omega_{n+1} \setminus \overline{\Omega_{n-2}}$ és létezik a t-hez (és n-hez) olyan $i \in I$, hogy $V_{n,t} \subseteq U_i$. Legyen $J := \bigcup_{n\in\mathbb{N}} (\{n\} \times H_n)$. Nyilvánvaló, hogy a $(V_{n,t})_{(n,t)\in J}$ halmazrendszer nyílt befedése T-nek, mert $(K_n)_{n\in\mathbb{N}}$ befedése T-nek. Triviális továbbá az, hogy $(V_{n,t})_{(n,t)\in J}$ finomítása az $(U_i)_{i\in I}$ halmazrendszernek, ezért a T parakompaktságához elég volna azt igazolni, hogy $(V_{n,t})_{(n,t)\in J}$ lokálisan véges T-ben.

Ehhez legyen $t \in T$ rögzített és $m := \min\{n \in \mathbb{N} | t \in \Omega_n\}$. Az m definíciója szerint $t \in \Omega_m$ és $t \notin \Omega_{m-1}$, következésképpen $t \notin \overline{\Omega_{m-2}}$, hiszen $\overline{\Omega_{m-2}} \subseteq \Omega_{m-1}$. Ez az jelenti, hogy a $V := \Omega_m \setminus \overline{\Omega_{m-2}}$ nyílt környezete t-nek. Ha $(n,s) \in J$ olyan, hogy $V_{n,s} \cap V \neq \emptyset$, akkor $V_{n,s} \subseteq \Omega_{n+1} \setminus \overline{\Omega_{n-2}} \subseteq T \setminus \Omega_{n-2}$ és $V \subseteq \Omega_m$ miatt $n \leq m+1$, különben $n-2 \geq m$ teljesülne, így $\Omega_{n-2} \supseteq \Omega_m$, tehát igaz volna a $V_{n,s} \cap V \subseteq (T \setminus \Omega_{n-2}) \cap \Omega_m = \emptyset$ összefüggés. Ez azt jelenti, hogy

$$\{\ (n,s) \in J \mid V_{n,s} \cap V \neq \emptyset\ \} \subseteq \bigcup_{n=0}^{m+1} (\{n\} \times H_n)\,,$$

és itt a jobb oldalon véges halmaz áll. Ebből következik, hogy a $(V_{n,t})_{(n,t)\in J}$ halmazrendszer lokálisan véges. ■

A bizonyításból látható, hogy σ-kompakt lokálisan kompakt tér bármely nyílt befedésének létezik olyan megszámlálható (indexhalmazú) finomítása, amely lokálisan véges befedés, és amelynek minden tagja relatív kompakt nyílt halmaz, hiszen a $V_{n,t}$ nyílt halmazokról feltehetjük a relatív kompaktságot is.

28.13.4. Tétel. (Lokálisan kompakt tér parakompaktságának jellemzése) *Ha T lokálisan kompakt tér, akkor a következő állítások ekvivalensek.*

(i) *T parakompakt tér.*

(ii) *Létezik T-nek relatív kompakt nyílt halmazokból álló lokálisan véges befedése.*

(iii) *Létezik T-nek σ-kompakt nyílt halmazokból álló diszjunkt befedése.*

(iii)$'$ *Létezik T-nek σ-kompakt nyílt halmazokból álló pontonként véges befedése.*

Bizonyítás. (i)⇒(ii) Jelölje $\mathscr{T}_c$ a T relatív kompakt nyílt részhalmazainak halmazát. Ekkor $(U)_{U\in\mathscr{T}_c}$ nyílt befedése T-nek, ezért a T parakompaktsága miatt vehetjük a T-nek olyan $(\Omega_i)_{i\in I}$ nyílt befedését, amely lokálisan véges finomítása az $(U)_{U\in\mathscr{T}_c}$ halmazrendszernek. Tehát minden $I \ni i$-hez van olyan $U \subseteq T$ relatív kompakt nyílt halmaz, hogy $\Omega_i \subseteq U$, így Ω_i is relatív kompakt nyílt halmaz.

(ii)⇒(iii) Legyen $(\Omega_i)_{i\in I}$ a T relatív kompakt nyílt halmazokból álló lokálisan véges befedése. Jelölje R azon $(t,t') \in T \times T$ párok halmazát, amelyekhez van olyan $n \in \mathbb{N}$ és olyan $(i_k)_{k\in n+1}$ rendszer I-ben, hogy $t \in \Omega_{i_0}$, $t' \in \Omega_{i_n}$ és minden $k < n$ természetes számra $\Omega_{i_k} \cap \Omega_{i_{k+1}} \neq \emptyset$. Könnyen látható, hogy R ekvivalencia-reláció T felett. Az $(\Omega)_{\Omega\in T/R}$ halmazrendszer diszjunkt befedése T-nek, ezért elég volna azt igazolni, hogy minden $\Omega \in T/R$ halmaz *nyílt* és *σ-kompakt* halmaz T-ben.

Ha $\Omega \in T/R$, akkor $t \in \Omega$ esetén van olyan $i \in I$, hogy $t \in \Omega_i$; ekkor az R reláció értelmezése alapján triviális, hogy minden $\Omega_i \ni t'$-re $(t,t') \in R$, vagyis $t' \in \Omega$, így $\Omega_i \subseteq \Omega$. Ezért minden $\Omega \in T/R$ halmaz nyílt T-ben, és ebből az is következik, hogy minden $\Omega \in T/R$ halmaz zárt is T-ben, hiszen $T \setminus \Omega = \bigcup_{\substack{\Omega'\in T/R\\ \Omega'\neq\Omega}} \Omega'$ is nyílt T-ben. Tehát csak azt kell igazolni, hogy minden $\Omega \in T/R$ halmaz σ-kompakt.

Legyen $\Omega \in T/R$ és $t \in \Omega$ rögzített. Rekurzióval értelmezzük *azt* az $(U_n)_{n\in\mathbb{N}}$ halmazsorozatot, amelyre $U_0 := \bigcup_{\substack{i\in I\\ t\in\Omega_i}} \Omega_i$ és minden $\mathbb{N}^* \ni n$-re $U_n := \bigcup_{\substack{i\in I\\ \Omega_i\cap U_{n-1}\neq\emptyset}} \Omega_i$.

Teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén van olyan $I_n \subseteq I$ *véges* halmaz, hogy $U_n = \bigcup_{i\in I_n} \Omega_i$ és minden $I_n \ni i$-re $\Omega_i \subseteq \Omega$. Ez $n = 0$ esetén igaz, mert $I_0 := \{i \in I | t \in \Omega_i\}$ véges halmaz, hiszen az $(\Omega_i)_{i\in I}$ befedés pontonként (sőt lokálisan) véges, és a definíció szerint $U_0 = \bigcup_{i\in I_0} \Omega_i$, továbbá $t \in \Omega$ miatt és az R reláció értelmezése alapján minden $I_0 \ni i$-re $\Omega_i \subseteq \Omega$. Legyen most $n \in \mathbb{N}$ és $I_n \subseteq$ olyan véges halmaz, hogy $U_n = \bigcup_{i\in I_n} \Omega_i$ és minden $I_n \ni i$-re $\Omega_i \subseteq \Omega$. A rekurzív definíció szerint $U_{n+1} = \bigcup_{\substack{i\in I\\ \Omega_i\cap U_n\neq\emptyset}} \Omega_i$.

Az $\overline{U_n}$ halmaz kompakt, mert az indukciós hipotézis alapján U_n véges sok relatív kompakt halmaz uniója. Az $(\Omega_i)_{i\in I}$ befedés lokális végessége miatt kiválaszthatunk olyan $(V_s)_{s\in\overline{U_n}}$ rendszert, hogy minden $\overline{U_n} \ni s$-re V_s nyílt környezete s-nek, és az $\{i \in I | \Omega_i \cap V_s \neq \emptyset\}$ halmaz véges. Legyen $H \subseteq \overline{U_n}$ olyan véges halmaz, hogy $\overline{U_n} \subseteq \bigcup_{s\in H} V_s$. Ekkor

$$\{\, i \in I \mid \Omega_i \cap U_n \neq \emptyset \,\} \subseteq \{\, i \in I \mid \Omega_i \cap \bigcup_{s\in H} V_s \neq \emptyset \,\} \subseteq \bigcup_{s\in H} \{\, i \in I \mid \Omega_i \cap V_s \neq \emptyset \,\},$$

tehát az $I_{n+1} := \{i \in I | \Omega_i \cap U_n \neq \emptyset\}$ halmaz véges, és a rekurzív definíció alapján

$U_{n+1} = \bigcup_{i \in I_{n+1}} \Omega_i$. Ha $i \in I_{n+1}$ és $t' \in \Omega_i \cap U_n$, akkor $t' \in \Omega$, hiszen az indukciós hipotézis következtében $U_n \subseteq \Omega$; ezért az R reláció értelmezése alapján $\Omega_i \subseteq \Omega$. Ezzel a teljes indukciót végrehajtottuk.

Tehát minden $n \in \mathbb{N}$ esetén U_n relatív kompakt nyílt halmaz T-ben, mert véges sok relatív kompakt nyílt halmaz uniója relatív kompakt nyílt halmaz, továbbá $U_n \subseteq \Omega$. Megmutatjuk, hogy $\Omega = \bigcup_{n \in \mathbb{N}} U_n$. Valóban, legyen $t' \in \Omega$, és vegyünk olyan $n \in \mathbb{N}$ számot és olyan I-ben haladó $(i_k)_{k \in n+1}$ rendszert, hogy $t \in \Omega_{i_0}$, $t' \in \Omega_{i_n}$ és minden $k < n+1$ természetes számra $\Omega_{i_k} \cap \Omega_{i_{k+1}} \neq \emptyset$. Ekkor minden $k \leq n$ természetes számra $\Omega_{i_k} \subseteq U_k$. Ha nem így volna, akkor értelmezhetnének az

$$m := \min\{\, k \in \mathbb{N} \mid (k \leq n) \wedge (\Omega_{i_k} \setminus U_k \neq \emptyset) \,\}$$

számot. Világos, hogy $\Omega_{i_0} \subseteq U_0$, hiszen $t \in \Omega_{i_0}$; ezért $m > 0$. Ekkor viszont $\Omega_{i_{m-1}} \subseteq U_{m-1}$ és $\Omega_{i_{m-1}} \cap \Omega_{i_m} \neq \emptyset$, tehát $U_{m-1} \cap \Omega_{i_m} \neq \emptyset$, így az U_m értelmezése szerint $\Omega_{i_m} \subseteq U_m$, holott $\Omega_{i_m} \setminus U_m \neq \emptyset$. Tehát minden $k \leq n$ természetes számra $\Omega_{i_k} \subseteq U_k$, így $t' \in \Omega_{i_n} \subseteq U_n$. Ezzel megmutattuk, hogy $\Omega = \bigcup_{n \in \mathbb{N}} U_n$.

Minden $n \in \mathbb{N}$ esetén $U_n \subseteq \Omega$ és Ω zárt T-ben, ezért $\overline{U_n} \subseteq \Omega$, így $\Omega = \bigcup_{n \in \mathbb{N}} \overline{U_n}$ is teljesül. De minden $\mathbb{N} \ni n$-re $\overline{U_n}$ kompakt halmaz T-ben, ezért az Ω halmaz σ-kompakt.

(iii)$\Rightarrow$(iii)$'$ Nyilvánvaló, mert minden diszjunkt halmazrendszer pontonként véges.

(iii)$'$ $\Rightarrow$(i) Ha $(T_\alpha)_{\alpha \in A}$ pontonként véges nyílt befedése T-nek és minden $A \ni \alpha$-ra T_α σ-kompakt részhalmaza T-nek, akkor minden $\alpha \in A$ esetén a T_α topologikus altér lokálisan kompakt és σ-kompakt, így az előző állítás szerint parakompakt nyílt halmaz T-ben; tehát T is parakompakt. ■

28.13.5. Következmény. *Ha a T lokálisan kompakt tér parakompakt és összefüggő, akkor T σ-kompakt.*

Bizonyítás. A hipotézis és az előző tétel alapján létezik olyan $(T_\alpha)_{\alpha \in A}$ diszjunkt halmazrendszer, amely befedése T-nek és minden $A \ni \alpha$-ra a T_α halmaz nyílt és σ-kompakt T-ben. Minden $\alpha \in A$ esetén $T \setminus T_\alpha = \bigcup_{\beta \in A \setminus \{\alpha\}} T_\beta$, ezért T_α zárt T-ben. A T összefüggősége alapján minden $A \ni \alpha$-ra $T_\alpha = T$ vagy $T_\alpha = \emptyset$. Tehát $A \neq \emptyset$ esetén van olyan $\alpha \in A$, hogy $T = T_\alpha$, így T σ-kompakt. Ha $A = \emptyset$, akkor $T = \emptyset$, tehát T σ-kompakt. ■

28.14. Megszámlálható bázisú lokálisan kompakt terek jellemzése

28.14.1. Tétel. (Megszámlálható bázisú lokálisan kompakt terek jellemzése) *Ha T lokálisan kompakt tér, és T' egypontú kompaktifikációja T-nek, akkor a következő állítások ekvivalensek.*

(i) *T megszámlálható bázisú.*

(ii) *T' metrizálható kompakt tér.*

(iii) *T metrizálható és σ-kompakt.*

Bizonyítás. (i)⇒(ii) A kompakt terek metrizálhatóságának jellemzési tétele alapján elég azt megmutatni, hogy ha T megszámlálható bázisú, akkor T' is megszámlálható bázisú. Jelölje ω a végtelen távoli pontot T'-ben, és legyen $\mathfrak{B}$ megszámlálható topologikus bázisa T-nek. Tudjuk, hogy a $\mathrm{B}_c := \{U \in \mathfrak{B} | U$ relatív kompakt$\}$ halmaz szintén topologikus bázisa T-nek. Ebből következik, hogy $T = \bigcup_{U \in \mathrm{B}_c} \overline{U}$, ezért a T topologikus tér σ-kompakt. Ezért létezik a T relatív kompakt nyílt részhalmazainak olyan $(\Omega_n)_{n\in\mathbb{N}}$ sorozata, hogy $T = \bigcup_{n\in\mathbb{N}} \Omega_n$ és minden $\mathbb{N} \ni n$-re $\overline{\Omega_n} \subseteq \Omega_{n+1}$.

Megmutatjuk, hogy a $\mathfrak{B} \cup \{T' \setminus \overline{\Omega_n} | n \in \mathbb{N}\}$ halmaz topologikus bázisa a T' kompakt térnek. Valóban, legyen Ω' tetszőleges nyílt részhalmaza T'-nek. Ha $\omega \in \Omega'$, akkor $T' \setminus \Omega'$ olyan kompakt halmaz T'-ben, amely része T-nek, tehát ez T-ben is kompakt halmaz, így létezik olyan $n \in \mathbb{N}$, hogy $T' \setminus \Omega' \subseteq \Omega_n \subseteq \overline{\Omega_n}$, tehát $\omega \in T' \setminus \overline{\Omega_n} \subseteq \Omega'$. Ha $t \in T \cap \Omega'$, akkor van olyan $U \in \mathfrak{B}$, hogy $t \in U \subseteq T \cap \Omega'$, mert a $T \cap \Omega'$ halmaz nyílt T-ben, és $\mathfrak{B}$ topologikus bázisa T-nek.

(ii)⇒(iii) Metrizálható topologikus tér minden topologikus altere metrizálható, ezért ha (ii) teljesül, akkor T metrizálható, hiszen T topologikus altere T'-nek. Továbbá, metrizálható topologikus tér M_1-tér, ezért ha ω a végtelen távoli pont T'-ben és (ii) teljesül, akkor létezik az ω nyílt környezeteinek olyan $(U_n)_{n\in\mathbb{N}}$ sorozata, hogy az $\{U_n | n \in \mathbb{N}\}$ halmaz környezetbázisa ω-nak T'-ben. Ekkor a $(T' \setminus U_n)_{n\in\mathbb{N}}$ halmazsorozat befedése T-nek, hiszen $\bigcap_{n\in\mathbb{N}} U_n = \{\omega\}$. Továbbá, minden $\mathbb{N} \ni n$-re $T' \setminus U_n$ kompakt halmaz T'-ben és részhalmaza T-nek, ezért T-ben is kompakt. Ebből következik, hogy a T topologikus tér σ-kompakt.

(iii)⇒(i) Legyen $(K_n)_{n\in\mathbb{N}}$ a T kompakt részhalmazainak olyan sorozata, amely befedése T-nek. A hipotézis alapján minden $\mathbb{N} \ni n$-re a K_n topologikus altér kompakt és metrizálható, ezért a kompakt terek metrizálhatóságának jellemzése alapján a K_n topologikus altér megszámlálható bázisú, így szeparábilis is. Kiválasztunk olyan $(D_n)_{n\in\mathbb{N}}$ halmazsorozatot, hogy minden $n \in \mathbb{N}$ esetén $D_n \subseteq K_n$ megszámlálható sűrű halmaz a K_n topologikus altérben. Ha $t \in T$ és V környezete t-nek T-ben, akkor van olyan $n \in \mathbb{N}$, hogy $t \in K_n$, és ekkor $V \cap K_n$ környezete t-nek a K_n topologikus altérben, következésképpen $\emptyset \neq (V \cap K_n) \cap D_n = V \cap D_n$. Ez azt jelenti, hogy az $\bigcup_{n\in\mathbb{N}} D_n$ megszámlálható halmaz sűrű a T topologikus térben, vagyis T szeparábilis. Ugyanakkor T metrizálható is, ezért megszámlálható bázisú. ■

28.15. Félmetrizálható tér parakompaktsága

28.15.1. Lemma. *Ha egy topologikus tér bármely nyílt befedésének létezik olyan lokálisan véges finomítása, amely zárt befedése a térnek, akkor a topologikus tér parakompakt.*

Bizonyítás. Legyen T olyan topologikus tér, ahogy T bármely nyílt befedésének létezik olyan lokálisan véges finomítása, amely zárt befedése T-nek. Legyen $(U_\alpha)_{\alpha\in A}$ nyílt befedése a T topologikus térnek.

Először – a hipotézis alapján – veszünk olyan $(V_\beta)_{\beta\in B}$ lokálisan véges finomítását $(U_\alpha)_{\alpha\in A}$-nak, amely befedése T-nek. (A hipotézis alapján ilyen létezik, sőt még azt is feltehetnénk, hogy minden $\beta \in B$ esetén V_β zárt halmaz T-ben. Azonban a $(V_\beta)_{\beta\in B}$ halmazrendszer zártságának a továbbiakban nincs jelentősége.) Kiválasztunk egy olyan

$f : B \to A$ függvényt, amelyre minden $\beta \in B$ esetén $V_\beta \subseteq U_{f(\beta)}$.

A $(V_\beta)_{\beta\in B}$ halmazrendszer lokálisan végessége folytán minden $t \in T$ pontnak létezik olyan Ω nyílt környezete, hogy $\{\beta \in B|\Omega \cap V_\beta \neq \emptyset\}$ véges halmaz. Ezért kiválasztható olyan $(\Omega_t)_{t\in T}$ halmazrendszer, hogy minden $t \in T$ pontra Ω_t nyílt környezete t-nek és $\{\beta \in B|\Omega_t \cap V_\beta \neq \emptyset\}$ véges halmaz.

Az $(\Omega_t)_{t\in T}$ halmazrendszer nyílt befedése a T topologikus térnek, így a hipotézis alapján vehetjük ennek olyan $(F_\gamma)_{\gamma\in\Gamma}$ lokálisan véges finomítását, amely zárt befedése a T topologikus térnek. (Itt már egészen lényeges, hogy minden $\gamma \in \Gamma$ esetén F_γ zárt halmaz T-ben.) Minden $\beta \in B$ esetén legyen $C_\beta := \bigcup\limits_{\substack{\gamma\in\Gamma,\\ V_\beta\cap F_\gamma=\emptyset}} F_\gamma$. Megmutatjuk, hogy az $\big(U_{f(\beta)} \setminus C_\beta\big)_{\beta\in B}$ halmazrendszer olyan lokálisan véges finomítása $(U_\alpha)_{\alpha\in A}$-nak, amely nyílt befedése a T topologikus térnek (amiből következik, hogy T parakompakt).

Ha $\beta \in B$, akkor

$$V_\beta \cap C_\beta = \bigcup_{\substack{\gamma\in\Gamma,\\ V_\beta\cap F_\gamma=\emptyset}} (V_\beta \cap F_\gamma) = \emptyset,$$

tehát $V_\beta \subseteq T\setminus C_\beta$, ugyanakkor az $f : B \to A$ függvény defincziója szerint $V_\beta \subseteq U_{f(\beta)}$, ezért $V_\beta \subseteq U_{f(\beta)}\cap(T\setminus C_\beta) = U_{f(\beta)}\setminus C_\beta$. Mivel a $(V_\beta)_{\beta\in B}$ halmazrendszer befedése T-nek, ebből következik, hogy az $\big(U_{f(\beta)} \setminus C_\beta\big)_{\beta\in B}$ halmazrendszer is befedése T-nek. Továbbá világos, hogy minden $\beta \in B$ esetén $U_{f(\beta)} \setminus C_\beta$ nyílt halmaz T-ben, mert $U_{f(\beta)}$ nyílt halmaz és C_β zárt, mert egyenlő az $(F_\gamma)_{\gamma\in\Gamma;\ V_\beta\cap F_\gamma=\emptyset}$ lokálisan véges zárt halmazrendszer uniójával (26.3.7.). Az nyilvánvaló, hogy $U_{f(\beta)}\setminus C_\beta$ finomítása az $(U_\alpha)_{\alpha\in A}$ halmazrendszernek.

Már csak az $\big(U_{f(\beta)} \setminus C_\beta\big)_{\beta\in B}$ halmazrendszer lokális végességét kell igazolni. Legyen $t \in T$ rögzített pont. Az $(F_\gamma)_{\gamma\in\Gamma}$ halmazrendszer lokálisan végessége miatt van olyan U nyílt környezete t-nek T-ben, hogy $\Gamma_* := \{\gamma \in \Gamma|U \cap F_\gamma \neq \emptyset\}$ véges halmaz. Az $(F_\gamma)_{\gamma\in\Gamma}$ halmazrendszer finomítása $(\Omega_t)_{t\in T}$-nek, ezért rögzíthetünk olyan $g : \Gamma_* \to T$ függvényt, amelyre minden $\gamma \in \Gamma_*$ esetén $F_\gamma \subseteq \Omega_{g(\gamma)}$. Az $(\Omega_t)_{t\in T}$ halmazrendszer definíciója szerint minden $\gamma \in \Gamma_*$ indexre $\{\beta \in B|\Omega_{g(\gamma)}\cap V_\beta \neq \emptyset\}$ véges halmaz. Ebből g definíciója alapján nyilvánvalóan következik, hogy minden $\gamma \in \Gamma_*$ esetén $\{\beta \in B|F_\gamma\cap V_\beta \neq \emptyset\}$ véges halmaz. A bizonyítást azzal zárjuk, hogy igazoljuk a

$$\{\beta \in B|U \cap \big(U_{f(\beta)} \setminus C_\beta\big) \neq \emptyset\} \subseteq \bigcup_{\gamma\in\Gamma_*} \{\beta \in B|F_\gamma \cap V_\beta \neq \emptyset\} \tag{$*$}$$

összefüggést, amiből a jobb oldalon álló halmaz végessége miatt következik, hogy $\{\beta \in B|U \cap \big(U_{f(\beta)} \setminus C_\beta\big) \neq \emptyset\}$ véges, tehát az $\big(U_{f(\beta)} \setminus C_\beta\big)_{\beta\in B}$ halmazrendszer lokálisan véges.

Legyen $\beta \in B$ olyan, hogy $U \cap \big(U_{f(\beta)} \setminus C_\beta\big) \neq \emptyset$, és legyen $s \in U \cap \big(U_{f(\beta)} \setminus C_\beta\big)$. Ekkor $s \notin C_\beta$, így C_β definíciója szerint $s \notin \bigcup\limits_{\substack{\gamma\in\Gamma,\\ V_\beta\cap F_\gamma=\emptyset}} F_\gamma$. Ugyanakkor $(F_\gamma)_{\gamma\in\Gamma}$ befedése T-nek, ezért $s \in \bigcup\limits_{\substack{\gamma\in\Gamma,\\ V_\beta\cap F_\gamma\neq\emptyset}} F_\gamma$. Mivel $s \in U$ is igaz, ezért $s \in \bigcup\limits_{\substack{\gamma\in\Gamma,\\ V_\beta\cap F_\gamma\neq\emptyset}} (U \cap F_\gamma)$, tehát létezik olyan $\gamma \in \Gamma$, hogy $V_\beta \cap F_\gamma \neq \emptyset$ és $s \in U \cap F_\gamma$. Ekkor Γ_* definíciója szerint $\gamma \in \Gamma_*$, és $\beta \in B$ olyan, hogy $V_\beta \cap F_\gamma \neq \emptyset$. Ez azt jelenti, hogy β eleme a $(*)$ összefüggés jobb oldalán álló halmaznak, tehát a $(*)$ tartalmazás helyes. ■

28.15.2. Lemma. *Ha egy reguláris topologikus tér bármely nyílt befedésének létezik olyan lokálisan véges finomítása, amely (nem feltétlenül nyílt) befedése a térnek, akkor a tér bármely nyílt befedésének létezik olyan lokálisan véges finomítása, amely zárt befedése a térnek.*

Bizonyítás. Legyen T olyan reguláris tér, hogy T minden nyílt befedésének létezik olyan lokálisan véges finomítása, amely (nem feltétlenül nyílt) befedése T-nek. Legyen $(U_\alpha)_{\alpha\in A}$ nyílt befedése a T topologikus térnek.

Ha $t \in T$, akkor van olyan $\alpha \in A$, hogy $t \in U_\alpha$, tehát U_α nyítsága miatt U_α környezete t-nek, ezért T regularitása miatt létezik t-nek olyan V nyílt környezete, hogy $\overline{V} \subseteq U_\alpha$ (27.4.5.). Tehát kiválaszthatunk olyan $(V_t)_{t\in T}$ halmazrendszert, hogy minden $t \in T$ pontra V_t nyílt környezete t-nek, és van olyan $\alpha \in A$, hogy $\overline{V_t} \subseteq U_\alpha$.

Ekkor $(V_t)_{t\in T}$ nyílt befedése a T topologikus térnek, így a hipotézis szerint vehetjük olyan $(W_\beta)_{\beta\in B}$ olyan (nem feltétlenül nyílt) befedését T-nek, amely lokálisan véges finomítása a $(V_t)_{t\in T}$ halmazrendszernek. Megmutatjuk, hogy a $(\overline{W_\beta})_{\beta\in B}$ halmazrendszer olyan lokálisan véges finomítása $(U_\alpha)_{\alpha\in A}$-nak, amely zárt befedése T-nek.

Mivel $(W_\beta)_{\beta\in B}$ befedése T-nek, így $(\overline{W_\beta})_{\beta\in B}$ még inkább befedése T-nek.

A $(W_\beta)_{\beta\in B}$ halmazrendszer finomítása $(V_t)_{t\in T}$-nek, ezért $\beta \in B$ esetén van olyan $t \in T$, hogy $W_\beta \subseteq V_t$, ugyanakkor t-hez létezik olyan $\alpha \in A$, hogy $\overline{V_t} \subseteq U_\alpha$, így $\overline{W_\beta} \subseteq \overline{V_t} \subseteq U_\alpha$. Ez azt jelenti, hogy $(\overline{W_\beta})_{\beta\in B}$ finomítása $(U_\alpha)_{\alpha\in A}$-nak.

Azt kell még igazolni, hogy a $(\overline{W_\beta})_{\beta\in B}$ halmazrendszer lokálisan véges a T topologikus térben. Ehhez legyen $t \in T$ rögzített pont. A $(W_\beta)_{\beta\in B}$ halmazrendszer lokális végessége folytán van olyan U nyílt környezete t-nek, hogy $\{\beta \in B | U \cap W_\beta \neq \emptyset\}$ véges halmaz. Ha $\beta \in B$ olyan, hogy $U \cap \overline{W_\beta} \neq \emptyset$, akkor rögzítve egy $s \in U \cap \overline{W_\beta}$ pontot kapjuk, hogy U nyílt környezete s-nek és $s \in \overline{W_\beta}$, így $U \cap W_\beta \neq \emptyset$. Ez azt jelenti, hogy $\{\beta \in B | U \cap \overline{W_\beta} \neq \emptyset\} \subseteq \{\beta \in B | U \cap W_\beta \neq \emptyset\}$ (és persze akkor ezek a halmazok egyenlőek), így $\{\beta \in B | U \cap \overline{W_\beta} \neq \emptyset\}$ véges halmaz. Ezért a $(\overline{W_\beta})_{\beta\in B}$ halmazrendszer lokálisan véges a T topologikus térben. ■

A 28.15.1. és 28.15.2. lemmák érdekes következménye a parakompaktság következő jellemzése a reguláris terek körében.

28.15.3. Állítás. *Reguláris topologikus tér pontosan akkor parakompakt, ha a tér bármely nyílt befedésének létezik olyan lokálisan véges finomítása, amely zárt befedése a térnek.*

Bizonyítás. Ha egy topologikus tér parakompakt, akkor bármely nyílt befedésének létezik lokálisan véges finomítása, amely befedése a térnek, ezért reguláris tér esetén 28.15.2. alapján a tér bármely nyílt befedésének létezik olyan lokálisan véges finomítása, amely zárt befedése a térnek, tehát a feltétel szükséges.

Megfordítva, 28.15.1. szerint a feltétel elégséges a parakompaktsághoz, még nem reguláris topologikus tér esetén is. ■

28.15.4. Definíció. *Azt mondjuk, hogy az $(U_\alpha)_{\alpha\in A}$ halmazrendszer* **σ-lokálisan véges** *a T topologikus térben, ha minden $\alpha \in A$ esetén $U_\alpha \subseteq T$ és létezik olyan $(A_\beta)_{\beta\in B}$ halmazrendszer, hogy B megszámlálható, $A = \bigcup_{\beta\in B} A_\beta$, és minden $\beta \in B$ esetén az $(U_\alpha)_{\alpha\in A_\beta}$ halmazrendszer lokálisan véges a T topologikus térben. Azt mondjuk, hogy a $\mathfrak{B}$ halmaz* **σ-lokálisan véges** *a T topologikus térben, ha az $(U)_{U\in\mathfrak{B}}$ halmazrendszer σ-lokálisan véges a T topologikus térben.*

Tehát a T topologikus tér részhalmazaiból álló $(U_\alpha)_{\alpha\in A}$ halmazrendszer σ-lokális végessége azt jelenti, hogy az A indexhalmaz felbontható megszámlálható sok részhalmazának uniójára úgy, hogy az azokon képezett részrendszerek lokálisan végesek a T topologikus térben. Speciálisan, ha A megszámlálható, akkor az $(U_\alpha)_{\alpha\in A}$ halmazrendszer triviálisan σ-lokálisan véges, ugyanakkor $(U_\alpha)_{\alpha\in A}$ nem szükségképpen lokálisan véges. (Például, a $(]-n,n[)_{n\in\mathbb{N}}$ halmazsorozat nem lokálisan véges nyílt befedése $\mathbb{R}$-nek az euklidészi topológia szerint, de – megszámlálható indexhalmazú lévén – nyilvánvalóan σ-lokálisan véges.)

28.15.5. Lemma. *Topologikus tér bármely σ-lokálisan véges nyílt befedésének létezik olyan lokálisan véges finomítása, amely (nem feltétlenül nyílt) befedése a térnek.*

Bizonyítás. Legyen $(U_\alpha)_{\alpha\in A}$ σ-lokálisan véges nyílt befedése a T topologikus térnek. Vegyünk olyan $(A_n)_{n\in\mathbb{N}}$ halmazsorozatot, hogy $A = \bigcup_{n\in\mathbb{N}} A_n$, és minden $n\in\mathbb{N}$ esetén az $(U_\alpha)_{\alpha\in A_n}$ halmazrendszer lokálisan véges. Minden $n\in\mathbb{N}$ esetén legyen $T_n := \bigcup_{\alpha\in A_n} U_\alpha$ és $V_n := \bigcup_{k=0}^{n} T_k$. Világos, hogy minden $n\in\mathbb{N}$ esetén V_n olyan nyílt halmaz T-ben, hogy $V_n\subseteq V_{n+1}$ és $T_n\subseteq V_n$. Bevezetve a $V_{-1} := \emptyset$ definíciót, látható, hogy a $(V_n\setminus V_{n-1})_{n\in\mathbb{N}}$ diszjunkt halmazrendszer befedése T-nek, de ennek a tagjai már nem szükségképpen nyílt halmazok. Legyen $B := \bigcup_{n\in\mathbb{N}}(\{n\}\times A_n)$, és vezessük be az $(U_\alpha\cap(V_n\setminus V_{n-1}))_{(n,\alpha)\in B}$ halmazrendszert, amely nyilvánvalóan finomítása az $(U_\alpha)_{\alpha\in A}$ halmazrendszernek.
Megmutatjuk, hogy $(U_\alpha\cap(V_n\setminus V_{n-1}))_{(n,\alpha)\in B}$ befedése T-nek. Legyen $t\in T$ rögzített pont. Mivel a $(V_n\setminus V_{n-1})_{n\in\mathbb{N}}$ diszjunkt halmazrendszer befedése T-nek, így (egyértelműen) létezik olyan $n\in\mathbb{N}$, hogy $t\in V_n\setminus V_{n-1}$. Ekkor $t\in V_n=\bigcup_{k=0}^{n}T_k$, de $t\notin\bigcup_{k=0}^{n-1}T_k$, ezért $t\in T_n$, így T_n definíciója szerint van olyan $\alpha\in A_n$, hogy $t\in U_\alpha$, tehát ekkor $(n,\alpha)\in B$ és $t\in U_\alpha\cap(V_n\setminus V_{n-1})$.
Megmutatjuk, hogy az $(U_\alpha\cap(V_n\setminus V_{n-1}))_{(n,\alpha)\in B}$ halmazrendszer lokálisan véges a T topologikus térben. Legyen $t\in T$ rögzített pont. Mivel $(T_n)_{n\in\mathbb{N}}$ befedése T-nek, így vehetünk egy $n\in\mathbb{N}$ számot, amelyre $t\in T_n=\bigcup_{\alpha\in A_n}U_\alpha$. Minden $k\le n$ természetes számra az $(U_\alpha)_{\alpha\in A_n}$ halmazrendszer lokálisan véges a T topologikus térben, így vehetünk olyan $(W_k)_{0\le k\le n}$ halmazrendszert, hogy minden $k\le n$ természetes számra W_k környezte t-nek T-ben, és az $\{\alpha\in A_k | U_\alpha\cap W_k\ne\emptyset\}$ halmaz véges. Mivel $t\in T_n$ és T_n nyílt halmaz T-ben, így feltehető, hogy minden $k\le n$ természetes számra $W_k\subseteq T_n$ (különben áttérnénk a $(W_k)_{0\le k\le n}$ halmazrendszerről a $(W_k\cap T_n)_{0\le k\le n}$ halmazrendszerre). Ekkor $W := \bigcap_{k=0}^{n} W_k$ környezete t-nek T-ben. Be fogjuk bizonyítani, hogy az

$$\{\ (m,\alpha)\in B\ |\ (U_\alpha\cap(V_m\setminus V_{m-1}))\cap W\ne\emptyset\ \}$$

halmaz véges. Legyen $(m,\alpha)\in B$ olyan, hogy $(U_\alpha\cap(V_m\setminus V_{m-1}))\cap W\ne\emptyset$. Ekkor W definíciója szerint $\bigcap_{k=0}^{n}((U_\alpha\cap(V_m\setminus V_{m-1}))\cap W_k)\ne\emptyset$, tehát minden $k\le n$ természetes számra $(U_\alpha\cap(V_m\setminus V_{m-1}))\cap W_k\ne\emptyset$. Ekkor $m\le n$ teljesül, mert ha $n<m$ igaz volna,

akkor $n \leq m-1$ miatt $T_n \subseteq V_{m-1}$, ezért $(V_m \setminus V_{m-1}) \cap T_n = \emptyset$, ami lehetetlen, mert ez a halmaz $W_n \subseteq T_n$ miatt tartalmazza a nem üres $(U_\alpha \cap (V_m \setminus V_{m-1})) \cap W_n$ halmazt. Tehát $m \leq n$, így $(U_\alpha \cap (V_m \setminus V_{m-1})) \cap W_m \neq \emptyset$, és $(m, \alpha) \in B$ miatt $\alpha \in A_m$. Ezért $\alpha \in \{\beta \in A_m | U_\beta \cap W_m \neq \emptyset\}$, amiből következik, hogy

$$\{(m,\alpha) \in B |\, (U_\alpha \cap (V_m \setminus V_{m-1})) \cap W \neq \emptyset\} \subseteq [\![0,n]\!] \times \bigcup_{k=0}^{n} \{\beta \in A_k | U_\beta \cap W_k \neq \emptyset\}.$$

Itt a jobb oldalon véges halmaz áll, ezért $\{(m,\alpha) \in B |\, (U_\alpha \cap (V_m \setminus V_{m-1})) \cap W \neq \emptyset\}$ véges halmaz. Ez azt jelenti, hogy $(U_\alpha \cap (V_n \setminus V_{n-1}))_{(n,\alpha)\in B}$ lokálisan véges a T topologikus térben, így ez a halmazrendszer eleget tesz a követelményeknek. ■

Az előző állítás bizonyításából látható, hogy a követelményeket kielégítő

$$(U_\alpha \cap (V_n \setminus V_{n-1}))_{(n,\alpha)\in B}$$

halmazrendszer tagjai általában valóban nem nyílt halmazok, de előállnak két nyílt halmaz különbségeként, hiszen minden $(n, \alpha) \in B$ esetén nyilvánvalóan teljesül az $U_\alpha \cap (V_n \setminus V_{n-1}) = (U_\alpha \cap V_n) \setminus V_{n-1}$ egyenlőség.

28.15.6. Lemma. *Félmetrizálható topologikus tér bármely nyílt befedésének létezik olyan σ-lokálisan véges finomítása, amely nyílt befedése a térnek.*

Bizonyítás. Legyen T félmetrizálható topologikus tér és d olyan félmetrika a T halmaz felett, amely T topológiáját generálja. Legyen $(U_\alpha)_{\alpha\in A}$ nyílt befedése T-nek, és az A indexhalmazon rögzítünk egy $\leq$ *jólrendezést* (6.15.2.).

Minden $(n, \alpha) \in \mathbb{N} \times A$ esetén legyen

$$F_{n,\alpha} := \{\ t \in T \mid \mathrm{B}_{1/2^n}(t; d) \subseteq U_\alpha\ \};$$

$$G_{n,\alpha} := \begin{cases} F_{n,\alpha} & \text{, ha } \alpha \text{ a legkisebb eleme } A\text{-nak,} \\ \bigcap\limits_{\substack{\beta\in A,\\ \beta<\alpha}} (F_{n,\alpha} \setminus F_{n+1,\beta}) & \text{, ha } \alpha \text{ nem a legkisebb eleme } A\text{-nak;} \end{cases}$$

$$V_{n,\alpha} := \bigcup_{s\in G_{n,\alpha}} \mathrm{B}_{1/2^{n+3}}(s; d).$$

(I) Megmutatjuk, hogy a $(V_{n,\alpha})_{(n,\alpha)\in\mathbb{N}\times A}$ halmazrendszer nyílt befedése T-nek. Nyilvánvaló, hogy minden $(n, \alpha) \in \mathbb{N} \times A$ párra $V_{n,\alpha}$ nyílt halmaz T-ben, mivel nyílt gömbök uniója. Legyen $t \in T$ rögzítve. Mivel az $(U_\alpha)_{\alpha\in A}$ halmazrendszer befedése T-nek, így létezik olyan $\alpha \in A$, hogy $t \in U_\alpha$: legyen $\alpha := \min\{\alpha' \in A | t \in U_{\alpha'}\}$. Ekkor $t \in U_\alpha$, és az U_α halmaz nyíltsága folytán van olyan $r > 0$ valós szám, hogy $\mathrm{B}_r(t; d) \subseteq U_\alpha$. Legyen $n \in \mathbb{N}$ olyan, hogy $\dfrac{1}{2^n} \leq r$. Ekkor $\mathrm{B}_{1/2^n}(t; d) \subseteq \mathrm{B}_r(t; d) \subseteq U_\alpha$, tehát $t \in F_{n,\alpha}$. Ugyanakkor $\beta \in A$, $\beta < \alpha$ esetén $t \notin F_{n+1,\beta}$, különben $t \in \mathrm{B}_{1/2^{n+1}}(t; d) \subseteq U_\beta$ teljesülne, ami α minimalitása miatt lehetetlen. Ezért $G_{n,\alpha}$ definíciója szerint $t \in G_{n,\alpha}$, következésképpen $V_{n,\alpha}$ definíciója alapján $t \in \mathrm{B}_{1/2^{n+3}}(t; d) \subseteq V_{n,\alpha}$.

(II) Megmutatjuk, hogy minden $n \in \mathbb{N}$ esetén a $(V_{k,\alpha})_{(k,\alpha)\in\{n\}\times A}$ halmazrendszer lokálisan véges T-ben, tehát a $(V_{n,\alpha})_{(n,\alpha)\in\mathbb{N}\times A}$ halmazrendszer σ-lokálisan véges, hiszen $\mathbb{N} \times A = \bigcup\limits_{n\in\mathbb{N}} (\{n\} \times A)$.

Ehhez először azt igazoljuk, hogy minden $\alpha, \beta \in A$ esetén, ha $\alpha \neq \beta$, akkor

$$d(G_{n,\alpha}, G_{n,\beta}) := \inf_{(t,t')\in G_{n,\alpha}\times G_{n,\beta}} d(t,t') \geq \frac{1}{2^{n+1}}.$$

A félmetrika szimmetrikussága miatt nyilvánvalóan feltehetjük, hogy $\beta < \alpha$. Legyen $(t,t') \in G_{n,\alpha} \times G_{n,\beta}$ rögzített. Mivel $\beta < \alpha$ miatt α nem a legkisebb eleme A-nak, így $G_{n,\alpha}$ definíciója szerint

$$t \in G_{n,\alpha} = \bigcap_{\substack{\gamma\in A,\\ \gamma<\alpha}} (F_{n,\alpha} \setminus F_{n+1,\gamma}) \subseteq F_{n,\alpha} \setminus F_{n+1,\beta},$$

tehát $t \in F_{n,\alpha}$ és $t \notin F_{n+1,\beta}$. Ekkor $F_{n+1,\beta}$ definíciója szerint $\mathrm{B}_{1/2^{n+1}}(t;d) \nsubseteq U_\beta$, így vehetünk olyan $s \in \mathrm{B}_{1/2^{n+1}}(t;d)$ elemet, hogy $s \notin U_\beta$. Mivel $t' \in G_{n,\beta} \subseteq F_{n,\beta}$, így $\mathrm{B}_{1/2^n}(t';d) \subseteq U_\beta$, tehát $s \notin U_\beta$ következtében $s \notin \mathrm{B}_{1/2^n}(t';d)$, vagyis $d(s,t') \geq \frac{1}{2^n}$. Ugyanakkor fennáll a $d(s,t) < \frac{1}{2^{n+1}}$ egyenlőtlenség, ezért $d(t,t') \geq \frac{1}{2^{n+1}}$, különben a háromszög-egyenlőtlenség alapján $\frac{1}{2^n} \leq d(s,t') \leq d(s,t) + d(t,t') < \frac{1}{2^{n+1}} + \frac{1}{2^{n+1}} = \frac{1}{2^n}$ teljesülne, ami lehetetlen. Ezzel beláttuk, hogy minden $(t,t') \in G_{n,\alpha} \times G_{n,\beta}$ esetén $d(t,t') \geq \frac{1}{2^{n+1}}$, következésképpen $d(G_{n,\alpha}, G_{n,\beta}) := \inf_{(t,t')\in G_{n,\alpha}\times G_{n,\beta}} d(t,t') \geq \frac{1}{2^{n+1}}$.

Megmutatjuk, hogy ha $n \in \mathbb{N}$ és $\alpha, \beta \in A$ és $\alpha \neq \beta$, akkor

$$d(V_{n,\alpha}, V_{n,\beta}) := \inf_{(t,t')\in V_{n,\alpha}\times V_{n,\beta}} d(t,t') \geq \frac{1}{2^{n+2}}.$$

Valóban, legyen $(t,t') \in V_{n,\alpha} \times V_{n,\beta}$ rögzített. Ekkor a definíció szerint léteznek olyan $s \in G_{n,\alpha}$ és $s' \in G_{n,\beta}$ pontok, hogy $t \in \mathrm{B}_{1/2^{n+3}}(s;d)$ és $t' \in \mathrm{B}_{1/2^{n+3}}(s';d)$. Tehát $d(t,s) < \frac{1}{2^{n+3}}$ és $d(t',s') < \frac{1}{2^{n+3}}$, ugyanakkor az előző bekezdés alapján $d(s,s') \geq \frac{1}{2^{n+1}}$, hiszen $(s,s') \in G_{n,\alpha} \times G_{n,\beta}$ és $\alpha \neq \beta$. Ezért $d(t,t') \geq \frac{1}{2^{n+2}}$, különben a háromszög-egyenlőtlenség szerint $\frac{1}{2^{n+1}} \leq d(s,s') \leq d(s,t) + d(t,t') + d(t',s') < \frac{1}{2^{n+3}} + \frac{1}{2^{n+2}} + \frac{1}{2^{n+3}} = \frac{1}{2^{n+1}}$ teljesülne, ami lehetetlen. Ezzel beláttuk, hogy minden $(t,t') \in V_{n,\alpha} \times V_{n,\beta}$ esetén $d(t,t') \geq \frac{1}{2^{n+2}}$, következésképpen $d(V_{n,\alpha}, V_{n,\beta}) := \inf_{(t,t')\in V_{n,\alpha}\times V_{n,\beta}} d(t,t') \geq \frac{1}{2^{n+2}}$.

Legyen $n \in \mathbb{N}$ és $t \in T$ rögzítve. Megmutatjuk, hogy ha $r > 0$ olyan valós szám, hogy $r \leq \frac{1}{2^{n+3}}$, akkor az $\{\alpha \in A | \mathrm{B}_r(t;d) \cap V_{n,\alpha} \neq \emptyset\}$ halmaz legfeljebb egy elemű. Legyenek ugyanis $\alpha, \beta \in A$ olyanok, hogy $\mathrm{B}_r(t;d) \cap V_{n,\alpha} \neq \emptyset$ és $\mathrm{B}_r(t;d) \cap V_{n,\beta} \neq \emptyset$. Rögzítsünk $t' \in \mathrm{B}_r(t;d) \cap V_{n,\alpha}$ és $t'' \in \mathrm{B}_r(t;d) \cap V_{n,\beta}$ pontokat. Ekkor $d(t',t) < r$ és $d(t'',t) < r$, ugyanakkor $t' \in V_{n,\alpha}$ és $t'' \in V_{n,\beta}$ miatt léteznek olyan $s' \in G_{n,\alpha}$ és $s'' \in G_{n,\beta}$ pontok, hogy $t' \in \mathrm{B}_{1/2^{n+3}}(s';d)$ és $t'' \in \mathrm{B}_{1/2^{n+3}}(s'';d)$, tehát $d(t',s') < \frac{1}{2^{n+3}}$ és $d(t'',s'') < \frac{1}{2^{n+3}}$. Ezekből a háromszög-egyenlőtlenség alapján következik, hogy

$$d(s',s'') \leq d(s',t') + d(t',t) + d(t,t'') + d(t'',s'') <$$
$$< \frac{1}{2^{n+3}} + r + r + \frac{1}{2^{n+3}} = 2\cdot\frac{1}{2^{n+3}} + 2\cdot r \leq \frac{1}{2^{n+2}} + 2\cdot\frac{1}{2^{n+3}} = \frac{1}{2^{n+1}},$$

ezért $\alpha = \beta$, különben $(s', s'') \in G_{n,\alpha} \times G_{n,\beta}$ és $d(G_{n,\alpha}, G_{n,\beta}) \geq \frac{1}{2^{n+1}}$ miatt $d(s', s'') \geq \frac{1}{2^{n+1}}$ teljesülne.

Ez azt jelenti, hogy $n \in \mathbb{N}$ esetén van olyan $r > 0$ valós szám (ti. bármely $r \in]0, 1/2^{n+3}]$ ilyen), hogy $\{\alpha \in A | \mathrm{B}_r(t; d) \cap V_{n,\alpha} \neq \emptyset\}$ legfeljebb egy elemű halmaz, tehát véges, vagyis a $(V_{n,\alpha})_{\alpha \in A}$ halmazrendszer lokálisan véges a T topologikus térben. Ez azzal ekvivalens, hogy $n \in \mathbb{N}$ esetén a $(V_{k,\alpha})_{(k,\alpha) \in \{n\} \times A}$ halmazrendszer lokálisan véges T-ben.

(III) Triviális, hogy a $(V_{n,\alpha})_{(n,\alpha) \in \mathbb{N} \times A}$ halmazrendszer finomítása az $(U_\alpha)_{\alpha \in A}$ halmazrendszernek, mert minden $(n, \alpha) \in \mathbb{N} \times A$ esetén $V_{n,\alpha} \subseteq U_\alpha$, hiszen $t \in V_{n,\alpha}$ esetén $V_{n,\alpha}$ definíciója alapján van olyan $s \in G_{n,\alpha} \subseteq F_{n\alpha}$, hogy $t \in \mathrm{B}_{1/2^{n+2}}(s; d)$, így $s \in F_{n,\alpha}$ miatt $t \in \mathrm{B}_{1/2^{n+2}}(s; d) \subseteq \mathrm{B}_{1/2^n}(s; d) \subseteq U_\alpha$.

Az (I), (II) és (III) állítások szerint a $(V_{n,\alpha})_{(n,\alpha) \in \mathbb{N} \times A}$ halmazrendszer olyan σ-lokálisan véges finomítása az $(U_\alpha)_{\alpha \in A}$ halmazrendszernek, amely nyílt befedése a T topologikus térnek. ■

28.15.7. Tétel. (**Stone-tétel.**) *Minden félmetrizálható topologikus tér parakompakt.*

Bizonyítás. Legyen $(U_\alpha)_{\alpha \in A}$ nyílt befedése a T félmetrizálható topologikus térnek. A 28.15.6. lemma szerint vehetjük ennek olyan $(V_\beta)_{\beta \in B}$ σ-lokálisan véges finomítását, amely nyílt befedése T-nek. A 28.15.5. lemma alapján $(V_\beta)_{\beta \in B}$-nak vehetjük olyan $(W_\gamma)_{\gamma \in \Gamma}$ lokálisan véges finomítását, amely (nem feltétlenül nyílt) befedése a térnek. Ekkor $(W_\gamma)_{\gamma \in \Gamma}$ olyan lokálisan véges finomítása az $(U_\alpha)_{\alpha \in A}$ halmazrendszernek, amely (nem feltétlenül nyílt) befedése T-nek. Ezzel megmutattuk, hogy T olyan topologikus tér, amelyre teljesül a 28.15.2. lemma hipotézise, hiszen T reguláris (27.4.6.), és bármely nyílt befedésének van olyan lokálisan véges finomítása, amely befedése T-nek. Ezért 28.15.2. alapján T bármely nyílt befedésének létezik olyan lokálisan véges finomítása, amely zárt befedése T-nek, így 28.15.1. szerint T parakompakt. ■

A Tyihonov-lemma (27.4.9.) szerint minden reguláris Lindelöf-tér normális. A Stone-tétel bizonyítását követve, a Tyihonov-lemmát a következőképpen élesíthetjük.

28.15.8. Állítás. *Minden reguláris Lindelöf-tér parakompakt.*

Bizonyítás. Lindelöf-térben bármely nyílt befedésnek létezik megszámlálható részbefedése, tehát létezik olyan σ-lokálisan véges finomítása, amely nyílt befedése a térnek. Innen kezdve pontosan ugyanúgy érvelhetünk, mint a Stone-tétel bizonyításában, csak a 28.15.2. lemma alkalmazásánál fel kell használnunk a tér regularitását is. ■

28.16. Nagata–Szmirnov metrizációs tétel

A σ-lokálisan véges halmazrendszerek fogalmának és a 28.15.6. lemmának alkalmazásával jellemzést adhatunk a félmetrizálható topologikus terekre, a reguláris topologikus terek körében. Ehhez szükségünk lesz a következő lemmára.

28.16.1. Lemma. *A $(T, \mathscr{T})$ topologikus tér pontosan akkor félmetrizálható, ha létezik olyan T feletti $(d_i)_{i \in I}$ félmetrika-rendszer, hogy I megszámlálható és $\mathscr{T} = \mathscr{T}_{(d_i)_{i \in I}}$.*

Bizonyítás. A feltétel triviálisan szükséges. Az elégségesség bizonyításához legyen $(d_i)_{i \in I}$ olyan félmetrika-rendszer T felett, hogy I megszámlálható és $\mathscr{T} = \mathscr{T}_{(d_i)_{i \in I}}$. Ekkor a definíció szerint $\mathscr{T} = \sup_{i\in I} \mathscr{T}_{d_i}$, ahol a szuprémumot a T halmaz feletti topológiák rendezett halmazában kell venni. Ha $I = \emptyset$, akkor $\sup_{i\in I} \mathscr{T}_{d_i}$ egyenlő a T feletti topológiák halmazának legkisebb elemével, vagyis az antidiszkrét topológiával, amely félmetrizálható a $T \times T \to \mathbb{R}_+$ azonosan 0 értékű félmetrika által. Ezért feltehető, hogy $I \neq \emptyset$. Ekkor I megszámlálhatósága miatt létezik $p : \mathbb{N} \to I$ szürjekció, és ekkor $\sup_{i\in I} \mathscr{T}_{d_i} = \sup_{n\in\mathbb{N}} \mathscr{T}_{d_{p(n)}}$. Ezért feltehető, hogy $I = \mathbb{N}$, tehát ekkor adott egy $(d_n)_{n\in\mathbb{N}}$ félmetrika-sorozat, amelyre $\mathscr{T} = \mathscr{T}_{(d_n)_{n\in\mathbb{N}}}$. Végül, minden $n \in \mathbb{N}$ esetén a $d_n \wedge 1 : T \times T \to \mathbb{R}_+$; $(t,s) \mapsto \min(d_n(t,s), 1)$ függvény olyan T feletti félmetrika, amely ekvivalens d_n-nel, vagyis $\mathscr{T}_{d_n} = \mathscr{T}_{d_n \wedge 1}$, ezért feltehető, hogy minden $n \in \mathbb{N}$ és $(t,s) \in T \times T$ esetén $d_n(t,s) \le 1$.

Legyen $(c_n)_{n\in\mathbb{N}}$ olyan $\mathbb{R}_+^*$-ben haladó sorozat, amelyre a $\sum_{n\in\mathbb{N}} c_n$ sor konvergens $\mathbb{R}$-ben, és értelmezzük a

$$d : T \times T \to \mathbb{R}_+; \quad (t,s) \mapsto \sum_{n=0}^{\infty} c_n d_n(t,s)$$

függvényt, amely nyilvánvalóan félmetrika T felett. Megmutatjuk, hogy $\mathscr{T} = \mathscr{T}_d$.

Legyen $\Omega \in \mathscr{T}_d$ és $t \in \Omega$. Ekkor van olyan $\rho \in \mathbb{R}_+^*$, hogy $\mathrm{B}_\rho(t;d) \subseteq \Omega$. Legyen $N \in \mathbb{N}$ olyan, hogy $\sum_{n=N+1}^{\infty} c_n < \rho/2$ és legyen $r \in \mathbb{R}_+^*$ olyan szám, hogy $\left(\sum_{n=0}^{N} c_n\right) r < \rho/2$. Ha $s \in \bigcap_{n=0}^{N} \mathrm{B}_r(t;d_n)$, vagyis minden $n \le N$ természetes számra $d_n(s,t) < r$, akkor

$$d(s,t) = \sum_{n=0}^{N} c_n d_n(s,t) + \sum_{n=N+1}^{\infty} c_n d_n(s,t) < \left(\sum_{n=0}^{N} c_n\right) r + \sum_{n=N+1}^{\infty} c_n < \frac{\rho}{2} + \frac{\rho}{2} = \rho,$$

ami azt jelenti, hogy $\bigcap_{n=0}^{N} \mathrm{B}_r(t;d_n) \subseteq \mathrm{B}_\rho(t;d) \subseteq \Omega$. Mivel $\bigcap_{n=0}^{N} \mathrm{B}_r(t;d_n)$ a t pontnak környezete a $\mathscr{T}_{(d_n)_{n\in\mathbb{N}}} = \mathscr{T}$ topológia szerint, így t belső pontja Ω-nak $\mathscr{T}$ szerint, tehát $\Omega \in \mathscr{T}$. Ez azt jelenti, hogy $\mathscr{T}_d \subseteq \mathscr{T}$.

Megfordítva, legyen $\Omega \in \mathscr{T}$ és $t \in \Omega$. Ekkor a $\mathscr{T}_{(d_n)_{n\in\mathbb{N}}}$ topológia definíciója szerint van olyan $H \subseteq \mathbb{N}$ nem üres véges halmaz és olyan $r \in \mathbb{R}_+^*$, hogy $\bigcap_{n\in H} \mathrm{B}_r(t;d_n) \subseteq \Omega$. Legyen $\rho \in \mathbb{R}_+^*$ olyan, hogy $\rho \le r \cdot \min_{n\in H} c_n$. Ha $s \in \mathrm{B}_\rho(t;d)$, vagyis $d(s,t) < \rho$, akkor minden $n \in H$ esetén $c_n d_n(s,t) \le \sum_{m=0}^{\infty} c_m d_m(t,s) = d(s,t) < \rho$, ezért $d_n(s,t) < \frac{\rho}{c_n} \le r$, tehát $s \in \bigcap_{n\in N} \mathrm{B}_r(t;d_n)$. Ebből következik, hogy $\mathrm{B}_\rho(t;d) \subseteq \bigcap_{n\in H} \mathrm{B}_r(t;d_n) \subseteq \Omega$, így t belső pontja Ω-nak a $\mathscr{T}_d$ topológia szerint, tehát $\Omega \in \mathscr{T}_d$. Ez azt jelenti, hogy $\mathscr{T} \subseteq \mathscr{T}_d$. ■

28.16.2. Tétel. (**Nagata–Szmirnov metrizációs tétel.**) *Reguláris topologikus tér pontosan akkor félmetrizálható, ha létezik σ-lokálisan véges nyílt topologikus bázisa.*

Bizonyítás. (*Szükségesség.*) Legyen T félmetrizálható topologikus tér, és d olyan félmetrika T felett, amely a T topológiáját generálja. Legyen $(r_n)_{n\in\mathbb{N}}$ olyan $\mathbb{R}_+^*$-ban haladó sorozat, amelyre teljesül az, hogy minden $n \in \mathbb{N}$ esetén $r_{n+1} \le r_n/2$. Minden $n \in \mathbb{N}$ számra a $(\mathrm{B}_{r_n}(t;d))_{t\in T}$ rendszer nyílt befedése T-nek, így 28.15.6.

szerint ennek létezik olyan σ-lokálisan véges finomítása, amely nyílt befedése T-nek. Ezért kiválaszthatunk olyan $\left((\Omega_{n,i})_{i\in I_n}\right)_{n\in\mathbb{N}}$ sorozatot, hogy minden $n \in \mathbb{N}$ esetén $(\Omega_{n,i})_{i\in I_n}$ olyan σ-lokálisan véges finomítása $(\mathrm{B}_{r_n}(t;d))_{t\in T}$-nek, amely nyílt befedése T-nek. Ekkor kiválaszthatunk olyan $\left((I_{n.m})_{m\in\mathbb{N}}\right)_{m\in\mathbb{N}}$ sorozatot, hogy minden $n \in \mathbb{N}$ esetén $I_n = \bigcup_{m\in\mathbb{N}} I_{n,m}$ és az $(\Omega_{n,i})_{i\in I_{n,m}}$ halmazrendszer lokálisan véges T-ben. Vezessük be az $A := \bigcup_{(n,m)\in\mathbb{N}\times\mathbb{N}} (\{n\} \times I_{n,m})$ halmazt. Megmutatjuk, hogy az $(\Omega_{n,i})_{(n,i)\in A}$ halmazrendszer σ-lokálisan véges nyílt topologikus bázisa a T topologikus térnek.

Az $(\Omega_{n,i})_{(n,i)\in A}$ halmazrendszer σ-lokálisan véges T-ben, mert ha minden $(n,m) \in \mathbb{N}\times\mathbb{N}$ párra $A_{n,m} := \{n\} \times I_{n,m}$, akkor $A = \bigcup_{(n,m)\in\mathbb{N}\times\mathbb{N}} A_{n,m}$ és $\mathbb{N}\times\mathbb{N}$ megszámlálható halmaz, és minden $(n,m) \in \mathbb{N}\times\mathbb{N}$ párra az $(\Omega_{n,i})_{(n,i)\in A_{n,m}}$ halmazrendszer lokálisan véges T-ben, hiszen $t \in T$ esetén az $(\Omega_{n,i})_{i\in I_n}$ halmazrendszer lokális végessége folytán van olyan V környezete t-nek, hogy $\{i \in I_n | V \cap \Omega_{n,i} \neq \emptyset\}$ véges halmaz, és világos, hogy $I_{n,m} \subseteq T_n$ miatt az $\{(n,i) \in A_{n,m} | V \cap \Omega_{n,i} \neq \emptyset\} \to \{i \in I_n | V \cap \Omega_{n,i} \neq \emptyset\}$; $(n,i) \mapsto i$ leképezés injekció, ezért $\{(n,i) \in A_{n,m} | V \cap \Omega_{n,i} \neq \emptyset\}$ is véges halmaz.

Legyen $\Omega \subseteq T$ nyílt halmaz és $t \in \Omega$. Mivel $\lim_{n\to\infty} r_n = 0$, így rögzíthetünk olyan $n \in \mathbb{N}$ számot, hogy $\mathrm{B}_{r_n}(t;d) \subseteq \Omega$. Az $(\Omega_{n+1,i})_{i\in I_{n+1}}$ halmazrendszer befedése T-nek, ezért vehetünk olyan $i_* \in I_{n+1}$ indexet, amelyre $t \in \Omega_{n+1,i_*}$. Az $(\Omega_{n+1,i})_{i\in I_{n+1}}$ halmazrendszer finomítása a $\left(\mathrm{B}_{r_{n+1}}(s;d)\right)_{s\in T}$ gömb-rendszernek, így van olyan $s \in T$, hogy $\Omega_{n+1,i_*} \subseteq \mathrm{B}_{r_{n+1}}(s;d)$. Megmutatjuk, hogy $\Omega_{n+1,i_*} \subseteq \Omega$. Valóban, ha $t' \in \Omega_{n+1,i_*}$, akkor $\Omega_{n+1,i_*} \subseteq \mathrm{B}_{r_{n+1}}(s;d)$ miatt $d(t',s) < r_{n+1}$, így $t \in \Omega_{n+1,i_*}$ következtében $d(t,s) < r_{n+1}$ is igaz, ezért $d(t',t) \leq d(t',s) + d(s,t) < 2r_{n+1} \leq r_n$, így $t' \in \mathrm{B}_{r_n}(s;d) \subseteq \Omega$. Ez azt jelenti, hogy T minden nyílt részhalmaza előáll az $(\Omega_{n,i})_{(n,i)\in A}$ halmazrendszer valamely részrendszerének uniójaként, vagyis $(\Omega_{n,i})_{(n,i)\in A}$ nyílt topologikus bázis a T topologikus térben.

(*Elégségesség.*) Legyen $(B_i)_{i\in I}$ σ-lokálisan véges nyílt topologikus bázisa T-nek, és $(I_n)_{n\in\mathbb{N}}$ olyan halmazsorozat, hogy $I = \bigcup_{n\in\mathbb{N}} I_n$ és minden $n \in \mathbb{N}$ esetén $(B_i)_{i\in I_n}$ lokálisan véges T-ben. Legyen $\mathfrak{B} := \{B_i | i \in I\}$ és minden $n \in \mathbb{N}$ számra $\mathfrak{B}_n := \{B_i | i \in I_n\}$.

Minden $U \subseteq T$ halmazra és $n \in \mathbb{N}$ számra legyen

$$U_n := \bigcup_{\substack{V\in\mathfrak{B}_n,\\ \overline{V}\subseteq U}} V.$$

Világos, hogy minden $U \subseteq T$ és $n \in \mathbb{N}$ esetén a $(V)_{V\in\mathfrak{B}_n,\ \overline{V}\subseteq U}$ rendszer lokálisan véges T-ben, mert ez részrendszere a lokálisan véges $(V)_{V\in\mathfrak{B}_n}$ rendszernek, ezért 26.3.6. alapján

$$\overline{U_n} = \overline{\bigcup_{\substack{V\in\mathfrak{B}_n,\\ \overline{V}\subseteq U}} V} = \bigcup_{\substack{V\in\mathfrak{B}_n,\\ \overline{V}\subseteq U}} \overline{V} \subseteq U. \tag{1}$$

Ebből könnyen belátható, hogy T-ben minden nyílt halmaz F_σ-halmaz, tehát előáll megszámlálható sok zárt halmaz uniójakét. Valóban, ha $U \subseteq T$, akkor (1) alapján $\bigcup_{n\in\mathbb{N}} \overline{U_n} \subseteq U$, és ha U nyílt, akkor $t \in U$ esetén, T regularitása miatt létezik t-nek olyan W zárt környezete T-ben, hogy $W \subseteq U$, és mivel $\mathfrak{B}$ nyílt topologikus bázis T-ben, így van olyan $V \in \mathfrak{B}$, hogy $t \in V \subseteq W$, tehát $\overline{V} \subseteq W \subseteq U$. Mivel $\mathfrak{B} = \bigcup_{n\in\mathbb{N}} \mathfrak{B}_n$, ez azt jelenti, hogy ha $U \subseteq T$ nyílt halmaz, akkor minden $t \in U$ ponthoz van olyan $n \in \mathbb{N}$ és $V \in \mathfrak{B}_n$, hogy $t \in V$ és $\overline{V} \subseteq U$, vagyis (U_n definíciója szerint) $t \in U_n$, következésképpen

$$\bigcup_{n\in\mathbb{N}} U_n \subseteq \bigcup_{n\in\mathbb{N}} \overline{U_n} \subseteq U \subseteq \bigcup_{n\in\mathbb{N}} U_n,$$

tehát $U = \bigcup_{n\in\mathbb{N}} \overline{U_n}$, így U F_σ-halmaz, és az is látható, hogy ha $\mathscr{T}$ jelöli T topológiáját, akkor

$$(\forall\, U \in \mathscr{T}) : \; U = \bigcup_{n\in\mathbb{N}} U_n = \bigcup_{n\in\mathbb{N}} \overline{U_n}. \tag{2}$$

Megmutatjuk, hogy T normális tér. Ehhez legyenek $F, F' \subseteq T$ olyan zárt halmazok, hogy $F \cap F' = \emptyset$. Ekkor $T \setminus F'$ nyílt halmaz T-ben, tehát ha minden $n \in \mathbb{N}$ esetén $\Omega(n) := (T \setminus F')_n$, akkor (2) alapján $T \setminus F' = \bigcup_{n\in\mathbb{N}} \Omega(n) = \bigcup_{n\in\mathbb{N}} \overline{\Omega(n)}$. Világos, hogy $F \subseteq T \setminus F'$ miatt $F \subseteq \bigcup_{n\in\mathbb{N}} \Omega(n)$ és minden $n \in \mathbb{N}$ esetén $\overline{\Omega(n)} \cap F' = \emptyset$. Az F és F' halmazok szerepét felcserélve kapjuk, hogy ha minden minden $n \in \mathbb{N}$ esetén $\Omega'(n) := (T \setminus F)_n$, akkor (2) alapján $T \setminus F = \bigcup_{n\in\mathbb{N}} \Omega'(n) = \bigcup_{n\in\mathbb{N}} \overline{\Omega'(n)}$. Világos, hogy $F' \subseteq T \setminus F$ miatt $F' \subseteq \bigcup_{n\in\mathbb{N}} \Omega'(n)$ és minden $n \in \mathbb{N}$ esetén $\overline{\Omega'(n)} \cap F = \emptyset$. Ekkor

$$\Omega := \bigcup_{n\in\mathbb{N}} \left(\Omega(n) \setminus \bigcup_{k=0}^{n} \overline{\Omega'(k)} \right), \qquad \Omega' := \bigcup_{n\in\mathbb{N}} \left(\Omega'(n) \setminus \bigcup_{k=0}^{n} \overline{\Omega(k)} \right)$$

nyílt halmazok T-ben. Állítjuk, hogy $F \subseteq \Omega$, $F' \subseteq \Omega'$ és $\Omega \cap \Omega' = \emptyset$, ami azt jelenti, hogy T normális tér.

Valóban, ha $t \in F$, akkor $F \subseteq \bigcup_{n\in\mathbb{N}} \Omega(n)$ miatt van olyan $n \in \mathbb{N}$, hogy $t \in \Omega(n)$, ugyanakkor minden $k \in \mathbb{N}$ esetén $\overline{\Omega'(k)} \cap F = \emptyset$, tehát $t \notin \bigcup_{k=0}^{n} \overline{\Omega'(k)}$, következésképpen $t \in \Omega(n) \setminus \bigcup_{k=0}^{n} \overline{\Omega'(k)} \subseteq \Omega$. Ezért $F \subseteq \Omega$, és teljesen hasonlóan igazolható, hogy $F' \subseteq \Omega'$.

Indirekt, tegyük fel, hogy $\Omega \cap \Omega' \neq \emptyset$, és legyen $t \in \Omega \cap \Omega'$. Ekkor léteznek olyan $m, n \in \mathbb{N}$ számok, hogy $t \in \Omega(m) \cap \Omega'(n)$ és $t \notin \bigcup_{k=0}^{m} \overline{\Omega'(k)}$ és $t \notin \bigcup_{k=0}^{n} \overline{\Omega(k)}$. Ha $m \leq n$, akkor $t \in \Omega(m)$ és $\overline{\Omega(m)} \subseteq \bigcup_{k=0}^{n} \overline{\Omega(k)}$ és $t \notin \bigcup_{k=0}^{n} \overline{\Omega(k)}$ miatt $t \notin \overline{\Omega(m)}$, ami lehetetlen. Hasonlóan, ha $n \leq m$, akkor $t \in \Omega'(n)$ és $\overline{\Omega'(n)} \subseteq \bigcup_{k=0}^{m} \overline{\Omega'(k)}$ és $t \notin \bigcup_{k=0}^{m} \overline{\Omega'(k)}$ miatt $t \notin \overline{\Omega'(n)}$, ami lehetetlen, és ez már ellentmondás. Ezért $\Omega \cap \Omega' = \emptyset$.

Tehát T normális tér, ezért ha $U \subseteq T$ nyílt halmaz és $n \in \mathbb{N}$, akkor (1) és a normális terekre vonatkozó Uriszon-tétel alapján van olyan $f \in \mathscr{C}(T; \mathbb{R})$ függvény, hogy $0 \leq f \leq 1$, és $\overline{U_n} \subseteq [f = 1]$, és $[f \neq 0] \subseteq U$. Tehát minden $U \subseteq T$ nyílt halmazhoz kiválasztható olyan $\mathscr{C}(T;\mathbb{R})$-ben haladó $(f_{U,n})_{n\in\mathbb{N}}$ sorozat, hogy minden $n \in \mathbb{N}$ számra $0 \leq f_{U,n} \leq 1$, és $\overline{U_n} \subseteq [f_{U,n} = 1]$, és $[f_{U,n} \neq 0] \subseteq U$.

Legyenek $m, n \in \mathbb{N}$ és $(t, s) \in T \times T$. Mivel a $\mathfrak{B}_m$ halmaz lokálisan véges T-ben, így létezik olyan V_t környezete t-nek és olyan V_s környezete s-nek, hogy $A_t := \{U \in \mathfrak{B}_m | V_t \cap U \neq \emptyset\}$ és $A_s := \{U \in \mathfrak{B}_m | V_s \cap U \neq \emptyset\}$ véges halmazok, és ekkor minden $(t', s') \in V_t \times V_s$ párra, ha $U \in \mathfrak{B}_m$ és $U \notin A_t \cup A_s$, akkor $V_t \cap U = \emptyset = V_s \cap U$, tehát $t' \notin U$ és $s' \notin U$, következésképpen $f_{U,n}(t') = 0 = f_{U,n}(s')$ (hiszen $[f_{U,n} \neq 0] \subseteq U$), így

$$\sum_{U\in\mathfrak{B}_m} |f_{U,n}(t') - f_{U,n}(s')| = \sum_{U\in A_t\cup A_s} |f_{U,n}(t') - f_{U,n}(s')|.$$

Ebből látható, hogy minden $m, n \in \mathbb{N}$ esetén jól értelmezett a

$$d_{m,n} : T \times T \to \mathbb{R}_+; \quad (t, s) \mapsto \sum_{U\in\mathfrak{B}_m} |f_{U,n}(t) - f_{U,n}(s)|$$

függvény, és ez folytonos a $T \times T$ topologikus szorzattéren, hiszen $T \times T$ minden pontjának valamely $\mathscr{T} \times \mathscr{T}$ szerinti környezetén egyenlő véges sok folytonos (ti. $T \times T \to \mathbb{R}_+;\ (t', s') \mapsto |f_{U,n}(t') - f_{U,n}(s')|$ alakú) függvény összegével.

Nyilvánvaló, hogy minden $n \in \mathbb{N}$ számra d_n félmetrika a T halmaz felett. Meg fogjuk mutatni, hogy $\mathscr{T}' := \mathscr{T}_{(d_{m,n})_{(m,n)\in\mathbb{N}\times\mathbb{N}}}$ egyenlő T topológiájával, vagyis $\mathscr{T}$-vel. Ebből az előző lemma alapján következik, hogy a $\mathscr{T}$ topológia metrizálható.

Legyen $\Omega \in \mathscr{T}'$ és $t \in T$. Ekkor a $\mathscr{T}'$ topológia definíciója szerint létezik olyan $H \subseteq \mathbb{N}\times\mathbb{N}$ nem üres véges halmaz és olyan $r \in \mathbb{R}_+^*$ szám, hogy

$$\bigcap_{(m,n)\in H} \mathrm{B}_r(t; d_{m,n}) \subseteq \Omega.$$

Ha $(m, n) \in \mathbb{N} \times \mathbb{N}$, akkor a $d_{m,n}(t, \cdot) : T \to \mathbb{R}$ parciális függvény folytonos $\mathscr{T}$ és $\mathscr{E}_\mathbb{R}$ szerint, ezért a $\mathrm{B}_r(t; d_{m,n}) = [d_{m,n}(t, \cdot) < r]$ halmaz $\mathscr{T}$-nyílt, így H végessége folytán $\bigcap_{(m,n)\in H} \mathrm{B}_r(t; d_{m,n}) \in \mathscr{T}$, ezért t belső pontja Ω-nak $\mathscr{T}$ szerint. Tehát $\Omega \in \mathscr{T}$, ami azt jelenti, hogy $\mathscr{T}' \subseteq \mathscr{T}$.

Megfordítva, legyen $\Omega \in \mathscr{T}$ és $t \in \Omega$. A (2) kijelentés szerint $\Omega = \bigcup_{m\in\mathbb{N}} \Omega_m$, tehát vehetünk olyan $m \in \mathbb{N}$ számot, hogy $t \in \Omega_m$, ami Ω_m definíciója szerint azt jelenti, hogy rögzíthetünk olyan $V \in \mathfrak{B}_m$ halmazt, hogy $t \in V$ és $\overline{V} \subseteq \Omega$. Mivel $V \in \mathscr{T}$, így ismét a (2) kijelentés szerint $V = \bigcup_{n\in\mathbb{N}} V_n$, ezért rögzíthetünk olyan $n \in \mathbb{N}$ számot, hogy $t \in V_n$. Legyen $r \in \mathbb{R}$ tetszőleges olyan szám, amelyre $0 < r \leq 1$. Megmutatjuk, hogy $\mathrm{B}_r(t; d_{m,n}) \subseteq \Omega$ teljesül. Valóban, legyen $s \in \mathrm{B}_r(t; d_{m,n})$, vagyis $d_{m,n}(t, s) < r$. Ekkor $V \in \mathfrak{B}_m$ és $t \in V_n \subseteq [f_{V,n} = 1]$ és $0 \leq f_{V,n}(s) \leq 1$ miatt

$$1 - f_{V,n}(s) = |f_{V,n}(t) - f_{V,n}(s)| \leq \sum_{U\in\mathfrak{B}_m} |f_{U,n}(t) - f_{U,n}(s)| = d_{m,n}(t, s) < r \leq 1,$$

amiből következik, hogy $f_{V,n}(s) > 0$, tehát $s \in [f_{V,n} \neq 0] \subseteq V$. Mivel $V \subseteq \Omega$ (sőt még $\overline{V} \subseteq \Omega$ is igaz), ebből kapjuk, hogy $s \in \Omega$. Tehát $\mathrm{B}_r(t; d_{m,n}) \subseteq \Omega$ és a $\mathrm{B}_r(t; d_{m,n})$ gömb környezete t-nek a $\mathscr{T}'$ topológia szerint, ezért t belső pontja Ω-nak $\mathscr{T}'$ szerint. Tehát $\Omega \in \mathscr{T}'$, ami azt jelenti, hogy $\mathscr{T} \subseteq \mathscr{T}'$. ■

29. fejezet

Folytonos függvények lokálisan kompakt terek felett

29.1. Pontonként konvergens és egyenletesen konvergens általánosított függvénysorozatok

Jelölés. Ha T és T' topologikus terek, akkor $\mathscr{C}(T;T')$ jelöli a $T \to T'$ folytonos függvények halmazát.

29.1.1. Definíció. *Legyen T halmaz, T' Hausdorff-tér és $(f_i)_{i\in I}$ olyan általánosított sorozat, hogy minden $I \ni i$-re $f_i : T \to T'$ függvény. Ekkor $\lim\limits_{i,\ I} f_i$ jelöli azt a $T \rightarrowtail T'$ függvényt, amelynek definíciós tartománya a*

$$\{t \in T|\ \textit{az } (f_i(t))_{i\in I} \textit{ általánosított sorozat konvergens } T'\textit{-ben}\},$$

halmaz, és minden $t \in \mathrm{Dom}\Big(\lim\limits_{i,\ I} f_i\Big)$ esetén

$$\Big(\lim_{i,\ I} f_i\Big)(t) := \lim_{i,\ I} f_i(t).$$

A $\lim\limits_{i,\ I} f_i$ függvényt az $(f_i)_{i\in I}$ olyan általánosított függvénysorozat **pontonkénti limeszfüggvényének** *nevezzük. Azt mondjuk, hogy az $(f_i)_{i\in I}$ általánosított függvénysorozat* **pontonként konvergens** *az $E \subseteq T$ halmazon, ha $E \subseteq \mathrm{Dom}\Big(\lim\limits_{i,\ I} f_i\Big)$.*

Tehát az előző definíció feltételei mellett az $(f_i)_{i\in I}$ általánosított függvénysorozat akkor és csak akkor pontonként konvergens az $E \subseteq T$ halmazon, ha

$$(\forall\ t \in E)(\exists\ t' \in T')(\forall\ V' \in \mathscr{T}'(t'))(\exists\ j \in I)(\forall\ i \in I):\ (i \geq j\ \Rightarrow\ f_i(t) \in V'),$$

ahol $\mathscr{T}'$ jelöli a T' topológiáját.

A *pontonkénti approximáció problémája* a következőképpen fogalmazható meg. Legyen T halmaz, T' Hausdorff-tér és $H \subseteq \mathscr{F}(T;T')$. Azt kérdezzük, hogy milyen tulajdonságúak azok az $f : T \rightarrowtail T'$ függvények, amelyekhez létezik olyan H-ban haladó $(f_i)_{i\in I}$ általánosított sorozat, hogy $f = \lim\limits_{i,\ I} f_i$; ezeket a függvényeket mondjuk H-beli függvényekkel *pontonként approximálhatóknak*.

Metrikus térbe érkező függvények általánosított sorozatára értelmezhető az egyenletes konvergencia fogalma.

29.1.2. Definíció. *Legyen T halmaz, M metrikus tér, és $(f_i)_{i\in I}$ olyan általánosított sorozat, hogy minden $I \ni i$-re $f_i : T \to M$ függvény. Azt mondjuk, hogy az $(f_i)_{i\in I}$ általánosított függvénysorozat* **egyenletesen konvergens** *az $E \subseteq T$ halmazon, ha pontonként konvergens az E halmazon, és az $f := \lim_{i,\ I} f_i$ pontonkénti limeszfüggvényre*

$$\lim_{i,\ I}\left(\sup_{t\in E} d(f_i(t), f(t))\right) = 0.$$

Tehát – az előző definíció feltételei mellett – az $(f_i)_{i\in I}$ általánosított függvénysorozat pontosan akkor egyenletesen konvergens az $E \subseteq T$ halmazon, ha pontonként konvergens az E halmazon, és az $f := \lim_{i,\ I} f_i$ pontonkénti limeszfüggvényre

$$(\forall\, \varepsilon \in \mathbb{R}_+^*)(\exists\, j \in I)(\forall\, i \in I) :\ (i \geq j\ \Rightarrow\ \sup_{t\in E} d(f_i(t), f(t)) \leq \varepsilon)$$

teljesül, ahol d jelöli az M metrikáját. Ez úgy is írható, hogy

$$(\forall\, \varepsilon \in \mathbb{R}_+^*)(\exists\, j \in I)(\forall\, i \in I)(\forall\, t \in E) :\ (i \geq j \Rightarrow\ d(f_i(t), f(t)) \leq \varepsilon).$$

Legyen T halmaz, M metrikus tér, és $(f_i)_{i\in I}$ olyan általánosított sorozat, hogy minden $I \ni i$-re $f_i : T \to M$ függvény. Ha az $(f_i)_{i\in I}$ egyenletesen konvergens az $E \subseteq T$ halmazon, akkor $(f_i)_{i\in I}$ az E minden részhalmazán is egyenletesen konvergens. Ha $(E_\alpha)_{\alpha\in A}$ olyan *véges* rendszer, hogy minden $\alpha \in A$ esetén $E_\alpha \subseteq T$ és $(f_i)_{i\in I}$ egyenletesen konvergens az E_α halmazon, akkor $(f_i)_{i\in I}$ egyenletesen konvergens az $\bigcup_{\alpha\in A} E_\alpha$ halmazon is.

29.1.3. Állítás. *Legyen T halmaz, M metrikus tér és $\mathscr{F}^b(T; M)$ a $T \to M$ korlátos függvények halmaza a*

$$\mathbf{d} : \mathscr{F}^b(T; M) \times \mathscr{F}^b(T; M) \to \mathbb{R}_+; \quad (f, g) \mapsto \sup_{t\in T} d(f(t), g(t))$$

sup-metrikával ellátva, ahol d az M metrikája. Legyen $f \in \mathscr{F}^b(T; M)$ és $(f_i)_{i\in I}$ egy $\mathscr{F}^b(T; M)$-ben haladó általánosított sorozat. Az $(f_i)_{i\in I}$ általánosított függvénysorozat pontosan akkor konvergál f-hez a sup-metrika szerint, ha $f = \lim_{i,\ I} f_i$ és az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletesen konvergens a T halmazon.

Bizonyítás. Tegyük fel, hogy $(f_i)_{i\in I}$ konvergál f-hez a $\mathscr{T}_{\mathbf{d}}$ topológia szerint, ahol $\mathbf{d}$ a sup-metrika $\mathscr{F}^b(T; M)$ felett. Minden $T \ni t$-re és $I \ni i$-re $d(f_i(t), f(t)) \leq \mathbf{d}(f_i, f)$, ahol d jelöli az M feletti metrikát. Ebből látható, hogy minden $t \in T$ esetén $f(t) = \lim_{i,\ I} f_i(t)$, vagyis $f = \lim_{i,\ I} f_i$. Ha $\varepsilon \in \mathbb{R}_+^*$ tetszőleges, akkor van olyan $i_\varepsilon \in I$, hogy minden $I \ni i$-re, ha $i \geq i_\varepsilon$, akkor $\sup_{t\in T} d(f_i(t), f(t)) \leq \mathbf{d}(f_i, f) \leq \varepsilon$, tehát minden $T \ni t$-re $d(f_i(t), f(t)) \leq \varepsilon$. Ez azt jelenti, hogy az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletesen konvergens a T halmazon.

Megfordítva, tegyük fel, hogy $f = \lim_{i,\ I} f_i$ és az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletesen konvergens a T halmazon. Legyen V az f környezete $\mathscr{F}^b(T; M)$-ben a $\mathscr{T}_{\mathbf{d}}$ topológia szerint. Vegyünk olyan $\varepsilon \in \mathbb{R}_+^*$ számot, hogy $\overline{\mathrm{B}}_\varepsilon(f; \mathbf{d}) \subseteq V$. Az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletes konvergenciája miatt van olyan $i_\varepsilon \in I$, hogy minden $i \in I$ és $t \in T$ esetén, ha $i \geq i_\varepsilon$, akkor $d(f_i(t), f(t)) \leq \varepsilon$, vagyis minden $i \in I$ esetén, ha $i \geq i_\varepsilon$, akkor $\mathbf{d}(f_i, f) := \sup_{t\in T} d(f_i(t), f(t)) \leq \varepsilon$. Ez azt jelenti, hogy $i \in I$ és $i \geq i_\varepsilon$ esetén $f_i \in \overline{\mathrm{B}}_\varepsilon(f; \mathbf{d}) \subseteq V$, azaz $(f_i)_{i\in I}$ konvergál f-hez a sup-metrika szerint. ■

29.1.4. Definíció. *Legyen T topologikus tér, M metrikus tér és $(f_i)_{i\in I}$ olyan általánosított sorozat, hogy minden $I \ni i$-re $f_i : T \to M$ függvény. Azt mondjuk, hogy az $(f_i)_{i\in I}$ általánosított függvénysorozat* **lokálisan egyenletesen konvergens** *az $E \subseteq T$ halmazon, ha minden $t \in E$ pontnak létezik olyan V környezete T-ben, hogy $(f_i)_{i\in I}$ egyenletesen konvergens az $E \cap V$ halmazon.*

Tehát – az előző definíció feltételei mellett – az $(f_i)_{i\in I}$ általánosított függvénysorozat pontosan akkor lokálisan egyenletesen konvergens az $E \subseteq T$ halmazon, ha pontonként konvergens az E halmazon, és az $f := \lim\limits_{i,\ I} f_i$ pontonkénti limeszfüggvényre

$$(\forall\ t \in E)(\exists\ V \in \mathscr{T}(t))(\forall\ \varepsilon \in \mathbb{R}_+^*)(\exists\ j \in I)(\forall\ i \in I) :$$
$$(i \geq j \Rightarrow \sup_{s \in E \cap V} d(f_i(s), f(s)) \leq \varepsilon)$$

teljesül, ahol $\mathscr{T}$ jelöli a T topológiáját és d jelöli az M metrikáját. Ez úgy is írható, hogy

$$(\forall\ t \in E)(\exists\ V \in \mathscr{T}(t))(\forall\ \varepsilon \in \mathbb{R}_+^*)(\exists\ j \in I)(\forall\ i \in I)(\forall\ s \in E \cap V) :$$
$$(i \geq j \ \Rightarrow\ d(f_i(s), f(s)) \leq \varepsilon).$$

29.1.5. Állítás. *Legyen T topologikus tér, M metrikus tér és $(f_i)_{i\in I}$ olyan általánosított sorozat, hogy minden $I \ni i$-re $f_i : T \to M$ függvény. Ha az $(f_i)_{i\in I}$ általánosított függvénysorozat lokálisan egyenletesen konvergens a T halmazon, akkor $(f_i)_{i\in I}$ a T minden kompakt részhalmazán egyenletesen konvergens. Ha T lokálisan kompakt és $(f_i)_{i\in I}$ a T minden kompakt részhalmazán egyenletesen konvergens, akkor $(f_i)_{i\in I}$ lokálisan egyenletesen konvergens a T halmazon.*

Bizonyítás. Tegyük fel, hogy az $(f_i)_{i\in I}$ általánosított függvénysorozat lokálisan egyenletesen konvergens a T halmazon és legyen $f := \lim\limits_{i,\ I} f_i$. Rögzítünk egy $K \subseteq T$ kompakt halmazt, és kiválasztunk egy olyan $(V_t)_{t\in T}$ rendszert, hogy minden $t \in K$ pontra V_t nyílt környezete t-nek, és $(f_i)_{i\in I}$ egyenletesen konvergens V_t-n. Ekkor a K kompaktsága miatt van olyan $H \subseteq K$ véges halmaz, hogy $K \subseteq \bigcup\limits_{t\in K} V_t$. Világos, hogy $(f_i)_{i\in I}$ egyenletesen konvergens az $\bigcup\limits_{t\in H} V_t$ halmazon, ezért a K halmazon is egyenletesen konvergens.

Megfordítva, ha $(f_i)_{i\in I}$ a T minden kompakt részhalmazán egyenletesen konvergens és T lokálisan kompakt, akkor $(f_i)_{i\in I}$ a T minden pontjának valamely környezetén egyenletesen konvergens, így $(f_i)_{i\in I}$ lokálisan egyenletesen konvergens a T halmazon. ■

Az *egyenletes* (illetve *lokálisan egyenletes*) *approximáció problémája* a következőképpen fogalmazható meg. Legyen T halmaz (illetve topologikus tér), M metrikus tér és $H \subseteq \mathscr{F}(T; M)$. Azt kérdezzük, hogy milyen tulajdonságúak azok az $f : T \rightarrowtail M$ függvények, amelyekhez létezik olyan H-ban haladó $(f_i)_{i\in I}$ általánosított sorozat, hogy $f = \lim\limits_{i,\ I} f_i$, és $(f_i)_{i\in I}$ egyenletesen (illetve lokálisan egyenletesen) konvergens a $\mathrm{Dom}(f)$ halmazon; ezeket a függvényeket mondjuk H-beli függvényekkel *egyenletesen* (illetve *lokálisan egyenletesen*) *approximálhatóknak.*

29.2. A folytonosság öröklődése pontonkénti limeszfüggvényre

A következő tétel teljes jellemzést ad arra, hogy topologikus tér egy pontjában folytonos függvények általánosított sorozatának pontonkénti limeszfüggvénye folytonos legyen az adott pontban.

29.2.1. Tétel. *Legyen T topologikus tér, M metrikus tér és $(f_i)_{i\in I}$ olyan általánosított sorozat, hogy minden $I \ni i$-re $f_i : T \to M$ függvény. Tegyük fel, hogy $(f_i)_{i\in I}$ pontonként konvergens a T halmazon, és legyen $f := \lim\limits_{i,\ I} f_i$. Ha $t \in T$ olyan pont, hogy minden $I \ni i$-re f_i folytonos t-ben, akkor a következő állítások ekvivalensek:*

(i) *Az f függvény folytonos a t pontban.*

(ii) *Minden $\varepsilon \in \mathbb{R}_+^*$ számhoz létezik olyan olyan $j \in I$, hogy minden $i \in I$, $i \geq j$ indexhez létezik t-nek olyan V környezete T-ben, hogy minden $V \ni t'$ -re $d(f_i(t'), f(t')) < \varepsilon$.*

(iii) *Minden $\varepsilon \in \mathbb{R}_+^*$ és $j \in I$ esetén létezik olyan $i \in I$, $i \geq j$ index, és létezik a t-nek olyan V környezete T-ben, hogy minden $V \ni t'$-re $d(f_i(t'), f(t')) < \varepsilon$.*

(iv) *Minden $\varepsilon \in \mathbb{R}_+^*$ számhoz létezik olyan $i \in I$ és olyan V környezete t-nek T-ben, hogy minden $V \ni t'$ -re $d(f_i(t'), f(t')) < \varepsilon$.*

Bizonyítás. (i)⇒(ii) Legyen $\varepsilon \in \mathbb{R}_+^*$ rögzített, és az f függvény t-beli folytonossága alapján vegyük a t-nek olyan $V(\varepsilon)$ környezetét T-ben, hogy minden $V(\varepsilon) \ni t'$-re $d(f(t'), f(t)) < \varepsilon/3$. Az f definíciója alapján az $(f_i(t))_{i\in I}$ általánosított sorozat konvergál $f(t)$-hez M-ben, így van olyan $j \in I$, hogy minden $i \in I$, $i \geq j$ indexre $d(f_i(t), f(t)) < \varepsilon/3$. Ha $i \in I$ olyan, hogy $i \geq j$, akkor az f_i függvény t-beli folytonossága alapján létezik t-nek olyan V_i környezete T-ben, hogy minden $V_i \ni t'$-re $d(f_i(t'), f_i(t)) < \varepsilon/3$ teljesül; ekkor a $V := V(\varepsilon) \cap V_i$ halmaz olyan környezete t-nek T-ben, hogy minden $V \ni t'$-re

$$d(f_i(t'), f(t')) \leq d(f_i(t'), f_i(t)) + d(f_i(t), f(t)) + d(f(t), f(t')) < \varepsilon.$$

Tehát minden $\mathbb{R}_+^* \ni \varepsilon$-hoz találtunk olyan $I \ni j$-t, hogy minden $i \in I$, $i \geq j$ indexhez létezik a t-nek olyan V környezete, amelynek minden t' elemére $d(f_i(t'), f(t')) < \varepsilon$ teljesül, így (ii) következik (i)-ből.

(ii)⇒(iii) Legyen $\varepsilon \in \mathbb{R}_+^*$ és a (ii) alapján vegyünk olyan $j_\varepsilon \in I$ indexet, hogy minden $i \in I$, $i \geq j_\varepsilon$ indexhez létezik t-nek olyan V környezete T-ben, hogy minden $V \ni t'$-re $d(f_i(t'), f(t')) < \varepsilon$. Ekkor minden $j \in I$ esetén az I felfelé irányítottsága miatt vehetünk olyan $I \ni i$-t, hogy $i \geq j$ és $i \geq j_\varepsilon$; ekkor az i-hez létezik t-nek olyan V környezete T-ben, hogy minden $V \ni t'$-re $d(f_i(t'), f(t')) < \varepsilon$. Ezért (iii) közetkezik (ii)-ből.

(iii)⇒(iv) Logikai trivialitás, mert $I \neq \emptyset$.

(iv)⇒(i) Legyen $\varepsilon \in \mathbb{R}_+^*$ rögzített, és az $\varepsilon/3$ számhoz a (iv) alapján vegyünk olyan $i \in I$ indexet és a t-nek olyan V' környezetét T-ben, hogy minden $V' \ni t'$-re $d(f_i(t'), f(t')) < \varepsilon/3$. Speciálisan, $t \in V'$ miatt $d(f_i(t), f(t)) < \varepsilon/3$ is teljesül. Az f_i függvény folytonos t-ben, ezért létezik t-nek olyan V'' környezete T-ben, hogy minden $V'' \ni t'$-re $d(f_i(t'), f_i(t)) < \varepsilon/3$. Ekkor $V := V' \cap V''$ olyan környezete t-nek T-ben, hogy minden $t' \in V$ pontra

$$d(f(t'), f(t)) \leq d(f(t'), f_i(t')) + d(f_i(t'), f_i(t)) + d(f_i(t), f(t)) < \varepsilon$$

teljesül, ami azt jelenti, hogy f folytonos a t pontban. ■

29.2.2. Tétel. *Legyen T topologikus tér, M metrikus tér és $(f_i)_{i\in I}$ olyan általánosított sorozat, hogy minden $I \ni i$-re $f_i \in \mathscr{C}(T; M)$. Ha az $(f_i)_{i\in I}$ általánosított függvénysorozat lokálisan egyenletesen konvergens a T halmazon, akkor $\lim\limits_{i,\ I} f_i \in \mathscr{C}(T; M)$.*

Bizonyítás. Jelölje d az M metrikáját, $f := \lim_{i,\, I} f_i$, és legyen $t \in T$ rögzített pont. Vegyünk tetszőleges $\varepsilon \in \mathbb{R}_+^*$ számot. A t pontnak olyan V környezetét keressük T-ben, amelyre $f\langle V\rangle \subseteq \mathrm{B}_\varepsilon(f(t); d)$.

Először vegyük a t-nek olyan V_1 környezetét, amelyen az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletesen konvergens, vagyis $\lim_{i,\, I}\Big(\sup_{t'\in V_1} d(f_i(t'), f(t'))\Big) = 0$. Ekkor az $\varepsilon/3$ számhoz vehetünk olyan $j \in I$ indexet, hogy minden $I \ni i$-re, ha $i \geq j$, akkor $\sup_{t'\in V_1} d(f_i(t'), f(t')) \leq \varepsilon/3$. Tehát, ha $i \in I$ és $i \geq j$, akkor minden $V_1 \ni t'$-re $d(f_i(t'), f(t')) \leq \varepsilon/3$. Ezért $i \in I$ és $i \geq j$ esetén $d(f_i(t), f(t)) \leq \varepsilon/3$ is igaz, hiszen $t \in V_1$. A hipotézis alapján az $f_j : T \to M$ függvény folytonos a t pontban, tehát a t-nek van olyan V_2 környezete T-ben, hogy minden $t' \in V_2$ esetén $d(f_j(t'), f_j(t)) < \varepsilon/3$. Tehát $V := V_1 \cap V_2$ olyan környezete t-nek T-ben, hogy minden $V \ni t'$-re

$$d(f(t'), f(t)) \leq d(f(t'), f_j(t')) + d(f_j(t'), f_j(t)) + d(f_j(t), f(t)) < 3 \cdot \frac{\varepsilon}{3} = \varepsilon,$$

vagyis $f\langle V\rangle \subseteq \mathrm{B}_\varepsilon(f(t); d)$. ■

Figyeljük meg, hogy az előző állítás bizonyításában csak azt használtuk fel, hogy $f = \lim_{i,\, I} f_i$, és minden $t \in T$ pontnak létezik olyan V környezete T-ben, amelyre $\inf_{i\in I}\Big(\sup_{t'\in V} d(f_i(t'), f(t'))\Big) = 0$. Ez határozottan gyengébb feltételnek tűnik annál, hogy $(f_i)_{i\in I}$ lokálisan egyenletesen konvergál f-hez a T halmazon.

Jelölés. Ha E halmaz, F normált tér és f olyan függvény, hogy $E \subseteq \mathrm{Dom}(f)$ és $\mathrm{Im}(f) \subseteq F$, akkor

$$|||f|||_E := \sup_{t\in E} \|f(t)\|,$$

ha $E \neq \emptyset$, míg $|||f|||_\emptyset := 0$; továbbá a $|||f|||_{\mathrm{Dom}(f)}$ szimbólum helyett az egyszerűbb $|||f|||$ jelet alkalmazzuk.

Ha T halmaz és F normált tér, akkor a $T \to F$ korlátos függvények $\mathscr{F}^b(T;F)$ halmaza a pontonként értelmezett műveletekkel ellátva vektortér ugyanazon test felett, amely felett F vektortér, és az $\mathscr{F}^b(T;F) \to \mathbb{R}_+;\ f \mapsto |||f|||_T$ *sup-normával* ellátva normált tér, és a $|||\cdot|||_T$ norma éppen a sup-metrikát generálja.

29.2.3. Definíció. *Ha T lokálisan kompakt tér és F normált tér, akkor egy $f : T \to F$ függvényt* **végtelenben eltűnőnek** *nevezünk, ha minden $\varepsilon \in \mathbb{R}_+^*$ esetén van olyan $K \subseteq T$ kompakt halmaz, hogy minden $T \setminus K \ni t$-re $\|f(t)\| < \varepsilon$. Ha T lokálisan kompakt tér és F normált tér, akkor $\mathscr{K}(T;F)$ jelöli a $T \to F$ kompakt tartójú folytonos függvények halmazát, és $\overline{\mathscr{K}}(T;F)$ jelöli a $T \to F$ végtelenben eltűnő folytonos függvények halmazát.*

29.2.4. Állítás. *Ha T lokálisan kompakt tér és F normált tér, akkor $\overline{\mathscr{K}}(T;F)$ egyenlő a $\mathscr{K}(T;F)$ függvényhalmaz sup-norma szerinti lezártjával $\mathscr{F}^b(T;F)$-ben.*

Bizonyítás. Legyen $f \in \overline{\mathscr{K}}(T;F)$. Vegyünk tetszőleges $(\varepsilon_n)_{n\in\mathbb{N}}$ zérussorozatot $\mathbb{R}_+^*$-ban. Az f függvény végtelenben eltűnő, ezért kiválaszthatjuk a T kompakt részhalmazainak olyan $(K_n)_{n\in\mathbb{N}}$ sorozatát, hogy minden $n \in \mathbb{N}$ és $t \in T \setminus K_n$ esetén $\|f(t)\| < \varepsilon_n$. A lokálisan kompakt terekre vonatkozó Uriszon-tételt alkalmazva kiválasztunk olyan $(\varphi_n)_{n\in\mathbb{N}}$ sorozatot, hogy minden $n \in \mathbb{N}$ esetén $\varphi_n : T \to \mathbb{R}$ kompakt tartójú folytonos függvény,

$0 \leq \varphi_n \leq 1$ és $K_n \subseteq [\varphi_n = 1]$. Ekkor a $\mathscr{K}(T;F)$-ben haladó $(\varphi_n f)_{n\in\mathbb{N}}$ függvénysorozat egyenletesen konvergál f-hez a T halmazon. Valóban, ha $\varepsilon \in \mathbb{R}_+^*$ és $N \in \mathbb{N}$ olyan, hogy minden $n > N$ természetes számra $\varepsilon_n < \varepsilon$, akkor minden $n > N$ természetes számra és $T \setminus K_n \ni t$-re $\|f(t) - (\varphi_n f)(t)\| = (1 - \varphi_n(t))\|f(t)\| < \varepsilon_n < \varepsilon$, míg $\varphi_n f = f$ a K_n halmazon.

Legyen $(f_n)_{n\in\mathbb{N}}$ olyan sorozat $\mathscr{K}(T;F)$-ben, amely egyenletesen konvergál az $f : T \to F$ függvényhez a T halmazon. Az előző tétel alapján f folytonos. Legyen $\varepsilon \in \mathbb{R}_+^*$ és vegyünk olyan $n \in \mathbb{N}$ számot, hogy minden $T \ni t$-re $\|f_n(t) - f(t)\| < \varepsilon$. Ha $t \in T \setminus \mathrm{supp}(f_n)$, akkor $f_n(t) = 0$ miatt $\|f(t)\| \leq \|f(t) - f_n(t)\| + \|f_n(t)\| < \varepsilon$, vagyis az ε számhoz a $K := \mathrm{supp}(f_n)$ kompakt halmaz olyan, hogy minden $T \setminus K \ni t$-re $\|f(t)\| < \varepsilon$. Ez azt jelenti, hogy f végtelenben eltűnő. ■

Topologikus tér zárt részhalmazainak általánosított sorozatokkal való jellemzése alapján az előző állítás úgy is megfogalmazható, hogy lokálisan kompakt téren értelmezett, normált térbe ható korlátos függvény pontosan akkor végtelenben eltűnő és folytonos, ha egyenletesen approximálható kompakt tartójú folytonos függvényekkel. Tehát az előbbi állítás szintén az egyenletes approximáció témakörébe tartozik.

29.3. Stone-féle approximációs tétel

29.3.1. Definíció. *Ha T halmaz és H olyan halmaz, amelynek elemei T-n értelmezett függvények, akkor azt mondjuk, hogy H* **szétválasztó T felett***, ha minden $T \ni t, t'$-re, $t \neq t'$ esetén létezik olyan $f \in H$, hogy $f(t) \neq f(t')$.*

Például, a Hahn–Banach-tételből következik, hogy egy normált tér felett a folytonos lineáris funkcionálok halmaza szétválasztó. A definíció szerint nyilvánvaló, hogy ha T teljesen reguláris T_1-tér, akkor a $\mathscr{C}(T;[0,1])$ függvényhalmaz szétválasztó T felett.

A következő állításban megfogalmazzuk a pontonkénti approximáció problémája megoldhatóságának természetes *szükséges* feltételét, abban a speciális esetben, amikor lokálisan kompakt téren értelmezett, $\mathbb{K}$-ba érkező függvények approximációjáról van szó.

29.3.2. Állítás. *Ha T lokálisan kompakt tér és $H \subseteq \mathscr{F}(T;\mathbb{K})$ olyan részhalmaz, hogy minden $f : T \to [0,1]$ kompakt tartójú folytonos függvényhez van olyan H-ban haladó $(f_i)_{i\in I}$ általánosított sorozat, hogy $f = \lim\limits_{i,\ I} f_i$, akkor H szétválasztó T felett.*

Bizonyítás. Ha $t, t' \in T$ és $t \neq t'$, akkor a lokálisan kompakt terekre vonatkozó Uriszon-tétel szerint a $\{t\}$ kompakt halmazhoz és a $T \setminus \{t'\}$ nyílt halmazhoz van olyan $f : T \to [0,1]$ kompakt tartójú folytonos függvény, amelyre $\{t\} \subseteq [f = 1]$ (azaz $f(t) = 1$) és $\mathrm{supp}(f) \subseteq T \setminus \{t'\}$, tehát $f(t') = 0$. A hipotézis szerint van olyan H-ban haladó $(f_i)_{i\in I}$ általánosított sorozat, hogy $f := \lim\limits_{i,\ I} f_i$. Ekkor $1 = f(t) := \lim\limits_{i,\ I} f_i(t)$, így van olyan $i_1 \in I$, hogy minden $I \ni i$-re, ha $i \geq i_1$, akkor $f_i > 1/2$. Ugyanakkor $0 = f(t') := \lim\limits_{i,\ I} f_i(t')$, így van olyan $i_2 \in I$, hogy minden $I \ni i$-re, ha $i \geq i_2$, akkor $f_i < 1/2$. Az I előrendezett halmaz felfelé irányított, ezért van olyan $i \in I$, hogy $i \geq i_1, i_2$; ekkor $f_i(t) > 1/2 > f_i(t')$ és $f_i \in H$. ■

29.3.3. Definíció. *Ha T halmaz, akkor egy $H \subseteq \mathscr{F}(T;\mathbb{R})$ függvényhalmazt T feletti* **lineáris függvényhálónak** *nevezünk, ha H lineáris altere a $\mathscr{F}(T;\mathbb{R})$ függvénytérnek, és minden $h \in H$ esetén a $|h| : T \to \mathbb{R};\ t \mapsto |h(t)|$ függvény eleme H-nak.*

29.3.4. Állítás. *Ha T halmaz és $H \subseteq \mathscr{F}(T;\mathbb{R})$ lineáris altér, akkor a következő állítások ekvivalensek.*

(i) *H lineáris függvényháló T felett.*

(ii) *Minden $f, f' \in H$ esetén az $\inf(f, f') : T \to \mathbb{R};\ t \mapsto \min(f(t), f'(t))$ függvény eleme H-nak.*

(iii) *Minden $f, f' \in H$ esetén a $\sup(f, f') : T \to \mathbb{R};\ t \mapsto \max(f(t), f'(t))$ függvény eleme H-nak.*

(iv) *Minden $f \in H$ esetén az $f^+ : T \to \mathbb{R};\ t \mapsto \max(f(t), 0)$ függvény eleme H-nak.*

(v) *Minden $f \in H$ esetén az $f^- : T \to \mathbb{R};\ t \mapsto \max(-f(t), 0)$ függvény eleme H-nak.*

Bizonyítás. Ha $f, f' : T \to \mathbb{R}$ függvények, akkor

$$\inf(f, f') = \frac{1}{2}(f + f' - |f - f'|), \quad \sup(f, f') = \frac{1}{2}(f + f' + |f - f'|),$$

$$\sup(f, f') = -\inf(-f, -f'), \quad f^+ = \sup(f, 0), \quad f^- = f^+ - f, \quad |f| = f + 2f^-.$$

Ezekből azonnal következik az állítás. ■

Ha H lineáris függvényháló a T halmaz felett és $(f_i)_{i \in I}$ tetszőleges nem üres véges rendszer H-ban, akkor a

$$\sup_{i \in I} f_i : T \to \mathbb{R}; \quad t \mapsto \max_{i \in I} f_i(t),$$

$$\inf_{i \in I} f_i : T \to \mathbb{R}; \quad t \mapsto \min_{i \in I} f_i(t)$$

függvények elemei H-nak. Ez az előző állításból az I indexhalmaz számossága szerinti teljes indukcióval következik.

Jelölés. Ha T halmaz, akkor a $T \to \mathbb{R}$ azonosan 1 függvényt 1_T jelöli.

29.3.5. Tétel. (Stone-tétel) *Legyen T kompakt Hausdorff-tér és H olyan lineáris függvényháló T felett, hogy $1_T \in H \subseteq \mathscr{C}(T;\mathbb{R})$. A H halmaz pontosan akkor sűrű $\mathscr{C}(T;\mathbb{R})$-ben a sup-norma szerint, ha H szétválasztó T felett.*

Bizonyítás. Ha $T = \emptyset$, akkor az állítás triviálisan igaz (és érdektelen), ezért feltehető, hogy $T \neq \emptyset$. Csak az elégségesség szorul bizonyításra, tehát feltesszük, hogy H szétválasztó T felett.

Először megjegyezzük, hogy minden $t, t' \in T$ és $\alpha, \alpha' \in \mathbb{R}$ esetén, ha $t \neq t'$, akkor létezik olyan $f \in H$, hogy $f(t) = \alpha$ és $f(t') = \alpha'$. Valóban, a H halmaz szétválasztó T felett, tehát van olyan $h \in H$, hogy $h(t) \neq h(t')$; ekkor az $f := \left(\frac{\alpha h(t') - \alpha' h(t)}{h(t') - h(t)}\right).1_T + \left(\frac{\alpha' - \alpha}{h(t') - h(t)}\right).h \in H$ függvényre $f(t) = \alpha$ és $f(t') = \alpha'$.

Legyen $f \in \mathscr{C}(T;\mathbb{R})$ rögzített függvény és $\varepsilon \in \mathbb{R}_+^*$. Megmutatjuk, hogy létezik olyan $h \in H$, amelyre $\|\|f - h\|\| \leq \varepsilon$.

Ha $t, t' \in T$ és $t \neq t'$, akkor létezik olyan $h \in H$, hogy $h(t) = f(t)$ és $h(t') = f(t')$. Ha $t, t' \in T$ és $t = t'$, akkor $h := f(t).1_T \in H$ olyan, hogy $h(t) = f(t)$ és $h(t') = f(t')$. Ezért kiválaszthatunk olyan $(h_{(t,t')})_{(t,t') \in T \times T}$ rendszert, hogy minden $(t, t') \in T \times T$ esetén $h_{(t,t')}(t) = f(t)$ és $h_{(t,t')}(t') = f(t')$.

Legyen $t' \in T$ rögzített pont. Ha $t \in T$, akkor $h_{(t,t')}(t) = f(t) < f(t) + \varepsilon$, vagyis $t \in [h_{(t,t')} - f < \varepsilon]$, és a $h_{(t,t')} - f : T \to \mathbb{R}$ függvény folytonos, tehát a $[h_{(t,t')} - f < \varepsilon]$ halmaz nyílt környezete t-nek. A T kompaktsága miatt létezik olyan $(t_i)_{i\in I}$ véges rendszer T-ben, amelyre $T = \bigcup_{i\in I}[h_{(t_i,t')} - f < \varepsilon]$. Világos, hogy $I \neq \emptyset$, mert $T \neq \emptyset$. Legyen $h := \inf_{i\in I} h_{(t_i,t')}$; ekkor $h \in H$ és $t \in I$ esetén van olyan $i \in I$, hogy $h_{(t_i,t')}(t) < f(t) + \varepsilon$, tehát $h(t) < f(t) + \varepsilon$. Ugyanakkor $h(t') := \min_{i\in I} h_{(t_i,t')}(t') = f(t')$.

Ezzel megmutattuk, hogy minden $t' \in T$ esetén van olyan $h \in H$, hogy minden $T \ni t$-re $h(t) < f(t) + \varepsilon$ és $h(t') = f(t')$. Kiválaszthatunk tehát olyan $(h_{t'})_{t'\in T}$ rendszert, hogy minden $T \ni t'$-re $h_{t'} \in H$, $h_{t'}(t') = f(t')$ és minden $T \ni t$-re $h_{t'}(t) < f(t) + \varepsilon$.

Ha $t' \in T$, akkor $h_{t'}(t') = f(t') > f(t') - \varepsilon$, vagyis $t' \in [h_{t'} - f > -\varepsilon]$, és a $h_{t'} - f : T \to \mathbb{R}$ függvény folytonos, így $[h_{t'} - f > -\varepsilon]$ nyílt környezete t'-nek. A T kompaktsága miatt létezik olyan $(t'_j)_{j\in J}$ véges rendszer T-ben, hogy $T = \bigcup_{j\in J}[h_{t'_j} - f > -\varepsilon]$. Világos, hogy $J \neq \emptyset$, mert $T \neq \emptyset$. Értelmezzük a $h := \sup_{j\in J} h_{t'_j}$ függvényt. Ekkor $h \in H$, és $t \in T$ esetén van olyan $j \in J$, hogy $h_{t'_j}(t) > f(t) - \varepsilon$, tehát $h(t) > f(t) - \varepsilon$. Ugyanakkor minden $T \ni t$-re és $J \ni j$-re $h_{t'_j}(t) < f(t) + \varepsilon$, tehát $h(t) < f(t) + \varepsilon$. Ez azt jelenti, hogy minden $T \ni t$-re $f(t) - \varepsilon < h(t) < f(t) + \varepsilon$, következésképpen $|||h - f||| \leq \varepsilon$. ■

29.4. Stone–Weierstrass approximációs tétel

Ha T halmaz, akkor az $\mathscr{F}(T;\mathbb{K})$ függvényhalmaz a pontonként értelmezett összeadással, számmal vett szorzással és a szorzással ellátva *algebra* a $\mathbb{K}$ test felett; ennek részalgebráit nevezzük T feletti *függvényalgebráknak.* Tehát egy $A \subseteq \mathscr{F}(T;\mathbb{K})$ halmaz pontosan akkor függvényalgebra T felett, ha minden $f, g \in A$ és $\lambda \in \mathbb{K}$ esetén $f + g, fg, \lambda f \in A$ és $A \neq \emptyset$.

Megjegyezzük, hogy ha T halmaz és A lineáris altere $\mathscr{F}(T;\mathbb{K})$-nak, akkor A pontosan akkor függvényalgebra T felett, ha minden $f \in A$ esetén $f^2 \in A$. Ez abból következik, hogy minden $f, g : T \to \mathbb{K}$ függvényre $fg = \dfrac{1}{4}((f+g)^2 - (f-g)^2)$.

29.4.1. Lemma. *Minden $K \subseteq \mathbb{R}$ kompakt halmazhoz létezik $\mathbb{R} \to \mathbb{R}$ polinomiális függvényeknek olyan $(p_n)_{n\in\mathbb{N}}$ sorozata, amely egyenletesen konvergál az euklidészi abszolútérték-függvényhez a K halmazon, és minden $\mathbb{N} \ni n$-re $p_n(0) = 0$.*

Bizonyítás. (I) Először megmutatjuk, hogy elegendő olyan $(p_n)_{n\in\mathbb{N}}$ sorozat létezését igazolni, amelynek mindegyik tagja $\mathbb{R} \to \mathbb{R}$ polinomiális függvény, és egyenletesen konvergál az euklidészi abszolútérték-függvényhez a $[-1, 1]$ intervallumon, és minden $\mathbb{N} \ni n$-re $p_n(0) = 0$. Valóban, legyen $(p_n)_{n\in\mathbb{N}}$ ilyen sorozat és $K \subseteq \mathbb{R}$ tetszőleges kompakt halmaz. Ekkor van olyan $c \in \mathbb{R}_+^*$, hogy $K \subseteq [-c, c]$, és ha minden $n \in \mathbb{N}$ esetén bevezetjük a

$$\widetilde{p}_n : \mathbb{R} \to \mathbb{R}; \quad t \mapsto c \cdot p_n(t/c)$$

függvényt, akkor $(\widetilde{p}_n)_{n\in\mathbb{N}}$ olyan sorozat, amelynek minden tagja $\mathbb{R} \to \mathbb{R}$ polinomiális függvény, minden $\mathbb{N} \ni n$-re $\widetilde{p}_n(0) = 0$, valamint

$$\sup_{t\in K} |\widetilde{p}_n(t) - |t|| \leq \sup_{t\in[-c,c]} |c \cdot p_n(t/c) - |t|| = c \cdot \sup_{t\in[-c,c]} |p_n(t/c) - |t/c|| =$$

$$= c \cdot \sup_{t \in [-1,1]} \left| p_n(t) - |t| \right|,$$

és a jobb oldal tart 0-hoz, ha n tart végtelenhez, ezért $(\widetilde{p}_n)_{n\in\mathbb{N}}$ egyenletesen konvergál az euklidészi abszolútérték-függvényhez a K halmazon.

(II) Megmutatjuk, hogy ha létezik $\mathbb{R} \to \mathbb{R}$ polinomiális függvényeknek olyan $(q_n)_{n\in\mathbb{N}}$ sorozata, amely egyenletesen konvergál a $\sqrt{\cdot}$ függvényhez a $[0,1]$ intervallumon és minden $\mathbb{N} \ni n$-re $q_n(0) = 0$, akkor létezik $\mathbb{R} \to \mathbb{R}$ polinomiális függvényeknek olyan $(p_n)_{n\in\mathbb{N}}$ sorozata, amely egyenletesen konvergál az euklidészi abszolútérték-függvényhez a $[-1,1]$ intervallumon, és minden $\mathbb{N} \ni n$-re $p_n(0) = 0$. Valóban, a $\left(q_n \circ \mathrm{id}_{\mathbb{R}}^2\right)_{n\in\mathbb{N}}$ függvénysorozat mindegyik tagja $\mathbb{R} \to \mathbb{R}$ polinomiális függvény, és minden $n \in \mathbb{N}$ esetén $\left(q_n \circ \mathrm{id}_{\mathbb{R}}^2\right)(0) = 0$, valamint minden $n \in \mathbb{N}$ és $t \in [-1,1]$ esetén $\left| q_n(t^2) - \sqrt{t^2} \right| = \left| q_n(t^2) - |t| \right|$, amiből következik, hogy

$$\lim_{n\to\infty} \left(\sup_{t\in[-1,1]} \left| q_n(t^2) - |t| \right| \right) = 0,$$

vagyis $\left(q_n \circ \mathrm{id}_{\mathbb{R}}^2\right)_{n\in\mathbb{N}}$ egyenletesen konvergál $|\cdot|_{\mathbb{R}}$-hez a $[-1,1]$ intervallumon.

Ezért (I) alapján elegendő ilyen tulajdonságú $(q_n)_{n\in\mathbb{N}}$ függvénysorozatot találni.

(III) Legyen $\mathfrak{P}$ az $\mathbb{R} \to \mathbb{R}$ polinomiális függvények halmaza, és értelmezzük a

$$g : \mathfrak{P} \to \mathfrak{P}; \quad q \mapsto q + \frac{1}{2}\left(\mathrm{id}_{\mathbb{R}} - q^2\right)$$

leképezést. Jelölje $(q_n)_{n\in\mathbb{N}}$ a g függvény és az $\mathbb{R} \to \mathbb{R}$ azonosan 0 függvény, mint kezdőpont által generált iterációs sorozatot. Tehát $(q_n)_{n\in\mathbb{N}}$ az a sorozat, amelyre q_0 az $\mathbb{R} \to \mathbb{R}$ azonosan 0 függvény, és minden $\mathbb{N} \ni n$-re $q_n : \mathbb{R} \to \mathbb{R}$ polinomiális függvény és

$$q_{n+1} = q_n + \frac{1}{2}\left(\mathrm{id}_{\mathbb{R}} - q_n^2\right).$$

Megmutatjuk, hogy a $(q_n)_{n\in\mathbb{N}}$ függvénysorozatra teljesülnek a (II)-ben megfogalmazott tulajdonságok, vagyis minden $\mathbb{N} \ni n$-re $q_n(0) = 0$ és $(q_n)_{n\in\mathbb{N}}$ egyenletesen konvergál az $\sqrt{\cdot}$ függvényhez a $[0,1]$ intervallumon, vagyis

$$\lim_{n\to\infty} \left(\sup_{t\in[0,1]} \left| q_n(t) - \sqrt{t} \right| \right) = 0.$$

A definíció szerint $q_0(0) = 0$, és ha az $n \in \mathbb{N}$ számra $q_n(0) = 0$ teljesül, akkor $q_{n+1}(0) = q_n(0) + \dfrac{1}{2}(-q_n(0)^2) = 0$, ezért a teljes indukció elve alapján minden $\mathbb{N} \ni n$-re $q_n(0) = 0$.

Teljes indukcióval igazoljuk, hogy minden $n \in \mathbb{N}$ esetén minden $[0,1] \ni t$-re $0 \le q_n(t) \le \sqrt{t}$. Ez triviálisan teljesül, ha $n = 0$, mert minden $\mathbb{R} \ni t$-re $q_0(t) = 0$. Tegyük fel, hogy $n \in \mathbb{N}$ olyan, hogy minden $[0,1] \ni t$-re $0 \le q_n(t) \le \sqrt{t}$. Ekkor

$$\sqrt{t} - q_{n+1}(t) = \sqrt{t} - q_n(t) - \frac{1}{2}\left(t - q_n(t)^2\right) =$$

$$= \sqrt{t} - q_n(t) - \frac{1}{2}(\sqrt{t} - q_n(t))(\sqrt{t} + q_n(t)) = (\sqrt{t} - q_n(t))\left(1 - \frac{1}{2}(\sqrt{t} + q_n(t))\right),$$

és az indukciós hipotézis szerint $\sqrt{t} - q_n(t) \ge 0$, valamint $\dfrac{1}{2}(\sqrt{t} + q_n(t)) \le \dfrac{1}{2}(\sqrt{t} + \sqrt{t}) = \sqrt{t} \le 1$, ezért $\sqrt{t} - q_{n+1}(t) \ge 0$ teljesül, továbbá $0 \le q_n(t) \le \sqrt{t}$ alapján

$q_{n+1}(t) = q_n(t) + \dfrac{1}{2}(t - q_n(t)^2) \geq q_n(t) \geq 0$. Ebből az is látható, hogy a $(q_n(t))_{n\in\mathbb{N}}$ számsorozat monoton növő.

Ugyancsak teljes indukcióval igazoljuk, hogy $t \in [0,1]$ esetén minden $\mathbb{N} \ni n$-re

$$\sqrt{t} - q_n(t) \leq \frac{2\sqrt{t}}{2 + n\sqrt{t}}.$$

Ha $n = 0$, akkor itt triviális egyenlőség van, mert $q_0(t) = 0$. Tegyük fel, hogy $n \in \mathbb{N}$ olyan, amelyre teljesül ez az egyenlőtlenség. Ekkor az indukciós hipotézis és $q_n(t) \geq 0$ miatt

$$\sqrt{t} - q_{n+1}(t) = (\sqrt{t} - q_n(t))\left(1 - \frac{1}{2}(\sqrt{t} + q_n(t))\right) \leq$$

$$\leq \frac{2\sqrt{t}}{2 + n\sqrt{t}}\left(1 - \frac{1}{2}(\sqrt{t} + q_n(t))\right) \leq \frac{2\sqrt{t}}{2 + n\sqrt{t}}\left(1 - \frac{1}{2}\sqrt{t}\right) \leq \frac{2\sqrt{t}}{2 + (n+1)\sqrt{t}},$$

mert átrendezéssel triviálisan adódik, hogy

$$\frac{1 - \frac{1}{2}\sqrt{t}}{2 + n\sqrt{t}} \leq \frac{1}{2 + (n+1)\sqrt{t}}.$$

Nyilvánvaló, hogy $n \in \mathbb{N}^*$ és $t \in [0,1]$ esetén $\dfrac{2\sqrt{t}}{2 + n\sqrt{t}} \leq \dfrac{2}{n}$, ezért $0 \leq \sqrt{t} - q_n(t) \leq \dfrac{2}{n}$, amiből következik, hogy minden $n \in \mathbb{N}^*$ számra

$$\sup_{t\in[0,1]} \left|\sqrt{t} - q_n(t)\right| \leq \frac{2}{n}$$

teljesül, így $\lim\limits_{n\to\infty}\left(\sup\limits_{t\in[0,1]}\left|\sqrt{t} - q_n(t)\right|\right) = 0$. ■

Jelölés. Ha T halmaz és $f : T \to \mathbb{K}$ függvény, akkor $\overline{f}$ jelöli a $T \to \mathbb{K}$; $t \mapsto \overline{f(t)}$ függvényt, és az $\overline{f}$ függvényt az f **konjugáltjának** nevezzük.

29.4.2. Tétel. (Stone–Weierstrass-tétel) *Legyen T kompakt Hausdorff-tér és A olyan függvényalgebra T felett, amelyre $1_T \in A \subseteq \mathscr{C}(T;\mathbb{K})$ és minden $f \in A$ esetén $\overline{f} \in A$. Az A halmaz pontosan akkor sűrű $\mathscr{C}(T;\mathbb{K})$-ban a sup-norma szerint, ha A szétválasztó T felett.*

(**Megjegyzés**. Természetesen $\mathbb{K} = \mathbb{R}$ esetén minden $A \ni f$-re $\overline{f} = f \in A$ automatikusan teljesül, azonban $\mathbb{K} = \mathbb{C}$ esetén a konjugáltakra vonatkozó feltétel nem triviális és szükséges.)

Bizonyítás. Csak az elégségességet kell igazolunk, tehát feltesszük, hogy A szétválasztó T felett.

(I) Először a $\mathbb{K} = \mathbb{R}$ esetre bizonyítunk. Jelölje $\overline{A}$ az A halmaz sup-norma szerinti lezártját $\mathscr{C}(T;\mathbb{R})$-ben. Ekkor $\overline{A}$ lineáris altere $\mathscr{C}(T;\mathbb{R})$-nek, mert normált tér lineáris alterének lezártja lineáris altér. Továbbá, $1_T \in A \subseteq \overline{A}$ teljesül. Az A szétválasztó T felett, ezért $A \subseteq \overline{A}$ miatt $\overline{A}$ még inkább szétválasztó T felett. Ezért a Stone-tétel alapján elég azt igazolni, hogy $\overline{A}$ lineáris függvényháló T felett, vagyis minden $f \in \overline{A}$ esetén $|f| \in \overline{A}$. Valóban, ha így volna, akkor a Stone-tétel alapján $\overline{A}$ sűrű volna $\mathscr{C}(T;\mathbb{R})$-ben a sup-norma szerint, ugyanakkor zárt is, tehát $\overline{A} = \mathscr{C}(T;\mathbb{R})$ teljesülne.

Megmutatjuk, hogy ha minden $f \in A$ esetén $|f| \in \overline{A}$ teljesül, akkor $\overline{A}$ lineáris függvényháló T felett. Valóban, legyen $f \in \overline{A}$, és $(f_n)_{n\in\mathbb{N}}$ olyan A-ban haladó sorozat, amelyre $\lim\limits_{n\to\infty} |||f_n - f||| = 0$. A feltevés szerint minden $\mathbb{N} \ni n$-re $|f_n| \in \overline{A}$, továbbá $|||\,|f_n| - |f|\,||| \leq |||f_n - f|||$, ezért az $\overline{A}$-ben haladó $(|f_n|)_{n\in\mathbb{N}}$ sorozat a sup-normában konvergál $|f|$-hez. Ebből következik, hogy $|f| \in \overline{A}$, hiszen $\overline{A}$ zárt $\mathscr{C}(T;\mathbb{R})$-ben a sup-norma szerint.

Tehát elég azt igazolni, hogy $f \in A$ esetén $|f| \in \overline{A}$, vagyis $|f|$ egyenletesen approximálható a T halmazon A-beli függvényekkel. Legyen $f \in A$ rögzített. Az $\mathrm{Im}(f)$ halmaz kompakt $\mathbb{R}$-ben, ezért az előző lemma szerint létezik $\mathbb{R} \to \mathbb{R}$ polinomiális függvényeknek olyan $(p_n)_{n\in\mathbb{N}}$ sorozata, amely egyenletesen konvergál az $|\cdot|_{\mathbb{R}}$ függvényhez az $\mathrm{Im}(f)$ halmazon. Minden $n \in \mathbb{N}$ esetén

$$|||p_n \circ f - |f|\,||| = \sup_{t\in T} |p_n(f(t)) - |f(t)|| = \sup_{\lambda\in\mathrm{Im}(f)} |p_n(\lambda) - |\lambda|| = |||p_n - |\cdot|_{\mathbb{R}}|||,$$

tehát a $(p_n \circ f)_{n\in\mathbb{N}}$ függvénysorozat a sup-norma szerint konvergál az $|f|$ függvényhez. Ugyanakkor minden $p : \mathbb{R} \to \mathbb{R}$ polinomiális függvényhez van olyan $n \in \mathbb{N}$ és $(c_k)_{k\in n} \in \mathbb{R}^n$, hogy $p = \sum\limits_{k\in n} c_k \mathrm{id}_{\mathbb{R}}^k$, következésképpen $p \circ f = \sum\limits_{k\in n} c_k f^k \in A$, mert A valós függvényalgebra T felett és $1_T \in A$. Ezért minden $\mathbb{N} \ni n$-re $p_n \circ f \in A$, így $|f| \in \overline{A}$.

(II) Most feltesszük, hogy $\mathbb{K} = \mathbb{C}$. Legyen $A_{\mathbb{R}} := \{f \in A | \mathrm{Im}(f) \subseteq \mathbb{R}\}$. Nyilvánvaló, hogy $A_{\mathbb{R}}$ valós függvényalgebra T felett, és $A_{\mathbb{R}} \subseteq \mathscr{C}(T;\mathbb{R})$, valamint $1_T \in A_{\mathbb{R}}$. Továbbá, minden $f \in A$ esetén $\Re\circ f = \dfrac{1}{2}(f+\overline{f}) \in A$ és $\Im\circ f = \dfrac{1}{2i}(f-\overline{f}) \in A$, ezért $\Re\circ f, \Im\circ f \in A_{\mathbb{R}}$. Ez azt jelenti, hogy minden $A \ni f$-hez léteznek olyan $f_1, f_2 \in A_{\mathbb{R}}$, amelyekre $f = f_1 + i f_2$. Ebből triviálisan következik, hogy ha A szétválasztó T felett, akkor $A_{\mathbb{R}}$ is szétválasztó T felett. A valós függvényalgebrákra vonatkozó Stone–Weierstrass-tételt (vagyis az (I) állítást) alkalmazva $A_{\mathbb{R}}$-re kapjuk, hogy ha A szétválasztó T felett, akkor $A_{\mathbb{R}}$ a sup-norma szerint sűrű $\mathscr{C}(T;\mathbb{R})$-ben. Ekkor $f \in \mathscr{C}(T;\mathbb{C})$ esetén minden $\mathbb{R}_+^* \ni \varepsilon$-hoz léteznek olyan $g_1, g_2 \in A_{\mathbb{R}}$, hogy $|||\Re \circ f - g_1||| < \varepsilon/2$ és $|||\Im \circ f - g_2||| < \varepsilon/2$, így a $g := g_1 + i g_2 \in A$ függvényre

$$|||f - g||| \leq |||\Re \circ f - g_1\,||| + |||\,\Im \circ f - g_2||| < \varepsilon.$$

Ez azt jelenti, hogy A sűrű $\mathscr{C}(T;\mathbb{C})$-ben a sup-norma szerint. ■

29.4.3. Tétel. (Stone–Weierstrass-tétel lokálisan kompakt terekre) *Legyen T lokálisan kompakt tér és A olyan függvényalgebra T felett, amelyre $A \subseteq \overline{\mathscr{K}}(T;\mathbb{K})$ és minden $f \in A$ esetén $\overline{f} \in A$. Az A halmaz pontosan akkor sűrű $\overline{\mathscr{K}}(T;\mathbb{K})$-ban a sup-norma szerint, ha A szétválasztó T felett és minden $T \ni t$-hez van olyan $f \in A$, hogy $f(t) \neq 0$.*

Bizonyítás. Csak az elégségességet kell igazolnunk, tehát feltesszük, hogy A szétválasztó T felett, és minden $T \ni t$-hez van olyan $f \in A$, hogy $f(t) \neq 0$. Legyen T' egypontú kompaktifikációja T-nek, és jelölje ω a végtelen távoli pontot T'-ben. Legyen

$$\widetilde{A} := \{\, c.1_{T'} + f^\circ \mid (c \in \mathbb{K}) \wedge (f \in A)\,\},$$

ahol $f \in A$ esetén f° jelöli az f függvény 0-val vett kiterjesztését T-ről T'-re, tehát $f^\circ(\omega) := 0$ és minden $T \ni t$-re $f^\circ(t) = f(t)$. Nyilvánvaló, hogy $\widetilde{A}$ olyan függvényalgebra T' felett, amelyre $1_{T'} \in \widetilde{A} \subseteq \mathscr{C}(T';\mathbb{K})$, valamint minden $\widetilde{A} \ni f$-re $\overline{f} \in \widetilde{A}$. Az A

halmaz szétválasztó T felett, és minden $T \ni t$-hez van olyan $f \in A$, hogy $f(t) \neq 0$, ezért $\widetilde{A}$ szétválasztó T' felett. Valóban, $\widetilde{A}$ nyilvánvalóan szétválasztja a T pontjait, és ha $t \in T$, valamint $f \in A$ olyan, hogy $f(t) \neq 0$, akkor $f^\circ \in \widetilde{A}$ és $f^\circ(t) = f(t) \neq 0 = f^\circ(\omega)$. A Stone–Weierstrass-tételt alkalmazzuk a T' kompakt Hausdorff-térre és az $\widetilde{A}$ függvényalgebrára; tehát $\widetilde{A}$ sűrű $\mathscr{C}(T';\mathbb{K})$-ban a sup-norma szerint.

Legyen $f \in \overline{\mathscr{K}}(T;\mathbb{K})$ rögzített függvény. Ekkor $f^\circ \in \mathscr{C}(T';\mathbb{K})$, tehát van olyan $(c_n)_{n\in\mathbb{N}}$ sorozat $\mathbb{K}$-ban és olyan $(f_n)_{n\in\mathbb{N}}$ sorozat A-ban, hogy $\lim\limits_{n\to\infty} |||c_n.1_{T'} + f_n^\circ - f^\circ||| = 0$. Ekkor a $(c_n.1_{T'} + f_n^\circ)_{n\in\mathbb{N}}$ függvénysorozat pontonként is konvergens a T' halmazon, ezért $0 = f^\circ(\omega) = \lim\limits_{n\to\infty}(c_n + f_n^\circ(\omega)) = \lim\limits_{n\to\infty} c_n$. Ebből következik, hogy $\lim\limits_{n\to\infty} |||f_n^\circ - f^\circ||| = 0$. Ha $n \in \mathbb{N}$, akkor nyilvánvalóan $|||f_n - f||| = |||f_n^\circ - f^\circ|||$, ezért f eleme az A halmaz sup-norma szerinti lezártjának. ■

Emlékeztetünk arra, hogy ha T halmaz és $(f_i)_{i\in I}$ olyan rendszer, hogy minden $I \ni i$-re $f_i : T \to \overline{\mathbb{R}}$ függvény, akkor a

$$\sup_{i\in I} f_i : T \to \overline{\mathbb{R}}; \quad t \mapsto \sup_{i\in I} f_i(t),$$

$$\inf_{i\in I} f_i : T \to \overline{\mathbb{R}}; \quad t \mapsto \inf_{i\in I} f_i(t)$$

függvényeket az $(f_i)_{i\in I}$ függvényrendszer *felső*, illetve *alsó burkolójának* nevezzük. Itt a jobb oldalon álló szuprémumot és infimumot az $\overline{\mathbb{R}}$ rendezett halmazban kell venni.

29.4.4. Tétel. (Dini-tétel) *Legyen T lokálisan kompakt tér és $(f_i)_{i\in I}$ olyan $\mathscr{K}(T;\mathbb{R})$-ben haladó általánosított sorozat, amely monoton növő (tehát minden $I \ni i, j$-re, ha $i \leq j$, akkor $f_i \leq f_j$). Ha $f := \sup\limits_{i\in I} f_i \in \mathscr{K}(T;\mathbb{R})$, akkor $f = \lim\limits_{i,\ I} f_i$ és az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletesen konvergens a T halmazon, vagyis minden $\mathbb{R}_+^* \ni \varepsilon$-hoz létezik olyan $i_\varepsilon \in I$, hogy minden $i \in I$, $i \geq i_\varepsilon$ és $t \in T$ esetén $|f_i(t) - f(t)| < \varepsilon$.*

Bizonyítás. Ha $t \in T$, akkor az $\mathbb{R}$-ben haladó $(f_i(t))_{i\in I}$ általánosított sorozat monoton növő, és a hipotézis szerint $\sup\limits_{i\in I} f_i(t) = f(t) < +\infty$, ezért $(f_i(t))_{i\in I}$ konvergens $\mathbb{R}$-ben és $f(t) = \lim\limits_{i,\ I} f_i(t)$. Tehát csak azt kell igazolni, hogy az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletesen konvergens a T halmazon.

Először arra a speciális esetre bizonyítunk, amikor minden $I \ni i$-re $f_i \geq 0$. A hipotézis szerint f kompakt tartójú és minden $I \ni i$-re $0 \leq f_i \leq f$, ezért $\mathrm{supp}(f_i) \subseteq \mathrm{supp}(f)$. Legyen $\varepsilon \in \mathbb{R}_+^*$ tetszőleges. Minden $i \in I$ esetén az f (előírt) folytonossága miatt az $\Omega_i(\varepsilon) := [f - f_i < \varepsilon]$ halmaz nyílt T-ben, és világos, hogy $\mathrm{supp}(f) \subseteq \bigcup\limits_{i\in I} \Omega_i(\varepsilon)$. Ebből a $\mathrm{supp}(f)$ kompaktsága miatt következik olyan $J \subseteq I$ véges halmaz létezése, amelyre $\mathrm{supp}(f) \subseteq \bigcup\limits_{i\in J} \Omega_i(\varepsilon)$. Ugyanakkor az $(\Omega_i(\varepsilon))_{i\in I}$ általánosított halmazsorozat a tartalmazás tekintetében monoton növő, mert az $(f_i)_{i\in I}$ általánosított függvénysorozat monoton növő. Továbbá, az I előrendezett halmaz felfelé irányított, nem üres, és J véges, ezért van olyan $i_\varepsilon \in I$, hogy minden $i \in J$ esetén $i \leq i_\varepsilon$; ekkor $\bigcup\limits_{i\in J} \Omega_i(\varepsilon) \subseteq \Omega_{i_\varepsilon}(\varepsilon)$. Tehát $i \in I$ és $i \geq i_\varepsilon$ esetén $\mathrm{supp}(f) \subseteq \Omega_{i_\varepsilon}(\varepsilon) \subseteq \Omega_i(\varepsilon)$, ezért $T = \Omega_i(\varepsilon)$, hiszen f és f_i a $T \setminus \mathrm{supp}(f)$ halmazon a 0-val egyenlők. Tehát, ha $i \in I$ és $i \geq i_\varepsilon$, akkor minden $T \ni t$-re $f_i(t) - \varepsilon < f_i(t) \leq f(t) < f_i(t) + \varepsilon$, vagyis $|f_i(t) - f(t)| < \varepsilon$. Ez azt jelenti, hogy az $(f_i)_{i\in I}$ általánosított függvénysorozat egyenletesen konvergens a T halmazon.

Most elvetjük azt a hipotézist, hogy minden $I \ni i$-re $f_i \geq 0$. Legyen $\alpha \in I$ rögzített és $I_\alpha := \{i \in I | i \geq \alpha\}$. Az I_α halmaz az I felett előrendezés megszorításával ellátva szintén felfelé irányított előrendezett halmaz, továbbá az $(f_i - f_\alpha)_{i \in I_\alpha}$ általánosított függvénysorozat $\mathscr{K}(T;\mathbb{R})$-ben halad, monoton növő, és $\sup\limits_{i \in I_\alpha}(f_i - f_\alpha) = \left(\sup\limits_{i \in I_\alpha} f_i\right) - f_\alpha \in \mathscr{K}(T;\mathbb{R})$, mert nyilvánvalóan $\sup\limits_{i \in I_\alpha} f_i = \sup\limits_{i \in I} f_i$. Ugyanakkor minden $I_\alpha \ni i$-re $f_i - f_\alpha \geq 0$, ezért az előzőek alapján az $(f_i - f_\alpha)_{i \in I_\alpha}$ általánosított függvénysorozat egyenletesen konvergens a T halmazon. Ebből azonnal következik, hogy az $(f_i)_{i \in I}$ általánosított függvénysorozat is egyenletesen konvergens a T halmazon. ■

A Dini-tétel gyakran alkalmazott speciális esete a következő: ha T lokálisan kompakt tér és $(f_n)_{n \in \mathbb{N}}$ olyan $\mathscr{K}(T;\mathbb{R})$-ben haladó sorozat, amely monoton növő és $f := \sup\limits_{n \in \mathbb{N}} f_n \in \mathscr{K}(T;\mathbb{R})$, akkor f egyenlő az $(f_n)_{n \in \mathbb{N}}$ függvénysorozat pontonkénti limeszfüggvényével, és az $(f_n)_{n \in \mathbb{N}}$ függvénysorozat egyenletesen konvergens a T halmazon.

29.5. Kompakt terek metrizálhatóságának jellemzése folytonos függvényekkel

29.5.1. Tétel. (Kompakt terek metrizálhatósága) *Ha T kompakt Hausdorff-tér, akkor a következő állítások ekvivalensek.*

(i) *T metrizálható.*

(ii) *Minden M szeparábilis metrikus térre a $\mathscr{C}(T;M)$ függvénytér a sup-metrikával ellátva szeparábilis.*

(iii) *A $\mathscr{C}(T;[0,1])$ függvénytér a sup-metrikával ellátva szeparábilis.*

(iv) *Létezik olyan $H \subseteq \mathscr{C}(T;[0,1])$ megszámlálható halmaz, amely szétválasztó T felett.*

Bizonyítás. (i)⇒(ii) Jelölje d_M az M metrikáját, és legyen d olyan metrika T felett, amely a T topológiáját generálja. Rögzítsünk egy $\mathbb{R}_+^*$-ban haladó zérussorozatot, és minden $m, n \in \mathbb{N}$ esetén legyen

$$C_{m,n} := \{f \in \mathscr{C}(T;M) | (\forall (t,t') \in T \times T) : d(t,t') \leq \varepsilon_m \Rightarrow d_M(f(t), f(t')) \leq \varepsilon_n\}.$$

A (T,d) pár kompakt metrikus tér, ezért a Heine-tétel alapján minden $T \to M$ folytonos függvény egyenletesen folytonos a d és d_M metrikák szerint. Tehát minden $\mathbb{N} \ni n$-hez és $\mathscr{C}(T;M) \ni f$-hez van olyan $\delta \in \mathbb{R}_+^*$, hogy minden $(t,t') \in T \times T$ esetén, ha $d(t,t') < \delta$, akkor $d_M(f(t), f(t')) < \varepsilon_n$; ugyanakkor $\lim\limits_{m \to \infty} \varepsilon_m = 0$ miatt van olyan $m \in \mathbb{N}$, hogy $\varepsilon_m < \delta$, ezért $f \in C_{m,n}$. Ez azt jelenti, hogy minden $n \in \mathbb{N}$ esetén $\mathscr{C}(T;M) = \bigcup\limits_{m \in \mathbb{N}} C_{m,n}$. A T halmaz teljesen korlátos a d metrika szerint, ezért kiválasztható olyan $(T_m)_{m \in \mathbb{N}}$ halmazsorozat, hogy minden $\mathbb{N} \ni m$-re $T_m \subseteq T$ véges halmaz és $T = \bigcup\limits_{t \in T_m} \mathrm{B}_{\varepsilon_m}(t;d)$. Legyen $D \subseteq M$ megszámlálható sűrű halmaz (a d_M metrika szerint). Minden $m, n \in \mathbb{N}$ esetén minden $\varphi : T_m \to D$ függvényre legyen

$$C_{m,n,\varphi} := \{\ f \in C_{m,n}\ |\ (\forall\ t \in T_m) :\ d_M(f(t), \varphi(t)) \leq \varepsilon_n\ \}.$$

Ha $m, n \in \mathbb{N}$ és $f : T \to M$ tetszőleges függvény, akkor $\overline{D} = M$ miatt minden $t \in T_m$ pontra $D \cap \overline{\mathrm{B}}_{\varepsilon_n}(f(t); d_M) \neq \emptyset$, tehát a T_m végessége folytán $\prod\limits_{t \in T_m} \left(D \cap \overline{\mathrm{B}}_{\varepsilon_n}(f(t); d_M)\right) \neq \emptyset$, és ha φ eleme ennek a szorzathalmaznak, akkor $\varphi : T_m \to D$ olyan függvény, hogy minden $T_m \ni t$-re $d_M(f(t), \varphi(t)) \le \varepsilon_n$. Ebből következik, hogy minden $\mathbb{N} \ni m, n$-re

$$C_{m,n} = \bigcup_{\varphi \in \mathscr{F}(T_m;D)} C_{m,n,\varphi}.$$

Értelmezzük most a

$$\Phi := \{ (m,n,\varphi) \mid (m \in \mathbb{N}) \wedge (n \in \mathbb{N}) \wedge (\varphi \in \mathscr{F}(T_m;D)) \wedge (C_{m,n,\varphi} \neq \emptyset) \} \subseteq$$
$$\subseteq \bigcup_{m \in \mathbb{N}} (\{m\} \times \mathbb{N} \times \mathscr{F}(T_m;D))$$

halmazt. Minden $\mathbb{N} \ni m$-re $\{m\} \times \mathbb{N} \times \mathscr{F}(T_m;D)$ megszámlálható halmaz, ezért Φ is megszámlálható. A kiválasztási axióma alkalmazásával vegyünk egy

$$\left(f_{(m,n,\varphi)}\right)_{(m,n,\varphi)\in\Phi} \in \prod_{(m,n,\varphi)\in\Phi} C_{m,n,\varphi}$$

elemet. Megmutatjuk, hogy az $\{f_{(m,n,\varphi)} | (m,n,\varphi) \in \Phi\}$ megszámlálható halmaz sűrű $\mathscr{C}(T;M)$-ben a d_M által meghatározott sup-metrika szerint. Legyen $f \in \mathscr{C}(T;M)$ rögzített, és $\varepsilon \in \mathbb{R}_+^*$ tetszőleges. Legyen $n \in \mathbb{N}$ olyan, hogy $\varepsilon_n \le \varepsilon/4$. Láttuk, hogy

$$\mathscr{C}(T;M) = \bigcup_{m\in\mathbb{N}} C_{m,n} = \bigcup_{m\in\mathbb{N}} \Big(\bigcup_{\varphi\in\mathscr{F}(T_m;D)} C_{m,n,\varphi} \Big),$$

ezért vehetünk olyan $m \in \mathbb{N}$ számot és $\varphi \in \mathscr{F}(T_m;D)$ függvényt, hogy $f \in C_{m,n,\varphi}$. Ekkor $C_{m,n,\varphi} \neq \emptyset$, ezért $(m,n,\varphi) \in \Phi$. Állítjuk, hogy $\sup\limits_{t\in T} d_M(f(t), f_{(m,n,\varphi)}(t)) \le \varepsilon$. Legyen ugyanis $t \in T$ tetszőleges; ekkor $T = \bigcup\limits_{s\in T_m} \mathrm{B}_{\varepsilon_m}(s;d)$ miatt létezik olyan $s \in T_m$, hogy $t \in \mathrm{B}_{\varepsilon_m}(s;d)$, vagyis $d(t,s) < \varepsilon_m$. A definíció szerint $C_{m,n,\varphi} \subseteq C_{m,n}$, ezért $f \in C_{m,n}$, így $d_M(f(t), f(s)) \le \varepsilon_n$. Ugyanakkor a $C_{m,n,\varphi}$ halmaz definíciója, $f \in C_{m,n,\varphi}$ és $s \in T_m$ alapján $d_M(f(s), \varphi(s)) \le \varepsilon_n$. Továbbá, $f_{(m,n,\varphi)} \in C_{m,n,\varphi}$, tehát $s \in T_m$ miatt $d_M\left(f_{(m,n,\varphi)}(s), \varphi(s)\right) \le \varepsilon_n$, és $f_{(m,n,\varphi)} \in C_{m,n}$, valamint $d(t,s) < \varepsilon_m$ miatt $d_M\left(f_{(m,n,\varphi)}(t), f_{(m,n,\varphi)}(s)\right) \le \varepsilon_n$. Ezekből az egyenlőtlenségekből következik, hogy

$$d_M(f(t), f_{(m,n,\varphi)}(t)) \le d_M(f(t), f(s)) + d_M(f(s), \varphi(s)) +$$
$$+ d_M\left(\varphi(s), f_{(m,n,\varphi)}(s)\right) + d_M\left(f_{(m,n,\varphi)}(s), f_{(m,n,\varphi)}(t)\right) \le 4\varepsilon_n \le \varepsilon.$$

Ezért $\sup\limits_{t\in T} d_M(f(t), f_{(m,n,\varphi)}(t)) \le \varepsilon$.

(ii)⇒(iii) Triviális, mert a $[0,1]$ intervallum az euklidészi metrikával ellátva szeparábilis.

(iii)⇒(iv) Ha $H \subseteq \mathscr{C}(T;[0,1])$ olyan halmaz, amely sűrű a sup-metrika szerint, akkor H szükségképpen szétválasztó T felett.

(iv)⇒(i) A (iv)-ből következik olyan $\mathscr{C}(T;[0,1])$-ben haladó $(f_n)_{n\in\mathbb{N}}$ sorozat létezése, hogy az $\{f_n | n \in \mathbb{N}\}$ függvényhalmaz szétválasztó T felett. Ekkor a

$$\varphi : T \to [0,1]^{\mathbb{N}}; \quad t \mapsto (f_n(t))_{n\in\mathbb{N}}$$

függvény injektív és folytonos a $[0,1]^{\mathbb{N}}$ feletti szorzattopológia szerint, mert ha $n \in \mathbb{N}$ esetén $\mathrm{pr}_n : [0,1]^{\mathbb{N}} \to [0,1];\ f \mapsto f(n)$ az n-edik projekció-függvény, akkor $\mathrm{pr}_n \circ \varphi = f_n : T \to [0,1]$ folytonos függvény. Az $\mathrm{Im}(\varphi)$ topologikus altér Hausdorff-tér, és láttuk, hogy $\varphi : T \to \mathrm{Im}(\varphi)$ folytonos bijekció. Tehát a T kompaktsága miatt φ *homeomorfizmus* a T topologikus tér és az $\mathrm{Im}(\varphi)$ topologikus altér között. Ugyanakkor az $\mathrm{Im}(\varphi)$ topologikus altér metrizálható, mert a $[0,1]^{\mathbb{N}}$ euklidészi kocka is az. Ezért T metrizálható topologikus tér. ∎

V. rész

Bevezetés a matematikai struktúrák elméletébe

30. fejezet

Struktúra típusok és morfikus struktúra típusok

30.1. Struktúra típusok és morfikus struktúra típusok értelmezése

Jelölés. Ha X és Y halmazok, akkor $\mathscr{F}(X;Y)$ jelöli az $X \to Y$ függvények halmazát és $\mathscr{B}ij(X;Y)$ jelöli az $X \to Y$ bijekciók halmazát.

30.1.1. Definíció. *A* $(D, \Sigma_{st}, \Sigma_{tr})$ *metahármast* **struktúra típusnak** *nevezzük, ha*

– D *olyan osztály, hogy minden* $X \in D$ *esetén minden* X *halmazzal ekvipotens halmaz eleme* D*-nek (amit úgy fejezünk ki, hogy a* D *osztály ekvipotenciálisan telített), és*

– Σ_{st} *olyan függvény, amely a* D *osztályon értelmezett, és*

– Σ_{tr} *olyan függvény, amely az* $\bigcup\limits_{(X,Y)\in D\times D} \mathscr{B}ij(X;Y)$ *osztályon értelmezett és minden* $X \in D$*,* $Y \in D$ *és* $f : X \to Y$ *bijekció esetén* $\Sigma_{tr}(f) : \Sigma_{st}(X) \to \Sigma_{st}(Y)$ *függvény, és teljesülnek a következő tulajdonságok:*

$(\mathrm{ST_I})$ *Minden* $X \in D$ *halmazra* $\Sigma_{tr}(\mathrm{id}_X) = \mathrm{id}_{\Sigma_{st}(X)}$*;*

$(\mathrm{ST_{II}})$ *Minden* $X, Y, Z \in D$ *halmazra és* $f : X \to Y$ *és* $g : Y \to Z$ *bijekcióra*

$$\Sigma_{tr}(g \circ f) = \Sigma_{tr}(g) \circ \Sigma_{tr}(f).$$

°A kategórialemélet nyelvén ez azt jelenti, hogy egy struktúra típus a $\mathscr{B}ij\mathscr{E}ns$ kategória önmagába ható kovariáns funktora.°

A továbbiakban megállapodunk abban, hogy ha a $(D, \Sigma_{st}, \Sigma_{tr})$ metahármas struktúra típus, akkor ezt az egyetlen Σ szimbólummal jelöljük, és a D osztályt D_Σ-val jelöljük, és minden $X \in D$ halmazra $\Sigma_{st}(X)$ helyett azt írjuk, hogy Σ_X, valamint minden $X, Y \in D$ halmazra és $f : X \to Y$ bijekcióra $\Sigma_{tr}(f)$ helyett a $\Sigma(f)$ jelölést alkalmazzuk. A D_Σ osztályt az adott struktúra típus *hatástartományának* nevezzük, és $X \in D$ esetén a Σ_X halmaz elemeit az X feletti Σ*-típusú struktúráknak* nevezzük, továbbá, $X, Y \in D$ és $f \in \mathscr{B}ij(X;Y)$ esetén a $\Sigma(f) : \Sigma_X \to \Sigma_Y$ függvényt az X és Y feletti Σ-típusú struktúrák közti *átviteli függvénynek* mondjuk.

Ha Σ olyan struktúra típus, hogy $\mathrm{D}_\Sigma \neq \emptyset$ és $\mathrm{D}_\Sigma \neq \{\emptyset\}$ (és természetesen minden érdekes esetben így van), akkor Σ nem matematikai objektum, mert az ekvipotenciális telítettség folytán ekkor D_Σ nem halmaz.

Az $(\mathrm{ST_I})$ és $(\mathrm{ST_{II}})$ tulajdonságokból nyilvánvalóan következik, hogy ha Σ struktúra típus és $X, Y \in \mathrm{D}_\Sigma$, és $f : X \to Y$ bijekció, akkor a $\Sigma(f) : \Sigma_X \to \Sigma_Y$ függvény is bijekció és $(\Sigma(f))^{-1} = \Sigma(f^{-1})$.

30.1.2. Definíció. *Ha Σ struktúra típus, akkor* **Σ-típusú térnek** *nevezünk minden olyan (X, s) párt, amelyre $X \in \mathrm{D}_\Sigma$ és $s \in \Sigma_X$. Ha Σ struktúra típus, akkor a Σ-típusú terek osztályát $\tau(\Sigma)$ jelöli.*

30.1.3. Definíció. *A $(\Sigma, \mathrm{Mor}_\Sigma)$ metapárt* **morfikus struktúra típusnak** *nevezzük, ha Σ struktúra típus és Mor_Σ olyan függvény, amely a $\tau(\Sigma) \times \tau(\Sigma)$ osztályon van értelmezve, és minden $(X, s), (Y, t) \in \tau(\Sigma)$ esetén $\mathrm{Mor}_\Sigma((X, s), (Y, t)) \subseteq \mathscr{F}(X; Y)$, továbbá teljesülnek a következők:*

$(\mathrm{MST_I})$ *Minden $(X, s), (Y, t), (Z, r) \in \tau(\Sigma)$ esetén, ha $f \in \mathrm{Mor}_\Sigma((X, s), (Y, t))$ és $g \in \mathrm{Mor}_\Sigma(((Y, t), (Z, r))$, akkor $g \circ f \in \mathrm{Mor}_\Sigma((X, s), (Z, r))$.*

$(\mathrm{MST_{II}})$ *Minden $(X, s), (Y, t) \in \tau(\Sigma)$ esetén, minden $f : X \to Y$ bijekcióra: $\Sigma(f)s = t$ pontosan akkor teljesül, ha $f \in \mathrm{Mor}_\Sigma((X, s), (Y, t))$ és $f^{-1} \in \mathrm{Mor}_\Sigma((Y, t), (X, s))$.*

A továbbiakban megállapodunk abban, hogy ha a $(\Sigma, \mathrm{Mor}_\Sigma)$ metapár morfikus struktúra típus, akkor ezt az egyetlen Σ szimbólummal jelöljük, és magát Σ-t nevezzük morfikus struktúra típusnak. Ez a konvenció mindaddig nem vezethet félreértésre, amíg adott Σ struktúra típushoz csak egyetlen olyan Mor_Σ függvényt tekintünk, amelyre a $(\Sigma, \mathrm{Mor}_\Sigma)$ metapár morfikus struktúra típus. Azonban látni kell, hogy adott Σ struktúra típushoz általában több olyan Mor_Σ függvény is létezik, amelyre $(\Sigma, \mathrm{Mor}_\Sigma)$ morfikus struktúra típus, tehát általában Σ nem határozza meg Mor_Σ-t egyértelműen.

30.2. Σ-típusú tér automorfizmuscsoportjai

A következő állítást gyakran használjuk, anélkül, hogy külön hivatkoznánk rá.

30.2.1. Állítás. *Legyen Σ morfikus struktúra típus, $X, Y \in \mathrm{D}_\Sigma$ és $f : X \to Y$ bijekció. Ha $s \in \Sigma_X$, akkor $f \in \mathrm{Mor}_\Sigma((X, s), (Y, \Sigma(f)s))$.*

Bizonyítás. A $t := \Sigma(f)s \in \Sigma_Y$ struktúrára $(\mathrm{MST_{II}})$ szerint $f \in \mathrm{Mor}_\Sigma((X, s), (Y, t))$ és $f^{-1} \in \mathrm{Mor}_\Sigma((Y, t), (X, s))$ teljesül, tehát $f \in \mathrm{Mor}_\Sigma((X, s), (Y, \Sigma(f)s))$. ■

30.2.2. Állítás. *Legyen Σ morfikus struktúra típus és $(X, s) \in \tau(\Sigma)$. Ekkor $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, s))$ és az*

$$\mathrm{Aut}_\Sigma(X, s) := \{f \in \mathscr{B}ij(X; X) | \Sigma(f)s = s\}$$

halmaz része $\mathrm{Mor}_\Sigma((X, s), (X, s))$-nek, és ez a $\circ$ művelettel ellátva csoport.

Bizonyítás. Az előző állítást alkalmazva az $Y := X$ és $f := \mathrm{id}_X$ választással kapjuk, hogy $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, \Sigma(\mathrm{id}_X)s))$, és $(\mathrm{ST_I})$ alapján $\Sigma(\mathrm{id}_X)s = s$, következésképpen $\mathrm{id}_X \in \mathrm{Aut}_\Sigma((X, s), (X, s))$. Ha $f : X \to X$ olyan bijekció, hogy $\Sigma(f)s = s$, akkor az $(\mathrm{ST_I})$ és $(\mathrm{ST_{II}})$ szerint $\Sigma(f^{-1})s = (\Sigma(f))^{-1}s = s$. Ha $f, g : X \to X$ olyan bijekciók, hogy $\Sigma(f)s = s = \Sigma(g)s$, akkor az $(\mathrm{ST_{II}})$ szerint $\Sigma(g \circ f)s = \Sigma(g)(\Sigma(f)s) = \Sigma(g)s = s$. Ez azt jelenti, hogy az $\mathrm{Aut}_\Sigma(X, s)$ halmaz részcsoportja az X halmaz teljes permutáció-csoportjának. ■

30.2.3. Definíció. *Legyen* Σ *morfikus struktúra típus és* $(X, s) \in \tau(\Sigma)$. *Ekkor az* $\mathrm{Aut}_\Sigma(X, s) := \{f \in \mathscr{B}ij(X; X) | \Sigma(f)s = s\}$ *halmazt a* $\circ$ *művelettel ellátva az* (X, s) Σ*-típusú tér* **teljes automorfizmus-csoportjának** *nevezzük. Az* $\mathrm{Aut}_\Sigma(X, s)$ *csoport részcsoportjait az* (X, s) Σ*-típusú tér* **automorfizmus-csoportjainak** *nevezzük.*

30.3. Morfizmusok struktúra típusok között

30.3.1. Definíció. *Legyenek* Σ *és* Σ' *olyan struktúra típusok, hogy* $\mathrm{D}_\Sigma \subseteq \mathrm{D}_{\Sigma'}$. *Az* F *függvényt* Σ *és* Σ' *közötti* **morfizmusnak** *nevezünk, ha az* F *minden* $X \in \mathrm{D}_\Sigma$ *halmazhoz hozzárendel egy* $F_X : \Sigma_X \to \Sigma'_X$ *függvényt úgy, hogy minden* $X, Y \in \mathrm{D}_\Sigma$ *és* $f \in \mathscr{B}ij(X; Y)$ *esetén a következő diagram kommutatív:*

$$\begin{array}{ccc} \Sigma_X & \xrightarrow{\Sigma(f)} & \Sigma_Y \\ {\scriptstyle F_X}\downarrow & & \downarrow{\scriptstyle F_Y} \\ \Sigma'_X & \xrightarrow{\Sigma'(f)} & \Sigma'_Y \end{array}$$

vagyis $F_Y \circ \Sigma(f) = \Sigma'(f) \circ F_X$. *Azt mondjuk, hogy* F **monomorfizmus** *(illetve* **epimorfizmus***, illetve* **bimorfizmus***), ha minden* $X \in \mathrm{D}_\Sigma$ *halmazra az* $F_X : \Sigma_X \to \Sigma'_X$ *függvény injektív (illetve szürjektív, illetve bijektív).*

Tehát a definíció szerint csak olyan Σ és Σ' struktúra típusok között létezhet morfizmus, amelyekre $\mathrm{D}_\Sigma \subseteq \mathrm{D}_{\Sigma'}$ teljesül.

Ha Σ struktúra típus, akkor az a D_Σ-n értelmezett függvény, amely minden $X \in \mathrm{D}_\Sigma$ halmazhoz id_{Σ_X}-t rendeli nyilvánvalóan bimorfizmus Σ és Σ között. Ezt a bimorfizmust $\mathbf{1}_\Sigma$ jelöli.

30.3.2. Definíció. *Legyenek* Σ, Σ' *és* Σ'' *struktúra típusok, és* F *morfizmus* Σ *és* Σ' *között, valamint* F' *morfizmus* Σ' *és* Σ'' *között. Ekkor az* F' *és* F *(ilyen sorrendű)* **szorzatának** *nevezzük és* $F' \bullet F$*-fel jelöljük azt a* D_Σ*-n értelmezett függvényt, amely minden* $X \in \mathrm{D}_\Sigma$ *halmazhoz hozzárendeli az* $(F' \bullet F)_X := F'_X \circ F_X : \Sigma_X \to \Sigma''_X$ *függvényt.*

Nyilvánvaló, hogy ha Σ, Σ' és Σ'' struktúra típusok, és F morfizmus Σ és Σ' között, valamint F' morfizmus Σ' és Σ'' között, akkor $F' \bullet F$ morfizmus a Σ és Σ'' struktúra típusok között.

30.3.3. Definíció. *A* Σ *és* Σ' *struktúra típusok közötti* F *morfizmust* **izomorfizmusnak** *nevezzük, ha létezik olyan* F' *morfizmus a* Σ' *és* Σ *struktúra típusok között, hogy* $F' \bullet F = \mathbf{1}_\Sigma$ *és* $F \bullet F' = \mathbf{1}_{\Sigma'}$. *Ha létezik izomorfizmus a* Σ *és* Σ' *struktúra típusok között, akkor ezeket* **izomorfaknak** *nevezzük.*

30.3.4. Állítás. *Legyenek* Σ *és* Σ' *struktúra típusok, és tegyük fel, hogy* $\mathrm{D}_\Sigma = \mathrm{D}_{\Sigma'}$. *Legyen* F *olyan függvény, amely minden* $X \in \mathrm{D}_\Sigma$ *halmazhoz hozzárendel egy* $F_X : \Sigma_X \to \Sigma'_X$ *függvényt. Ekkor a következő állítások ekvivalensek.*

(i) *F bimorfizmus a Σ és Σ' struktúra típusok között.*

(ii) *F monomorfizmus és epimorfizmus a Σ és Σ' struktúra típusok között.*

(iii) *F izomorfizmus a Σ és Σ' struktúra típusok között.*

Bizonyítás. Az (i)$\Leftrightarrow$(ii) kijelentés nyilvánvalóan következik abból, hogy két halmaz között ható függvény pontosan akkor bijekció, ha injekció és szürjekció.

(i)$\Rightarrow$(iii) Legyen F bimorfizmus a Σ és Σ' struktúra típusok között. Ekkor minden $X \in \mathrm{D}_\Sigma$ halmazra az $F_X : \Sigma_X \to \Sigma'_X$ leképezés bijekció, ezért képezhető az $F'_X := (F_X)^{-1} : \Sigma'_X \to \Sigma_X$ leképezés. Ilymódon értelmeztünk egy olyan F' leképezést, amely minden $X \in \mathrm{D}_\Sigma = \mathrm{D}_{\Sigma'}$ halmazhoz hozzárendel egy $F'_X : \Sigma'_X \to \Sigma_X$ függvényt.

Megmutatjuk, hogy F' morfizmus a Σ' és Σ struktúra típusok között. Valóban, ha $X, Y \in \mathrm{D}_{\Sigma'} = \mathrm{D}_\Sigma$, akkor minden $f : X \to Y$ bijekcióra $F_Y \circ \Sigma(f) = \Sigma'(f) \circ F_X$, ezért jobbról $(F_X)^{-1}$-gyel és balról $(F_Y)^{-1}$-gyel komponálva kapjuk, hogy $\Sigma(f) \circ (F_X)^{-1} = (F_Y)^{-1} \circ \Sigma'(f)$, vagy ami ugyanaz: $F'_Y \circ \Sigma'(f) = \Sigma(f) \circ F'_X$. Ez azt jelenti, hogy F' morfizmus a Σ' és Σ struktúra típusok között.

Az F' definícója és a morfizmusok szorzatának értelmezése alapján nyilvánvaló, hogy $F \bullet F' = \mathbf{1}_{\Sigma'}$ és $F' \bullet F = \mathbf{1}_\Sigma$, hiszen minden $X \in \mathrm{D}_\Sigma = \mathrm{D}_{\Sigma'}$ esetén $(F \bullet F')_X := F_X \circ F'_X := F_X \circ (F_X)^{-1} = \mathrm{id}_{\Sigma'_X}$ és $(F' \bullet F)_X := F'_X \circ F_X := (F_X)^{-1} \circ F_X = \mathrm{id}_{\Sigma_X}$ Ezért F izomorfizmus Σ és Σ' struktúra típusok között.

(iii)$\Rightarrow$(i) Legyen F izomorfizmus a Σ és Σ' struktúra típusok között, és vegyünk olyan F' morfizmust a Σ' és Σ struktúra típusok között, amelyre $F' \bullet F = \mathbf{1}_\Sigma$ és $F \bullet F' = \mathbf{1}_{\Sigma'}$. Ekkor a morfizmusok szorzatának definíciója szerint minden $X \in \mathrm{D}_\Sigma = \mathrm{D}_{\Sigma'}$ esetén $F_X \circ F'_X =: (F \bullet F')_X = \mathrm{id}_{\Sigma'_X}$ és $F'_X \circ F_X =: (F' \bullet F)_X = \mathrm{id}_{\Sigma_X}$, így az $F_X : \Sigma_X \to \Sigma'_X$ függvény bijekció, tehát F bimorfizmus a Σ és Σ' struktúra típusok között. ■

30.3.5. Definíció. *Legyenek Σ és Σ' olyan morfikus struktúra típusok, hogy $\mathrm{D}_\Sigma \subseteq \mathrm{D}_{\Sigma'}$. Az F függvényt a Σ és Σ' morfikus struktúra típusok közötti* **morfizmusnak** *(illetve* **monomorfizmusnak***, illetve* **epimorfizmusnak***, illetve* **bimorfizmusnak***, illetve* **izomorfizusnak***) nevezünk, ha F* **morfizmus** *(illetve* **monomorfizmus***, illetve* **epimorfizmus***, illetve* **bimorfizmus***, illetve* **izomorfizus***) a Σ és Σ' struktúra típusok között. A Σ és Σ' morfikus struktúra típusokat* **izomorfaknak** *nevezzük, ha a Σ és Σ' struktúra típusok izomorfak.*

30.4. Rendezés a struktúrák között

30.4.1. Állítás. *Legyen Σ morfikus struktúra típus és $X \in \mathrm{D}_\Sigma$ rögzített halmaz. A Σ_X halmazon (tehát az X feletti Σ-típusú struktúrák halmazán) értelmezzük a $\leq$ bináris relációt úgy, hogy minden $s, t \in \Sigma_X$ esetén*

$$s \leq t \overset{\mathrm{df}}{\Leftrightarrow} \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,t),(X,s)).$$

Ekkor a $\leq$ bináris reláció rendezés a Σ_X halmaz felett.

Bizonyítás. Ha $s \in \Sigma_X$, akkor az $(\mathrm{MST_{II}})$ alapján $\Sigma(\mathrm{id}_X)s = s$ pontosan akkor teljesül, ha $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,s),(X,s))$. Az $(\mathrm{ST_I})$ miatt $\Sigma(\mathrm{id}_X) = \mathrm{id}_{\Sigma_X}$, ezért minden $s \in \Sigma_X$ esetén $\Sigma(\mathrm{id}_X)s = s$. Tehát a $\leq$ reláció reflexív a Σ_X halmazon.

Legyenek $s, t \in \Sigma_X$ olyanok, hogy $s \leq t$ és $t \leq s$. Ekkor $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,t),(X,s))$ és $(\mathrm{id}_X)^{-1} = \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,s),(X,t))$, így az $(\mathrm{MST_{II}})$ alapján $\Sigma(\mathrm{id}_X)t = s$. Az $(\mathrm{ST_I})$ miatt $\Sigma(\mathrm{id}_X) = \mathrm{id}_{\Sigma_X}$, ezért $t = s$. Tehát a $\leq$ reláció antiszimmetrikus.

Legyenek $r, s, t \in \Sigma_X$ olyanok, hogy $r \leq s$ és $s \leq t$. Ekkor $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,s),(X,r))$ és $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,t),(X,s))$, amiből az $(\mathrm{MST_I})$ alapján következik, hogy $\mathrm{id}_X = \mathrm{id}_X \circ \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,t),(X,r))$. Ezért $r \leq t$, vagyis a $\leq$ reláció tranzitív. ■

30.4.2. Definíció. *Ha Σ morfikus struktúra típus, akkor minden $X \in \mathrm{D}_\Sigma$ halmazra, az előző állításban értelmezett Σ_X feletti $\leq$ rendezést a Σ_X struktúra halmaz feletti* **természetes rendezésnek** *nevezzük, és a Σ_X halmazt ezzel a rendezéssel ellátva rendezett halmaznak tekintjük.*

30.4.3. Állítás. *Legyen Σ morfikus struktúra típus és legyenek $X, Y \in \mathrm{D}_\Sigma$. Ekkor minden $s \in \Sigma_X$ és $t \in \Sigma_Y$ esetén*

$$\mathrm{Mor}_\Sigma((X,s),(Y,t)) = \bigcap_{\substack{(s',t') \in \Sigma_X \times \Sigma_Y \\ s \leq s',\ t' \leq t}} \mathrm{Mor}_\Sigma((X,s'),(Y,t')).$$

Bizonyítás. Triviális, hogy a jobb oldalon álló halmaz részhalmaza a bal oldalon álló halmaznak. Megfordítva, ha $f \in \mathrm{Mor}_\Sigma((X,s),(Y,t))$ és $s' \in \Sigma_X$, $t' \in \Sigma_Y$ olyanok, hogy $s \leq s'$ és $t' \leq t$, akkor a definíció alapján $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,s'),(X,s))$ és $\mathrm{id}_Y \in \mathrm{Mor}_\Sigma((Y,t),(Y,t'))$, amiből az $(\mathrm{MST_I})$ alapján következik, hogy $f = \mathrm{id}_Y \circ f \circ \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,s'),(Y,t'))$. Ezért a bal oldalon álló halmaz részhalmaza a jobb oldalon álló halmaznak. ■

Megjegyezzük, hogy léteznek olyan fontos morfikus struktúra típusok (például az *algebrai* struktúra típusok), amelyek szerinti természetes rendezések megegyeznek az $=$ relációval.

30.4.4. Állítás. *Legyen Σ morfikus struktúra típus, $X, Y \in \mathrm{D}_\Sigma$ és $f : X \to Y$ bijekció. Ekkor minden $s_1, s_2 \in \Sigma_X$ esetén*

$$s_1 \leq s_2 \ \Leftrightarrow\ \Sigma(f)s_1 \leq \Sigma(f)s_2,$$

vagyis a $\Sigma(f) : \Sigma_X \to \Sigma_Y$ leképezés szigorúan rendezéstartó bijekció.

Bizonyítás. Legyenek $s_1, s_2 \in \Sigma_X$ olyanok, hogy $s_1 \leq s_2$, így $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,s_2),(X,s_1))$. Ekkor $(\mathrm{MST_{II}})$ alapján nyilvánvalóan $f \in \mathrm{Mor}_\Sigma((X,s_1),(Y,\Sigma(f)s_1))$, amiből $(\mathrm{MST_I})$ alkalmazásával kapjuk, hogy $f = f \circ \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X,s_2),(Y,\Sigma(f)s_1))$. $(\mathrm{ST_{II}})$ miatt $s_2 = \Sigma(f^{-1})\Sigma(f)s_2$, így ismét $(\mathrm{MST_{II}})$ alapján $f^{-1} \in \mathrm{Mor}_\Sigma((Y,\Sigma(f)s_2),(Y,\Sigma(f^{-1})\Sigma(f)s_2)) = \mathrm{Mor}_\Sigma((Y,\Sigma(f)s_2),(X,s_2))$. $(\mathrm{MST_I})$ alkalmazásával ebből kapjuk, hogy $\mathrm{id}_Y = f \circ f^{-1} \in \mathrm{Mor}_\Sigma((Y,\Sigma(f)s_2),(Y,\Sigma(f)s_1))$, vagyis $\Sigma(f)s_1 \leq \Sigma(f)s_2$. Tehát a $\Sigma(f) : \Sigma_X \to \Sigma_Y$ leképezés monoton növő.

Ebből következik, hogy a $\Sigma(f^{-1}) : \Sigma_Y \to \Sigma_X$ leképezés is monoton növő, így $(\Sigma(f))^{-1} = \Sigma(f^{-1})$ miatt $\Sigma(f)$ szigorúan rendezéstartó. ■

30.4.5. Következmény. *Legyen Σ morfikus struktúra típus, $X, Y \in \mathrm{D}_\Sigma$ és $f : X \to Y$ bijekció. Ekkor minden $s \in \Sigma_X$ és $t \in \Sigma_Y$ esetén a következő kijelentések ekvivalensek.*

(i) $f \in \mathrm{Mor}_\Sigma((X,s),(Y,t))$.

(ii) $\Sigma(f^{-1})t \leq s$.

(iii) $t \leq \Sigma(f)s$.

Bizonyítás. (i) $\Rightarrow$ (ii) Az $(\mathrm{MST_{II}})$ miatt $f^{-1} \in \mathrm{Mor}_\Sigma((Y,t),(X,\Sigma(f^{-1})t))$, ezért az $(\mathrm{MST_I})$ alapján kapjuk, hogy ha $f \in \mathrm{Mor}_\Sigma((X,s),(Y,t))$, akkor $\mathrm{id}_X = f^{-1} \circ f \in \mathrm{Mor}_\Sigma((X,s),(X,\Sigma(f^{-1})t))$, vagyis $\Sigma(f^{-1})t \leq s$.

(ii) $\Rightarrow$ (iii) Ha $\Sigma(f^{-1})t \leq s$, akkor 30.4.4. és $(\Sigma(f))^{-1} = \Sigma(f^{-1})$ következtében $t = \Sigma(f)\Sigma(f^{-1})t \leq \Sigma(f)s$.

(iii) $\Rightarrow$ (i) Az $(\mathrm{MST_{II}})$ miatt $f \in \mathrm{Mor}_\Sigma((X,s),(Y,\Sigma(f)s))$, ezért az $(\mathrm{MST_I})$ alapján kapjuk, hogy ha $t \leq \Sigma(f)s$, vagyis $\mathrm{id}_Y \in \mathrm{Mor}_\Sigma((Y,\Sigma(f)s),(Y,t))$, akkor $f = \mathrm{id}_Y \circ f \in \mathrm{Mor}_\Sigma((X,s),(Y,t))$. ■

30.5. Struktúra típusok adaptációja (illesztése)

30.5.1. Definíció. *Legyen* $(\Sigma^\lambda)_{\lambda\in L}$ *struktúra típus metarendszer. Azt mondjuk, hogy a* Σ *struktúra típus a* $(\Sigma^\lambda)_{\lambda\in L}$ *struktúra típus metarendszer* **adaptáltja**, *ha teljesülnek a következők.*

($\mathrm{AD_I}$) $\mathrm{D}_\Sigma \subseteq \bigcap\limits_{\lambda\in L} \mathrm{D}_{\Sigma^\lambda}$.

($\mathrm{AD_{II}}$) *Minden* $X \in \mathrm{D}_\Sigma$ *esetén* $\Sigma_X \subseteq \prod\limits_{\lambda\in L} \Sigma^\lambda_X$.

($\mathrm{AD_{III}}$) *Minden* $X, Y \in \mathrm{D}_\Sigma$ *halmazra és* $f : X \to Y$ *bijekcióra és* $(s_\lambda)_{\lambda\in L} \in \Sigma_X$ *rendszerre:* $\Sigma(f)\left((s_\lambda)_{\lambda\in L}\right) = (\Sigma^\lambda(f)s_\lambda)_{\lambda\in L}$.

Megjegyezzük, hogy a matematikailag érdekes esetekben csak olyan $(\Sigma^\lambda)_{\lambda\in L}$ struktúra típus metarendszerek adaptáltjait tekintjük, ahol L *véges* halmaz.

Legyen a Σ struktúra típus a $(\Sigma^\lambda)_{\lambda\in L}$ struktúra típus metarendszer adaptáltja. Ekkor az ($\mathrm{AD_{III}}$) feltétel alapján látható, hogy minden $X, Y \in \mathrm{D}_\Sigma$ halmazra és $f : X \to Y$ bijekcióra a $\Sigma(f)$ átviteli függvényt egyértelműen meghatározza Σ_X és f, hiszen $\Sigma(f) := \left(\underset{\lambda\in L}{\times} \Sigma^\lambda(f)\right)\Big|_{\Sigma_X}$. Ezért egy adott $(\Sigma^\lambda)_{\lambda\in L}$ struktúra típus metarendszer adaptáltjainak általános előállítási módja a következő:

– Veszünk egy olyan függvényt, amely a $\bigcap\limits_{\lambda\in L} \mathrm{D}_{\Sigma^\lambda}$ osztály valamely D_Σ részosztályának minden X eleméhez hozzárendel egy $\Sigma_X \subseteq \prod\limits_{\lambda\in L} \Sigma^\lambda_X$ részhalmazt úgy, hogy minden $X, Y \in \mathrm{D}_\Sigma$ esetén, minden $f : X \to Y$ bijekcióra $\left(\underset{\lambda\in L}{\times} \Sigma^\lambda(f)\right)\langle\Sigma_X\rangle \subseteq \Sigma_Y$ teljesüljön.

– Ezután minden $X, Y \in \mathrm{D}_\Sigma$ és $f : X \to Y$ bijekció esetében – definíció szerint – legyen $\Sigma(f) := \left(\underset{\lambda\in L}{\times} \Sigma^\lambda(f)\right)\Big|_{\Sigma_X}$.

Könnyen látható, hogy ilymódon olyan Σ struktúra típust értelmeztünk, amely a $(\Sigma^\lambda)_{\lambda\in L}$ struktúra típus metarendszer adaptáltja, és e metarendszer minden adaptáltja előállítható ezen a módon.

Speciálisan, ha $(\Sigma^\lambda)_{\lambda\in L}$ struktúra típus metarendszer, és $\mathrm{D}_\Sigma := \bigcap\limits_{\lambda\in L} \mathrm{D}_{\Sigma^\lambda}$, és minden $X \in \mathrm{D}_\Sigma$ halmazra $\Sigma_X := \prod\limits_{\lambda\in L} \Sigma^\lambda_X$, valamint minden $X, Y \in \mathrm{D}_\Sigma$ halmazra és $f : X \to Y$ bijekcióra $\Sigma(f) := \underset{\lambda\in L}{\times} \Sigma^\lambda(f)$, akkor a Σ struktúra típus az adott metarendszer adaptáltja (ezt nevezzük a $(\Sigma^\lambda)_{\lambda\in L}$ struktúra típus metarendszer *triviális adaptáltjának*).

A definíció alapján nyilvánvaló, hogy adott struktúra típus metarendszernek sokféle adaptáltja létezhet. Most az adaptáció két nevezetes speciális esetéről lesz szó.

30.5.2. Definíció. *Legyen* Σ *struktúra típus. Azt mondjuk, hogy a* Σ' *struktúra típus a* Σ*-nak* **specializáltja**, *ha* Σ' *adaptáltja a* (Σ) *egy tagú struktúra típus metarendszernek.*

Tehát a Σ' struktúra típus pontosan akkor specializáltja a Σ struktúra típusnak, ha $\mathrm{D}_{\Sigma'} \subseteq \mathrm{D}_\Sigma$ és minden $X \in \mathrm{D}_{\Sigma'}$ halmazra $\Sigma'_X \subseteq \Sigma_X$, valamint minden $X, Y \in \mathrm{D}_{\Sigma'}$ halmazra és $f : X \to Y$ bijekcióra $\Sigma(f)\langle\Sigma'_X\rangle \subseteq \Sigma'_Y$ és $\Sigma'(f) := \Sigma(f)\Big|_{\Sigma'_X}$.

30.5.3. Definíció. *Azt mondjuk, hogy a Σ' struktúra típus a Σ struktúra típus alatt fekszik* (*vagy, hogy Σ' a Σ-ból* **struktúra elhagyással keletkezik**, *vagy Σ a Σ'-ből* **struktúra hozzávétellel keletkezik**) *, ha létezik olyan Σ'' struktúra típus, hogy Σ izomorf a (Σ', Σ'') struktúra típus metapár egyik adaptációjával.*

Jelölés. Legyen Σ struktúra típus és $\mathfrak{T} \subseteq \tau(\Sigma)$. Ekkor

$$\mathrm{D}_{\Sigma|\mathfrak{T}} := \{\ X \in \mathrm{D}_\Sigma \mid (\exists s) : (X, s) \in \mathfrak{T}\ \},$$

és minden $X \in \mathrm{D}_{\Sigma|\mathfrak{T}}$ esetén

$$(\Sigma|\mathfrak{T})_X := \{\ s \mid (X, s) \in \mathfrak{T}\ \}.$$

30.5.4. Definíció. *Legyen Σ struktúra típus és $\mathfrak{T} \subseteq \tau(\Sigma)$. Azt mondjuk, hogy létezik Σ-nak $\mathfrak{T}$ szerinti* **leszűkítése**, *ha teljesül a következő:*

(RE) *Minden $X, Y \in \mathrm{D}_{\Sigma|\mathfrak{T}}$ halmazra és $f : X \to Y$ bijekcióra*

$$\Sigma(f)\langle(\Sigma|\mathfrak{T})_X\rangle \subseteq (\Sigma|\mathfrak{T})_Y.$$

Ekkor minden $\mathrm{D}_{\Sigma|\mathfrak{T}} \ni X$-hez hozzárendelve a $(\Sigma|\mathfrak{T})_X$ halmazt, és minden $X, Y \in \mathrm{D}_{\Sigma|\mathfrak{T}}$ halmaz esetén minden $f : X \to Y$ bijekcióhoz hozzárendelve a $\Sigma(f)|_{(\Sigma|\mathfrak{T})_X}$ függvényt sturktúra típust kapunk, amit $\Sigma|\mathfrak{T}$-vel jelölünk, és a Σ struktúra típus $\mathfrak{T}$-szerinti **leszűkítésének** *nevezünk.*

Ha Σ struktúra típus, $\mathfrak{T} \subseteq \tau(\Sigma)$ és létezik Σ-nak $\mathfrak{T}$ szerinti leszűkítése, akkor nyilvánvaló, hogy $\Sigma|\mathfrak{T}$ specializáltja Σ-nak.

31. fejezet

Iniciális struktúrák

31.1. Iniciális struktúrák értelmezése

31.1.1. Definíció. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$, és $((X_i, s_i), f_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(X_i, s_i) \in \tau(\Sigma)$ és $f_i : X \to X_i$ függvény. Ekkor az $((X_i, s_i), f_i)_{i \in I}$ rendszer által előállított X feletti* **iniciális Σ-típusú struktúrának** *nevezünk minden olyan $s \in \Sigma_X$ elemet, amelyre teljesül a következő.*

(STI) *Minden $(X', s') \in \tau(\Sigma)$ térre és $f : X' \to X$ függvényre:*

$$f \in \mathrm{Mor}_\Sigma((X', s'), (X, s)) \;\Leftrightarrow\; (\forall i \in I) : f_i \circ f \in \mathrm{Mor}_\Sigma((X', s'), (X_i, s_i)).$$

Megjegyezzük, hogy ha Σ struktúra típus, $X \in \mathrm{D}_\Sigma$, és $((X_i, s_i), f_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(X_i, s_i) \in \tau(\Sigma)$ és $f_i : X \to X_i$ függvény, valamint $s \in \Sigma_X$ olyan, hogy teljesül rá (STI), akkor minden $i \in I$ esetén $f_i \in \mathrm{Mor}_\Sigma((X, s), (X_i, s_i))$, hiszen (STI)-ből az $(X', s') := (X, s)$ és $f := \mathrm{id}_X$ választással kapjuk, hogy

$$\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, s)) \;\Leftrightarrow\; (\forall i \in I) : f_i = f_i \circ \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X_i, s_i)),$$

és tudjuk, hogy $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, s))$.

31.1.2. Állítás. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$, és $((X_i, s_i), f_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(X_i, s_i) \in \tau(\Sigma)$ és $f_i : X \to X_i$ függvény. Ha $s \in \Sigma_X$ olyan, hogy teljesül rá az* (STI) *tulajdonság, akkor s az $\{s' \in \Sigma_X | (\forall i \in I) : f_i \in \mathrm{Mor}_\Sigma((X, s'), (X_i, s_i))\}$ struktúra-halmaz legkisebb eleme a Σ_X feletti természetes rendezésre nézve.*

Bizonyítás. Láttuk, hogy $s \in \{s' \in \Sigma_X | (\forall i \in I) : f_i \in \mathrm{Mor}_\Sigma((X, s'), (X_i, s_i))\}$. Továbbá, ha $s' \in \Sigma_X$ olyan, hogy minden $i \in I$ esetén $f_i \in \mathrm{Mor}_\Sigma((X, s'), (X_i, s_i))$, akkor minden $I \ni i$-re $f_i = f_i \circ \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s'), (X_i, s_i))$, vagyis (STI)-t alkalmazva az $\mathrm{id}_X : X \to X$ függvényre kapjuk, hogy $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s'), (X, s))$, ami azt jelenti, hogy $s \leq s'$ a Σ_X feletti természetes rendezés szerint. ■

31.1.3. Következmény. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$, és $((X_i, s_i), f_i)_{i \in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(X_i, s_i) \in \tau(\Sigma)$ és $f_i : X \to X_i$ függvény. Ekkor legfeljebb egy olyan $s \in \Sigma_X$ létezik, amely rendelkezik az* (STI) *tulajdonsággal, tehát az iniciális Σ-típusú struktúrák egyértelműen vannak meghatározva.*

Bizonyítás. Az 31.1.2. állításból nyilvánvalóan következik. ■

Tehát ha létezik, akkor beszélhetünk *az* $((X_i, s_i), f_i)_{i\in I}$ rendszer által előállított X feletti iniciális Σ-típusú struktúráról.

Azonban léteznek olyan morfikus struktúra típusok (°sok algebrai struktúra típus ilyen°), amelyekben még akkor sem feltétlenül létezik iniciális struktúra, ha I egy elemű indexhalmaz.

31.2. Speciális iniciális struktúrák

31.2.1. Definíció. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$, $(X', s') \in \tau(\Sigma)$ és $f : X \to X'$ függvény. Azt mondjuk, hogy az $s \in \Sigma_X$ struktúra az $s' \in \Sigma_{X'}$ struktúra f* **függvény által létesített Σ-típusú inverz képe**, *ha $s \in \Sigma_X$ egyenlő az $((X', s'), f)$ egy tagú rendszer által létesített X feletti iniciális Σ-típusú struktúrával. Az $s' \in \Sigma_{X'}$ struktúra f függvény által létesített Σ-típusú inverz képét $\overset{-1}{f}[s']_\Sigma$ jelöli.*

31.2.2. Állítás. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$, $(X', s') \in \tau(\Sigma)$ és $f : X \to X'$ bijekció. Ekkor létezik az s' struktúra f által létesített Σ-típusú inverz képe, és $\overset{-1}{f}[s']_\Sigma = \Sigma(f^{-1})s'$.*

Bizonyítás. Legyen $s := \Sigma(f^{-1})(s')$. Ekkor $(\mathrm{ST_{II}})$ és $(\mathrm{ST_I})$ miatt $s \in \Sigma_X$ olyan, hogy $\Sigma(f)(s) = \Sigma(f)(\Sigma(f^{-1})(s')) = \Sigma(f \circ f^{-1})(s') = \Sigma(\mathrm{id}_{X'})(s') = s'$, tehát $(\mathrm{MST_{II}})$ alapján $f \in \mathrm{Mor}_\Sigma((X, s), (X', s'))$ és $f^{-1} \in \mathrm{Mor}_\Sigma((X', s'), (X, s))$.
Legyen $(X'', s'') \in \tau(\Sigma)$ és $g : X'' \to X$ függvény. Ha $g \in \mathrm{Mor}_\Sigma((X'', s''), (X, s)))$, akkor $f \in \mathrm{Mor}_\Sigma((X, s), (X', s'))$ és $(\mathrm{MST_I})$ alapján $f \circ g \in \mathrm{Mor}_\Sigma((X'', s''), (X', s')))$. Megfordítva, ha $f \circ g \in \mathrm{Mor}_\Sigma((X'', s''), (X', s')))$, akkor $f^{-1} \in \mathrm{Mor}_\Sigma((X', s'), (X, s))$ és $(\mathrm{MST_I})$ alapján $g = f^{-1} \circ (f \circ g) \in \mathrm{Mor}_\Sigma((X'', s''), (X, s)))$. Ez azt jelenti, hogy s egyenlő az s' struktúra f által létesített Σ-típusú inverz képével. ■

31.2.3. Állítás. *Legyen Σ morfikus struktúra típus, $(X, s), (X', s') \in \tau(\Sigma)$ és $f : X \to X'$ olyan függvény, hogy létezik az s' struktúra f által létesített Σ-típusú inverz képe. Ekkor $f \in \mathrm{Mor}_\Sigma((X, s), (X', s'))$ pontosan akkor teljesül, ha $\overset{-1}{f}[s']_\Sigma \le s$.*

Bizonyítás. Az $\overset{-1}{f}[s']_\Sigma$ struktúra definíciója, az (STI) tulajdonság és a Σ_X feletti természetes rendezés értelmezése alapján teljesülnek a következő ekvivalenciák:

$$\overset{-1}{f}[s']_\Sigma \le s \Leftrightarrow \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, \overset{-1}{f}[s']_\Sigma)) \Leftrightarrow f = f \circ \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X', s')),$$

amit bizonyítani kellett. ■

Jelölés. Ha X halmaz és $Y \subseteq X$, akkor $\mathrm{in}_{Y,X}$ jelöli az $Y \to X$ kanonikus injekciót.

31.2.4. Definíció. *Legyen Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $Y \subseteq X$. Azt mondjuk, hogy az s struktúra* **leszűkíthető** *az Y halmazra, ha $Y \in \mathrm{D}_\Sigma$ és létezik az s struktúra $\mathrm{in}_{Y,X}$ által létesített Σ-típusú inverz képe; ekkor az $s|Y := \overset{-1}{\mathrm{in}}_{Y,X}[s]_\Sigma$ jelölést alkalmazzuk, és ezt* **az s struktúra Y-ra vett leszűkítésének** *nevezzük. Az $s \in \Sigma_X$ struktúra leszűkítéseit az s struktúra Σ-típusú* **részstruktúráinak** *nevezzük.*

Tehát, ha Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$, $Y \subseteq X$ és $Y \in \mathrm{D}_\Sigma$, akkor – ha létezik – akkor $s|Y \in \Sigma_Y$ az a Σ-típusú struktúra Y felett, amelyre minden $(X', s') \in \tau(\Sigma)$ esetén, minden $f : X' \to Y$ függvényre:

$$f \in \mathrm{Mor}_\Sigma((X', s'), (X, s)) \Leftrightarrow f \in \mathrm{Mor}_\Sigma((X', s'), (Y, s|Y)).$$

31.2.5. Állítás. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$ és $(s_i)_{i\in I}$ tetszőleges Σ_X-ben haladó rendszer. Ha létezik az $((X, s_i), \mathrm{id}_X)_{i\in I}$ rendszer által előállított X feletti iniciális Σ-típusú struktúra, akkor az egyenlő az $(s_i)_{i\in I}$ rendszer szuprémumával a Σ_X rendezett halmazban.*

Bizonyítás. Jelölje s az $((X, s_i), \mathrm{id}_X)_{i\in I}$ rendszer által előállított X feletti iniciális Σ-típusú struktúrát. Ekkor az s struktúra deiníciója és (STI) miatt minden $i \in I$ esetén $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X_i, s_i))$, azaz $s_i \leq s$. Ha $s' \in \Sigma_X$ olyan, hogy minden $i \in I$ esetén $s_i \leq s'$, akkor minden $I \ni i$-re $\mathrm{id}_X \circ \mathrm{id}_X = \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s'), (X, s_i))$, tehát az s struktúra definíciója és (STI) alapján $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s'), (X, s))$, azaz $s \leq s'$. ∎

Speciálisan, ha Σ olyan morfikus struktúra típus, hogy minden iniciális struktúra létezik benne (°például a topologikus struktúra típus°), akkor minden $X \in \mathrm{D}_\Sigma$ esetén a Σ_X rendezett halmaznak létezik legnagyobb eleme a természetes rendezés szerint, feltéve, hogy $\Sigma_X \neq \emptyset$.

31.2.6. Definíció. *Legyen Σ morfikus struktúra típus és $((X_i, s_i))_{i\in I}$ tetszőleges $\tau(\Sigma)$-ban haladó rendszer. Legyen $X := \prod_{i\in I} X_i$ és minden $i \in I$ esetén jelölje $\mathrm{pr}_i : X \to X_i$ a kanonikus projekciót. Azt mondjuk, hogy az $((X_i, s_i))_{i\in I}$ Σ-típusú tér-rendszernek létezik a* **Σ-típusú szorzata**, *ha $X \in \mathrm{D}_\Sigma$ és létezik a $((X_i, s_i), \mathrm{pr}_i)_{i\in I}$ rendszer által előállított iniciális X feletti Σ-típusú struktúra. Ha létezik az $((X_i, s_i))_{i\in I}$ Σ-típusú tér-rendszer szorzata, akkor az $((X_i, s_i), \mathrm{pr}_i)_{i\in I}$ rendszer által előállított X feletti Σ-típusú struktúrát $\times_{i\in I} s_i$ jelöli, és ezt az $(s_i)_{i\in I}$* **struktúra-rendszer Σ-típusú szorzatának** *nevezzük, továbbá, a $\left(\prod_{i\in I} X_i, \times_{i\in I} s_i\right)$ Σ-típusú teret az $((X_i, s_i))_{i\in I}$* **Σ-típusú tér-rendszer Σ-típusú szorzatának** *nevezzük.*

Tehát, ha Σ morfikus strutúra típus és az $((X_i, s_i))_{i\in I}$ Σ-típusú tér-rendszernek létezik a Σ-típusú szorzata, akkor $\prod_{i\in I} X_i \in \mathrm{D}_\Sigma$ és minden $(X', s') \in \tau(\Sigma)$ térre és $f : X' \to \prod_{i\in I} X_i$ függvényre teljesül az, hogy:

$$f \in \mathrm{Mor}_\Sigma\Big((X', s'), \Big(\prod_{i\in I} X_i, \times_{i\in I} s_i\Big)\Big) \Leftrightarrow (\forall i \in I) : \ \mathrm{pr}_i \circ f \in \mathrm{Mor}_\Sigma((X', s'), (X_i, s_i)).$$

A szorzatstruktúrákkal részletesebben az 5. pontban foglalkozunk.

31.2.7. Tétel. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$ és $((X_i, s_i), f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(X_i, s_i) \in \tau(\Sigma)$ és $f_i : X \to X_i$ függvény. Tegyük fel, hogy létezik az $((X_i, s_i))_{i\in I}$ Σ-típusú tér-rendszer Σ-típusú szorzata és létezik a $\times_{i\in I} s_i$ struktúra*

$$f : X \to \prod_{i\in I} X_i; \quad x \mapsto (f_i(x))_{i\in I}$$

függvény által létesített Σ-típusú inverz képe. Legyen $s := \overset{-1}{f}[\times_{i\in I} s_i]_\Sigma$. *Ekkor létezik az* $((X_i, s_i), f_i)_{i\in I}$ *rendszer által előállított iniciális* X *feletti Σ-típusú struktúra, és egyenlő* s*-sel.*

Bizonyítás. Legyen $(X', s') \in \tau(\Sigma)$ és $g : X' \to X$ függvény. Ekkor az $s := \overset{-1}{f}[\times_{i\in I} s_i]_\Sigma$ definíció, valamint a struktúra inverz képének és a struktúrák szorzatának értelmezése alapján igazak a következő ekvivalenciák:

$$g \in \mathrm{Mor}_\Sigma((X', s'), (X, s)) \Leftrightarrow f \circ g \in \mathrm{Mor}_\Sigma\Big((X', s'), \Big(\prod_{i\in I} X_i, \underset{i\in I}{\times} s_i\Big)\Big) \Leftrightarrow$$
$$\Leftrightarrow (\forall i \in I): \ \mathrm{pr}_i \circ (f \circ g) \in \mathrm{Mor}_\Sigma((X', s'), (X_i, s_i)) \Leftrightarrow$$
$$\Leftrightarrow (\forall i \in I): \ f_i \circ g \in \mathrm{Mor}_\Sigma((X', s'), (X_i, s_i)).$$

ahol kihasználtuk azt, hogy minden $i \in I$ esetén $\mathrm{pr}_i \circ f = f_i$. Ez azt jelenti, hogy s egyenlő az $((X_i, s_i), f_i)_{i\in I}$ rendszer által előállított iniciális X feletti Σ-típusú struktúrával. ■

31.2.8. Állítás. *Legyen a* Σ *morfikus truktúra típus a* $(\Sigma^\lambda)_{\lambda\in L}$ *morfikus struktúra típus metarendszer adaptáltja. Legyen* $(X, (s_\lambda)_{\lambda\in L}) \in \tau(\Sigma)$, $X' \in \mathrm{D}_\Sigma$ *és* $f : X' \to X$ *függvény. Tegyük fel, hogy minden* $\lambda \in L$ *esetén létezik az* $s_\lambda \in \Sigma^\lambda_X$ *struktúra* f *által létesített* Σ^λ*-típusú inverz képe. Ha* $\left(\overset{-1}{f}[s_\lambda]_{\Sigma^\lambda}\right)_{\lambda\in L} \in \Sigma_{X'}$, *akkor az* $(s_\lambda)_{\lambda\in L} \in \Sigma_X$ *struktúrának létezik az* f *által létesített Σ-típusú inverz képe, és* $\overset{-1}{f}[(s_\lambda)_{\lambda\in L}]_\Sigma = \left(\overset{-1}{f}[s_\lambda]_{\Sigma^\lambda}\right)_{\lambda\in L}$.

Bizonyítás. ■

31.3. Iniciális struktúrák tranzitivitása

31.3.1. Tétel. *Legyen* Σ *morfikus struktúra típus,* $X \in \mathrm{D}_\Sigma$ *és* $((X_i, s_i))_{i\in I}$ $\tau(\Sigma)$*-ban haladó rendszer. Legyen* $(I_j)_{j\in J}$ *olyan diszjunkt halmazrendszer, hogy* $I = \bigcup_{j\in J} I_j$. *Legyen minden* $j \in J$ *esetén* $X'_j \in \mathrm{D}_\Sigma$ *és* $h_j : X \to X'_j$ *függvény. Minden* $j \in J$ *és* $i \in I_j$ *esetén legyen* $g_{i,j} : X'_j \to X_i$ *függvény. Végül, minden* $i \in I$ *esetén legyen* $f_i := g_{i,j} \circ h_j : X \to X_i$, *ahol* $j \in J$ *az az egyértelműen meghatározott index, amelyre* $i \in I_j$. *Tegyük fel, hogy minden* $j \in J$ *esetén létezik az* $((X_i, s_i), g_{i,j})_{i\in I_j}$ *rendszer által előállított* X'_j *feletti iniciális Σ-típusú struktúra, amit* s'_j *jelöl. Tegyük fel továbbá, hogy létezik az* $((X'_j, s'_j), h_j)_{j\in J}$ *rendszer által előállított* X *feletti iniciális Σ-típusú struktúra, amit* s *jelöl. Ekkor létezik az* $((X_i, s_i), f_i)_{i\in I}$ *rendszer által előállított* X *feletti iniciális Σ-típusú struktúra és egyenlő* s*-sel.*

Bizonyítás. ■

Az 31.3.1. tételre a továbbiakban úgy hivatkozunk, mint az *iniciális struktúrák tranzitivitásának tétele.*

31.3.2. Következmény. *Legyen* Σ *morfikus struktúra típus,* $X, Y, Z \in \mathrm{D}_\Sigma$, $s \in \Sigma_Z$, *valamint legyenek* $f : X \to Y$ *és* $g : Y \to Z$ *függvények. Ha létezik az* $s \in \Sigma_Z$ *struktúra* g *által létesített Σ-típusú inverz képe, és létezik a* $\overset{-1}{g}[s]_\Sigma \in \Sigma_Y$ *struktúra* f *által létesített*

Σ-típusú inverz képe, akkor létezik az s struktúra $g \circ f$ által létesített Σ-típusú inverz képe, és

$$\overset{-1}{(g \circ f)}[s]_\Sigma = \overset{-1}{f}\left[\overset{-1}{g}[s]_\Sigma\right]_\Sigma.$$

Bizonyítás. ■

31.4. Részstruktúrák, generátorhalmazok

31.4.1. Állítás. *Legyen Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $Z \subseteq Y \subseteq X$ olyan halmazok, hogy s leszűkíthető Y-ra és $s|Y$ leszűkíthető Z-re. Ekkor s leszűkíthető Z-re és*

$$s|Z = (s|Y)|Z.$$

Bizonyítás. ■

31.4.2. Állítás. *Legyen Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $Z \subseteq X$ olyan halmaz, hogy s leszűkíthető Z-re. Ekkor minden $(Y, t) \in \tau(\Sigma)$ térre és minden $f : X \to Y$ függvényre teljesül az, hogy ha $f \in \mathrm{Mor}_\Sigma((X, s), (Y, t))$, akkor $f|_Z \in \mathrm{Mor}_\Sigma((Z, s|Z), (Y, t))$.*

Bizonyítás. ■

Azonban létezik olyan Σ morfikus struktúra típus (°például a topologikus struktúra típus°), hogy léteznek olyan $(X, s), (Y, t) \in \tau(\Sigma)$ terek, valamint létezik olyan $f : X \to Y$ függvény, hogy az s struktúra minden $Z \subseteq X$, $Z \neq X$ halmazra leszűkíthető és $f|_Z \in \mathrm{Mor}_\Sigma((Z, s|Z), (Y, t))$, de $f \notin \mathrm{Mor}_\Sigma((X, s), (Y, t))$. (°Ellenben algebrai struktúra típus esetében ilyen helyzet nem fordulhat elő.°)

31.4.3. Állítás. *Legyen a Σ morfikus truktúra típus a $(\Sigma^\lambda)_{\lambda \in L}$ morfikus struktúra típus metarendszer adaptáltja. Legyen $(X, (s_\lambda)_{\lambda \in L}) \in \tau(\Sigma)$, $Y \subseteq X$ és tegyük fel, hogy minden $\lambda \in L$ esetén az $s_\lambda \in \Sigma^\lambda_X$ struktúrának létezik a Σ^λ-típusú leszűkítése Y-ra. Ha $(s_\lambda|Y)_{\lambda \in L} \in \Sigma_Y$, akkor létezik az $(s_\lambda)_{\lambda \in L} \in \Sigma_X$ struktúrának Σ-típusú leszűkítése, és*

$$(s_\lambda)_{\lambda \in L}|Y = (s_\lambda|Y)_{\lambda \in L}.$$

Bizonyítás. ■

31.4.4. Definíció. *Legyen a Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $A \subseteq X$. Azt mondjuk, hogy az $Y \subseteq X$ halmaz az A-halmaz* **Σ-típusú s-generátuma**, *ha Y a tartalmazás tekintetében legkisebb olyan részhalmaza X-nek, amely tartalmazza A-t és amelyre az $s \in \Sigma_X$ struktúra leszűkíthető. Azt mondjuk, hogy az A halmaz* **Σ-típusú generátorhalmaza** *az (X, s) Σ-típusú térnek, ha létezik az A halmaz Σ-típusú s-generátuma, és az egyenlő X-szel.*

Nyilvánvaló, hogy ha Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $A \subseteq X$ olyan, hogy $s|A$ létezik, akkor létezik az A halmaz Σ-típusú s-generátuma és az egyenlő A-val.

Tehát, ha Σ morfikus struktúra típus és $(X, s) \in \tau(\Sigma)$, akkor az $A \subseteq X$ halmaz pontosan akkor Σ-típusú generátorhalmaza az (X, s) Σ-típusú térnek, ha minden $Y \subseteq X$ halmazra, amelyre $A \subseteq Y$ és $s|Y$ létezik: teljesül az, hogy $Y = X$.

31.4.5. Állítás. *Legyen Σ olyan morfikus struktúra típus, amelyre teljesül a következő tulajdonság:*

(SP) *Minden $(X, s) \in \tau(\Sigma)$ térre és az X részhalmazainak tetszőleges nem üres $(Y_i)_{i \in I}$ rendszerére teljesül az, hogy ha minden $i \in I$ esetén az s struktúra leszűkíthető Y_i-re, akkor az s struktúra leszűkíthető a $\bigcap_{i \in I} Y_i$ halmazra is.*

Ekkor minden $(X, s) \in \tau(\Sigma)$ térre és minden $A \subseteq X$ halmazra létezik A-nak a Σ-típusú s-generátuma, és az egyenlő a $\bigcap \{\, Y \subseteq X \mid A \subseteq Y$ és $s|Y$ létezik$\}$ halmazzal.

Bizonyítás. ■

31.4.6. Állítás. *Legyen Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $A \subseteq X$. Ha az $Y \subseteq X$ halmaz egyenlő az A halmaz Σ-típusú s-generátumával, akkor az A halmaz Σ-típusú generátorhalmaza az $(Y, s|Y)$ Σ-típus altérnek.*

Bizonyítás. ■

31.4.7. Definíció. *Legyen Σ morfikus struktúra típus és $(X, s) \in \tau(\Sigma)$. Azt mondjuk, hogy az A halmaz az (X, s) térnek* **szabad Σ-típusú generátorhalmaza***, ha minden $(Y, t) \in \tau(\Sigma)$ térhez és minden $f : A \to Y$ függvényhez létezik olyan $\overline{f} : X \to Y$ függvény, hogy $f \subseteq \overline{f}$ és $\overline{f} \in \mathrm{Mor}_\Sigma((X, s), (Y, t))$.*

Az elnevezés indoklását adja a következő állítás.

31.4.8. Állítás. *Legyen a Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $A \subseteq X$. Ha az A halmaz szabad Σ-típusú generátorhalmaza az (X, s) térnek, akkor A Σ-típusú generátorhalmaza (X, s)-nek.*

Bizonyítás. ■

31.5. Szorzatstruktúrák

31.5.1. Állítás. *Legyen Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és $((X_i, s_i))_{i \in I}$ olyan $\tau(\Sigma)$-ban haladó rendszer, amelynek létezik Σ-típusú szorzata. Minden $i \in I$ esetén legyen $f_i : X \to X_i$ leképezés, és*

$$f : X \to \prod_{i \in I} X_i; \quad x \mapsto (f_i(x))_{i \in I}.$$

Ekkor $f \in \mathrm{Mor}_\Sigma\Big((X, s), \Big(\prod_{i \in I} X_i, \bigtimes_{i \in I} s_i\Big)\Big)$ pontosan akkor teljesül, ha minden $i \in I$ esetén $f_i \in \mathrm{Mor}_\Sigma((X, s), (X_i, s_i))$.

Bizonyítás. Az állítás nyilvánvalóan következik a szorzatstruktúra definíciójából, (STI)-ből és abból, hogy minden $i \in I$ esetén $\mathrm{pr}_i \circ f = f_i$. ■

31.5.2. Következmény. *Legyen Σ morfikus struktúra típus és $((X_i, s_i))_{i \in I}$, $((Y_i, t_i))_{i \in I}$ olyan $\tau(\Sigma)$-ban haladó rendszerek, amelyeknek létezik Σ-típusú szorzatuk. Minden $i \in I$ esetén legyen $f_i : X_i \to Y_i$ függvény és legyen*

$$\bigtimes_{i \in I} f_i : \prod_{i \in I} X_i \to \prod_{i \in I} Y_i; \quad (x_i)_{i \in I} \mapsto (f_i(x_i))_{i \in I}.$$

Ekkor $f \in \mathrm{Mor}_\Sigma\Big(\Big(\prod_{i\in I} X_i, \times_{i\in I} s_i\Big), \Big(\prod_{i\in I} Y_i, \times_{i\in I} t_i\Big)\Big)$ *teljesüléséhez elégséges, és ha minden* $(i,j) \in I \times I$ *esetén* $\mathrm{Mor}_\Sigma((X_i, s_i),(Y_j,t_j)) \neq \emptyset$*, akkor szükséges is az, hogy minden* $I \ni i$*-re* $f_i \in \mathrm{Mor}_\Sigma((X_i,s_i),(Y_i,t_i))$.

Bizonyítás. ■

31.5.3. Állítás. *Legyen* Σ *morfikus struktúra típus,* $(X,s),(Y,t) \in \tau(\Sigma)$ *és* $f : X \to Y$ *függvény. Tegyük fel, hogy az* s *és* t *struktúráknak létezik a* Σ*-típusú szorzatuk, és az* $s\times t$ *szorzatstruktúra leszűkíthető az* f *függvény grafikonjára, amit* $\mathrm{gr}(f)$ *jelöl. Legyen*

$$g : X \to \mathrm{gr}(f); \quad x \mapsto (x, f(x)).$$

Ekkor $f \in \mathrm{Mor}_\Sigma((X,s),(Y,t))$ *pontosan akkor teljesül, ha* $\Sigma(g)s = (s \times t)|\mathrm{gr}(f)$.

Bizonyítás. ■

31.5.4. Állítás. (**Szorzatstruktúrák asszociativitása.**) *Legyen* Σ *morfikus struktúra típus,* $((X_i,s_i))_{i\in I}$ $\tau(\Sigma)$*-ban haladó rendszer és* $(I_j)_{j\in J}$ *olyan diszjunkt halmazrendszer, hogy* $I = \bigcup_{j\in J} I_j$*. Tegyük fel, hogy minden* $j \in J$ *esetén az* $(s_i)_{i\in I_j}$ *struktúra-rendszernek létezik a* Σ*-típusú szorzata, és a* $\Big(\times_{i\in I_j} s_i\Big)_{j\in J}$ *struktúra rendszernek is létezik a* Σ*-típusú szorzata. Ekkor az* $(s_i)_{i\in I}$ *struktúra-rendszernek is létezik a* Σ*-típusú szorzata, és az*

$$f : \prod_{i\in I} X_i \to \prod_{j\in J}\Big(\prod_{i\in I_j} X_i\Big)$$

kanonikus bijekcióra $\Sigma(f)\Big(\times_{i\in I} s_i\Big) = \times_{j\in J}\Big(\times_{i\in I_j} s_i\Big)$ *teljesül.*

Bizonyítás. ■

31.5.5. Következmény. (**Szorzatstruktúrák kommutativitása.**) *Legyen* Σ *morfikus struktúra típus és* $((X_i,s_i))_{i\in I}$ *olyan* $\tau(\Sigma)$*-ban haladó rendszer, amelynek létezik* Σ*-típusú szorzata. Ekkor az* I *halmaz minden* π *permutációjára teljesül, hogy az* $(s_{\pi(i)})_{i\in I}$ *struktúra-rendszernek létezik* Σ*-típusú szorzata, és az*

$$f : \prod_{i\in I} X_i \to \prod_{i\in I} X_{\pi(i)}; \quad (x_i)_{i\in I} \mapsto (x_{\pi(i)})_{i\in I}$$

kanonikus bijekcióra $\Sigma(f)\Big(\times_{i\in I} s_i\Big) = \Big(\times_{i\in I} s_{\pi(i)}\Big)$ *teljesül.*

Bizonyítás. ■

31.6. Projektív limeszek

31.6.1. Definíció. *Azt mondjuk, hogy az* $\Big((X_\alpha)_{\alpha\in A}, (p_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ *pár* **projektív rendszer***, ha* A *felfelé irányított rendezett halmaz, és* $(X_\alpha)_{\alpha\in A}$ *halmazrendszer, és* $(p_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}$ *olyan rendszer, hogy minden* $(\alpha,\beta) \in A\times A$*,* $\alpha \leq \beta$ *esetén* $p_{\alpha,\beta} : X_\beta \to X_\alpha$ *függvény és teljesülnek a következők:*

(PRO$_\mathrm{I}$) *Minden $\alpha \in A$ esetén $p_{\alpha,\alpha} = \mathrm{id}_{X_\alpha}$;*

(PRO$_\mathrm{II}$) *Minden $\alpha, \beta, \gamma \in A$ esetén, ha $\alpha \leq \beta$ és $\beta \leq \gamma$, akkor $p_{\alpha,\gamma} = p_{\alpha,\beta} \circ p_{\beta,\gamma}$.*

Továbbá, ekkor az

$$X := \{\ (x_\alpha)_{\alpha\in A} \in \prod_{\alpha\in A} X_\alpha \mid (\forall(\alpha,\beta) \in A \times A) : (\alpha \leq \beta \ \Rightarrow\ p_{\alpha,\beta}(x_\beta) = x_\alpha)\ \}$$

halmazt az adott projektív rendszer **projektív limeszének** *nevezzük és a* $\varprojlim_{\alpha,A} X_\alpha$ *szimbólummal jelöljük, valamint minden $\alpha \in A$ esetén a $p_\alpha := \mathrm{pr}_\alpha|_X : X \to X_\alpha$ függvényt a projektív limesz α-adik* **kanonikus projekciójának** *nevezzük.*

31.6.2. Állítás. *Legyen $\Big((X_\alpha)_{\alpha\in A}, (p_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ projektív rendszer és $X := \varprojlim_{\alpha,A} X_\alpha$.*

a) *Minden $\alpha, \beta \in A$ esetén, ha $\alpha \leq \beta$, akkor a következő diagram kommutatív:*

$$\begin{tikzcd} X \arrow[r, "p_\beta"] \arrow[dr, "p_\alpha"'] & X_\beta \arrow[d, "p_{\alpha,\beta}"] \\ & X_\alpha \end{tikzcd} .$$

b) *Legyen X' halmaz és $(f_\alpha)_{\alpha\in A}$ olyan rendszer, hogy minden $\alpha \in A$ esetén $f_\alpha : X' \to X_\alpha$ függvény, és minden $\alpha, \beta \in A$ esetén, ha $\alpha \leq \beta$, akkor a következő diagram kommutatív:*

$$\begin{tikzcd} X' \arrow[r, "f_\beta"] \arrow[dr, "f_\alpha"'] & X_\beta \arrow[d, "p_{\alpha,\beta}"] \\ & X_\alpha \end{tikzcd} .$$

Ekkor létezik egyetlen olyan $f : X' \to X$ függvény, minden $\alpha \in A$ esetén a következő diagram kommutatív:

$$\begin{tikzcd} X' \arrow[r, "f"] \arrow[dr, "f_\alpha"'] & X \arrow[d, "p_\alpha"] \\ & X_\alpha \end{tikzcd} .$$

Bizonyítás. a) Az X halmaz és a kanonikus projekciók *definíciója szerint* minden $\alpha, \beta \in A$ esetén, ha $\alpha \leq \beta$, akkor minden $x \in X$ rendszerre $p_{\alpha,\beta}(p_\beta(x)) = p_\alpha(x)$, ami azt jelenti, hogy $p_{\alpha,\beta} \circ p_\beta = p_\alpha$.

b) Ha $f : X' \to X$ olyan függvény, hogy minden $\alpha \in A$ esetén az

$$\begin{tikzcd} X' \arrow[r, "f"] \arrow[dr, "f_\alpha"'] & X \arrow[d, "p_\alpha"] \\ & X_\alpha \end{tikzcd}$$

diagram kommutatív, akkor minden $x' \in X$ és $\alpha \in A$ esetén $p_\alpha(f(x')) = f_\alpha(x')$, tehát a kanonikus projekciók értelmezése alapján $f(x') = (f_\alpha(x'))_{\alpha\in A}$. Ebből látható, hogy az adott feltétellel f egyértelműen van meghatározva, és világos, hogy az adott tulajdonságú f függvény létezésének bizonyításához azt kell igazolni, hogy az

$$X' \to \prod_{\alpha\in A} X_\alpha; \quad x' \mapsto f(x') := (f_\alpha(x'))_{\alpha\in A}$$

függvény X-be érkezik és rendelkezik a megkövetelt tulajdonsággal. Ehhez legyen $x' \in X'$. Ekkor az $f(x') := (f_\alpha(x'))_{\alpha\in A} \in \prod_{\alpha\in A} X_\alpha$ rendszer olyan, hogy minden $\alpha, \beta \in A$ esetén, ha $\alpha \leq \beta$, akkor

$$p_\alpha(f(x')) = f_\alpha(x') \stackrel{(*)}{=} p_{\alpha,\beta}(f_\beta(x')) = p_{\alpha,\beta}(p_\beta(f(x'))),$$

ahol a $\stackrel{(*)}{=}$ egyenlőségnél kihasználtuk, hogy a

$$\begin{tikzcd} X' \arrow[r, "f_\beta"] \arrow[dr, "f_\alpha"'] & X_\beta \arrow[d, "p_{\alpha,\beta}"] \\ & X_\alpha \end{tikzcd}$$

kommutatív. Tehát az X halmaz definíciója szerint $(f_\alpha(x'))_{\alpha\in A} \in X$. Továbbá az f függvény és a kanonikus projekciók definíciója alapján nyilvánvaló, hogy minden $\alpha \in A$ esetén $p_\alpha(f(x')) = f_\alpha(x')$ minden $X' \ni x'$-re igaz, tehát minden $\alpha \in A$ esetén az

$$\begin{tikzcd} X' \arrow[r, "f"] \arrow[dr, "f_\alpha"'] & X \arrow[d, "p_\alpha"] \\ & X_\alpha \end{tikzcd}$$

diagram kommutatív. ■

31.6.3. Állítás. *Legyen $(E_i)_{i\in I}$ halmazrendszer. Jelölje A az I halmaz véges részhalmazainak halmazát, és minden $\alpha, \beta \in A$ esetén jelölje $\alpha \leq \beta$ az $\alpha \subseteq \beta$ összefüggést (tehát az $(A, \leq)$ pár felfelé irányított rendezett halmaz). Minden $\alpha \in A$ esetén legyen $X_\alpha := \prod_{i\in\alpha} E_i$, valamint minden $\alpha, \beta \in A$ esetén, ha $\alpha \leq \beta$, akkor vezessük be a*

$$p_{\alpha,\beta} : X_\beta \to X_\alpha; \quad (x_i)_{i\in\beta} \mapsto (x_i)_{i\in\alpha}$$

függvényt. Ekkor az $\Big((X_\alpha)_{\alpha\in A}, (p_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ pár projektív rendszer, és az

$$f : \prod_{i\in I} E_i \to \varprojlim_{\alpha,A} X_\alpha; \quad (x_i)_{i\in I} \mapsto \big((x_i)_{i\in\alpha}\big)_{\alpha\in A}$$

függvény bijekció.

Bizonyítás. ■

31.6.4. Definíció. *Legyen $\Big((X_\alpha)_{\alpha\in A}, (p_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ projektív rendszer. Ha Σ morfikus struktúra típus és $(s_\alpha)_{\alpha\in A}$ olyan rendszer, hogy minden $A \ni \alpha$-ra $(X_\alpha, s_\alpha) \in \tau(\Sigma)$, akkor azt mondjuk, hogy az $(s_\alpha)_{\alpha\in A}$ Σ-típusú struktúra-rendszernek létezik* **projektív limesze***, az adott projektív rendszer szerint, ha $\varprojlim_{\alpha,A} X_\alpha \in \mathrm{D}_\Sigma$ és létezik az $((X_\alpha, s_\alpha), p_\alpha)_{\alpha\in A}$ rendszer által előállított $\varprojlim_{\alpha,A} X_\alpha$ feletti iniciális Σ-típusú struktúra; ekkor az így létrehozott $\varprojlim_{\alpha,A} X_\alpha$ feletti Σ-típusú struktúrát $\varprojlim_{\alpha,A} s_\alpha$ jelöli.*

32. fejezet

Finális struktúrák

32.1. Finális struktúrák értelmezése

32.1.1. Definíció. *Legyen* Σ *morfikus struktúra típus,* $X \in \mathrm{D}_\Sigma$*, és* $((X_i, s_i), f_i)_{i\in I}$ *olyan rendszer, hogy minden* $i \in I$ *esetén* $(X_i, s_i) \in \tau(\Sigma)$ *és* $f_i : X_i \to X$ *függvény. Ekkor az* $((X_i, s_i), f_i)_{i\in I}$ *rendszer által előállított* X *feletti* **finális Σ-típusú struktúrának** *nevezünk minden olyan* $s \in \Sigma_X$ *elemet, amelyre teljesül a következő.*

(STF) *Minden* $(X', s') \in \tau(\Sigma)$ *térre és* $f : X \to X'$ *függvényre:*

$$f \in \mathrm{Mor}_\Sigma((X, s), (X', s')) \;\Leftrightarrow\; (\forall i \in I) : f \circ f_i \in \mathrm{Mor}_\Sigma((X_i, s_i), (X', s')).$$

Megjegyezzük, hogy ha Σ struktúra típus, $X \in \mathrm{D}_\Sigma$, és $((X_i, s_i), f_i)_{i\in I}$ olyan rendszer, hogy minden $i \in I$ esetén $(X_i, s_i) \in \tau(\Sigma)$ és $f_i : X_i \to X$ függvény, valamint $s \in \Sigma_X$ olyan, hogy teljesül rá (STF), akkor minden $i \in I$ esetén $f_i \in \mathrm{Mor}_\Sigma((X_i, s_i), (X, s))$, hiszen (STF)-ből az $(X', s') := (X, s)$ és $f := \mathrm{id}_X$ választással kapjuk, hogy

$$\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, s)) \;\Leftrightarrow\; (\forall i \in I) : f_i = \mathrm{id}_X \circ f_i \in \mathrm{Mor}_\Sigma((X_i, s_i), (X, s)),$$

és tudjuk, hogy $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, s))$.

32.1.2. Állítás. *Legyen* Σ *morfikus struktúra típus,* $X \in \mathrm{D}_\Sigma$*, és* $((X_i, s_i), f_i)_{i\in I}$ *olyan rendszer, hogy minden* $i \in I$ *esetén* $(X_i, s_i) \in \tau(\Sigma)$ *és* $f_i : X_i \to X$ *függvény. Ha* $s \in \Sigma_X$ *olyan, hogy teljesül rá az* (STF) *tulajdonság, akkor* s *az* $\{s' \in \Sigma_X | (\forall i \in I) : f_i \in \mathrm{Mor}_\Sigma((X_i, s_i), (X, s'))\}$ *struktúra-halmaz legnagyobb eleme a* Σ_X *feletti természetes rendezésre nézve.*

Bizonyítás. Láttuk, hogy $s \in \{s' \in \Sigma_X | (\forall i \in I) : f_i \in \mathrm{Mor}_\Sigma((X_i, s_i), (X, s'))\}$. Továbbá, ha $s' \in \Sigma_X$ olyan, hogy minden $i \in I$ esetén $f_i \in \mathrm{Mor}_\Sigma((X_i, s_i), (X, s'))$, akkor az $\mathrm{id}_X : X \to X$ függvényre $(\mathrm{ST_I})$ és $(\mathrm{ST_{II}})$ miatt teljesül az, hogy minden $I \ni i$-re $f_i = \mathrm{id}_X \circ f_i \in \mathrm{Mor}_\Sigma((X_i, s_i), (X, s'))$, vagyis az (STF) alapján $\mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s), (X, s'))$, ami azt jelenti, hogy $s' \leq s$, a Σ_X feletti természetes rendezés szerint. ■

32.1.3. Következmény. *Legyen* Σ *morfikus struktúra típus,* $X \in \mathrm{D}_\Sigma$*, és* $((X_i, s_i), f_i)_{i\in I}$ *olyan rendszer, hogy minden* $i \in I$ *esetén* $(X_i, s_i) \in \tau(\Sigma)$ *és* $f_i : X_i \to X$ *függvény. Ekkor legfeljebb egy olyan* $s \in \Sigma_X$ *létezik, amely rendelkezik az* (STF) *tulajdonsággal, tehát a finális* Σ*-típusú struktúrák egyértelműen vannak meghatározva.*

Bizonyítás. Az 32.1.2. állításból nyilvánvalóan következik. ■

Tehát ha létezik, akkor beszélhetünk *az* $((X_i, s_i), f_i)_{i\in I}$ rendszer által előállított X feletti finális Σ-típusú struktúráról.

Azonban léteznek olyan morfikus struktúra típusok (°sok algebrai struktúra típus ilyen°), amelyekben még akkor sem feltétlenül létezik finális struktúra, ha I egy elemű indexhalmaz.

32.2. Speciális finális struktúrák

32.2.1. Definíció. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$, $(X', s') \in \tau(\Sigma)$ és $f : X' \to X$ függvény. Azt mondjuk, hogy az $s \in \Sigma_X$ struktúra az $s' \in \Sigma_{X'}$ struktúra f* **függvény által létesített Σ-típusú képe**, *ha $s \in \Sigma_X$ egyenlő az $((X', s'), f)$ egy tagú rendszer által létesített X feletti finális Σ-típusú struktúrával. Az $s' \in \Sigma_{X'}$ struktúra f függvény által létesített Σ-típusú képét $f[s']_\Sigma$ jelöli.*

32.2.2. Állítás. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$, $(X', s') \in \tau(\Sigma)$ és $f : X' \to X$ bijekció. Ekkor létezik az s' struktúra f által létesített Σ-típusú képe, és $f[s']_\Sigma = \Sigma(f)s'$.*

Bizonyítás. ∎

32.2.3. Állítás. *Legyen Σ morfikus struktúra típus, $(X, s), (X', s') \in \tau(\Sigma)$ és $f : X' \to X$ olyan függvény, hogy létezik az s' struktúra f által létesített Σ-típusú képe. Ekkor $f \in \mathrm{Mor}_\Sigma((X', s'), (X, s))$ pontosan akkor teljesül, ha $s \leq f[s']_\Sigma$.*

Bizonyítás. ∎

Jelölés. Ha X halmaz és R ekvivalencia-reláció X-ben, akkor $\mathrm{pr}_{X/R}$ jelöli az $X \to X/R$ kanonikus szürjekciót.

32.2.4. Definíció. *Legyen Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és R ekvivalencia-reláció X-ben. Azt mondjuk, hogy az s struktúra* **faktorizálható** *az R ekvivalencia-reláció szerint, ha $X/R \in \mathrm{D}_\Sigma$ és létezik az s struktúra $\mathrm{pr}_{X/R}$ által létesített Σ-típusú képe; ekkor az $s/R := \mathrm{pr}_{X/R}[s]_\Sigma$ jelölést alkalmazzuk, és ezt* **az s struktúra R szerinti faktorizáltjának** *nevezzük. Az $s \in \Sigma_X$ struktúra faktorizáltjait az s struktúra Σ-típusú* **faktorstruktúráinak** *nevezzük.*

Tehát ha Σ morfikus struktúra típus, $(X, s) \in \tau(\Sigma)$ és R ekvivalencia-reláció X-ben, akkor – ha létezik – $s/R \in \Sigma_{X/R}$ az a Σ-típusú struktúra X/R felett, amelyre minden $(X', s') \in \tau(\Sigma)$ esetén, minden $f : X/R \to X'$ függvényre, ha $f \circ \mathrm{pr}_{X/R} \in \mathrm{Mor}_\Sigma((X, s), (X', s'))$, akkor $f \in \mathrm{Mor}_\Sigma((X/R, s/R), (X', s'))$.

32.2.5. Állítás. *Legyen Σ morfikus struktúra típus, $X \in \mathrm{D}_\Sigma$ és $(s_i)_{i\in I}$ tetszőleges Σ_X-ben haladó rendszer. Ha létezik az $((X, s_i), \mathrm{id}_X)_{i\in I}$ rendszer által előállított X feletti finális Σ-típusú struktúra, akkor az egyenlő az $(s_i)_{i\in I}$ rendszer infimumával a Σ_X rendezett halmazban.*

Bizonyítás. ∎

Speciálisan, ha Σ olyan morfikus struktúra típus, hogy minden finális struktúra létezik benne (°például a topologikus struktúra típus°), akkor minden $X \in \mathrm{D}_\Sigma$ esetén a Σ_X rendezett halmaznak létezik legkisebb eleme a természetes rendezés szerint, feltéve, hogy $\Sigma_X \neq \emptyset$.

32.2.6. Definíció. *Legyen* Σ *morfikus struktúra típus és* $((X_i, s_i))_{i\in I}$ *tetszőleges* $\tau(\Sigma)$-*ban haladó rendszer. Legyen* $X := \sum_{i\in I} X_i := \bigcup_{i\in I}(\{i\} \times X_i)$ *(az* $(X_i)_{i\in I}$ *halmazrendszer* **diszjunkt uniója**), *és minden* $i \in I$ *esetén jelölje*

$$\mathrm{in}_i : X_i \to X; \quad x \mapsto (i, x)$$

a kanonikus injekciót. Azt mondjuk, hogy az $((X_i, s_i))_{i\in I}$ Σ-*típusú tér-rendszernek létezik a* Σ-**típusú összege**, *ha* $X \in \mathrm{D}_\Sigma$ *és létezik a* $((X_i, s_i), \mathrm{in}_i)_{i\in I}$ *rendszer által előállított finális* X *feletti* Σ-*típusú struktúra. Ha létezik az* $((X_i, s_i))_{i\in I}$ Σ-*típusú tér-rendszer összege, akkor az* $((X_i, s_i), \mathrm{in}_i)_{i\in I}$ *rendszer által előállított* X *feletti* Σ-*típusú struktúrát* $\sum_{i\in I} s_i$ *jelöli, és ezt az* $(s_i)_{i\in I}$ **struktúra-rendszer** Σ-**típusú összegének** *nevezzük, továbbá, a* $\left(\sum_{i\in I} X_i, \sum_{i\in I} s_i\right)$ Σ-*típusú teret az* $((X_i, s_i))_{i\in I}$ Σ-**típusú tér-rendszer** Σ-**típusú összegének** *nevezzük.*

32.2.7. Tétel. *Legyen* Σ *morfikus struktúra típus,* $X \in \mathrm{D}_\Sigma$ *és* $((X_i, s_i), f_i)_{i\in I}$ *olyan rendszer, hogy minden* $i \in I$ *esetén* $(X_i, s_i) \in \tau(\Sigma)$ *és* $f_i : X_i \to X$ *függvény. Tegyük fel, hogy létezik az* $((X_i, s_i))_{i\in I}$ Σ-*típusú tér-rendszer* Σ-*típusú összege és létezik a* $\sum_{i\in I} s_i$ *struktúra*

$$f : \sum_{i\in I} X_i \to X; \quad (i, x_i) \mapsto f_i(x_i)$$

függvény által létesített Σ-*típusú képe, továbbá legyen* $s := f\left[\sum_{i\in I} s_i\right]_\Sigma$. *Ekkor létezik az* $((X_i, s_i), f_i)_{i\in I}$ *rendszer által előállított finális* X *feletti* Σ-*típusú struktúra, és egyenlő* s-*sel.*

Bizonyítás. ■

32.2.8. Állítás. *Legyen a* Σ *morfikus truktúra típus a* $(\Sigma^\lambda)_{\lambda\in L}$ *morfikus struktúra típus metarendszer adaptáltja. Legyen* $(X, (s_\lambda)_{\lambda\in L}) \in \tau(\Sigma)$, $X' \in \mathrm{D}_\Sigma$ *és* $f : X \to X'$ *függvény. Tegyük fel, hogy minden* $\lambda \in L$ *esetén létezik az* $s_\lambda \in \Sigma^\lambda_X$ *struktúra* f *által létesített* Σ^λ-*típusú képe. Ha* $(f[s_\lambda]_{\Sigma^\lambda})_{\lambda\in L} \in \Sigma_{X'}$, *akkor az* $(s_\lambda)_{\lambda\in L} \in \Sigma_X$ *struktúrának létezik az* f *által létesített* Σ-*típusú képe, és* $f\left[(s_\lambda)_{\lambda\in L}\right]_\Sigma = (f[s_\lambda]_{\Sigma^\lambda})_{\lambda\in L}$.

Bizonyítás. ■

32.2.9. Definíció. *Legyen* Σ *morfikus truktúra típus,* $X \in \mathrm{D}_\Sigma$ *és* $(X_i, s_i)_{i\in I}$ *olyan* $\tau(\Sigma)$-*ban haladó rendszer, hogy minden* $i \in I$ *esetén* $X_i \subseteq X$. *Azt mondjuk, hogy az* $s \in \Sigma_X$ *struktúra az* $(s_i)_{i\in I}$ *struktúra-rendszer* Σ-*típusú* **induktív összege**, *ha* s *egyenlő az* $((X_i, s_i), in_{X_i,X})_{i\in I}$ *rendszer által előállított* X *feletti finális* Σ-*típusú struktúrával. Ekkor azt mondjuk, hogy az* (X, s) Σ-*típusú tér az* $(X_i, s_i)_{i\in I}$ Σ-*típusú tér-rendszer* **induktív összege**.

Tehát ha Σ morfikus truktúra típus és az (X, s) Σ-típusú tér egyenlő az $(X_i, s_i)_{i\in I}$ Σ-típusú tér-rendszer induktív összegével, akkor minden (Y, t) Σ-típusú térre és minden $f : X \to Y$ függvényre: $f \in \mathrm{Mor}_\Sigma((X, s), (Y, t))$ ekvivalens azzal, hogy minden $i \in I$ esetén $f|_{X_i} \in \mathrm{Mor}_\Sigma((X_i, s_i), (Y, t))$.

32.3. Finális struktúrák tranzitivitása

32.3.1. Tétel. *Legyen* Σ *morfikus struktúra típus,* $X \in \mathrm{D}_\Sigma$ *és* $((X_i, s_i))_{i\in I}$ $\tau(\Sigma)$*-ban haladó rendszer. Legyen* $(I_j)_{j\in J}$ *olyan diszjunkt halmazrendszer, hogy* $I = \bigcup_{j\in J} I_j$*. Legyen minden* $j \in J$ *esetén* $X'_j \in \mathrm{D}_\Sigma$ *és* $h_j : X'_j \to X$ *függvény. Minden* $j \in J$ *és* $i \in I_j$ *esetén legyen* $g_{i,j} : X_i \to X'_j$ *függvény. Végül, minden* $i \in I$ *esetén legyen* $f_i := h_j \circ g_{i,j} : X_i \to X$*, ahol* $j \in J$ *az az egyértelműen meghatározott index, amelyre* $i \in I_j$*. Tegyük fel, hogy minden* $j \in J$ *esetén létezik az* $((X_i, s_i), g_{i,j})_{i\in I_j}$ *rendszer által előállított* X'_j *feletti finális* Σ*-típusú struktúra, amit* s'_j *jelöl. Tegyük fel továbbá, hogy létezik az* $((X'_j, s'_j), h_j)_{j\in J}$ *rendszer által előállított* X *feletti finális* Σ*-típusú struktúra, amit* s *jelöl. Ekkor létezik az* $((X_i, s_i), f_i)_{i\in I}$ *rendszer által előállított* X *feletti finális* Σ*-típusú struktúra és egyenlő* s*-sel.*

Bizonyítás. ■

Az 32.3.1. tételre a továbbiakban úgy hivatkozunk, mint a *finális struktúrák tranzitivitásának tétele.*

32.3.2. Következmény. *Legyen* Σ *morfikus struktúra típus,* $X, Y, Z \in \mathrm{D}_\Sigma$*,* $s \in \Sigma_X$*, valamint legyenek* $f : X \to Y$ *és* $g : Y \to Z$ *függvények. Ha létezik az* $s \in \Sigma_X$ *struktúra* f *által létesített* Σ*-típusú képe, és létezik az* $f[s]_\Sigma \in \Sigma_Y$ *struktúra* g *által létesített* Σ*-típusú képe, akkor létezik az* s *struktúra* $g \circ f$ *által létesített* Σ*-típusú képe, és*

$$(g \circ f)[s]_\Sigma = g\,[f[s]_\Sigma]_\Sigma\,.$$

Bizonyítás. ■

32.4. Faktorstruktúrák, morfizmusok kanonikus faktorizációja

32.4.1. Tétel. (**Első izomorfiatétel**) *Legyen* Σ *morfikus struktúra típus,* $(X, s) \in \tau(\Sigma)$ *valamint legyenek* R *és* S *olyan ekvivalencia-relációk* X *felett, hogy* $S \subseteq R$*. Jelölje* R/S *az* R *reláció* S *szerinti faktorizáltját, ami ekvivalencia-reláció az* X/S *faktorhalmaz felett. Legyen* $f : (X/S)/(R/S) \to X/R$ *a kanonikus bijekció, és tegyük fel, hogy* $(X/S)/(R/S) \in \mathrm{D}_\Sigma$ *vagy* $X/R \in \mathrm{D}_\Sigma$*. A következő állítások ekvivalensek.*

(i) *Létezik az* $(s/S)/(R/S)$ Σ*-típusú faktorstruktúra.*

(ii) *Létezik az* s/S Σ*-típusú faktorstruktúra.*

(iii) *Léteznek az* $(s/S)/(R/S)$ *és* s/S Σ*-típusú faktorstruktúrák és*

$$\Sigma(f)((s/S)/(R/S)) = s/R.$$

Bizonyítás. ■

Jelölés. Legyenek X és Y halmazok, valamint $f : X \to Y$ függvény. Ekkor R_f jelöli az f által meghatározott ekvivalencia-relációt, azaz

$$R_f := \{\ (x, x') \in X \times X \mid f(x) = f(x')\ \}.$$

Továbbá, $\overset{\bullet}{f} : X/R_f \to f\langle X\rangle$ jelöli az f függvény kanonikus faktorizáltját, tehát azt az egyértelműen meghatározott bijekciót, amely kommutatívvá teszi a következő diagramot:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \mathrm{pr}_{X/R_f}}\Big\downarrow & & \Big\uparrow{\scriptstyle \mathrm{in}_{f\langle X\rangle,Y}} \\ X/R_f & \xrightarrow{\overset{\bullet}{f}} & f\langle X\rangle \end{array}$$

32.4.2. Állítás. *Legyen Σ morfikus struktúra típus, $(X,s),(Y,t) \in \tau(\Sigma)$ és $f : X \to Y$ függvény. Ha létezik az s/R_f Σ-típusú faktorstruktúra és a $t|f\langle X\rangle$ Σ-típusú részstruktúra, akkor a következő állítások ekvivalensek.*

(i) $f \in \mathrm{Mor}_\Sigma((X,s),(Y,t))$.

(ii) $\overset{\bullet}{f} \in \mathrm{Mor}_\Sigma((X/R_f, s/R_f),(f\langle X\rangle, t|f\langle X\rangle))$.

(iii) $t|f\langle X\rangle \le \Sigma(\overset{\bullet}{f})(s/R_f)$.

Bizonyítás. (i)⇒(ii) A definíciók és az (i) hipotézis szerint

$$f = \mathrm{in}_{f\langle X\rangle,Y} \circ \left(\overset{\bullet}{f} \circ \mathrm{pr}_{X/R_f}\right) \in \mathrm{Mor}_\Sigma((X,s),(Y,t)),$$

tehát a $t|f\langle X\rangle$ részstruktúra értelmezése alapján

$$\overset{\bullet}{f} \circ \mathrm{pr}_{X/R_f} \in \mathrm{Mor}_\Sigma((X,s),(f\langle X\rangle, t|f\langle X\rangle)).$$

Ez viszont az s/R_f faktorstruktúra értelmezése szerint azt jelenti, hogy

$$\overset{\bullet}{f} \in \mathrm{Mor}_\Sigma((X/R_f, s/R_f),(f\langle X\rangle, t|f\langle X\rangle)).$$

(ii)⇔(iii) ∎

Vigyázzunk arra, hogy az előző állítás (iii) pontjában általában nincs egyenlőség. Éppen ez a tény vezet a következő definícióra.

32.4.3. Definíció. *Legyen Σ morfikus struktúra típus és $(X,s),(Y,t) \in \tau(\Sigma)$. Ekkor egy $f : X \to Y$ függvényt Σ-típusú* **homomorfizmusnak** (*vagy rövidebben* **Σ-homomorfizmusnak**) *nevezünk, ha az (X,s) és (Y,t) Σ-típusú terek között, ha létezik az s/R_f Σ-típusú faktorstruktúra és a $t|f\langle X\rangle$ Σ-típusú részstruktúra, valamint $\Sigma(\overset{\bullet}{f})(s/R_f) = t|f\langle X\rangle$.*

A következő állítás elégséges feltételt ad ahhoz, hogy egy morfizmus homomorfizmus legyen.

32.4.4. Állítás. *Legyen Σ morfikus struktúra típus, $(X,s),(Y,t) \in \tau(\Sigma)$ és $f \in \mathrm{Mor}_\Sigma((X,s),(Y,t))$. Tegyük fel, hogy létezik az s/R_f Σ-típusú faktorstruktúra és a $t|f\langle X\rangle$ Σ-típusú részstruktúra. Ha létezik f-nek olyan $g : f\langle X\rangle \to X$ jobbinverze, hogy $g \in \mathrm{Mor}_\Sigma((f\langle X\rangle, t|f\langle X\rangle),(X,s))$ és létezik az $s|g\langle f\langle X\rangle\rangle$ Σ-típusú részstruktúra, akkor az f függvény Σ-homomorfizmus az (X,s) és (Y,t) Σ-típusú terek között, és a $g|_{f\langle X\rangle} : f\langle X\rangle \to g\langle f\langle X\rangle\rangle$ bijekcióra $\Sigma(g|_{f\langle X\rangle})(t|f\langle X\rangle) = s|g\langle f\langle X\rangle\rangle$ teljesül.*

Bizonyítás. ■

32.4.5. Állítás. *Legyen a Σ struktúra típus a $(\Sigma^\lambda)_{\lambda\in L}$ struktúra típus metarendszer adaptáltja, $(X,(s_\lambda)_{\lambda\in L})\in\tau(\Sigma)$ és R olyan ekvivalencia-reláció X felett, hogy minden $\lambda\in L$ esetén az s_λ struktúrának létezik az R szerinti Σ^λ-típusú faktorizáltja, valamint $(s_\lambda/R)_{\lambda\in L}\in\Sigma_X$. Ekkor az $(s_\lambda)_{\lambda\in L}$ struktúrának is létezik az R-szerinti Σ-típusú faktorizáltja, és $(s_\lambda)_{\lambda\in L}/R=(s_\lambda/R)_{\lambda\in L}$.*

Bizonyítás. ■

32.4.6. Állítás. *Legyen Σ morfikus struktúra típus és $(X_i,s_i)_{i\in I}$ olyan $\tau(\Sigma)$-ban haladó rendszer, amelynek létezik Σ-típusú szorzata. Minden $i\in I$ esetén legyen R_i olyan ekvivalencia-reláció X_i felett, amely szerint az s_i struktúrának létezik a Σ-típusú faktorizáltja. Legyen $f:\Big(\prod_{i\in I}X_i\Big)/\Big(\bigtimes_{i\in I}R_i\Big)\to\prod_{i\in I}(X_i/R_i)$ a kanonikus bijekció. Ha a $\bigtimes_{i\in I}s_i$ struktúrának létezik az $\bigtimes_{i\in I}R_i$ ekvivalencia-reláció szerinti Σ-típusú faktorizáltja, és az $(s_i/R_i)_{i\in I}$ struktúra-rendszernek létezik a Σ-típusú szorzata, akkor*

$$f\in\mathrm{Mor}_\Sigma\Big(\Big(\Big(\prod_{i\in I}X_i\Big)/\Big(\bigtimes_{i\in I}R_i\Big),\Big(\bigtimes_{i\in I}s_i\Big)/\Big(\bigtimes_{i\in I}R_i\Big)\Big),\Big(\prod_{i\in I}(X_i/R_i),\bigtimes_{i\in I}(s_i/R_i)\Big)\Big).$$

Bizonyítás. ■

Azonban az előző állítás feltételei mellett csak annyi állítható, hogy f bijektív morfizmus, de f nem szükségképpen izomorfizmus. (Ld. Top. Gén. R. §7.23. és Top. Gén. Ch. I., §5, Ex. 6.).

32.4.7. Állítás. *Legyen Σ morfikus struktúra típus, $(X,s)\in\tau(\Sigma)$ és R olyan ekvivalencia-reláció X felett, hogy létezik az s/R Σ-típusú faktorstruktúra. Ha $Y\subseteq X$ olyan teljes reprezentánshalmaza R-nek, hogy létezik az $s|Y$ Σ-típusú részstruktúra, akkor a $\mathrm{pr}_{X/R}|_Y:Y\to X/R$ bijekcióra $\mathrm{pr}_{X/R}|_Y\in\mathrm{Mor}_\Sigma((Y,s|Y),(X/R,s/R))$ teljesül.*

Bizonyítás. ■

32.5. Részstruktúrák faktorizáltjai, izomorfiatételek

32.5.1. Tétel. *Legyen Σ morfikus struktúra típus, $(X,s)\in\tau(\Sigma)$, R ekvivalencia-reláció X felett és $Y\subseteq X$. Tegyük fel, hogy léteznek az $s|R\langle Y\rangle$ és $s|Y$ Σ-típusú részsturktúrák, valamint az $(s|R\langle Y\rangle)/(R|R\langle Y\rangle)$ és $(s|Y)/(R|Y)$ Σ-típusú faktorstruktúrák.*

a) *Létezik egyetlen olyan $f:Y/(R|Y)\to R\langle Y\rangle/(R|R\langle Y\rangle)$ bijekció, amely kommutatívvá teszi a következő diagramot:*

$$\begin{tikzcd} Y/(R|Y) \arrow[r, "f"] & R\langle Y\rangle/(R|R\langle Y\rangle) \\ Y \arrow[u, "\mathrm{pr}_{Y/(R|Y)}"] \arrow[r, "\mathrm{in}_{Y,R\langle Y\rangle}"] & R\langle Y\rangle \arrow[u, "\mathrm{pr}_{R\langle Y\rangle/(R|R\langle Y\rangle)}"'] \end{tikzcd}$$

b) *Teljesül az, hogy*

$$f\in\mathrm{Mor}_\Sigma((Y/(R|Y),(s|Y)/(R|Y)),(R\langle Y\rangle/(R|R\langle Y\rangle),(s|R\langle Y\rangle)/(R|R\langle Y\rangle))).$$

c) *Ha létezik olyan* $g : R\langle Y\rangle \to Y$ *függvény, hogy* $g \in \mathrm{Mor}_\Sigma((R\langle Y\rangle, s|R\langle Y\rangle), (Y, s|Y))$ *és minden* $x \in R\langle Y\rangle$ *esetén* $(x, g(x)) \in R$*, akkor*

$$\Sigma(f)((s|Y)/(R|Y)) = (s|R\langle Y\rangle)/(R|R\langle Y\rangle).$$

Bizonyítás. ■

32.5.2. Definíció. *Legyen* Σ *morfikus struktúra típus és* $(X, s) \in \tau(\Sigma)$*. Az*

$$\begin{pmatrix} Y & Y' \\ R & R' \end{pmatrix}$$

2×2*-es mátrixot* (X, s)**-feletti** Σ**-típusú Zassenhaus-mátrixnak** *nevezzük, ha* Y *és* Y' *olyan részhalmazai* X*-nek, hogy léteznek az* $s|Y$ *és* $s|Y'$ Σ*-típusú részstruktúrák, valamint* R *olyan ekvivalencia-reláció* Y *és* R' *olyan ekvivalencia-reláció* Y' *felett, hogy léteznek az* $(s|Y)/R$ *és* $(s|Y')/R'$ Σ*-típusú faktorstruktúrák.*

32.5.3. Definíció. *Legyen* Σ *morfikus struktúra típus és* $(X, s) \in \tau(\Sigma)$*. Az* (X, s)*-feletti*

$$\begin{pmatrix} Y & Y' \\ R & R' \end{pmatrix}$$

Σ*-típusú Zassenhaus-mátrix* **generátorának** *nevezünk minden olyan* $Z \subseteq Y \cap Y'$ *halmazt, amelyre teljesülnek a következők.*

a) *Létezik az* $s|Z$ Σ*-típusú részstruktúra.*

b) $Y = R\langle Z\rangle$ *és* $Y' = R'\langle Z\rangle$*.*

c) $R|Z = R'|Z$*.*

32.5.4. Állítás. (**Zassenhaus–lemma.**) *Legyen* Σ *morfikus struktúra típus,* $(X, s) \in \tau(\Sigma)$ *és*

$$\begin{pmatrix} Y & Y' \\ R & R' \end{pmatrix}$$

Σ*-típusú Zassenhaus-mátrix* (X, s) *felett. Ha* Z *generátora ennek a Zassenhaus-mátrixnak, akkor létezik egyetlen olyan*

$$f : Y/R \to Y'/R'$$

bijekció, amely kommutatívvá teszi a következő diagramot:

$$\begin{array}{ccc} Y/R & \xrightarrow{f} & Y'/R' \\ {\scriptstyle \mathrm{pr}_{Y/R}}\uparrow & & \uparrow{\scriptstyle \mathrm{pr}_{Y'/R'}} \\ Y & \longrightarrow & Y' \\ {\scriptstyle \mathrm{in}_{Z,Y}}\uparrow & & \uparrow{\scriptstyle \mathrm{in}_{Z,Y'}} \\ Z & \xrightarrow{\mathrm{id}_Z} & Z \end{array}$$

továbbá ekkor

$$\Sigma(f)((s|Y)/R) = (s|Y')/R'.$$

Bizonyítás. ■

32.6. Összegstruktúrák

32.7. Induktív limeszek

32.7.1. Definíció. *Azt mondjuk, hogy az* $\Big((X_\alpha)_{\alpha\in A}, (j_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ *pár* **induktív rendszer***, ha* A *felfelé irányított rendezett halmaz, valamint* $(X_\alpha)_{\alpha\in A}$ *halmazrendszer, továbbá* $(j_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}$ *olyan rendszer, hogy minden* $(\alpha,\beta)\in A\times A$*,* $\alpha\leq\beta$ *esetén* $j_{\alpha,\beta}: X_\alpha\to X_\beta$ *függvény és teljesülnek a következők:*

($\mathrm{IND_I}$) *Minden* $\alpha\in A$ *esetén* $j_{\alpha,\alpha}=\mathrm{id}_{X_\alpha}$*;*

($\mathrm{IND_{II}}$) *Minden* $\alpha,\beta,\gamma\in A$ *esetén, ha* $\alpha\leq\beta$ *és* $\beta\leq\gamma$*, akkor* $j_{\alpha,\gamma}=j_{\beta,\gamma}\circ j_{\alpha,\beta}$*.*

32.7.2. Állítás. *Ha* $\Big((X_\alpha)_{\alpha\in A}, (j_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ *induktív rendszer, akkor az*

$$R := \Big\{((\alpha,x),(\beta,y))\in\Big(\bigsqcup_{\alpha\in A}X_\alpha\Big)\times\Big(\bigsqcup_{\alpha\in A}X_\alpha\Big) \mid$$
$$\mid (\exists\gamma\in A):\Big((\alpha\leq\gamma)\wedge(\beta\leq\gamma)\wedge(j_{\alpha,\gamma}(x)=j_{\beta,\gamma}(y))\Big)\Big\}$$

reláció ekvivalencia a $\bigsqcup_{\alpha\in A}X_\alpha := \bigcup_{\alpha\in A}(\{\alpha\}\times X_\alpha)$ *halmaz felett.*

Bizonyítás. Legyen $X:=\bigsqcup_{\alpha\in A}X_\alpha$.

Ha $(\alpha,x)\in X$, akkor ($\mathrm{IND_I}$) miatt $j_{\alpha,\alpha}(x)=x$, ezért $((\alpha,x),(\alpha,x))\in R$, vagyis az R reláció reflexív az X halmaz felett.

Ha $((\alpha,x),(\beta,y))\in R$ és $\gamma\in A$ olyan, hogy $\alpha,\beta\leq\gamma$ és $j_{\alpha,\gamma}(x)=j_{\beta,\gamma}(y)$, akkor $j_{\beta,\gamma}(y)=j_{\alpha,\gamma}(x)$, ezért $((\beta,y),(\alpha,x))\in R$. Ebből következik, hogy az R reláció szimmetrikus.

Tegyük fel, hogy $((\alpha,x),(\beta,y))\in R$ és $((\beta,y),(\gamma,z))\in R$. Legyenek $\delta',\delta''\in A$ olyanok, hogy $\alpha,\beta\leq\delta'$ és $\beta,\gamma\leq\delta''$ és $j_{\alpha,\delta'}(x)=j_{\beta,\delta'}(y)$ és $j_{\beta,\delta''}(y)=j_{\gamma,\delta''}(z)$. Az A rendezett halmaz felfelé irányítottsága miatt vehetünk olyan $\delta\in A$ elemet, amelyre $\delta',\delta''\leq\delta$. Ekkor

$$j_{\alpha,\delta}(x)\overset{(*)}{=}j_{\delta',\delta}\left(j_{\alpha,\delta'}(x)\right)=j_{\delta',\delta}\left(j_{\beta,\delta'}(y)\right)\overset{(*)}{=}j_{\beta,\delta}(y),$$
$$j_{\gamma,\delta}(z)\overset{(*)}{=}j_{\delta'',\delta}\left(j_{\gamma,\delta''}(z)\right)=j_{\delta'',\delta}\left(j_{\beta,\delta''}(y)\right)\overset{(*)}{=}j_{\beta,\delta}(y),$$

ahol a $\overset{(*)}{=}$ egyenlőségeknél az ($\mathrm{IND_{II}}$) feltételt alkalmaztuk. Tehát $\delta\in A$ olyan, hogy $\alpha,\gamma\leq\delta$ és $j_{\alpha,\delta}(x)=j_{\gamma,\delta}(z)$, így $((\alpha,x),(\gamma,z))\in R$, tehát az R reláció tranzitív. ■

32.7.3. Definíció. *Ha* $\Big((X_\alpha)_{\alpha\in A}, (j_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ *induktív rendszer, akkor a*

$$\Big(\bigsqcup_{\alpha\in A}X_\alpha\Big)/R$$

faktorhalmazt az adott induktív rendszer **induktív limeszének** *nevezzük és a*

$$\varinjlim_{\alpha,A}X_\alpha$$

szimbólummal jelöljük, ahol R az előző állításban bevezetett ekvivalencia a $\bigsqcup_{\alpha\in A} X_\alpha$ halmaz felett. Továbbá, ekkor minden $\alpha \in A$ esetén az $X_\alpha \to \bigsqcup_{\alpha\in A} X_\alpha$ kanonikus injekció, és a $\bigsqcup_{\alpha\in A} X_\alpha \to \varinjlim_{\alpha,A} X_\alpha$ kanonikus szürjekció kompozícióját j_α jelöli, tehát

$$j_\alpha : X_\alpha \to \varinjlim_{\alpha,A} X_\alpha$$

függvény.

32.7.4. Állítás. *Ha $\Big((X_\alpha)_{\alpha\in A}, (j_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\le\beta}}\Big)$ induktív rendszer és $X := \varinjlim_{\alpha,A} X_\alpha$, akkor a következő állítások ekvivalensek.*

(i) *Minden $\alpha \in A$ esetén a $j_\alpha : X_\alpha \to X$ leképezés injekció.*

(ii) *Minden $(\alpha,\beta) \in A \times A$ esetén, ha $\alpha \le \beta$, akkor a $j_{\alpha,\beta} : X_\alpha \to X_\beta$ függvény injekció.*

Bizonyítás. (i)⇒(ii) Ha $(\alpha,\beta) \in A \times A$, $\alpha \le \beta$ és $x, x' \in X_\alpha$ olyanok, hogy $j_{\alpha,\beta}(x) = j_{\alpha,\beta}(x')$, akkor $((\alpha,x),(\alpha,x')) \in R$, ahol R az előző állításban bevezetett ekvivalencia, tehát $j_\alpha(x) = j_\alpha(x')$, amiből j_α injektivitása miatt $x = x'$ következik.

(ii)⇒(i) Ha $\alpha \in A$ és $x, x' \in X_\alpha$ olyanok, hogy $j_\alpha(x) = j_\alpha(x')$, akkor j_α értelmezése alapján $((\alpha,x),(\alpha,x')) \in R$, ahol R az előző állításban bevezetett ekvivalencia, ezért R definíciója szerint van olyan $\beta \in A$, hogy $\alpha \le \beta$ és $j_{\alpha,\beta}(x) = j_{\alpha,\beta}(x')$, amiből $j_{\alpha,\beta}$ injektivitása miatt $x = x'$ következik. ■

32.7.5. Állítás. *Legyen $\Big((X_\alpha)_{\alpha\in A}, (j_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\le\beta}}\Big)$ induktív rendszer és $X := \varinjlim_{\alpha,A} X_\alpha$.*

a) *Minden $\alpha, \beta \in A$ esetén, ha $\alpha \le \beta$, akkor a következő diagram kommutatív:*

$$\begin{tikzcd} X_\alpha \arrow[r, "j_{\alpha,\beta}"] \arrow[dr, "j_\alpha"'] & X_\beta \arrow[d, "j_\beta"] \\ & X \end{tikzcd} .$$

b) *Ha X' halmaz és $(f_\alpha)_{\alpha\in A}$ olyan rendszer, hogy minden $\alpha \in A$ esetén $f_\alpha : X_\alpha \to X'$ függvény, és minden $\alpha, \beta \in A$ esetén, ha $\alpha \le \beta$, akkor a következő diagram kommutatív:*

$$\begin{tikzcd} X_\alpha \arrow[r, "j_{\alpha,\beta}"] \arrow[dr, "f_\alpha"'] & X_\beta \arrow[d, "f_\beta"] \\ & X' \end{tikzcd} ,$$

akkor létezik egyetlen olyan $f : X \to X'$ függvény, minden $\alpha \in A$ esetén a következő diagram kommutatív:

$$\begin{tikzcd} X_\alpha \arrow[r, "j_\alpha"] \arrow[dr, "f_\alpha"'] & X \arrow[d, "f"] \\ & X' \end{tikzcd} ,$$

Bizonyítás. a) Legyen $\widetilde{X} := \bigsqcup_{\alpha\in A} X_\alpha$ és R az előző állításban bevezetett ekvivalencia az $\widetilde{X}$ halmaz felett. Legyenek $\alpha, \beta \in A$, $\alpha \le \beta$ és $x \in X_\alpha$. Ekkor $(\alpha,x), (\beta, j_{\alpha,\beta}(x)) \in \widetilde{X}$ és

$\gamma := \beta \in A$ olyan, hogy $\alpha, \beta \leq \gamma$ és (IND$_\mathrm{I}$) miatt $j_{\alpha,\gamma}(x) = j_{\alpha,\beta}(x) = j_{\beta,\gamma}(j_{\alpha,\beta}(x))$, tehát $((\alpha, x), (\beta, j_{\alpha,\beta}(x))) \in R$, vagyis

$$j_\alpha(x) := \pi_{\widetilde{X},R}(\alpha, x) = \pi_{\widetilde{X},R}(\beta, j_{\alpha,\beta}(x)) =: j_\beta(j_{\alpha,\beta}(x)).$$

b) Legyenek $(\alpha, x), (\beta, y) \in \bigsqcup_{\alpha\in A} X_\alpha$ olyanok, hogy $((\alpha, x), (\beta, y)) \in R$. Legyen $\gamma \in A$ olyan, hogy $\alpha, \beta \leq \gamma$ és $j_{\alpha,\gamma}(x) = j_{\beta,\gamma}(y)$. Ekkor az $(f_\alpha)_{\alpha\in A}$ függvényrendszerre vonatkozó hipotézis alapján

$$f_\alpha(x) = f_\gamma(j_{\alpha,\gamma}(x)) = f_\gamma(j_{\beta,\gamma}(y)) = f_\beta(y).$$

Ez azt jelenti, hogy az R ekvivalencia részhalmaza az

$$\bigsqcup_{\alpha\in A} X_\alpha \to X'; \quad (\alpha, x) \mapsto f_\alpha(x)$$

függvény által meghatározott ekvivalenciának, ezért létezik egyetlen olyan

$$f : \Big(\bigsqcup_{\alpha\in A} X_\alpha\Big)/R \to X'$$

függvény, hogy minden $\alpha \in A$ esetén $f \circ j_\alpha = f_\alpha$. ■

32.7.6. Definíció. *Legyen* $\Big((X_\alpha)_{\alpha\in A}, (j_{\alpha,\beta})_{\substack{(\alpha,\beta)\in A\times A,\\ \alpha\leq\beta}}\Big)$ *induktív rendszer. Ha* Σ *morfikus struktúra típus és* $(s_\alpha)_{\alpha\in A}$ *olyan rendszer, hogy minden* $A \ni \alpha$*-ra* $(X_\alpha, s_\alpha) \in \tau(\Sigma)$*, akkor azt mondjuk, hogy az* $(s_\alpha)_{\alpha\in A}$ Σ*-típusú struktúra-rendszernek létezik* **induktív limesze***, az adott induktív rendszer szerint, ha* $\varinjlim_{\alpha,A} X_\alpha \in \mathrm{D}_\Sigma$*, és létezik az* $((X_\alpha, s_\alpha), j_\alpha)_{\alpha\in A}$ *rendszer által előállított* $\varinjlim_{\alpha,A} X_\alpha$ *feletti finális* Σ*-típusú struktúra; ekkor az így létrehozott* $\varinjlim_{\alpha,A} X_\alpha$ *feletti* Σ*-típusú struktúrát* $\varinjlim_{\alpha,A} s_\alpha$ *jelöli.*

33. fejezet

Iniciális és finális struktúrák kapcsolatai

33.1. Iniciális struktúrák faktorizációja

33.2. Finális struktúrák leszűkítése

33.3. Projektív limeszek induktív limeszei

33.4. Induktív limeszek projektív limeszei

34. fejezet

Kvázitopologikus struktúra típusok

34.1. Kvázitopologikus struktúra típusok értelmezése

Jelölés. Ha X és Y halmazok, $f \in \mathscr{F}(X;Y)$ és $n \in \mathbb{N}^*$, akkor

$$\overset{n}{\times} f : X^n \to Y^n; \quad (x_i)_{i \in n} \mapsto (f(x_i))_{i \in n}.$$

34.1.1. Definíció. *A Σ morfikus struktúra-típust* **kvázitopologikus struktúra-típusnak** *nevezzük, ha létezik egyetlen olyan $n \in \mathbb{N}^*$, hogy teljesülnek a következők:*

$(\mathrm{QTS_I})$ *Minden $X \in \mathrm{D}_\Sigma$ esetén $\Sigma_X \subseteq \mathscr{P}(\mathscr{P}(X^n))$.*

$(\mathrm{QTS_{II}})$ *Minden $(X, s), (X', s') \in \tau(\Sigma)$ esetén*

$$\mathrm{Mor}_\Sigma((X,s),(X',s')) = \left\{ f \in \mathscr{F}(X;X') \mid \{(\overset{n}{\times} f)^{-1}\langle A' \rangle | A' \in s'\} \subseteq s \right\}.$$

Ha $n \in \mathbb{N}^*$ az a szám, amelyre $(\mathrm{QTS_I})$ és $(\mathrm{QTS_{II}})$ teljesül, akkor azt mondjuk, hogy Σ n**-ed rendű** *kvázitopologikus struktúra-típus.*

34.1.2. Állítás. *Ha Σ olyan struktúra-típus, hogy létezik olyan $X \in \mathrm{D}_\Sigma$ és $s \in \Sigma_X$ és $A \in s$, amelyre $A \neq \emptyset$, akkor legfeljebb egy olyan $n \in \mathbb{N}^*$ létezik, amelyre $(\mathrm{QTS_I})$ és $(\mathrm{QTS_{II}})$ teljesül.*

Bizonyítás. ■

Az előző állításban megfogalmazott tulajdonsága minden fontosabb struktúra-típusnak megvan, ezért a kvázitopologikus struktúra-típusok definíciójában n-re megkövetelt egyértelműségi feltétel gyakorlatilag felesleges, de a "patologikus" esetek létezése miatt szükséges.

34.1.3. Állítás. *Legyen Σ n-ed rendű kvázitopologikus struktúra-típus. Ekkor minden $X, X' \in \mathrm{D}_\Sigma$ esetén minden $f : X \to X'$ bijekcióra és $s \in \Sigma_X$ struktúrára:*

$$\Sigma(f)s = \left\{ (\overset{n}{\times} f)\langle A \rangle \mid A \in s \right\}.$$

Bizonyítás. ■

Az előző állítás szerint a kvázitopologikus struktúra-típusok konstrukciójának legáltalánosabb módja a következő. Rögzítünk egy $n \in \mathbb{N}^*$ természetes számot és egy ekvipotenciálisan telített D osztályt. Ezután minden $X \in D$ halmazhoz hozzárendelünk egy $\Sigma_X \subseteq \mathscr{P}(\mathscr{P}(X^n))$ halmazt úgy, hogy ha $X, Y \in D$ és $f : X \to Y$ bijekció és $s \in \Sigma_X$, akkor

$$\left\{ \, (\overset{n}{\times} f)\langle A \rangle \mid A \in s \, \right\} \in \Sigma_Y.$$

Ezután legyen $\mathrm{D}_\Sigma := D$, és minden $X, Y \in D$ halmazra és $f : X \to Y$ bijekcióra és $s \in \Sigma_X$ elemre

$$\Sigma(f) := \left\{ \, (\overset{n}{\times} f)\langle A \rangle \mid A \in s \, \right\}.$$

Könnyen látható, hogy Σ struktúra-típus. Végül, minden $(X, s), (X', s') \in \tau(\Sigma)$ esetén legyen

$$\mathrm{Mor}_\Sigma((X, s), (X', s')) := \left\{ \, f \in \mathscr{F}(X; X') \mid \{(\overset{-1}{\overset{n}{\times} f})\langle A' \rangle | A' \in s'\} \subseteq s \, \right\}.$$

Nyilvánvaló, hogy ekkor Σ morfikus struktúra-típus és n-re és Σ-ra ($\mathrm{QTS_I}$) és ($\mathrm{QTS_{II}}$) teljesül. Ha Σ egyértelműen határozza meg n-et (ami például teljesül akkor, ha léteznek olyan $X \in \mathrm{D}_\Sigma$, $s \in \Sigma_X$ és $A \in s$, hogy $A \neq \emptyset$), akkor Σ n-ed rendű kvázitopologikus struktúra-típus.

34.2. Természetes rendezés kvázitopologikus struktúrák között

34.2.1. Állítás. *Legyen Σ n-ed rendű kvázitopologikus struktúra-típus. Ekkor minden $X \in \mathrm{D}_X$ esetén a Σ_X halmaz feletti természetes rendezés egyenlő a Σ_X halmaz feletti $\subseteq$ relációval.*

Bizonyítás. Ha $X \in \mathrm{D}_X$ és $s, s' \in \Sigma_X$, akkor a Σ_X halmaz feletti természetes rendezés definíciója és ($\mathrm{QTS_{II}}$) szerint:

$$s \leq s' \Leftrightarrow \mathrm{id}_X \in \mathrm{Mor}_\Sigma((X, s'), (X, s)) \Leftrightarrow \{(\overset{-1}{\overset{n}{\times} \mathrm{id}_X})\langle A \rangle | A \in s\} \subseteq s' \Leftrightarrow s \subseteq s'$$

teljesül, hiszen nyilvánvalóan $\overset{n}{\times} \mathrm{id}_X = \mathrm{id}_{X^n}$. ∎

34.2.2. Definíció. *Azt mondjuk, hogy a Σ kvázitopologikus struktúra-típus* **metszet-tulajdonságú**, *ha teljesül rá a következő állítás.*

(SEC) *Minden $X \in \mathrm{D}_\Sigma$ esetén, bármely Σ_X-ben haladó nem üres $(s_i)_{i \in I}$ rendszerre $\bigcap\limits_{i \in I} s_i \in \Sigma_X$.*

34.2.3. Következmény. *Legyen Σ olyan kvázitopologikus struktúra-típus, amely metszet-tulajdonságú.*

a) *Minden $X \in \mathrm{D}_\Sigma$ esetén teljesül az, hogy minden Σ_X-ben haladó nem üres $(s_i)_{i \in I}$ rendszernek létezik infimuma a Σ_X halmaz feletti természetes rendezés szerint, és ez az infimum egyenlő $\bigcap\limits_{i \in I} s_i$-vel.*

b) *Ha $X \in \mathrm{D}_\Sigma$ és $\Sigma_X \neq \emptyset$, akkor Σ_X-nek létezik legkisebb eleme a Σ_X halmaz feletti természetes rendezés szerint.*

c) *Ha $X \in \mathrm{D}_\Sigma$ olyan, hogy a Σ_X halmaznak létezik legnagyobb eleme a természetes rendezés szerint, akkor Σ_X a természetes rendezéssel ellátva* **teljes korlátos háló**.

Bizonyítás. Az a) állítás azonnal következik az előző állításból, és b) nyilvánvaló következménya a)-nak. Ha Σ_X-nek van legnagyobb eleme a természetes rendezés szerint és az $(s_i)_{i\in I}$ rendszer Σ_X-ben halad, akkor az $\bigcup\limits_{i\in I} s_i$ halmazt tartalmazó Σ_X-beli elemek halmaza nem üres (mert az előző állítás szerint Σ_X legnagyobb eleme benne van ebben a halmazban), és ekkor az $\bigcup\limits_{i\in I} s_i$ halmazt tartalmazó Σ_X-beli elemek metszete a metszet-tulajdonság miatt nyilvánvalóan az $(s_i)_{i\in I}$ rendszer szuprémuma lesz Σ_X-ben a természetes rendezés szerint. ■

Megjegyezzük, hogy a két legfontosabb kvázitopologikus struktúra-típus (ti. a topologikus és az uniform struktúra-típus) metszet-tulajdonságú, de van olyan fontos kvázitopologikus struktúra-típus, hogy nem minden Σ_X struktúra halmaznak létezik legnagyobb eleme a természetes rendezés szerint.

34.3. Kvázitopologikus struktúra képe és inverz képe

34.3.1. Állítás. *Legyen Σ n-ed rendű kvázitopologikus struktúra-típus, $(X, s) \in \tau(\Sigma)$, $X' \in \mathrm{D}_\Sigma$ és $f : X' \to X$ függvény. Legyen*

$$s'_* := \left\{ \; (\overset{n}{\times} f)^{-1}\langle A\rangle \mid A \in s \; \right\}.$$

a) *Ha létezik az s struktúra f által létesített Σ-típusú s' inverz képe, akkor $s'_* \subseteq s'$.*

b) *Ha $s'_* \in \Sigma_X$, akkor létezik az s struktúra f által létesített Σ-típusú s' inverz képe és $s'_* = s'$.*

Bizonyítás. ■

34.3.2. Következmény. *Legyen Σ n-ed rendű kvázitopologikus struktúra-típus, $(X, s) \in \tau(\Sigma)$ és $Y \subseteq X$. Legyen*

$$s_* := \{ \; A \cap Y^n \mid A \in s \; \}.$$

a) *Ha létezik az $s|Y$ Σ-típusú altérstruktúra, akkor $s_* \subseteq s|Y$.*

b) *Ha $Y \in \mathrm{D}_\Sigma$ és $s_0 \in \Sigma_Y$, akkor létezik az $s|Y$ Σ-típusú altérstruktúra és $s_* = s|Y$.*

Bizonyítás. ■

34.3.3. Állítás. *Legyen Σ n-ed rendű kvázitopologikus struktúra-típus, $(X, s) \in \tau(\Sigma)$, $X' \in \mathrm{D}_\Sigma$ és $f : X \to X'$ függvény. Legyen*

$$s'_* := \left\{ \; A' \in \mathscr{P}((X')^n) \mid (\overset{n}{\times} f)^{-1}\langle A'\rangle \in s \; \right\}.$$

a) *Ha létezik az s struktúra f által létesített Σ-típusú s' képe, akkor $s' \subseteq s'_0$.*

b) *Ha $s'_* \in \Sigma_{X'}$, akkor létezik az s struktúra f által létesített Σ-típusú s' képe és $s'_* = s'$.*

Bizonyítás. ■

34.3.4. Következmény. *Legyen Σ n-ed rendű kvázitopologikus struktúra-típus, $(X,s) \in \tau(\Sigma)$ és R ekvivalenciareláció X felett. Legyen*

$$s_* := \left\{ A \in \mathscr{P}((X/R)^n) \mid (\overset{n}{\times}\mathrm{pr}_{X,R})^{-1}\langle A\rangle \in s \right\}.$$

a) *Ha létezik az s/R Σ-típusú faktorstruktúra, akkor $s/R \subseteq s_*$.*

b) *Ha $X/R \in \mathrm{D}_\Sigma$ és $s_* \in \Sigma_{X/R}$, akkor létezik az s/R Σ-típusú faktorstruktúra és $s_* = s/R$.*

Bizonyítás. ■

34.4. Σ-homomorfizmusok kvázitopologikus terek között

34.5. Topologikus struktúrák

34.6. Uniform struktúrák

34.7. Metrikus struktúrák

35. fejezet

Algebrai struktúra típusok

36. fejezet

Univerzalitási tulajdonságok

36.1. Univerzalitási tulajdonságok értelmezése

36.2. Univerzális objektum egyértelműsége

36.3. Univerzális objektum létezése

36.4. Speciális topologikus univerzalitási tulajdonságok

36.5. Speciális algebrai univerzalitási tulajdonságok

37. fejezet

Rendezett struktúra típusok

38. fejezet

Topologikus algebrai struktúra típusok