Eötvös Loránd Tudományegyetem
Természettudományi Kar

A Hasse–Minkowski-tétel

BSc szakdolgozat

Írta: Bognár Barna
matematika BSc, matematikus szakirány

Témavezető: Zábrádi Gergely, egyetemi adjunktus
Algebra és Számelmélet tanszék

Budapest, 2013.

Köszönetnyilvánítás
Ezúton szeretnék köszönetet mondani témavezetőmnek, Zábrádi Gergelynek, az érdekes témafelvetésért, hogy a bennem felmerült legvadabb kérdésekre is igyekezett választ találni, és minden egyéb segítségért, amit e dolgozat megírásához nyújtott.
Szeretnék továbbá köszönetet mondani a családomnak, barátaimnak és mindenkinek, aki elviselni kényszerült, amíg e dolgozatot írtam.

Tartalomjegyzék

Bevezetés

A kvadratikus alakok története egészen a matematika ismert történetének legkorábbi szakaszáig nyúlik vissza. Az első problémák, amiket kvadratikus alakokkal kapcsolatban még az ókorban vizsgáltak, bizonyos konkrét, egész együtthatós kvadratikus alakok értékkészletének meghatározására, illetve gyökeinek megtalálására irányultak – elég csak a pitagoraszi számhármasok keresésére gondolnunk, ami voltaképpen az $x^2 + y^2 - z^2$ kvadratikus alak (pozitív) egész gyökeinek keresését jelenti.

Ilyen jellegű problémák időről időre feltűnnek a matematikusa történetében: Brahmagupta, indiai matematikus 628-ban már vizsgálja az $x^2 - ny^2$ egész számok feletti kvadratikus alak értékkészletét, speciálisan a Pell-egyenlet ($x^2 - ny^2 = 1$) megoldhatóságát is. Európából említhetnénk Pierre de Fermat munkásságát, aki 1640-ben leírta, hogy egy prímszám pontosan akkor állítható elő két négyzetszám összegeként (vagyis pontosan akkor vétetik fel az $x^2 + y^2$ egészek felett értelmezett kvadratikus alak által), ha kongruens 1-gyel modulo 4. (Egyébként nem tudjuk, Fermat be is bizonyította-e a tételt, ugyanis a tételt kijelentésként és nem problémaként fogalmazta meg, de nem maradt fent bizonyítás tőle. Az első ismert bizonyítást Euler írta le, 1749-ben.)

Mint látható, ezek a problémák mind bizonyos egész együtthatós kvadratikus alakok egész megoldásaival foglalkoznak. Mivel ismert, hogy az egész számok feletti kvadratikus alakok vizsgálata visszavezethető a racionális számok feletti kvadratikus alakok vizsgálatára, így egyáltalán nem meglepő, hogy egy idő után (mikor Lagrange és Euler a kétváltozós kvadratikus alakokra vonatkozó kutatásai nyomán a kvadratikus alakok általános elmélete is kialakulóban volt) a témával kapcsolatos számelméleti kutatások a racionális számok felett értelmezett kvadratikus alakok vizsgálata felé mozdultak el.

Így a 18-19. században a racionális (illetve egész) kvadratikus alakokkal kapcsolatos kutatás fő problémái a kvadratikus alakok ekvivalenciaosztályainak meghatározása, az egyes kvadratikus alkok értékkészletének meghatározása, az adott értéket kiadó pontok számának meghatározása, illetve a nemtriviális gyökök meghatározása lettek.

A kvadratikus alakok modern tárgyalásának kezdetei Hermann Minkowski német matematikus munkásságára vezethetők vissza. Minkowski az 1880-as években több különböző publikációt is megjelentetett, melyekben felépítette a racionális kvadratikus alakok elméletét. Végül 1890-ben belátta, hogy a racionális kvadratikus alakok ekvivalenciaosztályait egyértelműen meghatározzák bizonyos, a prímekkel kapcsolatban álló, invariánsok, amiket ő C_p-nek nevezett.

Nem sokkal később, 1897-ben Kurt Hensel bevezette a p-adikus számok fogalmát, ami elképesztő hatással volt a számelmélet fejlődésére. A kvadratikus alakok elméletében Helmut Hasse, Hensel egyik tanítványa, az elsők között alkalmazta mestere eredményeit. Ő fogalmazta át Minkowski eredményét, 1921-ben, a p-adikus kvadratikus alakokra, ami így azt mondja, hogy két racionális kvadratikus alak pontosan akkor ekvivalens egymással, ha minden p prímre mint p-adikus kvadratikus alakok ekvivalensek és mint valós kvadratikus alakok is ekvivalensek. Sőt, Hasse még többet bizonyított: bebizonyította, hogy bármely racionális számot egy racionális kvadratikus alak pontosan akkor vesz fel valamely nemnulla pontban, ha minden p prímre felveszi egy nemnulla pontban, mint $\mathbb{Q}_p$ feletti kvadratikus alak, és felveszi egy nemnulla pontban, mint $\mathbb{R}$ feletti kvadratikus alak. Nem sokkal később, 1924-ben, maga Hasse általánosította ezt az erősebb eredményt $\mathbb{Q}$ tetszőleges véges bővítésére.

A 20. század közepén Hasse eredményeinek különböző általánosításai foglalkoztatták a terület szakértőit. Az egyik legtermészetesebb általánosítás a 2-nél magasabb fokú homogén polinomokra való kiterjesztés lett volna – azonban Ernst Selmer, norvég matematikus 1951-ben belátta, hogy ez már a harmadfokú homogén polinomokra sem működik: a $3x^3 + 4y^3 + 5z^3$ polinomnak van

nemtriviális gyöke mind $\mathbb{R}$, mind a $\mathbb{Q}_p$ felett minden p prímre, azonban $\mathbb{Q}$ felett csak a triviális $(0,0,0)$ vektorra vesz fel 0-t értékként.

A '60-as években belátták azt is, hogy a tétel semmilyen alakja nem terjeszthető ki általában egy K testre, de belátták azt is, hogy Minkowski eredeti eredménye (a kvadratikus alakok ekvivalenciájáról), illetve Hasse erősebb eredménye (a kvadratikus alakok által felvett értékekről) nem minden test felett teljesül egyszerre – vannak testek, amikre csak Minkowski gyengébb állítása igaz.

Mindezen problémák ellenére az úgynevezett aritmetikai geometriában ma is fontos szerepet játszik az úgynevezett Hasse-elv, vagyis hogy egy polinomegyenlet „globális" (alapvetően $\mathbb{Q}$ vagy valamely véges bővítése feletti) megoldásait az egyenlet „lokális" (a globális test megfelelő bővítései – $\mathbb{Q}$ mellett a $\mathbb{Q}_p$-k és $\mathbb{R}$ – feletti) megoldásain keresztül keressük. Az ezzel kapcsolatos módszerek számtalan változatát alkalmazzák ma is az algebrai számelmélet kapcsolódó területein, és a téma nyitott kérdéseinek sokasága várja még megválaszolását.

Mint a fentiekből látszik, Minkowski és Hasse eredményei sokféle erősebb-gyengébb alakban megfogalmazhatóak. Ezeknek az eredményeknek különböző formáit szokták Hasse–Minkowski-tételként emlegetni.

A mi célunk az lesz, hogy a három éves egyetemi tananyagra támaszkodva – minden elméletet felépítve, ami az egyetemi tananyagban nem szerepel, de minél kevesebbet ismételve az ott már megismert tényeket – belássuk a Hasse–Minkowski-tétel azon formáját, mely szerint egy racionális együtthatós kvadratikus alaknak pontosan akkor van nemtriviális gyöke $\mathbb{Q}$ felett, ha van neki $\mathbb{R}$ felett, és $\mathbb{Q}_p$ felett minden p-re, illetve megvizsgáljuk ennek bizonyos közvetlen következményeit (köztük a $\mathbb{Q}$-ra vonatkozó tétel másik említett alakjait is).

Ennek megfelelően elsőként fel kell építenünk a p-adikus számok elméletét, majd meg kell vizsgálnunk általában a kvadratikus alakok, illetve speciálisan a racionális, p-adikus és valós kvadratikus alakok bizonyos tulajdonságait. Munkánk ezen felül kiegészül még több olyan fejezettel, amik, bár első ránézésre úgy tűnik, nem kapcsolódnak szorosan a dolgozat fő csapásához, komoly segítséget jelentenek (néhol egyenesen nélkülözhetetlenek) a Hasse–Minkowski-tétel megértéséhez, illetve a bizonyítását előkészítő állítások belátásához.

1. fejezet

Véges testek

Mindenek előtt vizsgáljuk meg a véges testek néhány tulajdonságát, mert ezekre szükségünk lesz a későbbiekben (a p-adikus számok, illetve a Hilbert-szimbólum vizsgálata során). Tulajdonképpen elegendeő lenne a prím elemszámú testek vizsgálata (a későbbiekben csak ezt fogjuk használni), ám mivel nagyrészt olyan eredményeket fogalmazunk meg, amik általában is igazak a véges testekben (és az általánosabb bizonyítás sem okoz komoly nehézséget), ezért a legtöbb állítást általánosan bizonyítjuk.

A fejezet során a következő jelöléseket használjuk: p mindig egy prímszámot, f egy tetszőleges pozitív egész számot jelöl. A p^f értéket q-nak fogjuk nevezni. $\mathbb{F}_q$-n természetesen a q elemű testet, K^*-on pedig a K test multiplikatív csoportját értjük.

1.1. Néhány tétel véges testekről

Először vizsgáljuk meg a véges testek néhány tulajdonságát:

1.1. Lemma. *Legyen p egy prím, f és u egy-egy pozitív egész szám, q pedig jelölje p^f-et. Ekkor $\sum_{x\in\mathbb{F}_q} x^u$ értéke -1, ha u osztható $(q-1)$-el, és 0 egyébként.*

Bizonyítás. Ha u osztható $(q-1)$-el, akkor minden $\mathbb{F}_q^*$-beli x-re $x^u = 1$ teljesül, hiszen $\mathbb{F}_q^*$ egy $(q-1)$ rendű ciklikus csoport. Így:

$$\sum_{x\in\mathbb{F}_q} x^u = 0^u + \sum_{x\in\mathbb{F}_q^*} x^u = (q-1)\cdot 1 = -1.$$

Ha u nem osztható $(q-1)$-el, akkor van $\mathbb{F}_q^*$-nek egy olyan eleme (y), amire $y^u \neq 1$ (ilyen például $\mathbb{F}_q^*$ generátoreleme). Ekkor:

$$\sum_{x\in\mathbb{F}_q} x^u = 0^u + \sum_{x\in\mathbb{F}_q^*} x^u = \sum_{x\in\mathbb{F}_q^*} (yx)^u = y^u \cdot \sum_{x\in\mathbb{F}_q^*} x^u\,.$$

Ebből:

$$(1-y^u)\cdot \sum_{x\in\mathbb{F}_q^*} x^u = 0, \text{ de } y^u \neq 1, \text{ így } \sum_{x\in\mathbb{F}_q^*} x^u = 0.$$

q.e.d.

1.2. Tétel (Chevalley-Warning)**.** *Legyenek $f_1, f_2, \ldots, f_k$ $\mathbb{F}_q$ feletti n változós polinomok, melyek közül nem mindegyik konstans 0. (q valamely p prímszám egy hatványát jelöli.) Tegyük fel továbbá, hogy $\sum_{i=1}^{k} \deg f_i < n$. Jelölje V a polinomok közös gyökeinek halmazát $\mathbb{F}_q^n$-ben. Ekkor $|V| \equiv 0 \pmod{p}$.*

Bizonyítás. Tekintsük a következő függvényt: $P = \prod_{i=1}^{k}(1-f_i^{q-1})$. Ekkor minden $x \in V$-re, minden $i = 1, \ldots, k$ számra $f_i(x)=0$, így $P(x) = \prod_{i=1}^{k}(1 - f_i(x)^{q-1}) = 1$. És minden $x \in \mathbb{F}_q^n \setminus V$-re létezik egy olyan $j = 1, \ldots, k$ szám, amire $f_j(x) \neq 0$, így $f_j(x)^{q-1} = 1$ (hiszen $\mathbb{F}_q^*$ $(q-1)$ elemű ciklikus csoport), azaz $P(x) = 0$. Tehát az így definiált P függvény valójában V karakterisztikus függvénye. Mivel $\mathbb{F}_q$ karakterisztikája p, és a P függvény V karakterisztikus függvénye, ezért $\sum_{x\in\mathbb{F}_q^n} P(x) \equiv |V| \pmod{p}$. Vagyis elegendő látni, hogy $\sum_{x\in\mathbb{F}_q^n} P(x) = 0$.

Mivel feltettük, hogy $\sum_{i=1}^{k} \deg f_i < n$, ezért $\deg P < n(q-1)$, azaz $P(x_1, \ldots, x_n)$ $\prod_{i=1}^{n} x_i^{\alpha_i}$ alakú monomok lineáris kombinációja, ahol az α_i-k nemnegatív egész számok, és $\sum_{i=1}^{n} \alpha_i < n(q-1)$. Ebből következik, hogy van egy olyan $j = 1, \ldots, n$ szám, amire $\alpha_j < q-1$. Feltehető, hogy $j = 1$.

Ha $\alpha_1 = 0$, akkor:

$$\sum_{x_1,\ldots,x_n\in\mathbb{F}_q} \prod_{i=1}^{n} x_i^{\alpha_i} = \left(\sum_{x_1\in\mathbb{F}_q} 1\right)\left(\sum_{x_2,\ldots,x_n\in\mathbb{F}_q} \prod_{i=2}^{n} x_i^{\alpha_i}\right) = q \cdot \left(\sum_{x_2,\ldots,x_n\in\mathbb{F}_q} \prod_{i=2}^{n} x_i^{\alpha_i}\right) = 0.$$

Ha $\alpha_1 \neq 0$, akkor, α_1 pozitív, és kisebb, mint $(q-1)$, így nem osztható $(q-1)$-el, tehát az előző lemma alapján:

$$\sum_{x_1,\ldots,x_n\in\mathbb{F}_q} \prod_{i=1}^{n} x_i^{\alpha_i} = \left(\sum_{x_1\in\mathbb{F}_q} x_1^{\alpha_1}\right)\left(\sum_{x_2,\ldots,x_n\in\mathbb{F}_q} \prod_{i=2}^{n} x_i^{\alpha_i}\right) = 0 \cdot \left(\sum_{x_2,\ldots,x_n\in\mathbb{F}_q} \prod_{i=2}^{n} x_i^{\alpha_i}\right) = 0.$$

Vagyis P minden m monomjára $\sum_{x\in\mathbb{F}_q^n} m(x) = 0$, így $\sum_{x\in\mathbb{F}_q^n} P(x) = 0$. Ezzel a tételt bebizonyítottuk.

q.e.d.

1.3. Következmény. Ha a tétel feltételeit kielégítő polinomoknak 0 a konstans tagjuk, akkor van egy nemtriviális közös gyökük, hiszen a 0 mindenképpen közös gyök, és $1 \not\equiv 0 \pmod{p}$

1.4. Következmény. Minden véges test fölötti, legalább három változós kvadratikus alak rendelkezik nemtriviális gyökkel.

1.5. Tétel. *Bármely p prímre, f pozitív egészre, és $q = p^f$ számra $\mathbb{F}_q^{*2}$ egy 2 indexű részcsoport $\mathbb{F}_q^*$-ban, ha p páratlan, és 1 indexű, ha $p = 2$.*

Bizonyítás. Tudjuk, hogy $\mathbb{F}_q^*$ egy $(q-1)$ elemű ciklikus csoport. Legyen egy generátoreleme x. Ekkor $\mathbb{F}_q^{*2} = \{x^2, x^4, \ldots, x^{2(q-1)}\} = \{x^{2k} | k = 1, 2, \ldots, (q-1)\}$.

Ha q páros (azaz $p = 2$), akkor $(q-1)$ páratlan, vagyis a $(q-1)$-nél nagyobb kitevőket mod $q-1$ tekintve különböző páratlan számokat kapunk (ha a maradékosztályokat a 1 és $(q-1)$ közötti számokkal reprezentáljuk). Vagyis: $\mathbb{F}_q^{*2} = \{x^2, x^4, \ldots, x^{q-2}, x, x^3, \ldots, x^{q-1}\} = \mathbb{F}_q^*$

Ha q páratlan (azaz $p > 2$), akkor $(q-1)$ páros, vagyis a $(q-1)$-nél nagyobb kitevőket mod $q-1$ tekintve páros számokat kapunk (függetlenül attól, hogy a mradékosztályokat milyen számokkal reprezentáljuk). Vagyis csak x páros kitevős hatványai lehetnek négyzetszámok. Ezek pedig mind négyzetszámok, hiszen minden $k = 0, \ldots, q-1$ számra $x^{2k} = (x^k)^2$. És mivel $\mathbb{F}_q^*$ egy páros rendű ciklikus csoport, így $|\mathbb{F}_q^{*2} : \mathbb{F}_q^*| = 2$ adódik.

q.e.d.

Megjegyzés. Ha p páratlan, akkor $\mathbb{F}_q^{*2} = \{x^k |\ k \text{ páros}\}$, ami pont az $\mathbb{F}_q^*$-ot $Z_2 = (\{1, -1\}, \cdot)$-ba képző $z \mapsto z^{\frac{q-1}{2}}$ csoporthomomorfizmus magtere. Így felírható a következő egzakt sorozat:

$$1 \quad \longrightarrow \quad \mathbb{F}_q^{*2} \quad \longrightarrow \quad \mathbb{F}_q^* \quad \longrightarrow \quad Z_2 \quad \longrightarrow \quad 1.$$

1.2. A Legendre-szimbólumok

Ebben a szakaszban a számelméletből ismert Legendre-szimbólumot kiterjesztjük $\mathbb{F}_q$-ra, illetve belátjuk, hogy tulajdonságai ettől nem változnak.

Először adjuk meg az új definíciót:

1.6. Definíció (Legendre-szimbólum)**.** *Legyen p egy prímszám, q egy (pozitív egész kitevős) hatványa, x pedig $\mathbb{F}_q$ egy eleme. Definiáljuk a $\left(\frac{x}{q}\right)$ Legendre-szinmólumot a következő képpen:*

$$\left(\frac{x}{q}\right) = \begin{cases} 1 & , \text{ ha } x \text{ négyzetszám } \mathbb{F}_q^*\text{-ban} \\ 0 & , \text{ ha } x = 0 \\ -1 & , \text{ ha } x \text{ nem négyzetszám } \mathbb{F}_q^*\text{-ban} \end{cases}.$$

Ez nyilván a páratlan prímekre definiált (hagyományos) Legendre-szimbólum kiterjesztése lesz.

Tetszőleges $x, y \in \mathbb{F}_q$-ra teljesül, hogy $\left(\frac{xy}{q}\right) = \left(\frac{x}{q}\right)\left(\frac{y}{q}\right)$, hiszen $p = 2$-re $\left(\frac{z}{q}\right)$ minden nemnulla z-re 1, $p > 2$-re pedig $\mathbb{F}_q^*$ generátorelemének páros kitevős hatványaira 1, a páratlan kitevősökre -1.

Ha $x \in \mathbb{F}_q^*$, és y x négyzetgyöke $\mathbb{F}_q$ algebrai lezártjában (Ω-ban), akkor $\left(\frac{x}{q}\right) = y^{q-1}$, mivel:

$x \in \mathbb{F}_q^*$ esetén $y^{2(q-1)} = x^{q-1} = 1$, tehát $y^{q-1} = \pm 1$. Mivel Ω algebrailag zárt, ezért a $z^{q-1} - 1$ polinomnak pontosan $(q-1)$ gyöke van (multiplicitással számolva) Ω-ban. Viszont $\mathbb{F}_q^* \subset \Omega$, és $\mathbb{F}_q^*$ minden eleme gyöke a polinomnak (és $\mathbb{F}_q^*$ pont $(q-1)$ elemű), tehát Ω egy eleme pontosan akkor $\mathbb{F}_q^*$-beli, ha gyöke $(z^{q-1}-1)$-nek. Ez pedig x mindkét négyzetgyökére egyszerre teljesül, hiszen ezek egymás ellentettjei. Ha pedig $x = 0$, akkor $y = 0$. Tehát $\left(\frac{x}{q}\right)$ valóban megegyezik y^{q-1}-el.

Ebből világosan látszik, hogy $\left(\frac{1}{q}\right) = 1$, és $\left(\frac{-1}{q}\right) = \sqrt{-1}^{q-1} = (-1)^{\frac{q-1}{2}}$, ha q páratlan, és 1, ha q páros (hiszen ez utóbbi esetben $\mathbb{F}_q$ minden eleme négyzetelem). $\left(\frac{2}{q}\right)$-ról pedig a következő látható:

Legyen α egy primitív 8-adik egységgyök Ω-ban. Legyen $y = \alpha + \alpha^{-1}$. Ekkor $\alpha^4 = -1$, így $\alpha^2 + \alpha^{-2} = 0$, amiből $y^2 = 2$ következik. Tehát (mint fönt láttuk) $\left(\frac{2}{q}\right) = y^{q-1}$.

Tudjuk, hogy $y^q = \alpha^q + \alpha^{-q}$. Ebből:

Ha $q \equiv \pm 1 \pmod 8$, akkor $y^q = \alpha + \alpha^{-1} = y$, tehát $\left(\frac{2}{q}\right) = y^{q-1} = 1$.

Ha $q \equiv \pm 5 \pmod 8$, akkor $y^q = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y$ (mivel $\alpha^4 = -1$), tehát $\left(\frac{2}{q}\right) = y^{q-1} = -1$.

Ha pedig q páros, akkor $2 = 0$, tehát $\left(\frac{2}{q}\right) = 0$. (Mellesleg ez megkapható a páratlan esetekhez hasonlóan is: $q = 2$-re $y^2 = \alpha^2 + \alpha^{-2}$, amiről már láttuk, hogy 0, $q = 4$-re $y^4 = \alpha^4 + \alpha^{-4} = -2 = 0$, $q > 4$-re pedig q osztható 8-al, tehát $y^q = \alpha^q + \alpha^{-q} = 2 = 0$. Tehát mindhárom esetben $y = 0$-t kapunk.)

Ekkor bevezethetjük a következő jelöléseket:

$\varepsilon(q) = 1, 0$, hogy $\left(\frac{-1}{q}\right) = (-1)^{\varepsilon(q)}$ teljesüljön, illetve $\omega(q) = 1, 0$, hogy $\left(\frac{2}{q}\right) = (-1)^{\omega(q)}$ teljesüljön (ekkor persze fel kell tennünk, hogy p páratlan).

1.7. Tétel (A Gauss-féle kvadratikus reciprocitási tétel)**.** *Legyenek p és r különböző páratlan prímek. Ekkor:*

$$\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right)(-1)^{\varepsilon(p)\varepsilon(r)}.$$

Bizonyítás. Legyen, Ω $\mathbb{F}_p$ algebrai lezártja, legyen $w \in \Omega$ egy primitív r-edik egységgyök. Mivel $w^r = 1$, ezért $x \in \mathbb{F}_r$ mellett w^x jóldefiniált (mivel x felfogható egész számként). Ekkor:

$$\sum_{x \in \mathbb{F}_r} w^x = w \sum_{x \in \mathbb{F}_r} w^x,$$

így (mivel $w \neq 1$)

$$\sum_{x \in \mathbb{F}_r} w^x = 0.$$

Most definiáljuk a következő elemet:

$$y = \sum_{x \in \mathbb{F}_r} \left(\frac{x}{r}\right) w^x.$$

A bionyításhoz még szükségünk lesz két lemmára:

1.8. Lemma. $y^2 = (-1)^{\varepsilon(r)} r$.

Bizonyítás.

$$y^2 = \left(\sum_{x\in\mathbb{F}_r} \left(\frac{x}{r}\right) w^x\right)\left(\sum_{z\in\mathbb{F}_r} \left(\frac{z}{r}\right) w^z\right) = \sum_{x,z\in\mathbb{F}_r} \left(\frac{xz}{r}\right) w^{x+z} = \sum_{u\in\mathbb{F}_r} w^u \sum_{t\in\mathbb{F}_r} \left(\frac{t(u-t)}{r}\right)$$

$\left(\frac{0}{r}\right) = 0$, így:

$$\begin{aligned}\sum_{t\in\mathbb{F}_r} \left(\frac{t(u-t)}{r}\right) &= \sum_{t\in\mathbb{F}_r^*} \left(\frac{t(u-t)}{r}\right) = \sum_{t\in\mathbb{F}_r^*} \left(\frac{-t^2}{r}\right)\left(\frac{1-ut^{-1}}{r}\right) = \sum_{t\in\mathbb{F}_r^*} \left(\frac{-1}{r}\right)\left(\frac{t^2}{r}\right)\left(\frac{1-ut^{-1}}{r}\right) = \\ &= \sum_{t\in\mathbb{F}_r^*} (-1)^{\varepsilon(r)} 1 \left(\frac{1-ut^{-1}}{r}\right) =: (-1)^{\varepsilon(r)} C_u,\end{aligned}$$

$$y^2 = (-1)^{\varepsilon(r)} \sum_{u\in\mathbb{F}_r} C_u w^u.$$

Ekkor: $C_0 = \sum_{t\in\mathbb{F}_r^*} \left(\frac{1}{r}\right) = r-1$, $u \neq 0$-ra pedig:

$$C_u = \sum_{t\in\mathbb{F}_r^*} \left(\frac{1-ut^{-1}}{r}\right) = \sum_{s\in\mathbb{F}_r, s\neq 1} \left(\frac{s}{r}\right) = \sum_{s\in\mathbb{F}_r} \left(\frac{s}{r}\right) - \left(\frac{1}{r}\right) = \sum_{s\in\mathbb{F}_r^*} \left(\frac{s}{r}\right) - 1 = -1,$$

hiszen $\mathbb{F}_r^*$-ban a négyzetelemek és a nem négyzetelemek száma megegyezik.

Így:

$$\sum_{u\in\mathbb{F}_r} C_u w^u = r - 1 - \sum_{q\in\mathbb{F}_r^*} w^u = r.$$

q.e.d.

1.9. Lemma. $y^{p-1} = \left(\frac{p}{r}\right)$.

Bizonyítás. Mivel Ω karakterisztikája p, így (mint már többször láttuk) $y^p = \sum_{x\in\mathbb{F}_r} \left(\frac{x}{r}\right)^p w^{xp}$. p páratlan, így $\left(\frac{x}{r}\right)^p = \left(\frac{x}{r}\right)$, $p \neq r$ miatt pedig $\mathbb{F}_r$-ben van p^{-1} elem, tehát:

$$y^p = \sum_{z\in\mathbb{F}_r} \left(\frac{zp^{-1}}{r}\right) w^z = \left(\frac{p^{-1}}{r}\right) y = \left(\frac{p}{r}\right) y,$$

azaz $y^{p-1} = \left(\frac{p}{r}\right)$.

q.e.d.

Az első lemmából: $y^2 = (-1)^{\varepsilon(r)} r$, így (mint a Legendre-szimbólum definíciója után megállapítottuk) $\left(\frac{(-1)^{\varepsilon(r)} r}{p}\right) = y^p = \left(\frac{p}{r}\right)$. A Legendre-szimbólum szorzattartásából, és $\varepsilon(p)$ definíciójából pedig $\left(\frac{(-1)^{\varepsilon(r)}}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(r)}$ következik.

Ezeket összerakva:

$$\left(\frac{p}{r}\right) = \left(\frac{(-1)^{\varepsilon(r)} r}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(r)} \left(\frac{r}{p}\right),$$

amivel a tételt bebizonyítottuk.

q.e.d.

Megjegyzés. A kvadratikus reciprocitási tétel állítása igaz a $p = r$ esetre is, sőt ekkor nem is kell feltennünk, hogy ez a prímszám páratlan. (Hiszen $\left(\frac{p}{p}\right) = 0$.)

Az állítás azonban nem igaz különböző paritású prímekre. Ellenpéldának megfelelőek a 2 és 3 számok:

$$\left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = -1 \neq 1 = (-1)^{1\cdot 0} \cdot 1 = (-1)^{\varepsilon(3)\varepsilon(2)} \left(\frac{3}{2}\right).$$

2. fejezet

A p-adikus számok

Most, hogy tisztáztuk a véges (és főleg a prímrendű) testek néhány tulajdonságát, ideje szemügyre vennünk az úgynevezett p-adikus számokat, amik elengedhetetlenül szükségesek főtételünk kimondásához. A p-adikus számtestet rengeteg ekvivalens módon lehet definiálni, de mi most itt csak egyre szorítkozunk.

Ebben a fejezetben p mindig egy prímszámot jelöl, Z_k-n pedig a k elemű ciklikus csoportot értjük, amit additívan írunk. A_n jelöli $\mathbb{Z}/p^n\mathbb{Z}$-t, a mod p^n maradékosztályok gyűrűjét. Ekkor van egy természetes homomorfizmus A_n és A_{n-1} között. Jelöljük ezt φ_n-el. φ_n nyilván szürjektív, és magja a p^{n-1}-el osztható számok részgyűrűje, azaz: $\ker\varphi_n = p^{n-1}A_n$.

2.1. p-adikus egészek

A p-adikus számok általunk választott definíciójához elsőként be kell vezetnünk a p-adikus egészek fogalmát:

2.1. Definíció (p-adikus egészek)**.**

$$\mathbb{Z}_p = \left\{ x \in \prod_{n=1}^{\infty} A_n \;\middle|\; \varphi_n(\pi_n(x)) = \pi_{n-1}(x) \right\},$$

ahol $\prod$ *a komplett direktszorzatot,* π_n *pedig az* n*-edik koordinátafüggvényt jelöli.*

$x \in \mathbb{Z}_p$ mellett $\pi_n(x)$-et jelöljük x_n-el, és nevezzük x n-edik (szám)jegyének.
$\mathbb{Z}_p$ egy igen fontos tulajdonsága a következő:

2.2. Állítás. $\mathbb{Z}_p$ *egy egységelemes integritási tartomány.*

Bizonyítás. Elsőként látnunk kell, hogy $\mathbb{Z}_p$ részgyűrűje $\prod_{n=1}^{\infty} A_n$-nek, de mivel φ_n homomorfizmus, ez triviálisan igaz. A_n minden n-re kommutatív, ezért $\mathbb{Z}_p$ kommutativitása is nyilvánvaló.

Ha x $\mathbb{Z}_p$ egy eleme, és van egy olyan n pozitív egész, hogy $x_n = 0$, akkor minden n-nél kisebb m pozitív egészre $x_m = 0$, mert φ_k homomorfizmus. Két $\mathbb{Z}_p$-beli elem (x és y) szorzata pontosan akkor 0, ha minden n pozitív egészre $x_n = 0$ vagy $y_n = 0$. Tehát, ha $xy = 0$, akkor x és y valamelyike (feltehetjük, hogy x) olyan, hogy minden N pozitív egészhez található egy $n > N$ pozitív egész, amire $x_n = 0$. Vagyis $x = 0$, azaz $\mathbb{Z}_p$ nullosztómentes.

Az egységelemességhez pedig elég látni, hogy a csupa egyes koordinátából álló szám egységelem, ami triviálisan teljesül.

$\mathfrak{q.e.d.}$

Tulajdonképpen most már be is vezethetnénk a p-adikus számok fogalmát. De inkább vizsgáljuk meg néhány tulajdonságukat, amelyekre szükségünk lesz a későbbiekben:

2.3. Állítás.

$$A \qquad 0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\pi_n} A_n \longrightarrow 0 \qquad \textit{sorozat exakt.}$$

Bizonyítás. Ha $\mathbb{Z}_p$ egy x elemére $px = 0$, akkor minden n pozitív egészre $px_n = 0$. Vagyis van A_n-nek egy olyan y_n eleme, amire $p^{n-1}y_n = x_n$. Ekkor $x_{n-1} = \varphi_n(x_n) = \varphi(p^{n-1})\varphi(y_n) = 0$, így $x = 0$. Tehát $\mathbb{Z}_p$-n az $x \mapsto px$ leképezés injektív, így az $x \mapsto p^n x$ leképezés is az.

$p^n\mathbb{Z}_p$ nyilván része π_n magjának. Most vegyünk egy x elemet $\mathbb{Z}_p$-ből, ami benne van $\ker \pi_n$-ben. Ekkor $x_n = 0$, és az összes n-nél kisebb m pozitív egészre is $x_m = 0$. Az n-nél nagyobb m egészekre x_m osztható p^n-el. Ekkor létezik pontosan egy elem A_{m-n}-ben (legyen y_m), aminek A_m-beli képére teljesül, hogy $x_m = p^n y_m$. Ebből $x_{m-1} = \varphi_m(x_m) = \varphi_m(p^n)\varphi_m(y_m) = p^n\varphi_m(y_m)$ következik, tehát létezik pontosan egy $y = (y_m)_{m=1}^{\infty}$, szám $\mathbb{Z}_p$-ben, amire $x = p^n y$ teljesül.

π_n szürjektivitása pedig nyilvánvaló.

q.e.d.

2.4. Lemma. *$\mathbb{Z}_p$ egy eleme pontosan akkor invertálható, ha nem osztható p-vel.*

Bizonyítás. Ha $x \in A_n$-re x nem osztható p-vel, akkor x (a természetes homomorfizmus mentén – nevezzük ezt φ-nek – vett) képe A_1-ben nem 0. Mivel $A_1 = \mathbb{F}_p$, ezért itt $\varphi(x)$ invertálható. Nevezzük $\varphi(x)^{-1}$ A_n-beli (egyik) ősképét y-nak. Ekkor $xy = 1 - (1 - xy)$, tehát $1 = \varphi(x)\varphi(y) = \varphi(1 - (1 - xy)) = 1 - \varphi(1 - xy)$, vagyis $\varphi(1 - xy) = 0$, azaz $1 - xy$ osztható p-vel, így létezik egy z elem A_n-ben, amire $1 - xy = pz$, másképp $xy = 1 - pz$ teljesül. Ebből $xy\sum_{i=0}^{n-1}(pz)^i = (1 - pz)\sum_{i=0}^{n-1}(pz)^i = 1 - (pz)^n = 1$ következik. Tehát x valóban invertálható.

Ha x osztható p-vel, és x invertálható, akkor létezik egy y elem A_n-ben, amire $x = py$. Ekkor $1 = xx^{-1} = p(yx^{-1})$, vagyis p invertálható. Ekkor p minden hatványa, így $p^n = 0$ is invertálható, ami lehetetlen.

Vagyis A_n egy eleme akkor és csak akkor invertálható, ha nem osztható p-vel. $\mathbb{Z}_p$ egy x eleme pedig akkor és csak akkor invertálható, ha minden n pozitív egészre x_n invertálható. Azaz x akkor és csak akkor invertálható, ha minden n-re x_n nem osztható p-vel. Ami pont azzal ekvivalens, hogy x nem osztható p-vel.

q.e.d.

Megjegyzés. A fenti feltétel nyilván megegyezik az $x_1 \neq 0$, azaz az $x_n \neq 0$ ($n \in \mathbb{Z}^+$) feltétellel.

2.5. Definíció (p-adikus egységek)**.** *$\mathbb{Z}_p$ egységeinek (invertálható elemeinek) halmazát U_p-vel jelöljük. $\mathbb{Z}_p$ egységeit nevezzük p-adikus egységeknek.*

Most pedig, hogy meghatároztuk a p-adikus egészek egységeit, adhatunk egy hasznos felbontást $\mathbb{Z}_p$ elemeire:

2.6. Lemma. *$\mathbb{Z}_p$ minden nemnulla x eleme egyértelműen felírható $x = p^n u$ alakban valamely n természetes számra és $u \in U_p$ elemre.*

Bizonyítás. $x \neq 0$, így létezik egy maximális n természetes szám, hogy p^n osztja x-et. Ekkor van $\mathbb{Z}_p$-ben egy u elem, amire $x = p^n u$. Mivel p nem osztja u-t, ezért u p-adikus egység.

Ha U_p egy v elemére, és egy m természetes számra $x = p^m v$, akkor $m = n$, mert m a legnagyobb természetes szám, amire x osztható p^m-mel. Így $p^n(u - v) = 0$, de mivel $\mathbb{Z}_p$ nullosztómentes, ezért ebből $u = v$ adódik.

q.e.d.

2.2. $\mathbb{Z}_p$ topológiája

A későbbiekben hasznunkra lesz, ha megismerkedünk a p-adikus egészek topológiájával – annál is inkább, mert ezt a topológiát fogjuk majd kiterjeszteni a p-adiuks számtestre is. Mindenek előtt azonban be kell vezetnünk a p-adikus értékelés fogalmát:

2.7. Definíció (p-adikus értékelés)**.** *$\mathbb{Z}_p$ egy x elemére a $\sup\{n \in \mathbb{N} | x$ osztható p^n-el$\}$ számot x p-adikus értékelésének nevezzük, és $o_p(x)$-el jelöljük.*

Megjegyzés. $\mathbb{Z}_p$ fölött o_p-re nyilván teljesülnek a következők:

$$o_p(x) = \infty \Leftrightarrow x = 0, \quad o_p(xy) = o_p(x) + o_p(y), \quad o_p(x + y) \geq \min\{o_p(x), o_p(y)\}.$$

Az ilyen függvényeket additív (esetleg exponenciális) értékeléseknek nevezzük.

A p-adikus értékeléshez (mint minden additív értékeléshez) egyértelműen tartozik egy abszolútérték , amit a következő képpen definiálunk: $|x|_p := e^{-o_p(x)}$. Ez nyilván teljesíti az abszolútérték definícióját ($|x|_p > 0$, kivéve $x = 0$-ra, amikor is $|x|_p = 0$, $|xy|_p = |x|_p|y|_p$, $|x+y|_p \leq |x|_p+|y|_p$). Az abszolútértékből természetesen adódik egy metrika ($d(x, y) = |x - y|$ – szimmetria pedig minden abszolútértékben teljesül), ami generál egy topológiát. Jelöljük $\mathbb{Z}_p$ így kapott metrikus topológiájában a nyílt halmazok rendszerét $\mathcal{M}$-mel.

Most definiáljunk egy másik topológiát is $\mathbb{Z}_p$-n. Mivel $\mathbb{Z}_p$-t $\prod_{n=1}^{\infty} A_n$ részhalmazaként definiáltuk, így elég az A_n-eket ellátni valamilyen topológiával, hogy $\mathbb{Z}_p$-n topológiát kapjunk (a $\prod_{n=1}^{\infty} A_n$-en értelmezett szorzattopológia altértopológiáját).

Vegyük az A_n-ek diszkrét topológiáját, és az ezek által $\mathbb{Z}_p$-n generált topológia nyílt halmazainak rendszerét jelöljük $\mathcal{U}$-val.

2.8. Lemma. $\mathcal{M} = \mathcal{U}$

Bizonyítás. Mondjuk azt, hogy halmazok egy $\mathcal{H}$ rendszere generálja $\mathcal{U}$-t, illetve $\mathcal{M}$-et, ha a legdurvább topológia $\mathbb{Z}_p$-n, ami $\mathcal{H}$ minden elemét tartalmazzal $\mathcal{U}$, illetve $\mathcal{M}$.

Tetszőleges a és x $\mathbb{Z}_p$-beli elemekre, és r pozitív számra $d(a, x) < r$ ekvivalens $o_p(a - x) > -\log r$-el. Tehát definíció szerint $\mathcal{M}$-et az $\{x \in \mathbb{Z}_p \mid a-x$ osztható p^n-el$\}$ alakú halmazok generálják (ahol a végigfut $\mathbb{Z}_p$-n, n pedig a természetes számokon). Nevezzük ezt a halmazrendszert $\mathcal{G}$-nek.

$\mathcal{U}$ egy generátora a $(\prod_{n=1}^{\infty} B_n) \cap \mathbb{Z}_p$ alakú halmazok rendszere, ahol B_n A_n részhalmaza minden n-re, és véges sok kivétellel $B_n = A_n$ is teljesül. Nevezzük ezt a halmazrendszert $\mathcal{H}$-nak.

Könnyen látható, hogy $\mathcal{H}$ bővebb $\mathcal{G}$-nél, hiszen $\{x \in \mathbb{Z}_p | a - x$ osztható p^n-el$\}$ voltaképpen azon x-ek halmaza, amiknek az utolsó n jegye megegyezik a utolsó n jegyével. Tehát a metrikus topológia durvább a generált topológiánál.

Most lássuk fordítva: vegyünk egy $(\prod_{n=1}^{\infty} B_n) \cap \mathbb{Z}_p$ alakú halmazt, és a legnagyobb n-et, amire $B_n \neq A_n$ jelöljük N-el. Most vegyük az összes $\mathbb{Z}_p$-beli a elemet, amire $a_n \in B_n$ minden n-re, nevezzük ezek halmazát $\mathcal{A}$-nak. Ekkor:

$$\bigcup_{a \in \mathcal{A}} \{x \in \mathbb{Z}_p | a - x \text{ osztható } p^N\text{-el}\} = \left(\prod_{n=1}^{\infty} B_n \right) \cap \mathbb{Z}_p,$$

így $\mathcal{M}$-nek része $\mathcal{H}$, vagyis a metrikus topológia finomabb a generált topológiánál.

Tehát a két topológia valóban megegyezik.

q.e.d.

Erre a lemmára azért volt szükségünk, hogy a $\mathbb{Z}_p$ topológiájára vonatkozó állításokat mindig a lehető legkényelmesebb, legegyszerűbb módon bizonyíthassuk. Viszont eddig semmi konkrétumot nem mondtunk erről a topológiáról. Ez most következik:

2.9. Állítás. *$\mathbb{Z}_p$ kompakt.*

Bizonyítás. Az A_n halmazok végesek, így (bármilyen topológiával) kompakt terek. Vagyis $\mathbb{Z}_p$ kompakt terek szorzatában egy altér. Tehát elég látni, hogy $\mathbb{Z}_p$ zárt.

Tekintsük a következő halmazokat minden N pozitív egészre, minden $n > N$ egészre, és A_N minden a elemére:

$$A(a, N, n) = \left\{ x \in \prod_{k=1}^{\infty} A_k \;\middle|\; x_N = a,\ (\varphi_{N+1} \circ \cdots \circ \varphi_n)(x_n) \neq a \right\}.$$

Ekkor $\bigcup_{n=N+1}^{\infty} A(a, N, n)$ azon $\prod_{k=1}^{\infty} A_k$-beli elemek halmaza, melyeknek N-edik jegye a, de valamelyik nagyobb jegyük miatt nem lehetnek $\mathbb{Z}_p$-beliek. Így $\bigcup_{a \in A_N} \bigcup_{n=N+1}^{\infty} A(a, N, n)$ azon elemek halmaza, melyeknek az N-edik jegyük után van egy olyan jegyük, ami kizárja, hogy $\mathbb{Z}_p$-beliek legyenek, és $\bigcup_{N=1}^{\infty} \bigcup_{a \in A_N} \bigcup_{n=N+1}^{\infty} A(a, N, n)$ azon elemek halmaza, amiknek van két „összeférhetetlen" jegyük. Vagyis ez pont $\mathbb{Z}_p$ komplementere $\prod_{k=1}^{\infty} A_k$-ban.

Most vegyük észre, hogy (bármilyen a, N és n esetén) $A(a, N, n)$ nyílt halmaz $\prod_{k=1}^{\infty} A_k$ szorzattopológiájában, hiszen csak az N-edik és az n-edik jegyének kell kielégítenie bizonyos kritériumokat. Így az ilyen típusú halmazok tetszőleges uniója is nyílt halmaz lesz, tehát $\mathbb{Z}_p$ zárt, amivel az állítást bizonyítottuk.

q.e.d.

2.10. Következmény. Mivel $\mathbb{Z}_p$ egy kompakt metrikus tér, ezért teljes.

2.11. Állítás. *$\mathbb{Z}$ sűrű $\mathbb{Z}_p$-ben.*

Bizonyítás. Minden $\mathbb{Z}_p$-beli x-re x_n reprezentálható egy nemnegatív egész számmal. Ekkor az $x_n (n \in \mathbb{Z}^+)$ egész számokból álló sorozat nyilvánvalóan x-hez tart $\mathbb{Z}_p$-ben. q.e.d.

Megjegyzés. A bizonyításból az is látszik, hogy a nemnegatív egészek halmaza sűrű $\mathbb{Z}_p$-ben. Hasonlóan látható, hogy a nempozitív egészek halmaza is sűrű. Sőt, a pozitív (illetve a negatív) egészek sűrű volta is egyszerűen adódik, hiszen a közelítő sorozatokat kezdhetjük az első nemnulla számjegytől, a nullát pedig megközelíthetjük a $p, p^2, p^3, \ldots$ sorozattal.

Megjegyzés. Feljebb említettük, hogy minden additív értékeléshez tartozik egy abszolút érték. Az így kapott abszolút értékek speciálisak – rájuk nem csak az $|x+y| \leq |x|+|y|$ feltétel, hanem az $|x+y| \leq \max\{|x|, |y|\}$ feltétel is teljesül (ezt nevezik ultrametrikus egyenlőtlenségnek). Azokat az abszolút értékeket, amik ennek az erősebb feltételnek is eleget tesznek nemarkhimédészi abszolút értéknek vagy (multiplikatív) értékeléseknek nevezzük. Az additív és multiplikatív értékelések között a megfeleltetés kölcsönösen egyértelmű.

Említettük azt is, hogy a fent definiált metrika valóban metrika, mert szimmetrikus. Ez minden függvényre igaz, amit egy abszolút értékből a fenti módon származtatunk. Általánosabban: az abszolút értékek „érzéketlenek" a -1-el való szorzásra. Valóban: $|-1|^2 = |1|$, így $|-1| = \pm|1|$, de mind $|1|$, mind $|-1|$ pozitív, tehát $|-1| = |1|$, ahonnan $|x| = |-x|$ (minden x-re) már azonnal adódik.

A p-adikus abszolút értéket egyébként szokás $|x|_p = p^{-o_p(x)}$ alakban is definiálni, de ez nyilván ekvivalens az általunk használt abszolút értékkel.

2.3. A p-adikus számtest és topológiája

Most eljött az ideje, hogy bevezessük a p-adikus számok fogalmát, illetve, hogy megmondjuk, $\mathbb{Z}_p$ topológiájának milyen kiterjesztését használjuk a p-adikus számtest topológiájaként:

2.12. Definíció. *p-adikus számtestnek $\mathbb{Z}_p$ hányadostetét nevezzük. A p-adikus számok testét $\mathbb{Q}_p$-vel jelöljük.*

Nyilvánvaló, hogy ekkor $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$, illetve hogy $\mathbb{Q}_p^*$ minden x eleme egyértelműen felírható $p^n u$ alakban, ahol $n \in \mathbb{Z}$ és $u \in U_p$. Ennek megfelelően a p-adikus értékelés, illetve a p-adikus abszolút érték definíciója kiterjeszthető $\mathbb{Q}_p$-re, ahol tetszőleges $x \in \mathbb{Q}_p$-re $o_p(x) \geq 0 \Leftrightarrow x \in \mathbb{Z}_p$ is teljesülni fog. (A p-adikus értékelés kiterjesztésénél természetesen nem a fenti supremum-os, hanem a vele $\mathbb{Z}_p$-n ekvivalens, „a $p^n u$ alak n-je" definíciót kell használni.)

2.13. Állítás. *$\mathbb{Q}_p$ a $d(x,y) = |x-y|_p$ metrikával lokálisan kompakt, benne $\mathbb{Z}_p$ nyílt részgyűrű, $\mathbb{Q}$ pedig sűrű résztest.*

Bizonyítás. A lokális kompaktsághoz elég azt belátnunk, hogy minden a elemére $\mathbb{Q}_p$-nek a $\overline{B}(a,1)$, a körüli, 1 sugarú zárt gömb kompakt, amihez elég, hogy teljesen korlátos. $\overline{B}(a,1) = \{x \in \mathbb{Q}_p | o_p(a-x) \geq 0\}$. Mivel minden x-re és y-ra $o_p(x-y) = o_p((x-a)-(y-a))$, ezért elég $a = 0$-t, illetve $\overline{B}(0,1) = \mathbb{Z}_p$-t vizsgálni, amiről viszont tudjuk, hogy kompakt (így teljesen korlátos).

$d(0,x) < r \Leftrightarrow o_p(x) > -\log r$, így $r = e$-re $B(0,r) = \{x \in \mathbb{Q}_p | o_p(x) > -1\} = \mathbb{Z}_p$, vagyis $\mathbb{Z}_p$ nyílt.

$\mathbb{Z}$ sűrű $\mathbb{Z}_p$-ben. $\mathbb{Q}_p$ elemei $\frac{x}{y}$ alakúak, ahol x és y is $\mathbb{Z}_p$-beliek, $y \neq 0$. Tehát van egy (x_n) és egy (y_n) sorozat $\mathbb{Z}$-ben, ahol y_n egyetlen n-re sem 0; $x_n \to x$, és $y_n \to y$. Így $\frac{x_n}{y_n} \in \mathbb{Q}$ és $\frac{x_n}{y_n} \to \frac{x}{y}$. q.e.d.

2.4. p-adikus polinomok

Tekintve, hogy a Hasse–Minkowski-tétel (bizonyos értelemben) részben $\mathbb{Q}_p$ feletti kvadratikus alakokról szól, nem meglepő, hogy szükségünk lesz néhány $\mathbb{Q}_p$ feletti polinomokkal kapcsolatos állításra is.

2.14. Definíció. *Egy f $\mathbb{Z}_p$ feletti polinomra jelölje f_n azt az A_n feletti polinomot, amit úgy kapunk, hogy f együtthatóira alkalmazzuk a π_n függvényt.*

2.15. Lemma. *Legyen $f^{(\alpha)}$ egy $\mathbb{Z}_p$ feletti m változós polinom minden α-ra valamely I halmazból. Ekkor az $f^{(\alpha)}$-knak pontosan akkor van közös gyökük minden $\alpha \in I$ esetén, ha minden n pozitív egészre az $f_n^{(\alpha)}$-knak van közös gyökük minden $\alpha \in I$ esetén.*

Bizonyítás. Az $f^{(\alpha)}$-k közös gyökének képe A_n^m-ben (π_n mentén, koordinátánként) gyöke lesz minden $f_n^{(\alpha)}$-nek.

A másik irányhoz elég látni, hogy az $f_n^{(\alpha)}$-ek közös gyökei „kompatibilisek", vagyis hogy van az $f_n^{(\alpha)}$-ek közös gyökeinek egy x_n sorozata, amire $(x_n(l))_{n=1}^{\infty} \in \mathbb{Z}_p$, minden $l = 1, \ldots, m$ esetén (ahol $x_n(l)$ x_n l-edik koordinátáját jelöli). Jelölje V_n az $f_n^{(\alpha)}$-ek közös gyökeinek halmazát, és legyen $B_{n,k}$ a V_{n+k} halmaz képe (koordinátánként, a természetes homomorfizmus mentén) A_n^m-ben. Ekkor $B_{n,k}$ része lesz V_n-nek is, hiszen ha egy x elem benne van V_{n+k}-ban, akkor ő gyöke az $f_{n+k}^{(\alpha)}$-knak, így az ő képe A_n^m-ben gyöke az $f_{n+k}^{(\alpha)}$-k (a természetes homomorfizmus mentén vett) képeinek, amik pont az $f_n^{(\alpha)}$-ek. Ebből nyilvánvaló, hogy fix n-re a $B_{n,k}$ halmazok nemüres, csökkenő sorozatot alkotnak V_n-ben, így (mivel A_n véges halmaz, és $V_n \subseteq A_n^m$) kellően nagy k-kra a $B_{n,k}$ halmazok egyenlőek. Nevezzük ezt a legkisebb $B_{n,k}$-t B_n-nek. Ekkor nyilvánvaló, hogy minden n-re $\varphi_{n+1}(B_{n+1}) = B_n$ (a leképezést koordinátánként értelmezve). Vagyis B_1 bármely x_1 elemének van ősképe B_2-ben (legyen ez x_2), annak van ősképe B_3-ban (x_3), és így tovább. Az így kapott x_n vektorok pedig a fenti értelemben nyilvánvalóan kompatibilisek, amivel az állítást bebizonyítottuk.

q.e.d.

2.16. Definíció. *Nevezzük $\mathbb{Z}_p^m$, illetve A_n^m azon elemeit, amik nem oszthatók p-vel, primitív elemeknek.*

2.17. Állítás. *Legyen $f^{(\alpha)}$ $\mathbb{Z}_p$ feletti m változós homogén polinom minden $\alpha \in I$-re valamely I halmazra. Ekkor a következők ekvivalensek:*

1. *Az $f^{(\alpha)}$-knak van nemtriviális közös gyökük $\mathbb{Q}_p^m$-ben.*
2. *Az $f^{(\alpha)}$-knek van közös primitív gyökük $\mathbb{Z}_p^m$-ben.*
3. *Minden n-re az $f_n^{(\alpha)}$-eknek van közös primitív gyökük A_n^m-ben.*

Bizonyítás. A 2. $\Rightarrow$ 1. irány triviálisan igaz. A visszafele irányhoz elég látni, hogy (homogén polinomokról lévén szó) a gyökök tetszőleges többszörösei is gyökök. Tehát az $f^{(\alpha)}$-k $\mathbb{Q}_p^m$-beli $x = (x_1, \ldots, x_m)$ közös gyökére: $p^{-min\{o_p(x_1),\ldots,o_p(x_n)\}}x$ $\mathbb{Z}_p^m$ primitív eleme, és gyöke az $f^{(\alpha)}$-knak.

A 2. $\Leftrightarrow$ 3. ekvivalencia pedig az előző lemma nyilvánvaló következménye.

q.e.d.

2.18. Lemma. *Legyen f egy $\mathbb{Z}_p$ feletti (egy változós) polinom. Amennyiben van egy olyan x elem $\mathbb{Z}_p$-ben, illetve olyan k, n egész számok, amikre: $0 \leq 2k < n$, $\pi_n(f(x)) = 0$ és $o_p(f'(x)) = k$ (ahol f' az f deriváltját jelöli), akkor van egy olyan y elem is $\mathbb{Z}_p$-ben, amire: $\pi_{n+1}(f(y)) = 0$, $o_p(f'(y)) = k$ és $\pi_{n-k}(y) = \pi_{n-k}(x)$.*

Bizonyítás. A feltételekből következik, hogy létezik egy olyan b p-adikus egész, és egy u p-adikus egység, amikre: $f(x) = p^n b$, illetve $f'(x) = p^k u$. Legyen $z = -bu^{-1}$, $y = x + p^{n-k}z$. A Taylor-formulák miatt vagy egy olyan a p-adikus egész, amire:

$$f(y) = f(x) + p^{n-k}zf'(x) + p^{2(n-k)}a = p^n(b + zu) + p^{2n-2k}a = p^{2n-2k}a,$$

így $\pi_{n+1}(f(y)) = 0$, mert $2n - 2k > n$.

A Taylor-formulát f'-re alkalmazva a fentihez hasonlóan kapjuk, hogy: $\pi_{n-k}(f'(y)) = \pi_{n-k}(p^k u)$, amiből (tekintve, hogy $k < n - k$, és u p-adikus egység) $o_p(f'(y)) = k$ adódik.

Az utolsó pont pedig y definíciójából nyilvánvaló.

q.e.d.

2.19. Tétel. *Legyen f egy m változós polinom $\mathbb{Z}_p$ felett, x egy elem $\mathbb{Z}_p^m$-ben, valamint legyenek k, n pozitív egészek és $j = 1, \ldots, m$ egy szám, amikre teljesülnek a következők:*

$$2k < n,\ f(x) \equiv 0 \pmod{p^n} \text{ és } o_p(\partial_j f(x)) = k.$$

Ekkor f-nek van egy y gyöke $\mathbb{Z}_p^m$-ben, amire koordinátánként igaz, hogy $\pi_{n-k}(x) = \pi_{n-k}(y)$.

Bizonyítás. Tekintsük először az $m = 1$ esetet. Ekkor (a fenti lemma értelmében) van egy x_1 elem $\mathbb{Z}_p$-ben, amire: $\pi_{n-k}(x_1) = \pi_{n-k}(x)$, $\pi_{n+1}(f(x_1)) = 0$, és $o_p(f'(x_1)) = k$. Hasonlóan látható, hogy léteznek $x_1, x_2, \ldots$ elemek $\mathbb{Z}_p$-ben, hogy minden l pozitív egészre $\pi_{n-k+l}(x_{l+1}) = \pi_{n-k+l}(x_l)$, $\pi_{n+l}(f(x_l)) = 0$, és $o_p(f'(x_l)) = k$. Ez egy Cauchy-sorozat. Mivel $\mathbb{Z}_p$ teljes, ezért a sorozatnak van határértéke, nevezzük y-nak. Erre nyilván: $f(y) = 0$ és $\pi_{n-k}(y) = \pi_{n-k}(x)$, amivel az állítást $m = 1$-re bebizonyítottuk.

$m > 1$ esetén tekintsük azt az $\tilde{f}$ egy változós polinomot, amit f-ből úgy állítunk elő, hogy a j-edik változó kivételével behelyettesítjük bele x koordinátáit. Ekkor van egy y_j elem $\mathbb{Z}_p$-ben, amire $\tilde{f}(y_j) = 0$ és $\pi_{n-k}(y_j) = \pi_{n-k}(x_j)$. Így $y = (x_1, \ldots, x_{j-1}, y_j, x_{j+1}, \ldots, x_n)$ megfelelő vektor lesz.

q.e.d.

2.20. Következmény. Minden $f \in \mathbb{Z}_p[x]$-re f_1 egyszeres gyökei felemelhetők f gyökeivé, hiszen f-nek pont azon gyökei az egyszeres gyökök, amikre f' nem 0. Tehát az $n = 1$, $k = 0$ esetből a felemelhetőség nyilvánvaló.

2.21. Következmény. Ha p páratlan prím, f pedig egy m változós kvadratikus alak $\mathbb{Z}_p$ fölött, aminek mátrixa $(A = (a_{ij})_{i,j=1}^n)$ invertálható, akkor minden $a \in \mathbb{Z}_p$-re az $f_1(x) = \pi_1(a)$ egyenlet primitív megoldásai felemelhetők az $f(x) = a$ egyenlet megoldásaivá, hiszen $\partial_i(f(x) - a) = 2\sum_{j=1}^m a_{ij}x_j$. Mivel pedig A invertálható, és $x = 0$ esetén minden i-re teljesül, hogy $2\sum_{j=1}^m a_{ij}x_j = 0$, ezért minden primitív megoldásra található olyan i, amire $\partial_i f \neq 0$. Tehát az előző következmény alapján valóban minden ilyen megoldás felemelhető.

2.22. Következmény. Legyen $f(x) = \sum_{i,j=1}^m a_{ij}x_ix_j$ egy $\mathbb{Z}_2$ feletti kvadratikus alak, amire $a_{ij} = a_{ji}$ minden i, j esetén. Legyen $a \in \mathbb{Z}_p$, x pedig egy primitív elem $\mathbb{Z}_p^m$-ben, amikre $f_3(x) = \pi_3(a)$ teljesül. Ekkor, ha van olyan $j = 1, \ldots, m$, amire $\partial_j f_4(x) \neq 0$, x felemelhető $f = a$ megoldásává.

Ez nyilvánvalóan látszik a tétel $n = 3$, $k = 1$ esetéből. A feltétel, hogy van olyan j, amire $\partial_j f_4(x) \neq 0$, teljesül, ha $\det(a_{ij}) \neq 0$.

Megjegyzés. Az utolsó következményben azért kellett $f(x)$ együtthatóinak szimmetrikusságát külön kiemelni, mert, míg a kvadratikus alakoknál ez általában feltehető (sőt, fel is szokás tenni), addig itt ez nem lehetséges, mivel $\mathbb{Z}_2$-ben nincs $\frac{1}{2}$ elem.

2.5. $\mathbb{Q}_p$ multiplikatív csoportja

Ebben a szakaszban $\mathbb{Q}_p$ multiplikatív csoportját fogjuk megvizsgálni. A végső célunk ezzel $\mathbb{Q}_p^{*2}$ karakterizációja, illetve a $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ csoport leírása, mert ezekre az információkra szükségünk lesz a $\mathbb{Q}_p$ feletti kvadratikus alakok vizsgálatánál. Először azonban egy sokkal általánosabb állítást bizonyítunk:

2.23. Lemma. *Legyen $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\mu} C \longrightarrow 0$ egy egzakt sorozat, ahol A, B és C is Abel-csoportok. Tegyük fel, hogy A és C rendre a, illetve c rendű véges csoportok, ahol a és c relatív prímek. Nevezzük C'-nek azon B-beli x elemek részcsoportját, amikre $cx = 0$. Ekkor $B = \varphi(A) \oplus C'$, C' pedig az egyetlen olyan részcsoport B-ben, ami izomorf C-vel.*

Bizonyítás. Mivel μ homomorfizmus, így $B/\ker\mu \simeq \mathrm{im}\mu$. Mivel A és C is véges, így B is az lesz. Ekkor (mivel a és c relatív prímek, valamint A, B és C is kommutatív) a véges Abel-csoportok alaptétele alapján B-nek van egyetlen részcsoportja, ami izomorf A-val (legyen $\tilde{A}$, ami meg kell egyezzen $\varphi(A)$-val), és egyetlen részcsoportja, ami izomorf C-vel (legyen $\tilde{C}$), B pedig ezek direktösszege. Sőt, az is nyilvánvaló, hogy $\tilde{C}$ része C'-nek, tehát elég látnunk, hogy C' is része $\tilde{C}$-nek. Ez pedig azért teljesül, mert ha B egy eleme $\alpha + \gamma$ alakú, ahol $\alpha \in \tilde{A}$, $\gamma \in \tilde{C}$, akkor $c\alpha + c\gamma = c\alpha$, ami (mivel a és c relatív prímek) pontosan akkor 0, ha $\alpha = 0$.

q.e.d.

Most vizsgáljuk meg U_p-t. Minden n pozitív egészre $U_{p,n}$ legyen $1+p^n\mathbb{Z}_p$, a $\pi_n^*|_{U_p}$ homomorfizmus (mint multiplikatív csoporthomomorfizmus) magja. Ekkor $U_p/U_{p,n}$ pont $\pi_n^*|_{U_p}$ képterével, vagyis $(\{x \in A_n \mid p \nmid x\}, \cdot)$-al lesz izomorf. (Ez $n = 1$-re pont $\mathbb{F}_p^*$ lesz.) Az $U_{p,n}$ halmazok nyilván nyíltak (1 körüli nyílt gömbök), és monoton csökkenő rendszert alkotnak.

Az $U_{p,n}/U_{p,n+1}$ csoport izomorf Z_p-vel (a p rendű ciklikus csoporttal), az $1+p^nx \mapsto x_1$ leképezés mentén, hiszen $\pi_{n+1}((1+p^nx)(1+p^ny)) = 1+p^n\pi_1(x+y)$ teljesül, és ha $\pi_1(x) = \pi_1(y)$, akkor van olyan z, hogy $(1+p^nx)(1+p^{n+1}z) = 1+p^ny$, hiszen ez pont azt jelenti, hogy $\pi_1(x) = \pi_1(y)$, és $(\pi_k(x)+1)(\pi_{k-1}(z)+1) = \pi_k(y)+1$ minden $k > 1$ egész számra, ami megoldható úgy, hogy $z \in \mathbb{Z}_p$ teljesüljön. Tehát $|U_{p,n}/U_{p,n+1}| = p$, így teljes indukcióval látható, hogy $|U_{p,1}/U_{p,n}| = p^{n-1}$.

2.24. Lemma. *U_p-nek létezik egyetlen $\mathbb{F}_p^*$-al izomorf részcsoportja. Nevezzük ezt V_p-nek. Ekkor: $U_p = V_p \times U_{p,1}$.*

Bizonyítás. A 2.23. lemmát alkalmazhatjuk az $1 \longrightarrow U_{p,1}/U_{p,n} \longrightarrow U_p/U_{p,n} \longrightarrow \mathbb{F}_p^* \longrightarrow 1$ egzakt sorra, hiszen $|U_{p,1}/U_{p,n}| = p^{n-1}$, míg $|\mathbb{F}_p^*| = p-1$, amik relatív prímek. Tehát $U_p/U_{p,n}$-nek van egyetlen $\mathbb{F}_p^*$-al izomorf részcsoportja, legyen ez $V_{p,n}$. Az $U_p/U_{p,n+1} \twoheadrightarrow U_p/U_{p,n}$ szürjekció nyilván $V_{p,n+1}$-et $V_{p,n}$-re képezi, vagyis $V_{p,n} = V_{p,m}$ minden n, m pozitív egészre. V_p egyértelműsége pedig a $V_{p,n}$-ek egyértelműségéből, és a $\pi_n^*(U_p) \simeq U_p/U_{p,n}$ összefüggésből adódik.

q.e.d.

2.25. Következmény. $\mathbb{Q}_p$ tartalmazza a $p-1$-edik egységgyököket.

2.26. Lemma. *Legyen x egy elem $U_{p,n} \setminus U_{p,n+1}$-ben. Ha $p > 2$ vagy $n > 1$, akkor $x^p \in U_{p,n+1} \setminus U_{p,n+2}$.*

Bizonyítás. $x \in U_{p,n} \setminus U_{p,n+1}$, tehát van egy u elem U_p-ben, amire $x = 1+p^nu$. Ekkor a binomiális tételből:

$$x^p = \sum_{k=0}^{p} \binom{p}{k} (p^nu)^k = 1 + p \cdot p^nu + p^{n+2}a = 1 + p^{n+1}(u+pa)$$

egy alkalmas $a \in \mathbb{Z}_p$ számra. De $u+pa \in U_p$, tehát $x^p \in U_{p,n+1} \setminus U_{p,n+2}$.

q.e.d.

2.27. Lemma. *$(U_{p,k}, \cdot) \simeq (\mathbb{Z}_p, +)$, ha $k = 1$ és $p \neq 2$, illetve ha $k = p = 2$.*

Bizonyítás. Tekintsük az $\alpha = 1+p^k$ elemet $U_{p,k} \setminus U_{p,k+1}$-ben. Ekkor az előző lemmából látható, hogy $\alpha^{p^n} \in U_{p,n+k} \setminus U_{p,n+k+1}$. Legyen α_n α képe $U_{p,k}/U_{p,n}$-ben, minden $n > k$ egészre. Ekkor $\alpha_n^{p^{n-k-1}} \neq 1$, de $\alpha_n^{p^{n-k}} = 1$. Viszont tudjuk, hogy $|U_{p,k}/U_{p,n}| = p^{n-k}$, tehát $U_{p,k}/U_{p,n}$ ciklikus csoport, vagyis izomorf $Z_{p^{n-k}}$-val, az $\alpha_n^l \mapsto l$ leképezés mentén. Ekkor a

$$\begin{array}{ccc} Z_{p^{n-k}} & \longrightarrow & U_{p,k}/U_{p,n} \\ \downarrow & & \downarrow \\ Z_{p^{n-k-1}} & \longrightarrow & U_{p,k}/U_{p,n-1} \end{array}$$

diagramm kommutatív. És mivel $\pi_n(U_{p,k}) \simeq U_{p,k}/U_{p,n}$, ezért $U_{p,k} \simeq \mathbb{Z}_p$.

q.e.d.

Másrészt, $\mathbb{Q}_p$ nemnulla elemei egyértelműen felírhatók p^nu alakban, ahol $n \in \mathbb{Z}$, $u \in U_p$. A 2.24. lemma alapján $U_p \simeq Z_{p-1} \times U_{p,1}$. Ha $p \neq 2$, akkor a 2.27. lemma miatt $U_{p,1} \simeq \mathbb{Z}_p$. $U_{2,1}$-re pedig tudjuk, hogy $U_{2,1}/U_{2,2} \simeq Z_2$, és $U_{2,2} \simeq \mathbb{Z}_2$. Azaz:

2.28. Tétel. *Minden $p > 2$ prímre:*

$$\mathbb{Q}_p^* \simeq Z_{p-1} \times \mathbb{Z} \times \mathbb{Z}_p,$$

$p = 2$-re pedig:

$$\mathbb{Q}_2^* \simeq Z_2 \times \mathbb{Z} \times \mathbb{Z}_2.$$

2.29. Tétel. *Bármely p páratlan prímre $\mathbb{Q}_p^*$ egy p^nu ($n \in \mathbb{Z}$, $u \in U_p$) eleme pontosan akkor négyzetelem, ha n páros, és $\pi_1(u) \in \mathbb{F}_p^* = U_p/U_{p,1}$ egy négyzetelem.*

Bizonyítás. Mivel $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}_p \times Z_{p-1}$, ahol p^nu-ban n reprezentálja $\mathbb{Z}$-t, $\mathbb{Z}_p$-ben pedig minden elem osztható kettővel ($\frac{1}{2} = (\frac{p^k+1}{2})_{k=1}^{\infty}$), ezért nyilvánvaló, hogy p^nu pontosan akkor négyzetelem, ha n páros, és u képe $U_p/U_{p,1}$-ben (vagyis π_1 mentén) négyzetelem.

q.e.d.

2.30. Következmény. $p \neq 2$-re $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*2} \simeq Z_2^2$.

2.31. Tétel. *$\mathbb{Q}_2^*$ egy $2^n u$ ($n \in \mathbb{Z}$, $u \in U_2$) eleme pontosan akkor négyzetelem, ha n páros, és $\pi_3(u) = 1$.*

Bizonyítás. Mivel $\mathbb{Q}_2^* \simeq \mathbb{Z} \times Z_2 \times \mathbb{Z}_2$, ahol $2^n u$-ban n reprezentálja $\mathbb{Z}$-t, a 2.27. lemmában konstruált $(U_{2,2}, \cdot) \simeq (\mathbb{Z}_2, +)$ izomorfizmus pedig, $2\mathbb{Z}_2$-t $U_{2,3}$-ba viszi, vagyis $U_{2,2}^2 = U_{2,3}$. Így $u \in U_2$ pontosan akkor négyzetelem, ha $\pi_3(u) = 1$.

q.e.d.

2.32. Következmény. $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times Z_2 \times U_{2,2}/U_{2,3} \simeq Z_2^3$.

2.33. Következmény. A 2.29., illetve a 2.31. tételekből látszik, hogy $\mathbb{Q}_p^{*2}$ nyílt $\mathbb{Q}_p$-ben (minden p prímre).

3. fejezet

A Hilbert-szimbólum

Most, hogy megvizsgáltuk a p-adikus számok pár fontos tulajdonságát, bevezethetjük az ún. Hilbert-szimbólumot. A Hilbert-szimbólumnak később fontos szerepe lesz a $\mathbb{Q}_p$ feletti kvadratikus alakok vizsgálata során.

Ebben a fejezetben K mindig egy testet jelöl, ami $\mathbb{R}$ vagy $\mathbb{Q}_p$ lehet (valamely p pozitív prímszámra). K_b-vel jelöljük a $K(\sqrt{b})$ testet minden $b \in K$-ra.

3.1. Definíciók

3.1. Definíció (Hilbert-szimbólum)**.** *Legyenek a és b K^* elemei. Ekkor a és b (K feletti) Hilbert-szimbólumának nevezzük a következőt:*

$$(a,b) = \begin{cases} 1 & \text{, ha } x^2 - ay^2 - bz^2\text{-nek van nemtriviális gyöke } K^3\text{-ben} \\ -1 & \text{, ha } x^2 - ay^2 - bz^2\text{-nek nincs nemtriviális gyöke } K^3\text{-ben.} \end{cases}$$

A Hilbert-szimbólum néhány tulajdonságának vizsgáltához érdemes bevezetnünk mégegy fogalmat:

3.2. Definíció. *Legyen L egy test, $L'|L$ pedig egy véges bővítése. Ekkor L' minden α eleméhez létezik egy $\varphi_\alpha : x \mapsto \alpha x$ L-lineáris leképezés L'-n. Mivel $L'|L$ véges, ezért L' tekinthető vektortérnek L fölött. Így tekintve értelmezhetjük φ_α determinánsát, mint a vektortéren értelmezett lineáris leképezés mátrixának determinánsát. Ezt (a bázisfüggetlen) L-beli értéket nevezzük α normájának $L'|L$-ben, és $N_{L'|L}(\alpha)$-val jelöljük.*

A definícióból nyilvánvaló, hogy $N_{L'|L}(\alpha\beta) = N_{L'|L}(\alpha)N_{L'|L}(\beta)$, és $N_{L'|L}(\alpha^{-1}) = N_{L'|L}(\alpha)^{-1}$ is teljesül L' minden α, β elemére valamint, hogy $N_{L'|L}(1) = 1$. Ekkor L'^* elemeinek normái csoportot alkotnak, amit a továbbiakban NL'^*-al jelölünk.

Mivel mi csak a $K_b|K$ bővítéssel foglalkozunk, így $N(\alpha)$ alatt majd $N_{K_b|K}(\alpha)$-t értünk, minden $\alpha \in K_b$ elemre. Tekintve, hogy (ha b nem négyzetelem K-ban) léteznek egyértelműen olyan x és y elemek K-ban, amire $\alpha = x + y\sqrt{b}$, így φ_α mátrixa az $(1, \sqrt{b})$ bázisban $\begin{pmatrix} x & by \\ y & x \end{pmatrix}$ lesz, aminek determinánsa $x^2 - by^2$. Tehát: NK_b^* pont az ilyen alakú elemek multiplikatív csoportja lesz, ha $b \notin K^{*2}$.

Ha pedig $b \in K^{*2}$, akkor $K_b = K$, és $N(\alpha) = \alpha$ minden K-beli α elemre, vagyis $NK_b^* = K^*$.

3.2. Alapvető tulajdonságok

Nyilvánvaló, hogy a Hilbert-szimbólum független a illetve b négyzetelemmel való szorzásától, valamint, hogy szimmetrikus. Tehát a Hilbert-szimbólum egy szimmetrikus leképezést ad $(K^*/K^{*2})^2$ és Z_2 (a kételemű ciklikus csoport) között.

3.3. Állítás. *K^* tetszőleges a és b elemeire $(a,b) = 1$, pontosan akkor, ha $a \in NK_b^*$.*

Bizonyítás. Ha b négyzetelem K^*-ban, akkor $(\sqrt{b})^2 - a0^2 - b1^2 = 0$, vagyis $(a,b) = 1$. Másfelől $NK_b^* = K^*$, vagyis a valóban NK_b^*-ban van.

Ha b nem négyzetelem K^*-ban, és $(a,b) = 1$, akkor vannak olyan x, y, z számok K-ban, amik nem mind 0-k, és amikre $x^2 - ay^2 - bz^2 = 0$. Ha $y = 0$, akkor $z \neq 0$ (különben $x = y = z = 0$ adódna), így $b = (xz^{-1})^2$, amit kizártunk. Vagyis $y \neq 0$, tehát $a = (xy^{-1})^2 - b(zy^{-1})^2 \in NK_b^*$.

Másfelől, ha $a = u^2 - bv^2$ K valamely u és v elemére, akkor $(u, 1, v)$ nemtriviális megoldása a Hilbert-szimbólumot definiáló egyenletnek, így $(a,b) = 1$.

q.e.d.

3.4. Következmény. K^* minden a és b elemére $a \in NK_b^* \Leftrightarrow b \in NK_a^*$.

3.5. Lemma. *A Hilbert-szimbólumra teljesülnek a következők:*

1. $(a, b^2) = 1$,
2. $(a, -a) = 1$,
3. $(a, 1-a) = 1$, *ha* $a \neq 1$,
4. $(a,b) = 1 \Rightarrow (ac, b) = (c, b)$,

ahol a, b és c K^* tetszőleges elemei.

Bizonyítás. Az 1. nyilván teljesül, hiszen $(b, 0, 1)$ megolsáda a Hilbert-szimbólumot definiáló egyenletnek.

A 2.-ra megoldás lesz a $(0, 1, 1)$, a 3.-ra pedig az $(1, 1, 1)$ vektor.

A 4.-nél pedig használjuk az előző állítást, mely szerint $(a,b) = 1$-ből következik, hogy a eleme NK_b^*-nak, ami részcsoportja K^*-nak, tehát c pontosan akkor van benne NK_b^*-ban, ha ac is benne van.

q.e.d.

3.6. Következmény. A lemma 2., 3. és 4. pontjából, valamint a Hilbert-szimbólum szimmetriájából következik, hogy $(a,b) = (a, -ab) = (a, (1-a)b)$ is teljesül (minden a-ra és b-re amire a Hilbert-szimbólumok értelmesek).

Megjegyzés. Az eddigi eredmények egy az egyben igazak $\mathbb{Q}$-ra is, hiszen nem használtuk ki K semmi olyan tulajdonságát, amivel $\mathbb{Q}$ nem rendelkezik.

3.3. A Hilbert-szimbólum kiszámítása

Ebben a szakaszban konkrét képleteket fogunk adni tetszőleges értékek Hilbert-szimbólumának kiszámítására.

Amennyiben $\mathbb{R}$ fölött vagyunk, akkor nyilván teljesül, hogy $(a,b) = -1 \Leftrightarrow a, b < 0$.

Most vizsgáljuk azt az esetet, ha $K = \mathbb{Q}_p$ valamely p prímre:

3.7. Lemma. *Legyen u egy p-adikus egység. Ha az $x^2 - py^2 - uz^2$ polinomnak van nemtriviális gyöke $\mathbb{Q}_p$ felett, akkor van olyan megoldása is, ahol $x, z \in U_p$, $y \in \mathbb{Z}_p$.*

Bizonyítás. A 2.17. állításból láthatjuk, hogy a polinomnak van primitív megoldása $\mathbb{Z}_p$ felett. Tegyük fel, hogy ez a megoldás nem felel meg a lemma állításának. Ekkor $\pi_1(x) = 0$ vagy $\pi_1(z) = 0$. Mivel $\pi_1(x^2 - uz^2) = 0$, és $\pi_1(u) \neq 0$, ezért $\pi_1(x) = \pi_1(z) = 0$. Így $\pi_2(py^2) = 0$, vagyis $\pi_1(y) = 0$, ami ellentmondás, hiszen ekkor (x, y, z) nem primitív.

q.e.d.

3.8. Tétel. *Ha $p \neq 2$, akkor:*

$$(p^n u, p^m v) = (-1)^{nm\varepsilon(p)} \left(\frac{u}{p}\right)^m \left(\frac{v}{p}\right)^n,$$

minden n és m egész számra, valamint u és v p-adikus egységre, ahol $\left(\frac{x}{p}\right)$ $\left(\frac{\pi_1(x)}{p}\right)$-t jelöli minden $x \in \mathbb{Z}_p$ esetén. ($\varepsilon(p)$-re pedig $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$, ld. a 6. oldalt.)

Bizonyítás. Mivel láttuk, hogy négyzetelemmel való szorzás nem befolyásolja a Hilbert-szimbólum értékét, ezért nyilván n és m konkrét értéke nem, csak a paritásuk fontos. Tehát elég az $n, m = 0, 1$ eseteket vizsgálni.

I $n = m = 0$:

Azt kell látnunk, hogy $(u, v) = 1$, azaz az $x^2 - uy^2 - vz^2$ polinomnak van egy nemtriviális gyöke. Ez teljesül az $A_1 = \mathbb{F}_p$-beli képén, az 1.4. következmény miatt. Mivel pedig a kvadratikus alak diszkriminánsa uv, ami invertálható, ezért a 2.21. következmény miatt van egy nemtriviális megoldása.

II $n = 1$, $m = 0$:

Ekkor azt kell látnunk, hogy $(pu, v) = \left(\frac{v}{p}\right)$. Viszont, a Hilbert-szimbólum tulajdonságainál (3.5. lemma) láttuk, hogy $(u, v) = 1$ miatt elég $(p, v) = \left(\frac{v}{p}\right)$-t igazolni. Ha v négyzetelem, akkor a Hilbert-szimbólum, illetve a Legendre-szimbólum definíciójából nyilvánvaló, hogy mindkét érték 1. Amennyiben v nem négyzetelem, akkor a 2.29. tétel alapján $\left(\frac{v}{p}\right) = -1$, és a fenti lemma szerint, ha $x^2 - py^2 - vz^2$-nek van nemtriviális gyöke, akkor van olyan is, hogy x és z p-adikus egység, y pedig p-adikus egész, amiből $\pi_1(x^2 - vz^2) = 0$, de ez (szintén a 2.29. tétel miatt) lehetetlen, hiszen ekkor py^2 négyzetszám lenne $\mathbb{Q}_p$-ben.

III $n = m = 1$:

Az állításunk az volt, hogy $(pu, pv) = (-1)^{\varepsilon(p)} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$. A Hilbert-szimbólum tulajdonságainál (3.6. következmény) láttuk, hogy $(pu, pv) = (pu, -p^2uv) = (pu, -uv)$, de az előző pontból következik, hogy $(pu, -uv) = \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{u}{p}\right) \left(\frac{v}{p}\right) = (-1)^{\varepsilon(p)} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$, ami pont az, amit bizonyítani akartunk.

q.e.d.

3.9. Tétel. $\mathbb{Q}_2$ *felett:*

$$(2^n u, 2^m v) = (-1)^{\alpha(u)\alpha(v) + m\beta(u) + n\beta(v)},$$

ahol n és m egész számok, u és v 2-adikus egységek, $\alpha(w) = \pi_1(\frac{w-1}{2})$, és $\beta(w) = \pi_1(\frac{w^2-1}{8})$ minden w 2-adikus egységre.

Bizonyítás. Az előző tétel bizonyításához hasonlóan itt is elég az $n, m = 0, 1$ eseteket vizsgálni.

I $n = m = 0$:

Bontsuk ezt további két esetre:

(a) $\pi_2(u) = 1$. Ebben az esetben azt kell igazolnunk, hogy $(u, v) = 1$. Ha $\pi_3(u) = 1$, akkor a 2.31. tétel alapján u négyzetelem $\mathbb{Q}_2$-ben, tehát $(u, v) = 1$. Ha pedig $\pi_3(u) = 5$, akkor $\pi_3(u + 4v) = 1$ (mivel v nem osztható 2-vel), így (szintén a 2.31. tétel alapján) van egy w 2-adikus egység, amire $u + 4v = w^2$. Ekkor a Hilbert-szimbólumot definiáló kvadratikus alaknak nemtriviális gyöke lesz a $(w, 1, 2)$ számhármas.

(b) $\pi_2(u) = \pi_2(v) = 3$. Ebben az esetben azt kell igazolnunk, hogy $(u, v) = -1$. Elég látnunk, hogy a definiáló egyenletnek nincs $\mathbb{Z}_2$ feletti primitív megoldása (hiszen homogén – ld. 2.17. állítás). Tegyük fel, hogy van. Ekkor erre a megoldásra $\pi_2(x^2 - 3y^2 - 3z^2) = \pi_2(x^2 + y^2 + z^2) = 0$. De A_2 négyzetelemei a 0 és az 1, tehát $\pi_2(x) = \pi_2(y) = \pi_2(z) = 0$, vagyis x, y és z is osztható 4-el, így a megoldás nem primitív, ami ellent mond a feltevésünknek.

II $n = 1$, $m = 0$:

Ekkor az állítás az, hogy $(2u, v) = (-1)^{\alpha(u)\alpha(v) + \beta(v)}$.

Először vizsgáljuk meg $(2, v)$-t. A fenti lemma alapján, ha $(2, v) = 1$, akkor az őt definiáló egyenletnek van olyan megoldása, amire x és z 2-adikus egységek, y pedig 2-adikus egész. Így $\pi_3(x^2) = \pi_3(z^2) = 1$, amiből $\pi_3(1 - 2y^2 - v) = 0$ következik. Tekintve, hogy A_3-ban

a négyzetelemek 0, 1 és 4, $\pi_3(v)$ csak 1 és -1 lehet, amiből $\beta(v) = 0$ adódik. Másfelől, ha $\pi_3(v) = 1$, akkor (a 2.31. tétel szerint) v négyzetszám, így $(2, v) = 1$, ha pedig $\pi_3(v) = -1$, akkor az $x^2 - 2y^2 - vz^2$ kvadratikus alak A_3-beli képének megoldása az $(1, 1, 1)$ vektor, ami a 2.22. következmény alapján felemelhető $\mathbb{Z}_2$-beli megoldássá. Vagyis ekkor is $(2, v) = 1$-et kapunk. Azaz $(2, v) = (-1)^{\beta(v)}$.

Ha $(2, v) = 1$ vagy $(u, v) = 1$, akkor $(2u, v) = (2, v)(u, v)$. Ha $(2, v) = (u, v) = -1$, akkor $\pi_3(u) = -1, 3$, és $\pi_3(v) = 3$. Ekkor u-t és v-t megfelelő négyzetelemekkel felszorozva adódik (a 2.31. tétel felhasználásával), hogy $(2u, v) = (-2, 3)$, vagy $(2u, v) = (6, -5)$, ez utóbbiak definiáló egyenletének pedig gyöke az $(1, 1, 1)$ számhármas, így $(2u, v) = 1 = (-1) \cdot (-1) = (2, v)(u, v)$, amivel (az előző pont alapján) az állítást beláttuk.

III $n = m = 1$:

A Hilbert-szimbólum tulajdonságaiból (3.6. következmény) látható, hogy:

$$(2u, 2v) = (2u, -4uv) = (2u, -uv) = (-1)^{\alpha(u)\alpha(-uv)+\beta(-uv)}.$$

Ezen felül:

$$\begin{aligned} \alpha(-uv) &= \pi_1\left(\frac{-uv-1}{2}\right) = \pi_1\left(\frac{v-1}{2} - \frac{v+uv}{2}\right) = \alpha(v) - \pi_1(v)\pi_1\left(\frac{u+1}{2}\right) = \\ &= \alpha(v) - 1(\alpha(u) + \pi_1(1)) = \alpha(v) - \alpha(u) - 1, \text{ vagyis} \end{aligned}$$

$$\alpha(u)\alpha(-uv) = \alpha(u)\alpha(v) - \alpha(u)(\alpha(u) + 1) = \alpha(u)\alpha(v),$$

ezen felül:

$$\beta(-uv) = \pi_1\left(\frac{u^2v^2-1}{8}\right) = \pi_1\left(\frac{v^2-1}{8} + \frac{u^2v^2-v^2}{8}\right) = \beta(v) + \pi_1(v^2)\beta(u) = \beta(u) + \beta(v),$$

amivel a tételt bebizonyítottuk.

q.e.d.

3.10. Tétel. *A Hilbert szimbólumhoz hozzárendelhető egy $[a, b] \in \mathbb{F}_2$ mennyiség, amire $(a, b) = (-1)^{[a,b]}$ teljesül (K^* minden a és b elemére). Ekkor $[.,.]$ egy nemelfajuló, szimmetrikus bilineáris forma K^*/K^{*2}-en, mint $\mathbb{F}_2$ feletti vektortéren.*

Mivel az előző fejezet végén láttuk, hogy $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq Z_2^3$ (2.32. következmény), $p > 2$-re $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq Z_2^2$ (2.30. következmény), $\mathbb{R}$-ről pedig nyilvánvaló, hogy $\mathbb{R}^*/\mathbb{R}^{*2} \simeq Z_2$, így valóban $\mathbb{F}_2$ feletti vektorterek. Ám, mivel az eredeti csoportok multiplikatívak (nem pedig additívak), így a bizonyításban is ennek megfelelően fogalmazunk.

Bizonyítás. A fügvény szimmetriája triviálisan igaz. A bilinearitáshoz így már elég a következőket látnunk minden a, a', b K^*-beli számra:

- $(aa', b) = (a, b)(a', b)$. Ez $p \neq 2$ mellett $\mathbb{Q}_p$-re a Legendre-szimbólum szorzattartása miatt nyilvánvaló. $\mathbb{Q}_2$-re már láttuk (az előző bizonyítás végén), hogy $\beta(uv) = \beta(-uv) = \beta(u) + \beta(v)$, illetve könnyen látható, hogy $\alpha(uv) = \pi_1(\frac{uv-1}{2}) = \alpha(u) + \pi_1(v)\alpha(v) = \alpha(u) + \alpha(v)$ (minden u, v 2-adikus egységre), így a fenti képletek alapján az állítás mindhárom esetben teljesül.

- $(1, a) = 1$. Ez (mivel az 1 mindenhol négyzetelem) megint csak nyilvánvaló.

A nemelfajultsághoz azt kell látnunk, hogy ha $(a, b) = 1$ minden K^*/K^{*2}-beli b-re, akkor $a = 1$ K^*/K^{*2}-ben. Ezt legegyszerűbben a K^*/K^{*2} csoportok reprezentánsain ellenőrizhetjük.

$\mathbb{Q}_2$-ben ezek, a 2.31. tétel alapján: ± 1, ± 5, valamint ezek kétszeresei. ($p^n u$ és $p^m v$ pontosan akkor egyenlő $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$-ben, ha n és m paritása megegyezik, valamint $\pi_3(u) = \pi_3(v)$.) Könnyen ellenőrizhető, hogy $u = \pm 1, \pm 5$-re $(5, 2u) = -1$, illetve hogy $(-1, -5) = -1$.

$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ reprezentánsai (a $p > 2$ esetben), a 2.29. tétel alapján: 1, u, p, pu, ahol $u \in U_p$ és $\left(\frac{u}{p}\right) = -1$. ($p^n v$ és $p^m w$ pontosan akkor egyenlőek $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-ben, ha n és m paritása egyenlő, valamint ha $\pi_1(v)$ és $\pi_1(w)$ egyszerre négyzetelem $\mathbb{F}_p^*$-ban.) Ekkor ellenőrizhető, hogy $(u, p) = -1$, illetve $(up, u) = -1$.

$\mathbb{R}$ esetében pedig ± 1 a reprezentánsok, tehát csak azt kell ellenőriznünk, hogy $(-1, -1) = -1$, ami nyilvánvaló.

Ezzel a tételt bebizonyítttuk.

q.e.d.

3.11. Következmény. Ha b K^* egy nem négyzet eleme, akkor NK_b^* egy 2 indexű részcsoport K^*-ban.

Bizonyítás. Vegyük a $\varphi_b(a) = (a, b)$ leképezést K^* és $(\{\pm 1\}, \cdot)$ között. Ez, mivel $[.,.]$ egy nemelfajuló bilineáris függvény, egy szürjektív homomorfizmus lesz. A 3.3. állításból látható, hogy magja pont NK_b^*. Vagyis K^*/NK_b^* izomorf $(\{\pm 1\}, \cdot)$-al.

q.e.d.

3.4. Elemek adott Hilbert-szimbólummal

Vezessük be a következő jelölést: minden a $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-beli elemre, és $\varepsilon = \pm 1$ számra $H_a^\varepsilon = \{x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} | (a, x) = \varepsilon\}$.

Ekkor H_1^1 nyilván megegyezik $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-el, H_1^{-1} pedig nyilván az üreshalmaz.

3.12. Lemma. *Ha $a \neq 1$ $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ egy eleme, akkor H_a^1 egy 2 indexű részcsoport $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-ben.*

Bizonyítás. Mivel láttuk, hogy a Hilbert-szimbólumból származtatott $[.,.]$ függvény egy nemelfajuló bilineáris forma, ezért az $x \mapsto (a, x)$ leképezés egy epimorfizmus lesz $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-ből $(\{\pm 1\}, \cdot)$-ra, vagyis:

$$|H_a^1| = |\ker(x \mapsto (a, x))| = \frac{\left|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right|}{|\{\pm 1\}|} = \frac{\left|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right|}{2}.$$

q.e.d.

3.13. Következmény.

$$|H_a^{-1}| = \left|\left(\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right) \setminus H_a^1\right| = \frac{\left|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right|}{2}.$$

3.14. Lemma. *Legyen $a, b \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, illetve $\varepsilon, \eta = \pm 1$. Tegyük fel továbbá, hogy sem H_a^ε, sem pedig H_b^η nem üres. Ekkor: $H_a^\varepsilon \cap H_b^\eta = \emptyset \Leftrightarrow a = b, \eta = -\varepsilon$.*

Bizonyítás. Mivel mind H_a^ε-nak, mind pedig H_b^η nemüres, és diszjunktak, így egyik sem lehet $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, tehát $a, b \neq 1$. Ekkor viszont mindkettejük elemszáma pont a fele $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ elemszámának, tehát egymás komplementerei. Mivel 1 benne van minden H_x^1 típusú halmazban, ezért $\eta = -\varepsilon$. Ekkor viszont $H_a^1 = H_b^1$ is teljesül, vagyis minden x-re $(a, x) = (b, x)$, így (mivel $[.,.]$ nemelfajuló), $a = b$ is igaz lesz. A feltételek elégségessége pedig nyilvánvaló.

q.e.d.

3.5. Racionális szám illesztése adott Hilbert-szimbólumokra

Ebben a szakaszban a különböző testek feletti Hilbert-szimbólumok kapcsolatáról látjuk be az ún. szorzatformulát, illetve (a fejezet utolsó tételeként) megvizsgáljuk, hogyan lehet bizonyos adatok mellett olyan racionális számot találni, hogy minden vizsgált testre a Hilbert-szimbóluma egy előre megadott ± 1 szám legyen.

Mivel $\mathbb{Q}$ része mind $\mathbb{R}$-nek, mind $\mathbb{Q}_p$-nek (tetszőleges p prímre), ezért bevezethetjük a következő jelöléseket:

3.15. Definíció. *Jelölje $(a, b)_p$ a és b $\mathbb{Q}_p$ fölötti Hilbert szimbólumát minden a és b $\mathbb{Q}^*$-beli elemre. Terjesszük ki továbbá a $\mathbb{Q}_p$ jelölést $p = \infty$-re, és értsük $\mathbb{Q}_\infty$ alatt $\mathbb{R}$-t. A pozitív prímek és a ∞ alkotta halmazt pedig nevezzük P-nek.*

3.16. Tétel (Szorzatformula)**.** *Minden a és b nemnulla racionális számra $(a,b)_p$ teljesül véges sok kivétellen minden $p \in P$-re. Ezen felül: $\prod_{p\in P}(a,b)_p = 1$.*

Bizonyítás. Mivel láttuk (a 3.10. tétel bizonyításában), hogy $(aa',b)_p = (a,b)_p(a',b)_p$ (minden a, a', b $\mathbb{Q}_p^*$-beli elemre), ezért elég az állítást arra az esete vizsgálni, ha a és b 1, -1 vagy (pozitív) prímszám.

- Ha a és b valamelyike 1, akkor $(a,b)_p = 1$ minden $p \in P$-re, tehát készen vagyunk.
- A Hilbert-szimbólumra adott képletek (ld. 3.8. és 3.9. tételek) alapján könnyen ellenőrizhető, hogy $(-1,-1)_p$ pontosan akkor -1, ha $p = 2$ vagy $p = \infty$.
- Szintén a képletek alapján ellenőrizhető, hogy $(-1,2)_p = 1$ minden $p \in P$-re. Ha q egy páratlan prím, akkor $(-1,q)_p = 1$, ha p q-tól különböző páratlan prím, $(-1,q)_\infty = 1$, $(-1,q)_2 = (-1)^{\alpha(q)}$, és $(-1,q)_q = \left(\frac{-1}{q}\right)$. Most vegyük észre, hogy a 6. oldalon írtak alapján prímhatványokra $\alpha = \varepsilon$, így $(-1,q)_2 = (-1,q)_q$.
- q prímre pedig láthatjuk, hogy $(q,q)_p = (q,-q^2)_p = (-1,q)_p(q,q)_p^2 = (-1,q)_p$ minden $p \in P$-re teljesül (felhasználva a Hilbert-szimbólum már ismert tulajdonságait – 3.6. következmény). Ha q páratlan, akkor $(2,q)_p = 1$, ha $p \neq 2, q$, és $(2,q)_2 = (-1)^{\beta(q)}$, valamint $(2,q)_q = \left(\frac{2}{q}\right)$, de a 6. oldalon írtak alapján ez a kettő megegyezik. Ha q és r különböző páratlan prímek, akkor pedig $(q,r)_p = 1$, ha $p \neq 2,q,r$, és $(q,r)_2 = (-1)^{\alpha(q)\alpha(r)}$, $(q,r)_q = \left(\frac{r}{q}\right)$, így a kvadratikus reciprocitási tétel (1.7. tétel), alapján $(q,r)_2(q,r)_q(q,r)_r = 1$.

q.e.d.

3.17. Tétel. *Legyenek $a_1, a_2, \ldots, a_n$ nemnulla racionális számok. Legyen továbbá $\varepsilon_{i,p}$ egy ± 1 szám minden $i = 1,\ldots,n$-re, illetve $p \in P$-re. Ezen feltételek mellett pontosan akkor létezik egy x nemnulla racionális szám, amire $(x,a_i)_p = \varepsilon_{i,p}$ (minden $i = 1,\ldots,n$, illetve minden $p \in P$ mellett), ha adott i mellett $\varepsilon_{i,p} = -1$ páros (így véges) sok $p \in P$-re teljesül, és ha minden $p \in P$-hez van egy x_p szám $\mathbb{Q}_p^*$-ban, amire $(x_p,a_i) = \varepsilon_{i,p}$ minden $i = 1,\ldots,n$-re.*

A tétel bizonyításához előbb egy lemmára van szükségünk:

3.18. Lemma. *Minden $p_0, p_1, \ldots, p_k$ P-beli elemre a $\prod_{i=0}^k \mathbb{Q}_{p_i}$ szorzatgyűrűnek sűrű részhalmaza a $(q,q,\ldots,q)$ alakú elemek halmaza, ahol $q \in \mathbb{Q}$.*

Bizonyítás. Az állítás nyilván ekvivalens azzal, hogy $\prod_{i=0}^k \mathbb{Q}_{p_i}$ minden y eleméhez, és minden η pozitív számhoz van olyan r racionális szám, amire $|y_i - r|_{p_i} < \eta$ minden $i = 0,\ldots k$-ra (ahol y_i az y i-edik koordinátáját jelöli, $|.|_\infty$ pedig a hagyományos abszolút érték). Feltehetjük, hogy $p_0 = \infty$. Feltehetjük azt is, hogy $y_i \in \mathbb{Z}_{p_i}$ minden $i = 1,\ldots,k$-ra, hiszen ez csak konstans szorzást jelent. (Létezik olyan a egész, amire ay_i p_i-adikus egész minden i-re, és ekkor $|ay_i - ar|_{p_i} = |a|_{p_i}|y_i - r|_{p_i}$.) Ekkor állítás pedig a következővel: minden η pozitív számra, és N pozitív egészre van olyan r racionális szám, amire $|y_0 - r| < \eta$, és $o_{p_i}(y_i - r) \geq N$ minden $i = 1,\ldots,k$-ra.

A kínai maradéktétel szerint van egy olyan a egész, amire $a = \pi_N(y_i)$, minden $i = 1,\ldots,k$-ra (π_N alatt mindig a megfelelő, $\mathbb{Z}_{p_i}$ feletti projekciót értve). Vegyünk egy $q \neq 1$ pozitív egész számot, ami nem osztható p_i-vel egyetlen $i = 1,\ldots,k$-ra sem. Ekkor található olyan b egész szám, és m pozitív egész, amire $|y_0 - (a + \frac{b}{q^m}(p_1 \cdot \cdots \cdot p_k)^N)| < \eta$. Így $r = a + \frac{b}{q^m}(p_1 \cdot \cdots \cdot p_k)^N$ megfelelő lesz.

q.e.d.

Most hozzákezdhetünk a tétel bizonyításához:

Bizonyítás. A tételben megfogalmazott feltételek szükségessége nyilvánvaló, vagyis elegendő egy olyan x nemnulla racionális számot találnunk, amire $(x,a_i)_p = \varepsilon_{i,p}$, minden $i = 1,\ldots,n$, illetve minden $p \in P$ számra.

Feltehetjük, hogy minden a_i egész, hiszen a Hilbert-szimbólum értéke érzéketlen a négyzetszámokkal való szorzásra. Legyen $S = \{p \in P | p = \infty,\ p = 2,$ vagy $p|a_i,$ valamely i-re$\}$, T pedig azon P-beli p elemek halmaza, amikhez van olyan i, amire $\varepsilon_{i,p} = -1$. Ezek mindketten véges halmazok, hiszen az a_i-k véges sokan vannak, és minden i-re csak véges sok $\varepsilon_{i,p} = -1$.

1. Ha $S \cap T = \emptyset$, és $T \neq \emptyset$ (a $T = \emptyset$ esetben az állítás triviális – $x = 1$ jó megoldás lesz), akkor legyen $m = 4 \prod_{p \in S \setminus \{\infty\}} p$, illetve $a = \prod_{p \in T} p$. Mivel S és T diszjunktak, és $2 \in S$, így a és m relatív prímek. A Dirichlet-tétel szerint van egy olyan q pozitív prím, amire $q \equiv a \pmod{m}$, és $q \notin S \cup T$, hiszen S és T véges halmazok. Most ellenőrizzük, hogy $x = aq$ megfelelő lesz:

   - $p \in S$-re $\varepsilon_{i,p} = 1$ minden $i = 1, \ldots, n$ esetén (hiszen S diszjunkt T-től). Ha $p = \infty$, akkor az állítás nyilvánvaló, mert $x > 0$. Ha $p \neq \infty$, akkor m definíciójából, látható, hogy $x \equiv a^2 \pmod{p}$, sőt $x \equiv a^2 \pmod{8}$ (mivel $2 \in S$). a relatív prím m-hez, így p-hez és 8-hoz is, amiből látható, hogy x négyzetelem $\mathbb{Q}_p^*$-ban (vö. 2.29., illetve 2.31. tétel), vagyis $(a_i, x)_p = 1$ minden i-re.

   - $p \notin S$-re minden a_i p-adikus egység. Mivel p páratlan prím, ezért $(a_i, x)_p = \left(\frac{a_i}{p}\right)^{o_{p_i}(x)}$ (ld. 3.8. tétel). Ha p nincs benne T-ben, és nem is q, akkor x p-adikus egység (nem osztható p-vel), vagyis $(a_i, x)_p = 1$, és mivel p nem T-beli, ezért $\varepsilon_{i,p}$ is 1 (minden $i = 1, \ldots, n$-re). Ha p T-beli, akkor $o_p(x) = 1$, vagyis $(a_i, x)_p = \left(\frac{a_i}{p}\right)$, másfelől van egy x_p szám $\mathbb{Q}_p^*$-ban, amire $(a_i, x_p)_p = \varepsilon_{i,p}$, minden i-re, és van olyan i, amire $\varepsilon_{i,p} = -1$, ezért $o_p(x_p)$ páratlan, így $\varepsilon_{i,p} = \left(\frac{a_i}{p}\right)$. Ha pedig $p = q$, akkor $(a_i, x)_p = \prod_{s \in P \setminus \{p\}} (a_i, x)_s = \prod_{s \in P \setminus \{p\}} \varepsilon_{i,s} = \varepsilon_{i,p}$.

2. A lemmából következik, hogy van egy olyan y racionális szám, amire minden $p \in S$-re és minden η pozitív számra $|y - x_p|_p < \eta$, vagyis $|\frac{y}{x_p} - 1|_p < \frac{\eta}{|x_p|_p}$. Mivel tudjuk, hogy $\mathbb{Q}_p^{*2}$ minden p-re nyílt $\mathbb{Q}_p^*$-ban (ld. 2.33. következmény, illetve $\mathbb{R}$-ben triviális), és S véges, így y választható olyannak, hogy $\frac{y}{x_p}$ négyzetelem legyen $\mathbb{Q}_p^*$-ban, minden S-beli p-re. Mivel a Hilbert-szimbólum értéke nem változik négyzetelemmel való szorzás esetén, ezért S-beli p-re $(a_i, y)_p = (a_i, x_p)_p = \varepsilon_{i,p}$, minden i-re. Most vagyük minden $p \in P$-re és $i = 1, \ldots, n$-re a $\eta_{i,p} = \varepsilon_{i,p}(a_i, y)_p$ számot. Ezek nyilván megfelelnek a tételben $\varepsilon_{i,p}$-re megkívánt feltételeknek, és mivel minden S-beli p-re, és minden i-re $\eta_{i,p} = 1$, ezért alkalmazható rá az előző pont (S nem függ az $\varepsilon_{i,p}$-k értékeitől), vagyis van egy olyan z nemnulla racionális szám, amire (minden p és i esetén) $(a_i, z)_p = \eta_{i,p}$ teljesül. Most az $x = yz$ számot véve minden $p \in P$-re, és minden $i = 1, \ldots, n$-re $(a_i, x)_p = (a_i, y)_p (a_i, z)_p = \varepsilon_{i,p} \eta_{i,p} = (a_i, y)_p \varepsilon_{i,p} (a_i, y)_p = \varepsilon_{i,p}$ teljesül, amivel a tételt bebizonyítottuk.

q.e.d.

4. fejezet

Lineáris algebrai áttekintés

Most, hogy végeztünk a Hilbert-szimbólum vizsgálatával, lassan rátérhetünk a kvadratikus alakok tárgyalására. Ám ez előtt, mintegy utolsó előkészítő lépésként, még meg kell vizsgálnunk bizonyos lineáris algebrai tényeket is. Mint ismeretes, az n változós kavadratikus alakok, és a az n dimenziós vektortéren értelmezett szimmetrikus bilineáris formák igen szoros kapcsolatban állnak egymással. (Bár ez a tény, illetve a köztük lévő kapcsolat mibenléte is közismert, a kvadratikus alakokról szóló fejezet elején röviden össze is foglaljuk ezt.) Éppen ezért ebben a fejezetben alapvetően a szimmetrikus bilineáris formák természetét fogjuk vizsgálni.

Ebben a fejezetben K egy tetszőleges 2-től különböző karakterisztikájú test lesz, V egy K fölötti, véges (n) dimenziós vektortér, $\langle .,. \rangle$ pedig egy szimmetrikus bilineáris forma (mondjuk röviden, hogy skalárszorzat) V fölött.

4.1. Alterek, bázisok

Először néhány apró állítást bizonyítunk, egy adott vektortér különvöző bázisaira, illetve a vektortér alterei és skalárszorzatai közötti kapcsolatra vonatkozóan.

4.1. Definíció. *V minden U alterére $q_U : V \to U^*$ legyen az a leképezés, ami V minden x eleméhez az $y \mapsto \langle x, y \rangle$ (U-ból K-ba képező) függvényt rendeli. Ekkor ($\langle .,. \rangle$ bilinearitása miatt) q_U egy homomorfizmus.*

4.2. Következmény. Nyilvánvalóan látszik, hogy $\langle .,. \rangle$ pontosan akkor nemelfajuló, ha q_V egy izomorfizmus.

4.3. Következmény. Amennyiben $\langle .,. \rangle$ nemelfajuló, úgy q_U minden U-ra szürjektív lesz, hiszen megegyezik a q_V bijekció, és a V^*-ból U^*-ra képező kanonikus szürjekció kompozíciójával.

4.4. Állítás. *Legyen V' egy véges dimenziós vektortér K fölött, és értelmezzünk rajta egy $\langle .,. \rangle'$ skalárszorzatot. Legyen továbbá f egy skalárszorzat-tartó homomorfizmus $(V, \langle .,. \rangle)$ és $(V', \langle .,. \rangle')$ között. Ha $\langle .,. \rangle$ nemelfajuló, akkor f injektív.*

Bizonyítás. Legyen x egy olyan eleme V-nek, amire $f(x) = 0$. Ekkor minden $y \in V$-re: $\langle x, y \rangle = \langle f(x), f(y) \rangle' = 0$, amiből $x = 0$ következik.

q.e.d.

4.5. Állítás. *Ha $\langle .,. \rangle$ nemelfajuló, akkor V minden U alterére: ${U^\perp}^\perp = U$, és $\dim U + \dim U^\perp = \dim V$.*

Bizonyítás. Mivel $\langle .,. \rangle$ nemelfajuló, így q_U szürjektív, ezért a

$$0 \longrightarrow U^\perp \hookrightarrow V \xrightarrow{q_U} U^* \longrightarrow 0$$

sorozat egzakt, amiből $\dim U + \dim U^\perp = \dim V$ azonnal következik. Hasonlóan igaz, hogy $\dim U^\perp + \dim {U^\perp}^\perp = \dim V$, így $\dim {U^\perp}^\perp = \dim U$, és tudjuk, hogy $U \leq {U^\perp}^\perp$, vagyis $U = {U^\perp}^\perp$.

q.e.d.

4.6. Következmény. Ha $\langle .,. \rangle$ nemelfajuló, akkor egyszerre lesz nem elfajuló U-ra, illetve $U^\perp$-re megszorítva, hiszen pontosan akkor nemelfajuló U-n, ha $U \cap U^\perp = 0$, és pontosan akkor nemelfajuló $U^\perp$-en, ha $U^\perp \cap U^{\perp\perp} = U^\perp \cap U = 0$.

Amennyiben $\langle .,. \rangle$ U-n (és így $U^\perp$-en) nemelfajuló, úgy $V = U \oplus U^\perp$.

4.7. Definíció. *Ha V kétdimenziós, és van olyan x, y bázisa, melyre x és y is izotróp (vagyis $\langle x,x \rangle = \langle y,y \rangle = 0$), de $\langle x,y \rangle \neq 0$, akkor $(V, \langle .,. \rangle)$-ot hiperbolikus síknak nevezzük.*

4.8. Lemma. *x legyen V egy nemnulla izotróp eleme. Ha $\langle .,. \rangle$ nemelfajuló, akkor minden ilyen x-hez van egy y elem V-ben, hogy* $\mathrm{span}(x,y)$ *egy hiperbolikus sík lesz.*

Bizonyítás. Mivel $\langle .,. \rangle$ nemelfajuló, így van egy olyan z elem V-ben, amire $\langle x,z \rangle = 1$. Ekkor $y = z - \frac{\langle z,z \rangle}{2} x$-re $\langle y,y \rangle = \langle z,z \rangle - \langle z,z \rangle \langle z,x \rangle + \left(\frac{\langle z,z \rangle}{2} \right)^2 \langle x,x \rangle = 0$, és $\langle x,y \rangle = \langle x,z \rangle - \frac{\langle z,z \rangle}{2} \langle x,x \rangle = 1$, amivel a lemmát bebizonyítottuk.

q.e.d.

4.9. Állítás. *Ha $\langle .,. \rangle$ nemelfajuló, és V-ben van egy nemnulla, izotróp vektor, akkor a V-ből K-ba képező $y \mapsto \langle y,y \rangle$ függvény szürjektív.*

Bizonyítás. Az előző lemma szeint van V-ben egy nemnulla, izotróp elem (legyen z), amire $\langle x,z \rangle = 1$. Most vegyük K egy a elemét. Ekkor: $\left\langle x + \frac{a}{2} z, x + \frac{a}{2} z \right\rangle = \langle x,x \rangle + a \langle x,z \rangle + \frac{a^2}{4} \langle z,z \rangle = a$.

q.e.d.

4.10. Definíció. *V fölött két bázist kapcsolódónak mondunk, ha van közös báziselemük.*

4.11. Állítás. *Ha $\langle .,. \rangle$ nemelfajuló, és $n \geq 3$, akkor V bármely két ortogonális bázisa „összeköthető" kapcsolódó ortogonális bázisok véges láncával.*

Bizonyítás. Legyen e és f V két ortogonális bázisa. (e elemei: $e_1, \ldots, e_n$, f elemei pedig $f_1, \ldots, f_n$.) Mivel $\langle .,. \rangle$ nemelfajuló, és e, illetve f ortogonálisak, ezért $\langle e_i, e_i \rangle, \langle f_i, f_i \rangle \neq 0$ minden $i = 1, \ldots, n$-re teljesül.

- Ha van olyan $i,j = 1, \ldots, n$, hogy $\langle e_i,e_i \rangle \langle f_j,f_j \rangle - \langle e_i,f_j \rangle^2 \neq 0$, akkor feltehetjük, hogy $i = j = 1$. Ekkor nyilvánvaló, hogy e_1 és f_1 lineárisan függetlenek. Az is látható, hogy $\mathrm{span}(e_1,f_1)$-en $\langle .,. \rangle$ nemelfajuló, mert ha λ és μ olyan K-beli elemek, amikre $\langle \lambda e_1 + \mu f_1, e_1 \rangle = 0 = \langle \lambda e_1 + \mu f_1, f_1 \rangle$ teljesül, akkor $\lambda(\langle e_1,e_1 \rangle \langle f_1,f_1 \rangle) = -\mu \langle e_1,f_1 \rangle \langle f_1,f_1 \rangle = \lambda \langle e_1,f_1 \rangle^2$ amiből $\lambda = 0$ következik. Tehát $\mu \langle f_1,f_1 \rangle = 0$, amiből pedig $\mu = 0$ adódik.

  Legyen $e' = f_1 - \frac{\langle e_1,f_1 \rangle}{\langle e_1,e_1 \rangle} e_1$ (ami értelmes, mert $\langle e_1,e_1 \rangle \neq 0$). Ekkor $e' \perp e_1$, és $\mathrm{span}(e_1,e') = \mathrm{span}(e_1,f_1)$. Hasonló igaz $f' = e_1 - \frac{\langle e_1,f_1 \rangle}{\langle f_1,f_1 \rangle} f_1$-re is.

  Most vegyük $\mathrm{span}(e_1,f_1)^\perp$ egy g ortogonális bázisát. Ekkor az $e \to (e_1,e',g) \to (f_1,f',g) \to f$ lánc jó lesz, hiszen $\langle .,. \rangle$ elmelfajuló, sőt nemelfajuló $\mathrm{span}(e_1,f_1)$-en sem, így $\mathrm{span}(e_1,f_1) \oplus \mathrm{span}(e_1,f_1)^\perp = V$. (ld. 4.6. következmény)

- Ha minden $i,j = 1, \ldots, n$-re $\langle e_i,e_i \rangle \langle f_j,f_j \rangle - \langle e_i,f_j \rangle^2 = 0$, akkor be fogjuk látni, hogy van egy olyan $x \in K$, hogy $f' = f_1 + x f_2$ nem izotróp, és $\mathrm{span}(e_1,f')$ egy kétdimenziós altér, amin $\langle .,. \rangle$ nemelfajuló.

  Akkor, és csak akkor létezik ilyen x, ha $\langle f',f' \rangle = \langle f_1,f_1 \rangle + x^2 \langle f_2,f_2 \rangle \neq 0$, és (mint az előző pontban láttuk) $0 \neq \langle e_1,e_1 \rangle \langle f',f' \rangle - \langle e_1,f' \rangle^2 = \langle e_1,e_1 \rangle \langle f_1,f_1 \rangle + x^2 \langle e_1,e_1 \rangle \langle f_2,f_2 \rangle - \langle e_1,f_1 \rangle^2 - 2x \langle e_1,f_1 \rangle \langle e_1,f_2 \rangle - x^2 \langle e_1,f_2 \rangle^2 = -2x \langle e_1,f_1 \rangle \langle e_1,f_2 \rangle$. Mivel a feltételből következik, hogy $\langle e_i,f_j \rangle$ semmilyen i-re, j-re nem lesz 0, ezért a most megfogalmazott két feltétel pont azt jeleni, hogy $x \neq 0$, és $x^2 \neq -\frac{\langle f_1,f_1 \rangle}{\langle f_2,f_2 \rangle}$. Ez legfeljebb három x-et zár ki, tehát ha K-nak legalább négy elem van, akkor valóban van megfelelő x.

  A $K = \mathbb{F}_2$ esetet kizárja, hogy $\mathrm{char} K \neq 2$, $\mathbb{F}_3$-ban pedig csak a 0 és az 1 négyzetelemek, így a feltételből $\langle e_i,e_i \rangle \langle f_j,f_j \rangle = 1$, minden i-re, j-re, és azaz $\frac{\langle f_1,f_1 \rangle}{\langle f_2,f_2 \rangle} = 1$, vagyis annak kell teljesülni, hogy $x^2 \neq 0, -1$, tehát $x = 1, 2$ bármelyike jó lesz.

  Mivel f' nem izotróp, ezért (az előző ponthoz hasonlóan) van egy olyan g vektor, hogy (f',g) $\mathrm{span}(f_1,f_2)$ egy ortonormált bázisát alkotja. Mivel $\mathrm{span}(e_1,f')$-en $\langle .,. \rangle$ nemelfajuló, ezért $\langle e_1,e_1 \rangle \langle f',f' \rangle - \langle e_1,f' \rangle^2 \neq 0$, vagyis alkalmazhatjuk az első pontot e-re és $(f',g,f_3,f_4,\ldots,f_n)$-re.

q.e.d.

4.2. Monomorfizmusok kiterjesztése

Ebben a szakaszban Witt tételét bizonyítjuk, a skalárszorzat-tartó monomorfizmusok kiterjeszthetőségéről. Erre azért lesz szükségünk, mert egy igen fontos következményét (4.14. következmény) használni fogjuk a kvadratikus alakok bizonyos tulajdonságainak igazolásához. A Witt-tétel bizonyítása előtt azonban be kell látnunk a következő lemmát:

4.12. Lemma. *Legyen V' egy véges dimenziós K feletti vektortér, $\langle .,. \rangle'$ pedig egy nemelfajuló skalárszorzat V'-n. Tegyük fel továbbá, hogy $\langle .,. \rangle$ nemelfajuló. Ekkor minden $U \leq V$ altérre, amin $\langle .,. \rangle$ már elfajuló, és minden $\varphi : U \rightarrowtail V'$ skalárszorzat-tartó monomorfizmusra φ kiterjeszthető egy $\varphi_1 : U_1 \rightarrowtail V'$ skalárszorzat-tartó monomorfizmussá, ahol $U < U_1 \leq V$, és U hipersík U_1-ben.*

Bizonyítás. Mivel U-n $\langle .,. \rangle$ elfajuló, ezért van U-nak egy olyan x nemnulla eleme, ami $U^\perp$-nek is eleme. Vegyünk most egy α lineáris leképezést U-ból K-ba, amire $\alpha(x) = 1$. (Ilyen leképezés mindenképpen létezik – például vegyünk egy x-et tartalmazó bázist U-ban, és legyen $\alpha(x) = 1$, a bázis összes többi v elemére pedig $\alpha(v) = 0$. Ezzel a lineáris leképezést egyértelműen meghatároztuk.) Mivel V-n $\langle .,. \rangle$ nemelfajuló, ezért (a 4.2. következmény miatt) kell lennie V-ben egy olyan y elemnek, hogy $\langle y, u \rangle = \alpha(u)$ minden U-beli u-ra.

Most tekintsük az $y - \frac{\langle y,y \rangle}{2} x$ elemet. Erre $\left\langle y - \frac{\langle y,y \rangle}{2} x, u \right\rangle = \langle y, u \rangle - \frac{\langle y,y \rangle}{2} \langle x, u \rangle = \alpha(u)$, minden $u \in U$ esetén, és $\left\langle y - \frac{\langle y,y \rangle}{2} x, y - \frac{\langle y,y \rangle}{2} x \right\rangle = \langle y, y \rangle - \langle y, y \rangle \langle y, x \rangle + \left(\frac{\langle y,y \rangle}{2} \right)^2 \langle x, x \rangle = \langle y, y \rangle (1 - \alpha(x)) = 0$. Vagyis feltehetjük, hogy $\langle y, y \rangle = 0$.

Abból, hogy $\langle y, x \rangle = \alpha(x) = 1$ rögtön következik, hogy $y \notin U$, vagyis az $U_1 := U \oplus \operatorname{span}(y)$ hipersíkként fogja tartalmazni U-t. Már csak azt kell látnunk, hogy innen van egy φ_1 skalárszorzat-tartó monomorfizmus V'-be, amire teljesül, hogy $\varphi_1|_U = \varphi$.

Most vegyük észre, hogy mivel φ skalárszorzat-tartó monomorfizmus, ezért $U' = \varphi(U)$-n $\langle .,. \rangle'$ elfajuló lesz, tehát rajta is igazak mindazok a megállapítások, amiket fent U-ra megtettünk. Sőt, az $x' = \varphi(x)$ elem, illetve az $\alpha' = \alpha \circ \varphi^{-1}$ is játszhatják x, illetve α szerepét, és ezekhez található egy megfelelő $y' \in V'$ elem, amire $\alpha'(u') = \langle y', u' \rangle'$ minden U'-beli u' elemre, és $\langle y', y' \rangle' = 0$. És most vegyük észre, hogy az U_1-en értelmezett, $U_1' = U' \oplus \operatorname{span}(y')$-be képező $\varphi_1(u + \lambda y) = \varphi(u) + \lambda y'$ leképezés megfelelő lesz.

q.e.d.

4.13. Tétel (Witt tétele)**.** *Legyenek V és V' két véges dimenziós K-vektortér, valamely K test felett, és legyenek rajtuk értelmezve a $\langle .,. \rangle$ (V-n), illetve a $\langle .,. \rangle'$ (V'-n) nemelfajuló, szimmetrikus bilineáris formák. Tegyük fel, hogy $(V', \langle .,. \rangle')$ és $(V, \langle .,. \rangle)$ izomorfak. Ekkor V minden U alterére, és minden $\varphi : (U, \langle .,. \rangle|_U) \rightarrowtail (V', \langle .,. \rangle')$ monomorfizmusra, φ kiterjeszthető egy egész V-n értelmezett, skalárszorzat-tartó monomorfizmussá.*

Bizonyítás. Mivel $(V', \langle .,. \rangle')$ és $(V, \langle .,. \rangle)$ izomorfak, feltehetjük, hogy $V' = V$, és $\langle .,. \rangle' = \langle .,. \rangle$. Az előző lemma alapján pedig az is feltehető, hogy $\langle .,. \rangle|_U$ nemelfajuló.

Most teljes indukciót fogunk alkalmazni $\dim U$-ra.

Ha $\dim U = 1$, akkor létezik egy nemizotróp elem U-ban (legyen ez x), ami generálja U-t (valójában U minden nemnulla eleme ilyen). A $\varphi(x)$ elemet nevezzük y-nak. Ekkor nyilván $\langle y, y \rangle = \langle x, x \rangle$. Tekintsük az $x + y$ és az $x - y$ elemeket. $\langle x + y, x + y \rangle = 2\langle x, x \rangle + 2\langle x, y \rangle$, illetve $\langle x - y, x - y \rangle = 2\langle x, x \rangle - 2\langle x, y \rangle$, amiből következik, hogy legalább az egyik nemizotróp, különben $\langle x, x \rangle = -\langle x, x \rangle \Rightarrow \langle x, x \rangle = 0$ adódna. Nevezzük az egyik nemizotrópot z-nek (ekkor a másik vektor $2x - z$ lesz).

Mivel z nem izotróp, ezért $V = z^\perp \oplus \operatorname{span}(z)$. Tekintsük V-nek azt a σ automorfizmusát, amire $\sigma(v + \lambda z) = v - \lambda z$ (ahol $v \in z^\perp$, és $\lambda \in K$ – σ voltaképpen a $z^\perp$-re való tükrözés). Könnyen ellenőrizhető, hogy $2x - z \perp z$, így $\sigma(2x - z) = 2x - z$, illetve $\sigma(z) = -z$, amiből $\sigma(x) = x - z = \pm y$ következik. Ekkor, (mivel $\langle x, x \rangle = \langle y, y \rangle = \langle -y, -y \rangle$) σ és $-\sigma$ valamelyike φ kiterjesztése lesz V-re. ($\pm\sigma$ skalárszorzat-tartása abból adódik, hogy $\operatorname{span}(z)$-n, illetve $z^\perp$-en is az identitás ± 1-szerese.)

Ha U nem egydimenziós, akkor (mivel $\langle .,. \rangle|_U$ nemelfajuló) felbontható egy $U_1 \neq 0$ és egy $U_2 \neq 0$ altér direktösszegére, sőt feltehető, hogy $U_1 \perp U_2$. Ennek megfelelően φ is felbomlik két

($\varphi_1 = \varphi|_{U_1}$, illetve $\varphi_2 = \varphi|_{U_2}$) komponensre. Ekkor az indukciós feltevés miatt φ_1 kiterjeszthető V egy σ_1 skalárszorzat-tartó automorfizmusává. Most tekintsük a $\varphi' = \sigma_1^{-1} \circ \varphi$ leképezést. Ez nyilván egy $U \rightarrowtail V$ skalárszorzat-tartó monomorfizmus lesz, amire $\varphi'|_{U_1} = \mathrm{Id}|_{U_1}$, tehát $\varphi'|_{U_2}$ egy a tétel feltételeinek megfelelő leképezés lesz U_2-ből V-be, vagyis az indukciós feltevés szerint kiterjeszthető egy $\sigma_2' : V \rightarrowtail\!\!\!\!\twoheadrightarrow V$ skalárszorzat-tartó automorfizmussá, sőt erről feltehetjük, hogy U_1-en identitásként viselkedik, hiszen az indukciós feltevést alkalmazhatjuk $U_2 \leq U_1^{\perp}$-re is. Ekkor σ_2' a $\varphi' = \sigma_1^{-1} \circ \varphi$ leképezés egy kiterjesztése lesz, tehát a $\sigma_1 \circ \sigma_2'$ leképezés kielégíti a feltételeket.

q.e.d.

4.14. Következmény. Ha egy $(V, \langle .,. \rangle)$ térnek két altere izomorf, akkor az ortogonális kiegészítő altereik is izomorfak.

4.3. Vektorterek és a Hilbert-szimbólum

Ebben a szakaszban a $\mathbb{Q}_p$ feletti vektorterek egy speciális tulajdonságát vizsgáljuk meg: Legyen p egy prímszám, vagy $p = \infty$. Ekkor $\mathrm{char}\mathbb{Q}_p = \infty$, vagyis nem 2, tehát a fentiek mind igazak $K = \mathbb{Q}_p$-re is. Tegyük fel továbbá, hogy $\langle .,. \rangle$ nemelfajuló, vagyis $\mathrm{disc}(\langle .,. \rangle) \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Vegyünk egy $e = (e_1, \ldots, e_n)$ ortogonális bázist, és legyen $a_i = \langle e_i, e_i \rangle$, minden $i = 1, \ldots, n$-re. Ekkor $\mathrm{disc}(\langle .,. \rangle) = \prod_{i=1}^n a_i$, mint $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ eleme. Vezessük be a következő jelölést: $\varepsilon(e) := \prod_{i<j}(a_i, a_j)$.

4.15. Tétel. *$\varepsilon(e)$ értéke állandó.*

Bizonyítás. Alkalmazzunk teljes indukciót n-re.

Ha $n = 1$, akkor az állítás triviális.

Ha $n = 2$, akkor $\varepsilon(e) = 1$ pontosan akkor, ha az $x^2 - a_1y^2 - a_2z^2$ polinomnak van nemtriviális gyöke. Ez kétféle módon történhet meg. Ha a megoldásban $x \neq 0$, akkor $a_1\left(\frac{y}{x}\right)^2 + a_2\left(\frac{z}{x}\right)^2 = 1$, ha pedig $x = 0$, akkor $\langle ye_1 + ze_2, ye_1 + ze_2 \rangle = a_1y^2 + a_2z^2 = 0$, vagyis $ye_1 + ze_2$ egy nemnulla, izotróp vektor, és így (a 4.9. állítás alapján) vannak olyan y', z' értékek, amikre $a_1y'^2 + a_2z'^2 = \langle y'e_1 + z'e_2, y'e_1 + z'e_2 \rangle = 1$. Vagyis ekkor $a_1x^2 + a_2y^2 = 1$-nek is van egy nemtriviális megoldása. Ennek fordítottja pedig nyilvánvaló, tehát az, hogy $a_1x^2 + a_2y^2 = 1$-nek nemtriviális megoldása, az ekvivalens azzal, hogy $\varepsilon(e) = 1$. Viszont (mint láttuk) ekvivalens azzal is, hogy van olyan $(x, y) \neq (0, 0)$, amire $\langle xe_1 + ye_2, xe_1 + ye_2 \rangle = 1$, vagyis, hogy van olyan v nemnulla vektor, amire $\langle v, v \rangle = 1$, ami valóban független e választásától.

Ha $n \geq 3$ esetén (a 4.11. állítás miatt) elegendő kapcsolódó ortogonális bázisokra bizonyítanunk. A Hilbert-szimbólum szimmetriája miatt feltehetjük, hogy $e_1 = f_1$, és $\varepsilon(e) = \varepsilon(f)$-et kell bizonyítanunk. Minden $i = 1, \ldots, n$-re legyen $b_i = \langle f_i, f_i \rangle$. Ekkor:

$$\begin{aligned}
\varepsilon(e) &= \prod_{i<j}(a_i, a_j) = \left(\prod_{j=2}^{n}(a_1, a_j)\right)\left(\prod_{2\leq i<j}(a_i, a_j)\right) = (a_1, \mathrm{disc}(\langle .,. \rangle)a_1^{-1}) \prod_{2\leq i<j}(a_i, a_j) = \\
&= (a_1, \mathrm{disc}(\langle .,. \rangle)a_1) \prod_{2\leq i<j}(a_i, a_j), \text{ és hasonlóan:} \\
\varepsilon(f) &= (b_1, \mathrm{disc}(\langle .,. \rangle)b_1) \prod_{2\leq i<j}(b_i, b_j).
\end{aligned}$$

Az indukciós feltevést $e_1^{\perp}$-re alkalmazva látható, hogy $\prod_{2\leq i<j}(a_i, a_j) = \prod_{2\leq i<j}(b_i, b_j)$, és $e_1 = f_1$ miatt $a_1 = b_1$, vagyis $(a_1, \mathrm{disc}(\langle .,. \rangle)a_1) = (b_1, \mathrm{disc}(\langle .,. \rangle)b_1)$, amivel az állítást beláttuk.

q.e.d.

5. fejezet

Kvadratikus alakok

Most, hogy minden szükséges előkészületet megtettünk, végre rátérhetünk a kvadratikus alakok vizsgálatára. Kezdjük talán a definícióval:

5.1. Definíció (Kvadratikus alak)**.** *Egy tetszőleges K test fölötti kvadratikus alakon, egy (véges változós) homogén, másodfokú polinomot értünk.*

Mivel nekünk csak $\mathbb{Q}$, $\mathbb{Q}_p$, valamint $\mathbb{R}$ feletti kvadratikus alakokkal lesz dolgunk, és a 2 karakterisztikájú testek felett a kvadratikus alakok közismerten kellemetlenül viselkednek, ezért a továbbiakban a következő jelöléssel élünk: K a fejezet további részében egy tetszőleges testet jelöl, melynek karakterisztikája nem 2.

5.1. A kvadratikus alakokról általában

Minden f kvadratikus alak felírható $f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$ alakban (ahol $a_{ij} \in K$). Mivel char$K \neq 2$, ezért feltehető, hogy $a_{ij} = a_{ji}$ (minden $i, j = 1, \ldots, n$-re), és így a felírás egyértelmű lesz. Ekkor az $A = (a_{ij})_{i,j=1}^{n}$ mátrixot a kvadratikus alak mátrixának nevezzük. Mint minden $n \times n$-es mátrix, ez is meghatároz egy bilineáris függvényt K^n felett: $\langle x, y \rangle = x^T A y$. Ez a bilineáris forma (mivel A szimmetrikus) egy szimmetrikus bilineáris forma (mondjuk röviden: skalárszorzat) lesz, amire $\langle x, x \rangle = f(x)$. Az is könnyen látható, hogy így $\langle x, y \rangle = \frac{f(x+y)-f(x)-f(y)}{2}$, amiből következik, hogy az n változós kvadratikus alakok, és a K^n feletti szimmetrikus bilineáris formák között egy bijekciót találtunk. Az f-hez rendelt skalárszozatot $\langle ., . \rangle_f$-el fogjuk jelölni.

5.2. Definíció. *Két (f és g) kvadratikus alakot ekvivalensnek mondunk, ha $(K^n, \langle ., . \rangle_f)$, és $(K^n, \langle ., . \rangle_g)$ izomorf.*

Ez nyilván egy ekvivalenciareláció lesz. A fenti technikailag azt jelenti, hogy egy f kvadratikus alak, aminek a mátrixa A, és egy g kvadratikus alak, aminek a mátrixa B pontosan akkor ekvivalens, ha van olyan P invertálható ($n \times n$-es) mátrix, amire $B = PAP^T$. Az is nyilvánvaló, hogy az f-hez rendelt bilineáris forma diszkriminánsa megegyezik minden f-el ekvivalkens kvadratikus alakhoz rendelt skalárszorzat diszkriminálnsával. Ezt a $(K^*/K^{*2} \cup \{0\}$-beli) értéket nevezzük f diszkriminánsának, és $d(f)$-el jelöljük. Amennyiben $d(f) \neq 0$, akkor f-et nemelfajulónak mondjuk. (Vegyük észre, hogy ez pont ekvivalens azzal, hogy az f-hez rendelt skalárszorzat nemelfajuló – ami ekvivalens azzal, hogy minden $g \sim f$ kvadratikus alakra $\langle ., . \rangle_g$ nemelfajuló.)

Most lássunk néhány állítást, amik segítségünkre lesznek a kvadratikus alakok nemtriviális gyökeinek kezelésében:

5.3. Lemma. *Ha f és g ekvivalens (n változós) kvadratikus alakok, akkor értékkészletük megegyezik.*

Bizonyítás. f éa g ekvivalens, tehát $(K^n, \langle ., . \rangle_f)$ és $(K^n, \langle ., . \rangle_g)$ izomorfak. Ekkor nyilvánvaló, hogy $x \mapsto \langle x, x \rangle_f = f(x)$ és $y \mapsto \langle y, y \rangle_g = g(y)$ értékkészlete megegyezik, amivel a lemmát bebizonyítottuk.

q.e.d.

5.4. Következmény. A lemma bizonyításából az is kiderül, hogy f-nek pontosan akkor van nemtriviális gyöke, ha g-nek is van.

Ezekből az állításokból azt láthatju, hogy amikor majd a különböző kvadratikus alakok nemtriviális gyökeit (vagy felvett értékeit) keressük, akkor mindig elegendő az ekvivalenciaosztályaikra, vagy ekvivalenciaosztályaik egy tetszőleges reprezentánsára szorítkoznunk.

Miután később látni fogjuk, hogy egy kvadratikus alakot vizsgálva, a nemtriviális gyöklétezésének igazolásához sokszor hasznos lehet tudni, bizonyos más kvadratikus alakok felvesznek-e egyes értékeket, így nem meglepő, hogy a következő állítás a későbbiekben hasznunkra válik:

5.5. Állítás. *Legyen f egy nemelfajuló, n változós kvadratikus alak, és tegyük fel, hopy létezik egy x K^n-beli nemnulla vektor, amire $f(x) = 0$. Ekkor f szürjektív leképezés K^n-ből K-ra.*

Bizonyítás. Ez a 4.9. állítás nyilvánvaló következménye.

q.e.d.

Megjegyzés. Az, hogy $x \in K^n$-re $f(x) = 0$, az pont azt jelenti, hogy x $\langle .,. \rangle_f$-re nézve izotróp.

Most pedig belátjuk, hogy a kvadratikus alakok minden ekvivalenciaosztályában van „szép" kvadratikus alak:

5.6. Állítás. *Minden f kvadratikus alakhoz van egy vele ekvivalens g kvadratikus alak, aminek a mátrixa diagolnális.*

Bizonyítás. Voltaképpen azt kell látnunk, hogy K^n-nek van egy olyan bázisa, ami az f által a kanonikus bázis felett generált bilineáris formára nézve ortogonális. Ez pedig nyilván ekvivalens azzal, hogy minden szimmetrikus bilineáris formához van egy rá nézve ortogonális bázis. Ez pedig (mivel feltettük, hogy char$K \neq 2$) valóban teljesül.

q.e.d.

5.7. Következmény. Minden f n változós kvadratikus alakra van olyan $m \leq n$ pozitív egész, és olyan $a_1, \ldots, a_m \in K$ számok, amikre: $f(x_1, x_2, \ldots, x_n) \sim a_1x_1^2 + a_2x_2^2 + \cdots + a_mx_m^2$.

m értéke nyilván egyértelmű. Ezt a számot nevezzük f rangjának, és $r(f)$-e jelöljük.

Most definiáljuk, majd karakterizáljuk is az úgynevezett hiperbolikus kvadratikus alakokat:

5.8. Definíció. *Egy f kétváltozós kvadratikus alakot hiperbolikusnak mondunk, ha $(K^2, \langle .,. \rangle_f)$ hiperbolikus sík. (ld. 4.7. definíció)*

5.9. Állítás. *Ha $f(x, y)$ egy hiperbolikus kvadratikus alak, akkor $f(x, y) \sim x^2 - y^2$.*

Bizonyítás. Mivel $(K^2, \langle .,. \rangle_f)$ hiperbolikus, így van két vektor (u és v), amikre: $\langle u, u \rangle_f = \langle v, v \rangle_f = 0$, illetve $\langle u, v \rangle_f = 2$ (char$K \neq 2$). Ekkor u és v nyilván egy bázisa K^2-nek. Most alkalmazzuk a következő automorfizmust K^2-en: $u \mapsto (1, 1)$; $v \mapsto (1, -1)$. Vegyük észre, hogy a $x^2 - y^2$-hez tartozó skalárszorzat a következő: $\langle (x_1, x_2), (y_1, y_2) \rangle = x_1y_1 - x_2y_2$, illetve, hogy $\langle (1, 1), (1, 1) \rangle = 0$, $\langle (1, -1), (1, -1) \rangle = 0$ és $\langle (1, 1), (1, -1) \rangle = 2$, tehát az automorfizmus egy izomorfizmus lesz $(K^2, \langle .,. \rangle_f)$ és $(K^2, \langle .,. \rangle)$ között.

q.e.d.

5.10. Következmény. $xy \sim x^2 - y^2$, hiszen az $(1, 0), (0, 1)$ bázist tekintve nyilvánvaló, hogy xy hiperbolikus.

Amennyiben van két vektorterünk, rajtuk pedig egy-egy szimmetrikus bilineáris forma, akkor a két vektortér direktösszegén ezek egy újabb szimmetrikus bilineáris formát generálnak: $(V_1, \langle .,. \rangle_1) \oplus (V_2, \langle .,. \rangle_2) = (V_1 \oplus V_2, \langle .,. \rangle)$, ahol $\langle u_1 + u_2, v_1 + v_2 \rangle = \langle u_1, v_1 \rangle_1 + \langle u_2, v_2 \rangle_2$, V_1 minden u_1 és v_1, valamint V_2 minden u_2 és v_2 elemére. Ekkor két tetszőleges kvadratikus alakra bevezethetjük a következő definíciót:

5.11. Definíció. *Legyen f egy n változós, g pedig egy m változós kvadratikus alak K fölött. Ekkor $f \oplus g$ alatt a következő $n+m$ változós kvadratikus alakot értjük: $(f \oplus g)(x, y) = f(x) + g(y)$, minden $x \in K^n$, $y \in K^m$ mellett.*

Nyilvánvalóan látszik, hogy $(K^n, \langle .,. \rangle_f) \oplus (K^m, \langle .,. \rangle_g) = (K^{n+m}, \langle .,. \rangle_{f \oplus g})$, ami magyarázza a definíció fontosságát, és a jelölés megválasztását is.

Lássunk is néhány példát, hol használható a kvadratikus alakok „direktösszege”:

5.12. Lemma. *Ha f nemelfajuló, és van nemtriviális gyöke, akkor f-hez vannak olyan f_0 és g kvadratikus alakok, ahol g $n-2$ változós, f_0 kétváltozós és hiperbolikus, és $f \sim f_0 \oplus g$.*

Bizonyítás. Az, hogy f-nek van nemtriviális gyöke, pont azt jelenti, hogy $(K^n, \langle .,. \rangle_f)$-ben van nemnulla, izotróp vektor. Ekkor a 4.8. lemma szerint K^n-nek van egy altere, $\langle .,. \rangle_f$-re nézve hiperbolikus sík (legyen U). Ekkor van ebben a síkban egy bázis (u és v), amire u és v is izotróp, de $\langle u, v \rangle_f = 1$. Tegyük fel, hogy $\lambda u + \mu v$ olyan, hogy U minden x elemére $\langle \lambda u + \mu v, x \rangle_f = 0$. Ekkor $\mu = \langle \lambda u + \mu v, u \rangle_f = 0$. Hasonlóan látható, hogy $\lambda = 0$, vagyis $\langle .,. \rangle_f$ U-ra megszorítva is nemelfajuló lesz. Így a 4.6. következmény szerint $K^n = U \oplus U^\perp$. Mivel $U \simeq K^2$, ezért létezik egy olyan $\langle .,. \rangle_0$ skalárszorzat K^2-en, amire $(U, \langle .,. \rangle_f|_U) \simeq (K^2, \langle .,. \rangle_0)$, és hasolóan van olyan $\langle .,. \rangle_1$ skalárszorzat K^{n-2}-n, amire $(U^\perp, \langle .,. \rangle_f|_{U^\perp}) \simeq (K^{n-2}, \langle .,. \rangle_1)$, így (mivel $U \perp U^\perp$, és U-n $\langle .,. \rangle_f$ nemelfajuló) $(K^n, \langle .,. \rangle_f) = (U, \langle .,. \rangle_f|_U) \oplus (U^\perp, \langle .,. \rangle_f|_{U^\perp}) \simeq (K^2, \langle .,. \rangle_0) \oplus (K^{n-2}, \langle .,. \rangle_1)$. Ekkor legyen f_0 a $\langle .,. \rangle_0$-hoz hozzárendelt, g pedig a $\langle .,. \rangle_1$-hez hozzárendelt kvadratikus alak. Így f_0 és g a feltételeket kielégítik.

q.e.d.

5.13. Állítás. *Legyen f nemelfajuló, a pedig egy nemnulla elem K-ból. Ekkor a következők ekvivalensek:*

1. *f felveszi a-t.*
2. *Van egy $n-1$ változós g kvadratikus alak, amire $f(x_1, \ldots, x_{n-1}, y) \sim g(x_1, \ldots, x_{n-1}) \oplus ay^2$.*
3. *$h(x_1, \ldots, x_n, y) := f(x_1, \ldots, x_n) \ominus ay^2$-nek van nemtriviális gyöke.*

($f \ominus g$ alatt természetesen $f \oplus (-g)$-t értünk.)

Bizonyítás. Ha f felveszi a-t, akkor van egy olyan x elem K^n-ben, amire $f(x) = a$. Mivel a nemnulla, f nemelfajuló, és $\langle x, x \rangle_f \neq 0$, ezért $K^n = \mathrm{span}(x) \oplus x^\perp$, amiből 2. adódik.

A 2. $\Rightarrow$ 3. implikáció nyilvánvaló, hiszen $g(x_1, \ldots, x_{n-1}) \oplus ay^2$ felveszi a-t, tehát f is felveszi, tehát h-nak van nemtriviális gyöke.

Ha pedig h-nak van nemtriviális gyöke (legyen $(x_1, \ldots, x_n, y)$), akkor $y = 0$ esetén f-nek nyilván van nemtriviális gyöke, így az 5.5. állítás szerint felveszi a-t; ha pedig $y \neq 0$, akkor $f\left(\frac{x_1}{y}, \ldots, \frac{x_n}{y}\right) = a$ teljesül.

q.e.d.

5.14. Állítás. *Legyen g és h két nemelfajuló kvadratikus alak, és tegyük fel, hogy $f = g \ominus h$. Ekkor a következők ekvivalensek:*

1. *f-nek van nemtriviális gyöke.*
2. *Van olyan a nemnulla elem K-ban, amit g és h is fölvesz.*
3. *Van olyan a nemnulla elem K-ban, amire $g(x) \ominus ay^2$-nek és $h(x) \ominus ay^2$-nek is van nemtriviális gyöke.*

Bizonyítás. Ha f-nek van egy nemtriviális gyöke, (x, y), ahol $g(x) = h(y)$, akkor két eset lehetséges: $g(x) = h(y) \neq 0$, vagy $g(x) = h(y) = 0$. Az első esetben a 2. pont nyilván igaz. A második esetben azt látjuk, hogy g és h valamelyikének van egy nemtriviális gyöke. Feltehetjük, hogy ez g. Mivel g nemelfajuló is, így minden értéket felvesz K-ból, tehát speciálisan felvesz egy h által is felvett nemnulla értéket, amivel a 2. pontot beláttuk. (h felvesz nemnulla értéket, mert nemelfajuló.)

A 2. $\Rightarrow$ 1. irány nyilvánvaló, a 2. $\Leftrightarrow$ 3. ekvivalencia pedig az előző állításból következik.

q.e.d.

5.15. Tétel. *Legyen f_1 és f_2 két nemelfajuló kvadratikus alak, amikhez léteznek olyan g_1, g_2, h_1, h_2 kvadratikus alakok, hogy $f_1 = g_1 \oplus h_1$, és $f_2 = g_2 \oplus h_2$. Ha f_1 és f_2, illetve g_1 és g_2 ekvivalensek, akkor h_1 és h_2 is ekvivalens lesz.*

Bizonyítás. Ez a 4.14. következményből nyilvánvaló.

q.e.d.

5.16. Következmény. Ha f nemelfajuló, akkor léteznek olyan $g_1, g_2, \ldots, g_m$ hiperbolikus kvadratikus alakok, és egy h kvadratikus alak, aminek nincs nemtriviális gyöke, hogy $f \sim g_1 \oplus \cdots \oplus g_m \oplus h$, és a felbontás ekvivalencia erejéig egyértelmű.

5.2. Kvadratikus alakok $\mathbb{Q}_p$ felett

Most megpróbáljuk valamelyest jellemezni a $\mathbb{Q}_p$ feletti kvadratikus alakok ekvivalenciaosztályait, illetve megmutatjuk, egy $\mathbb{Q}_p$ feletti kvadratikus alaknak milyen feltételek mellett van nemtriviális gyöke. A könnyebb kezelhetőség érdekében a következő jelöléseket használjuk:

Ebben a szakaszban p legyen egy tetszőleges prímszám (most nem engedjuk meg a $p = \infty$, $\mathbb{Q}_p = \mathbb{R}$ esetet), K pedig legyen $\mathbb{Q}_p$, a p-adikus számok teste. Kvadratikus alak alatt most nemelfajuló kvadratikus alakot értünk. f továbbra is egy K (azaz $\mathbb{Q}_p$) feletti, n változós (nemelfajuló) kvadratikus alakot jelöl.

5.17. Állítás. *Tudjuk, hogy léteznek olyan $a_1, \ldots, a_n \in \mathbb{Q}_p$ számok, amikre f ekvivalens az $a_1x_1^2 + \cdots + a_nx_n^2$ kvadratikus alakkal. Tekintsük a $\varepsilon(f) = \prod_{i<j}(a_i, a_j)$ számot. Ez az érték jóldefiniált, és állandó a kvadratikus alakok minden ekvivalenciaosztályában.*

Bizonyítás. Elegendő látnunk, hogy ha $a_1x_1^2 + \cdots + a_nx_n^2 \sim b_1x_1^2 + \cdots + b_nx_n^2$ valamely $a_1, \ldots, a_n$, $b_1, \ldots, b_n \in \mathbb{Q}_p$ értékekre, akkor $\prod_{i<j}(a_i, a_j) = \prod_{i<j}(b_i, b_j)$. Vegyük észre, hogy az kvadratikus alakok ekvivalenciájának definíciójából az következik, hogy két n változós kvadratikus alak pontosan akkor ekvivalens, ha az n dimenziós K feletti vektortérnek van egy olyan skalárszorzata, illetve két olyan bázisa, hogy a skalárszorzat mátrixát az egyik bázisban felírva az megyegyezik az egyik, a másik bázisban felírva pedig a másik kvadratikus alak mátrixával. Tehát tulajdonképpen azt akarjuk belátni, hogy ha van egy $\langle ., . \rangle$ skalárszorzatunk $\mathbb{Q}_p^n$-en, és van egy olyan $e_1, \ldots, e_n$ ortogonális bázisunk, amiben $\langle e_i, e_i \rangle = a_i$, valamint egy olyan $f_1, \ldots, f_n$ ortogonális bázisunk, amiben $\langle f_i, f_i \rangle = b_i$ (minden $i = 1, \ldots, n$-re), akkor $\prod_{i<j}(a_i, a_j) = \prod_{i<j}(b_i, b_j)$. De ezt már beláttuk, a 4.15. tételben.

q.e.d.

Megjegyzés. A fenti állítás bizonyításában sehol nem használtuk ki, hogy p prímszám – a bizonyítás egy az egyben átírható a $p = \infty$, azaz az $\mathbb{R}$ feletti esetre.

5.18. Tétel. *Bármely p prímre egy $\mathbb{Q}_p$ fölötti n változós nemelfajuló f kvadratikus alaknak pontosan akkor van nemtriviális gyöke, ha:*

1. *$n = 2$ és $d(f) = -1$,*
2. *$n = 3$, és $(-1, -d(f)) = \varepsilon(f)$,*
3. *$n = 4$, és $d(f) \neq 1$, vagy $d(f) = 1$ és $\varepsilon(f) = (-1, -1)$,*
4. *$n \geq 5$*

valamelyike teljesül.

Bizonyítás. Tudjuk, hogy vannak $a_1, \ldots, a_n$ nemnulla számok $\mathbb{Q}_p$-ben, amire $f(x_1, \ldots, x_n) \sim a_1x_1^2 + \cdots + a_nx_n^2$, és azt is tudjuk, hogy ekvivalens bilineáris formáknak egyszerre van nemtriviális gyökük. Tehát elég $f(x_1, \ldots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$-et tekintenünk.

$n = 1$-re nyilván egyetlen nemelfajuló kvadratikus alaknak sincs nemtriviális gyöke, vagyis csak az $n \geq 2$ eseteket kell vizsgálnunk:

1. $n = 2$-re f-nek pontosan akkor van nemtriviális gyöke, hogy $-\frac{a_1}{a_2}$ négyzetszám $\mathbb{Q}_p$-ben. De ezt $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-ben tekintve pont $1 = -\frac{a_1}{a_2} = -a_1a_2 = -d$-t kapjuk, tehát $d = -1$.

2. Az $n = 3$ esetben vegyük észre, hogy f-nek pontosan akkor van nemtriviális gyöke, ha $-a_3 f(x_1, x_2, x_3) = -a_3 a_1 x_1^2 - a_3 a_2 x_2^2 - a_3^2 x_3^2 \sim -a_3 a_1 x_1^2 - a_3 a_2 x_2^2 - x_3^2$-nek is van. Vagyis, a Hilbert-szimbólum definíciója szerint (3.1. definíció), pontosan akkor, ha $(-a_1 a_3, -a_2 a_3) = 1$. A 3.6. következményből látható, hogy minden $a \in \mathbb{Q}_p^*$-ra $(a, a) = (a, -a^2) = (a, -1)$. Ezek alapján:

$$\begin{aligned} 1 &= (-a_1 a_3, -a_2 a_3) = (-1,-1)(-1,a_2)(-1,a_3)(a_1,-1)(a_1,a_2)(a_1,a_3)(a_3,-1)(a_3,a_2)(a_3,a_3) = \\ &= (-1,-1)(-1,a_1)(-1,a_2)(-1,a_3)(a_1,a_2)(a_2,a_3)(a_3,a_1) = (-1,-1)(-1,a_1a_2a_3)\varepsilon(f) = \\ &= (-1,-d(f))\varepsilon(f), \end{aligned}$$

ami pont ekvivalens $(-1, -d(f)) = \varepsilon(f)$-el.

3. Az $n = 4$ eset bizonyításához felhasználjuk az 5.19. következmény 2. pontját, amit csak a tétel bizonyítása után mondunk ki, de csak a tétel $n = 3$ esetére lesz szükségünk hozzá. E szerint, $\mathbb{Q}_p^*$ egy a elemét pontosan akkor veszi fel egy 2 változós, nemelfajuló g kvadratikus alak értékként, ha $(a, -d(g)) = \varepsilon(g)$.

   Az 5.14. állítás 1. $\Leftrightarrow$ 2. ekvivalenciája alapján pontosan akkor van f-nek nemtriviális gyöke, ha van olyan a érték $\mathbb{Q}_p^*$-ban, amit $a_1x^2 + a_2y^2$ és $-a_3x^2 - a_4y^2$ is felvesz , vagyis ha van olyan $a \in \mathbb{Q}_p^*$, amire $(a, -a_1a_2) = (a_1, a_2)$ és $(a, -a_3a_4) = (a_3, a_4)$. Ez a 20. oldalon bevezetett $H_x^{\pm 1}$ jelölést használva pont azt jelenti, hogy $H_{-a_1a_2}^{(a_1,a_2)} \cap H_{-a_3a_4}^{(a_3,a_4)} \neq \emptyset$. Mivel mindkét halmaznak van eleme (pl. a_1 illetve $-a_3$), ezért a 3.14. lemma szerint pontosan akkor nem diszjunktak, ha $-a_1a_2 \neq -a_3a_4$, vagy ha $(a_1, a_2) \neq -(-a_3, -a_4)$.

   Az első feltétel pont azt mondja, hogy $d(f) \neq 1$. Amennyiben $a_1a_2 = a_3a_4$ mégis teljesül, akkor:

$$\begin{aligned} \varepsilon(f) &= (a_1,a_2)(a_1,a_3)(a_1,a_4)(a_2,a_3)(a_2,a_4)(a_3,a_4) = (a_1,a_2)(a_3,a_4)(a_1a_2,a_3a_4) = \\ &= (a_1,a_2)(a_3,a_4)(a_3a_4,a_3a_4) = (a_1,a_2)(a_3,a_4)(-1,a_3a_4) = \\ &= (a_1,a_2)(a_3,a_4)(-1,a_3)(-1,a_4) = (a_1,a_2)(a_3,-a_4)(-1,a_4)(-1,-1)(-1,-1) = \\ &= (a_1,a_2)(-a_3,-a_4)(-1,-1), \end{aligned}$$

   ami mellett pontosan akkor teljesül $(a_1, a_2) \neq -(-a_3, -a_4)$, ha $\varepsilon(f) \neq -(-1, -1)$, vagyis ha $\varepsilon(f) = (-1, -1)$.

4. $n \geq 5$-re nyilván elegendő az $n = 5$ esetet vizsgálnunk. Az 5.19. következmény (az előző pontban is felhasznált) 2. pontja, illetve a 3.12. lemma alapján minden 2 változós, nemelfajuló kvadratikus alak felveszi értékként $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ elemeinek legalább a felét. Ez nyilván igaz lesz a 2-nél több változós kvadratikus alakokra is. Tekintve, hogy $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ elemszáma legalább 4, így f-nek fel kell vennie egy $d(f)$-től különböző a értéket is $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-ből. Vagyis (az 5.13. állítás 1. $\Leftrightarrow$ 2. ekvivalenciája miatt) van egy g 4 változós, nemelfajuló kvadratikus alak, amire $f(x_1, \ldots, x_4, y) \sim ay^2 \oplus g(x_1, \ldots, x_4)$ teljesül. $d(g) = \frac{d(f)}{a} \neq 1$, így az előző pont alapján g-nek van nemtriviális gyöke, így ez f-re is nyilván teljesül.

q.e.d.

5.19. Következmény. Vegyük $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ egy a elemét. Jelöljük az $f \ominus ay^2$ kvadratikus alakot f_a-val. Ekkor az 5.14. állítás szerint f_a-nak pontosan akkor van nemtriviális gyöke, ha f felveszi a-t.

Vegyük észre, hogy $d(f_a) = -af(d)$, illetve hogy $\varepsilon(f_a) = \varepsilon(f)\prod_{i=1}^{n}(-a, a_i) = \varepsilon(f)(-a, d(f))$. Így a fenti tétel alapján f pontosan akkor veszi fel a-t, ha:

1. $n = 1$, és $-ad(f) = -1$, vagyis $a = d(f)$ (mint $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ elemei), vagy
2. $n = 2$, és $(-1, -(-ad(f))) = (-a, d(f))\varepsilon(f)$, vagyis $(a, -d(f)) = \varepsilon(f)$, vagy
3. $n = 3$, és $-ad(f) \neq 1$, vagy $-ad(f) = 1$ és $\varepsilon(f)(-a, d(f)) = (-1, -1)$, vagyis $a \neq -d(f)$ (mint $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ elemei), vagy $a = -d(f)$ (mint $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ elemei) és $(-1, -d(f)) = \varepsilon(f)$, vagy pedig

4. $n \geq 4$.

Megjegyzés. A fentiekből az is látszik, hogy ha f-nek nincs nemtriviális gyöke, akkor f $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ elemeiből pontosan

1. 1 darabot vesz fel, ha $n = 1$ (d-t).
2. $\frac{\left|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right|}{2}$-t vesz fel, ha $n = 2$ ($H_{-d(f)}^{\varepsilon(f)}$ elemeit).
3. $\left|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right| - 1$-et vesz fel, ha $n = 3$ ($-d(f)$-et nem veszi fel, mert $(-1, -d(f)) \neq \varepsilon(f)$).
4. $\left|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right|$ elemet vesz fel (minden elemet felvesz), ha $n \geq 4$.

5.20. Tétel. *Két tetszőleges f és g $\mathbb{Q}_p$ feletti n változós, nemelfajuló kvadratikus alak pontosan akkor ekvivalens, ha $d(f) = d(g)$ és $\varepsilon(f) = \varepsilon(g)$.*

Bizonyítás. A feltételek szükségességét már régebben tisztáztuk. Az elégségességet n-re alkalmazott teljes indukcióval fogjuk belátni:

$n = 1$-re az állítás triviális – $\varepsilon(f) = 1$ minden f-re, és $f(x) \sim d(f)x^2$.

$n > 1$ esetén az előző következményből látható, hogy f és g ugyanazokat az értékeket veszik fel $\mathbb{Q}_p^*$-ban. Vegyünk egy a értéket, amit felvesznek. Ekkor (az 5.13. állítás alapján) van egy olyan f_0 és egy olyan g_0 $n-1$ változós kvadratikus alak, amire $f(x_1, \ldots, x_n) \sim ax_1^2 \oplus f_0(x_2, \ldots, x_n)$, illetve $g(x_1, \ldots, x_n) \sim ax_1^2 \oplus g_0(x_2, \ldots, x_n)$. Mivel $d(f_0) = ad(f) = ad(g) = d(g_0)$, illetve $\varepsilon(f_0) = \varepsilon(f)(a, d(f_0)) = \varepsilon(g)(a, d(g_0)) = \varepsilon(g_0)$, ezért az indukciós feltevés szerint $f_0 \sim g_0$, amiből az állítás (az 5.15. tétel felhasználásával) már következik.

q.e.d.

5.21. Következmény. Ekvivalencia erejéig egyetlen 4 változós f kvadratikus alak van $\mathbb{Q}_p$ fölött, aminek nincs nemtiviális gyöke: erre $d(f) = 1$-nek, valamint $\varepsilon(f) = -(-1, -1)$-nek kell teljesülnie. Ha veszünk egy a és egy b elemet $\mathbb{Q}_p^*$-ból, amikre $(a, b) = -1$, akkor $f(t, x, y, z) = t^2 - ax^2 - by^2 + abz^2$ kvadratikus alak megfelelő lesz, hiszen $d(f) = (-a)(-b)ab = 1$ ($\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-ben tekintve), illetve

$$\begin{aligned} \varepsilon(f) &= (-a, -b)(-a, ab)(-b, ab) = (-1, -1)(-1, a)^3(-1, b)^3(a, b)^3(a, a)(b, b) = \\ &= -(-1, -1)(-1, a)(-1, b)(-1, a)(-1, b) = -(-1, -1). \end{aligned}$$

Most, hogy meghatároztuk, mi a feltétele annak, hogy bizonyos $\mathbb{Q}_p$ feletti kvadratikus alakok egy ekvivalenciaosztályba tartoznak, lássuk, milyen ekvivalenciaosztályok léteznek egyáltalán:

5.22. Állítás. *Legyen n egy pozitív egész szám, d $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ egy eleme, ε pedig ± 1. Pontosan akkor létezik egy n változós, nemelfajuló f kvadratikus alak $\mathbb{Q}_p$ fölött, aminek diszkriminánsa d, és $\varepsilon(f) = \varepsilon$, ha:*

1. *$n = 1$ és $\varepsilon = 1$, vagy*
2. *$n = 2$ és $d \neq -1$ vagy $\varepsilon = 1$, vagy*
3. *$n \geq 3$.*

Bizonyítás.

1. $n = 1$-re az állítás triviálisan igaz – $\varepsilon(f)$ definíció szerint az üresszorzat, ami 1-el egyenlő, $d(f) = d$-t pedig nyilván kielégíti dx^2.
2. Az $n = 2$-esetben mindenképpen lesznek a és b $\mathbb{Q}_p^*$-beli értékek, amikre $f(x, y) \sim ax^2 + by^2$. Ekkor $d(f) = ab$, $\varepsilon(f) = (a, b) = (a, -ab) = (a, -d(f))$ (a 3.6. következmény felhasználásával). Így, ha $d(f) = -1$, akkor $\varepsilon(f)$-nek mindenképpen 1-nek kell lennie. $d = -1$, $\varepsilon = 1$-re jó példa az $x^2 - y^2$, míg $d \neq -1$ esetén van egy olyan szám (a 3.12. lemma alapján), amire $(a, -d) = \varepsilon$, és ekkor $ax^2 + ady^2$ megfelelő lesz.
3. Az $n \geq 3$ esethez először vizsgáljuk meg $n = 3$-at. Vegyük $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ egy $-d$-től különböző a elemét. Ez előző pont alapján van egy g kétváltozós, nemelfajuló bilineáris forma, amire $d(g) = ad$, és $\varepsilon(g) = \varepsilon(a, d)$. Ekkor $f(x, y, z) = g(x, y) \oplus az^2$ megfelelő lesz, hiszen $d(f) = d(g)a = d$ ($\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-ben), illetve $\varepsilon(f) = \varepsilon(g)(a, d) = \varepsilon$. $n > 3$-ra pedig $f(x_1, x_2, x_3) + x_4^2 + \cdots + x_n^2$ nyilvánvalóan megfelelő lesz.

q.e.d.

5.23. Következmény. Ha p egy páratlan prím, akkor a $\mathbb{Q}_p$ fölötti n változós, nemelfajuló kvadratikus alakok ekvivalenciosztályainak száma

1. $n =$ 1-re 4,
2. $n =$ 2-re 7, és
3. $n \geq$ 3-ra 8,

hiszen a 2.30. következmény alapján $\mathbb{Q}_p^*/{\mathbb{Q}_p^*}^2$ elemszáma 4.

5.24. Következmény. A $\mathbb{Q}_2$ fölötti n változós, nemelfajuló kvadratikus alakok ekvivalenciosztályainak száma

1. $n =$ 1-re 8,
2. $n =$ 2-re 15, és
3. $n \geq$ 3-ra 16,

hiszen a 2.32. következmény alapján $\mathbb{Q}_2^*/{\mathbb{Q}_2^*}^2$ elemszáma 8.

5.3. Kvadratikus alakok $\mathbb{R}$ felett

Sylvester tehetetlenségi tétele, $\mathbb{R}^*/{\mathbb{R}^*}^2 = (\{\pm 1\}, \cdot)$ alapján nyilvánvaló, hogy minden $\mathbb{R}$ fölötti kvadratikus alakhoz egyértelműen léteznek olyan r és s természetes számok, amikre teljesül, hogy f ekvivalens az $x_1^2 + x_2^2 + \cdots + x_r^2 - y_1^2 - y_2^2 - \cdots - y_s^2$ kvadratikus alakkal (ekkor f rangja természetesen $r+s$). Hasonlóan nyilvánvaló, hogy (adott változószám mellett) az ekvivalenciaosztályokat egyértelműen meghatározza az (r, s) pár $(r + s \leq n)$.

Most vegyük észre, hogy f-nek pontosan akkor van nemtriviális gyöke, ha $r + s \neq n$, vagy ha $r, s \neq 0$. Az első eset nyilvánvaló; $r + s = n,\ \ r, s \neq 0$-ra $x_1 = y_1 = 1,\ \ x_i, y_j = 0$ $(i = 2, \ldots, r,$ $j = 2, \ldots, s)$ nyilván megoldás lesz; $r + s = n,\ \ r = 0$ esetén az összes nemnulla vektorra a kvadratikus alak értéke szigorúan negatív lesz, tehát nincs nemtriviális gyök, hasonlóan $r + s = n,\ \ s = 0$-ra az összen nemnulla vektorban f értéke szigorúan pozitív lesz, tehát szintén nincs nemtriviális gyök.

Definiáljuk a $\varepsilon(f)$ mennyiséget a $\mathbb{Q}_p$ (p prím) esethez hasonlóan (ld. 5.17. állítás). Ekkor (az állítás utáni megjegyzésből láthatóan) ε jóldefiniált, és az ekvivalenciaosztályokon állandó. Mivel $(-1, -1) = -1$ ($\mathbb{R}$ felett), ezért $\varepsilon(f) = (-1)^{\binom{s}{2}}$. Hasonló képlet adható $d(f)$-re is: $d(f) = (-1)^s$.

Most vegyük észre, hogy $\varepsilon(f)$ és $d(f)$ egyértelműen meghatározza s-et $\pmod 4$, vagyis $r(f) \leq$ 3-ra $\varepsilon(f)$ és $d(f)$ egyértelműen meghatározza f ekvivalenciaosztályát.

Észrevehetjük továbbá azt is, hogy az 5.18. tétel 1., 2. és 3. pontja teljesül $\mathbb{R}$ felett is, hiszen a bizonyításban sehol nem használjuk ki, hogy $p \neq \infty$. Ellenben a 4. pontban hivatkozunk arra, hogy $\mathbb{Q}_p^*/{\mathbb{Q}_p^*}^2$ elemszáma legalább 4, ami $\mathbb{R}$ felett nem teljesül (hiszen $\mathbb{R}^*/{\mathbb{R}^*}^2$ elemszáma 2), tehát ez a bizonyítás nem írható át $\mathbb{R}$-re. Sőt, a szakasz elején tárgyaltakból az is látszik, hogy maga az állítás sem helytálló $p = \infty$ esetén.

Ebből persze az is következik, hogy az 5.19. következmény 1., 2. és 3. pontja is igaz lesz $\mathbb{R}$ felett, míg a 4. pont állítása itt sem teljesül (szintén a szakasz elején írtak miatt).

6. fejezet

A Hasse–Minkowski-tétel és következményei

Végül eljutottunk a Hasse–Minkowski-tételhez. Ebben a fejezetben megadjuk a tétel bizonyítását, illetve megnézzük néhány következményét is.

6.1. A tétel bizonyítása

Jelölje P a (pozitív) prímek, és a ∞ alkotta halmazt. Legyen minden p prímre $\mathbb{Q}_p$ a p-adikus számok, $\mathbb{Q}_\infty$ pedig a valós számok teste.

Vegyünk egy tetszőleges, $\mathbb{Q}$ feletti n változós f kvadratikus alakot. Ekkor az előző fejezetből tudjuk, hogy létezik egy $r(f) \leq n$ pozitív egész ($r(f) = n$ pontosan akkor teljesül, ha f nemelfajuló), és léteznek olyan $a_1, a_2, \ldots, a_{r(f)}$ nemnulla racionális számok, hogy $f(x_1, x_2, \ldots, x_n) \sim a_1x_1^2 + a_2x_2^2 + \cdots + a_{r(f)}x_{r(f)}^2$. Mivel az együtthatók négyzetszámmal való szorzása nem befojásolja a kvadratikus alak ekvvivalenciaosztályát, így feltehető az is, hogy $a_1, a_2, \ldots, a_r$ négyzetmentes egész számok.

Mivel $\mathbb{Q}$ része a p-adikus számtesteknek, és $\mathbb{R}$-nek is, így f tekinthető egy $\mathbb{Q}_p$ feletti kvadratikus alaknak is, minden $p \in P$-re.

Ekkor f diszkriminánsa az $a_1a_2 \cdot \cdots \cdot a_n$ szám lesz (ahol minden $i = r(f)+1, \ldots, n$-re a_i-t 0-nak tekintjük). Minden $p \in P$-re $d_p(f)$ alatt az f, mint $\mathbb{Q}_p$ feletti kvadratikus alak diszkriminánsát értjük. Ez nyilván $d(f)$ képe lesz $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cup \{0\}$-ban.

$\varepsilon_p(f)$-en értelemszerűen $\prod_{i<j}(a_i, a_j)_p$-t értünk, minden $p \in P$ esetén. A szorzat-formuálból (3.16. tétel) nyilvánvaló, hogy $\prod_{p\in P} \varepsilon(f_p) = 1$.

Mivel minden f és g $\mathbb{Q}$ felett ekvivalens kvadratikus alak ekvivalens $\mathbb{R}$ felett tekintve is, ezért nyilvánvaló, hogy vannak olyan r és s természetes számok ($r + s = r(f)$), hogy az a_i-k ($i = 1, \ldots, r(f)$) közül pontosan r darab pozitív, és s darab negatív van.

A Hasse–Minkowski-tétel. *Egy tetszőleges racionális együtthatós f kvadratikus alaknak pontosan akkor van nemtriviális racionális gyöke , ha van nemtriviális gyöke minden p prímre a p-adikus számtestben, és van nemtriviális gyöke a valós számok között is.*

Bizonyítás. Elsőként vegyük érszre a megfogalmazott feltételek szükségességét – mivel $\mathbb{Q}$ része $\mathbb{Q}_p$-nek minden $p \in P$-re, így ha van f-nek (nemtriviális) racionális gyöke, az nyilván egy (nemtriviális) gyöke lesz $\mathbb{Q}_p$-ben is. Tehát csak az elégségességet kell bizonyítanunk így a továbbiakban feltesszük, hogy f-nek van nemtriviális gyöke $\mathbb{Q}_p$-ben minden $p \in P$-re, és azt fogjuk bebizonyítani, hogy van nemtriviális gyöke $\mathbb{Q}$-ban is.

Nyilvánvaló az is, hogy f pontosan akkor elfajuló ($\mathbb{Q}$ felett), ha elfajuló minden $p \in P$-re $\mathbb{Q}_p$ felett, ami azzal ekvivalens, hogy van olyan p, amire $\mathbb{Q}_p$ felett elfajuló. Ebben az esetben nyilván van f-nek nemtriviális gyöke ($\mathbb{Q}$ felett). Tehát a továbbiakban feltehetjük, hogy f nemelfajuló.

Mivel ekvivalens kvadratikus alakoknak egyszerre van nemtriviális gyökük (ld. 5.4. következmény), tehát a szakasz elején írtak szerint feltehetjük, hogy $f(x_1, \ldots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$, ahol

$a_1, \ldots, a_n$ négyzetmentes egész számok. Mivel pedig f-nek, és $a_1 f$-nek egyszerre van vagy nincs nemtriviális gyöke, ezért feltehetjük azt is, hogy $a_1 = 1$.

A tételt n-re (f változószámára) alkalmazott teljes indukcióval fogjuk belátni.

1. Ha $n = 1$, akkor $f(x) = x^2$, aminek nincs nemtriviális gyöke sem $\mathbb{Q}$, sem pedig $\mathbb{Q}_p$ felett (P bármely elemét is jelöli p), tehát az állítás nyilvánvalóan igaz.

2. $n = 2$ esetén $f(x, y) = x^2 - ay^2$, ahol $a > 0$ egy négyzetmentes pozitív egész, mivel csak így lehet f-nek nemtriviális gyöke $\mathbb{R}$-ben. $a = \prod_p p^{o_p(a)}$ (vö. 2.7. definíció), és mivel a négyzetmentes, ezért $o_p(a) = 0, 1$, minden p prímre. Mivel minden p prímre vannak $x_p, y_p \in \mathbb{Q}_p$ nemunlla számok (valamelyikük nemnulla, és ha az egyik nulla lenne, akkor a másik is nulla kellene legyen), amikre $x_p^2 = ay_p^2$, amiből következik, hogy a négyzetszám $\mathbb{Q}_p$-ben. Viszont a $\mathbb{Q}_p$-beli négyzetelemek karakterizációjából (2.29., illetve 2.31. tétel) látható, hogy ekkor minden p prímre $o_p(a)$ páros. Vagyis $o_p(a) = 0$ (minden p prímre); $f(x, y) = x^2 - y^2$, aminek nyilván van nemtriviális gyöke $\mathbb{Q}$-ban.

3. Az $n = 3$ esetben vannak olyan a és b négyzetmentes (nemnulla) egészek, hogy $f(x, y, z) = x^2 - ay^2 - bz^2$. Feltehetjük azt is, hogy $|a| \leq |b|$. Az állítást $m = |a| + |b|$-re alkalmazott teljes indukcióval bizonyítunk.

   $m = 2$ csak $a, b = \pm 1$ esetén lehet. Az $a, b = 1$ esetben $f(x, y, z) = x^2 + y^2 + z^2$ adódnak, de így nem lenne f-nek $\mathbb{R}$-beli nemtriviális gyöke, tehát ez az eset nem állhat fent. A többi lehetséges esetben feltehetjük, hogy $a = -1$, és így az $(1, 1, 0)$ számhármas gyöke lesz f-nek a racionális számok felett.

   $m > 2$ esetén $|b| \geq 2$ is teljesül, amiből az következik, hogy b felírható valamely alkalmas (pozitív egész) k-ra $\pm \prod_{i=1}^{k} p_i$ alakban, ahol $p_1, \ldots, p_k$ pozitív prímszámok. Mivel b négyzetmentes, ezért $i \neq j$ esetén $p_i \neq p_j$ adódik. Vegyünk egy tetszőleges i-t 1 és k között. Meg fogjuk mutatni, hogy a egy négyzetszám $\bmod p_i$ (vagy ha úgy tetszik, négyzetelem $\mathbb{F}_{p_i}$-ben).

   Ha $a \equiv 0 \pmod{p_i}$, akkor ez nyilvánvaló. Ha nem, akkor vegyük f egy nemtriviális gyökét $\mathbb{Q}_{p_i}$ felett – legyen ez (u, v, w). A 2.17. állítás miatt feltehetjük, hogy (u, v, w) $\mathbb{Z}_{p_i}^3$-beli és primitív (ld. 2.16. definíció). Mivel $p_i | b$, ezért $p_i | u^2 - av^2$ is teljesül. Látható, hogy v nem osztható p_i-vel, hiszen ha osztható volna, akkor u is osztható lenne p_i-vel, amiből bw^2 p_i^2-el, innen pedig w p_i-vel való oszthatósága következne, ellentmondva ezzel a primitivitás feltételének. Vagyis v tényleg nem osztható p_i-vel, azaz v egy nemnulla eleme $\mathbb{F}_{p_i}$-nek, tehát van inverze $\mathbb{F}_{p_i}$-ben – legyen ez v^{-1}. Ekkor v^{-1}-et, mint egész számot tekintve látható, hogy $a \equiv (uv^{-1})^2 \pmod{p_i}$, így a valóban négyzetelem $\bmod p_i$. Mivel pedig $\mathbb{Z}/b\mathbb{Z} = \prod_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z}$, ezért a egy négyzetszám $\bmod b$, vagyis vannak olyan s és t egészek, hogy $a + tb = s^2$ teljesül, sőt, feltehetjük, hogy $|s| \leq \frac{|b|}{2}$.

   Ekkor $tb = s^2 - a \in N(\mathbb{Q}_p)_a^*$ (ld. 16. oldal), minden $p \in P$-re. Vagyis a 3.3. állítás szerint $(a, tb)_p = 1$, de feltettük, hogy $(a, b)_p = 1$, így $(a, t)_p = 1$ is teljesül, vagyis $x^2 - ay^2 - tz^2$-nek van nemtriviális gyöke $\mathbb{Q}_p$-ben. Látható, hogy $|t| = \left|\frac{s^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|$, mivel $|b| \geq 2$. $t = cd^2$, ahol c négyzetmentes egész, d pedig egész szám. $|c| \leq |t| < |b|$, amiből $|a| + |c| < m$ következik, tehát az indukciós feltétel szerint $x^2 - ay^2 - cz^2 \sim x^2 - ay^2 - tz^2$-nek van nemtriviális gyöke $\mathbb{Q}$-ban. De a 3.3. állításhoz fűzött megjegyzés értelmében nekünk elég azt bizonyítani, hogy $b \in N\mathbb{Q}_a^*$, és éppen az imént láttuk, hogy $t, bt \in N\mathbb{Q}_a^*$. Vagyis (mivel $N\mathbb{Q}_a^*$ egy multiplikatív csoport) az állítás valóban teljesül.

4. Az n=4 esetben $f(x, y, z, w) = x^2 + ay^2 - (bz^2 + cw^2)$, ahol a, b és c négyzetmentes egész számok. Mivel minden $p \in P$-re f-nek van nemtriviális gyöke $\mathbb{Q}_p$-ben, ezért az 5.14. állítás értelmében minden $p \in P$-re van egy q_p nemnulla elem $\mathbb{Q}_p$-ben, amit $x^2 + ay^2$ és $bx^2 + cy^2$ is felvesz értékként. Ez viszont az 5.19. következmény 2. pontja szerint ekvivalens azzal, hogy $(q_p, -a)_p = (1, a)_p = 1$ és $(q_p, -bc)_p = (b, c)_p$. Mivel $\prod_{p \in P}(b, c)_p = 1$, és $(b, c)_p$ véges sok p kivételével 1, ezért a 3.17. tétel szerint létezik egy q nemnulla racionális szám, amelyre $(q, -a)_p = 1 = (1, a)_p$ és $(q, -bc)_p = (b, c)_p$ minden $p \in P$-re. Ekkor (az előbb hivatkozott 5.19. következmény 2. pontja miatt) mind $x^2 + ay^2$, mind pedig $bx^2 + cy^2$ felveszi q-t értékként ($\mathbb{Q}$ felett), amiből következik, hogy f-nek van nemtriviális gyöke $\mathbb{Q}$-ban.

5. Végül elérkeztünk az $n \geq 5$ esethez. Ekkor tudjuk, hogy vannak olyan $a_1, \ldots, a_{n-2}, b$ négyzetmentes egész számok, amikre $f(x_1, \ldots, x_{n-2}, y, z) = a_1x_1^2 + \cdots + a_{n-2}x_{n-2}^2 - (y^2 + bz^2)$ teljesül. Nevezzük $g(x_1, \ldots, x_{n-2})$-nek az $a_1x_1^2 + \cdots + a_{n-2}x_{n-2}^2$ kvadratikus alakot, $h(x, y)$-nak pedig az $x^2 + by^2$ kvadratikus alakot. Ekkor $f = g \ominus h$.

   Jelöljük S-el a következő halmazt:

$$S = \{p \in P \mid p = 2, \infty, \text{ vagy } \exists i = 1, \ldots, n-2 \;\; o_p(a_i) \neq 0\}.$$

   Vegyünk egy tetszőleges S-beli p elemet. Mivel f-nek van nemtriviális gyöke $\mathbb{Q}_p$ felett, ezért van $\mathbb{Q}_p$-ben egy olyan nemnualla a_p elem, amit g és h is felvesz ($\mathbb{Q}_p$ felett – ld. 5.14. állítás), vagyis vannak olyan $x_{p,i}$ $(i = 1, \ldots, n-2)$, y_p, z_p elemek $\mathbb{Q}_p$-ben, amikre $g(x_{p,1}, \ldots, x_{p,n-2}) = a_p = h(y_p, z_p)$ teljesül. A 3.18. lemma szerint tudunk egy $\mathbb{Q}$-beli a nemnulla elemet tetszőlegesen közel választani az a_p-k minegyikéhez, ahol $p \in S$ (hiszen S véges). Azaz a-t meg tudjuk úgy választani, hogy $\frac{a}{a_p}$ tetszőlegesen közel legyen 1-hez, minden $p \in S$-re. Vagyis a 2.33. következmény szerint a megválasztható úgy, hogy $\frac{a}{a_p}$ egy négyzetelem legyen $\mathbb{Q}_p^*$-ban. Ekkor, mivel g felveszi a_p-t értékként, $\mathbb{Q}_p$ felett, g felveszi a-t is értékként $\mathbb{Q}_p$ felett, minden $p \in S$-re.

   Ha p nem eleme S-nek, akkor (mint az S definíciól látható) $a_1, \ldots, a_{n-2}$ mind p-adikus egységek (ld. 2.5. definíció), tehát ugyanez igaz lesz $d_p(g)$-re is, és ebből, valamint a 3.8. tételből az is következik, hogy $\varepsilon_p(g) = 1$. Most pedig felhasználva az 5.19. következmény 3. és 4. pontját, valamint hogy $n \geq 5$, vagyis $r(g) \geq 3$ látható, hogy g felveszi a-t $\mathbb{Q}_p$ felett minden $p \notin S$-re.

   Vagyis g felveszi a-t értékként $\mathbb{Q}_p$ felett minden $p \in P$-re, így (az indukciós feltétel, illetve az 5.13. állítás alapján) g felveszi a-t $\mathbb{Q}$ felett is. Most vegyük észre, hogy a megválasztásánál csak azt követeltük meg, hogy kellően közel legyen a_p-hez minden $p \in S$-re, tehát egy minden y_p-hez kellően közeli y racionláis számot, valamint egy minden z_p-hez kellően közeli z racionális számot választva a megválasztható olyannak, hogy $a = h(y, z)$ is teljesüljön, vagyis hogy h is felvegye a-t $\mathbb{Q}$ felett. Mivel pedig $f = g \ominus h$ volt, ezért f-nek nyilván van nemtriviális gyöke $\mathbb{Q}$ felett.

q.e.d.

6.2. Közvetlen következmények

Most, hogy bebizonyítottuk a Hasse–Minkowski-tételt, lássunk néhány példát arra, hogyan tudjuk felhasználni:

6.1. Következmény. Minden a nemnulla racionális számra igaz, hogy pontosan akkor veszi fel f a-t $\mathbb{Q}$ felett, ha felveszi $\mathbb{Q}_p$ felett is, minden $p \in P$-re (ld. 5.13. állítás).

6.2. Következmény. Minden legalább 5 változós racionális kvadratikus alakra igaz, hogy pontosan akkor van nemtriviális gyöke $\mathbb{Q}$-ban, ha van nemtriviális gyöke $\mathbb{R}$-ben (vagyis ha indefinit) (ld. 5.18. tétel 4. pont).

6.3. Állítás. *Legyenek f_1 és f_2 n változós, nemelfajuló kvadratikus alakok $\mathbb{Q}$ felett. Ekkor f_1 és f_2 pontosan akkor ekvivalensek, ha $d(f_1) = d(f_2)$, $\varepsilon_p(f_1) = \varepsilon_p(f_2)$, minden $p \in P$-re, és $r_1 = r_2$, ahol r_i az f_i $\mathbb{R}$ feletti kanonikus alakjában szereplő pozitív együtthatók száma. A feltételek pontosan azzal ekvivalensek, hogy f_1 és f_2 ekvivalensek $\mathbb{Q}_p$ felett minden P-beli p-re.*

Bizonyítás. A feltételek szükségessége triviális. A kétféle feltétel pedig az 5.20. tétel, illetve az 5.3. szakaszban írtak alapján nyilván ekvivalens. Tehát elég a második feltétel elégségességét bizonyítanunk.

Teljes indukciót alkalmazunk n-re:

Az $n = 1$ esetben vegyünk egy a nemnulla értéket, amit felvesz f_1 ($\mathbb{Q}$ felett). Ekkor ezt felveszi minden $p \in P$-re $\mathbb{Q}_p$ felett is (hiszen $\mathbb{Q}$ része $\mathbb{Q}_p$-nek). Mivel $\mathbb{Q}_p$ felett f_1 és f_2 ekvivalensek, ezért $\mathbb{Q}_p$ felett f_2 is felveszi a-t. Viszont ekkor a 6.1. következmény szerint f_2 felveszi a-t $\mathbb{Q}$ felett is. Tehát f_1 és f_2 is ekvivalens ax^2-el.

$n > 1$-re az előzőhöz hasonló gondolatmenetet alakalmazunk, annyi különbséggel, hogy abból, hogy f_1 és f_2 is felveszi a-t, itt nem következik, hogy f_1 és f_2 is ekvivalens egy harmadik kvadratikus alakkal. Következik azonban, hogy léteznek olyan g_1, g_2 $n-1$ változós kvadratikus alakok, amikre $f_i(y, x_1, x_2, \ldots, x_{n-1}) \sim ay^2 \oplus g_i(x_1, x_2, \ldots, x_{n-1})$ $(i = 1, 2$ – ld. 5.13. állítás). Az 5.15. tétel alapján viszont nyilvánvaló, hogy $g_1 \sim g_2$ $\mathbb{Q}_p$ felett, minden $p \in P$-re, vagyis (az indukciós feltevés szerint) $g_1 \sim g_2$ $\mathbb{Q}$ felett is. Ezzel pedig az állítást bebizonyítottuk.

q.e.d.

6.4. Tétel. *Legyenek n, r és s pozitív egészek, $\varepsilon_p = \pm 1$ minden $p \in P$-re, és d racionális szám. Pontosan akkor létezik egy olyan nemelfajuló, racionális kvadratikus alak, amire $d(f) = d$, $\varepsilon_p(f) = \varepsilon_p$, minden P-beli p-re, és aminek diagonális alakjában pontosan r darab pozitív, és s darab negítav együttható szerepel, ha:*

1. *$r + s = n$,*
2. *d előjele megegyezik $(-1)^s$-el,*
3. *$\varepsilon_p = 1$, páros (így véges) sok $p \in P$ kivételével, és*
4. *$\varepsilon_\infty = (-1)^{\binom{s}{2}}$, továbbá*
5. *ha $n = 1$, akkor $\varepsilon_p = 1$, minden p-re, illetve*
6. *ha $n = 2$, akkor minden $p \in P$-re $\varepsilon_p = 1$, és $d_p = 1$ közül legalább az egyik teljesül (ahol d_p d képe $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.*

Bizonyítás. A feltételek szükségességét már mind láttuk: az 1. pont szükségessége nyilvánvaló, a 2. és a 4. pont szükségességét a 33. oldalon mutattuk meg, a 3. pontét a 34. oldalon vezettük le a szerozatformulából (3.16. tétel), az 5. és 6 pontokét pedig az 5.22. állításban bizonyítottuk.

Az $n = 1$ esetben a feltételek nyilván elégségesek, hiszen dx^2 megfelelő lesz.

$n = 2$-re a Hilbert-szimbólum (mint $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$feletti bilineáris forma) nemelfajultsága, illetve a 6. pont miatt látható, hogy minden $p \in P$ estén van egy olyan $x_p \in \mathbb{Q}_p^*$ szám, amire $(a_p, -d)_p = \varepsilon_p$. Ekkor a 3.17. tétel szerint kell lennie egy a nemnulla racionális számnak, amire $(a, -d)_p = \varepsilon_p$ teljesül, minden P-beli p mellett. (A 3.17. tétel feltételeit a 3. feltétel garantálja.) Mint már többször láttuk, $(a, a)_p = (a, -1)_p$ teljesül minden $p \in P$-re és $a \in \mathbb{Q}_p^*$-ra. Így az $ax^2 + ady^2$ kvadratikus alak a feltételeknek megfelelő lesz.

Az $n = 3$ esetet az előzőre vezetjük vissza. Legyen S azon P-beli p elemek halmaza, amikre $(-1, -d)_p = -\varepsilon_p$. A szorzatformulából (3.16. tétel), illetve a 3. pontból látható, hogy ez csak véges sok esetben teljesülhet ($(-1, -d)_p$ véges sok kivétellel 1, $-\varepsilon_p$ pedig véges sok kivétellel -1). Most minden S-beli p-re válasszunk egy a_p elemet $\mathbb{Q}_p^*$-ból úgy, hogy $a_p \neq -d_p$ teljesüljön. Ekkor a 3.18. lemmát felhasználva, a 3.17. tétel 2. pontjához hasonlóan látható, hogy van egy a nemnulla racionális szám, amit $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$-beli elemként tekintve megegyezik a_p-vel, minen S-beli p-re. Ekkor van egy g kétváltozós kvadratikus alak, amire $d(g) = ad$ és $\varepsilon_p(g) = (a, -d)_p \varepsilon_p$ teljesül, minden $p \in P$-re. Könnyen látható, hogy $f(x, y, z) = g(x, y) + az^2$ megfelelő lesz.

$n \geq 4$ esetén teljesnindukciót alkalmazunk n-re. Ha r nem nulla, akkor van egy $(r-1, s)$, d, ε_p paraméterekkel rendelkező $n-1$ változós, nemelfajuló g kvadratikus alak. Ekkor $g(x_1, \ldots, x_{n-1}) + x_n^2$ megfelelő lesz. H $r = 0$, akkor van egy $(0, n-1)$, $-d$, $(-1, -d)_p \varepsilon_p$ paraméterekkel rendelkező, $n-1$ változós, nemelfajuló g kvadratikus alak. Ekkor $g(x_1, \ldots, x_{n-1}) - x_n^2$ lesz megfelelő.

q.e.d.

A. függelék

Ostrowski tétele

A 10. oldalon, a p-adikus egészek topológiája kapcsán beszéltünk a p-adikus abszolútérték fogalmáról, amit a 11. oldalon kiterjesztettünk a teljes p-adikus számtestre, ezáltal megalkotva a p-adikus számok (egy lehetséges) topológiáját. Most vegyük észre a következőt:

A.1. Lemma. *Bármely p prímre a p-adikus számtest, a p-adikus abszolútérték által generált metrikával teljes metrikus teret alkot.*

Bizonyítás. Vegyünk $\mathbb{Q}_p$-ből egy tetszőleges (x_n) Cauchy-sorozatot. Tudjuk, hogy ekkor minden n-re egyértelműek létezik egy u_n p-adikus egység és egy k_n egész szám, amire $x_n = u_n p^{k_n}$ teljesül (ld. 11. oldal – k_n természetesen $o_p(x_n)$-el egyenlő). Tekintsünk most tetszőleges n és m pozitív egészeket, és vizsgáljuk $|x_n - x_m|_p$ értékét.

$$\begin{aligned} |x_n - x_m|_p &= \left|u_n p^{k_n} - u_m p^{k_m}\right|_p = \left|p^{\min\{k_n,k_m\}}\right|_p \left|u_n p^{k_n-\min\{k_n,k_m\}} - u_m p^{k_m-\min\{k_n,k_m\}}\right|_p = \\ &= e^{-\min\{k_n,k_m\}}, \text{ ha } k_n \neq k_m. \end{aligned}$$

Azonban Cauchy-sorozatról lévén szó, ez azt jelenti, hogy vagy $\min\{k_n, k_m\} \to \infty$ (ahol n és m is tart a végtelenhez), vagy létezik egy olyan N érték, hogy minden $n, m > N$ esetén $k_n = k_m$.

Az első esetben x_n nyilván 0-hoz tart. A második esetben létezik egy k egész szám, amire minden $n > N$ esetén $o_p(x_n) = k$. Vagyis minden N-nél nagyobb n-re és m-re $|x_n - x_m|_p = e^{-k}|u_n - u_m|_p$. Mivel az (x_n) sorozat Cauchy, így nyilván $|u_n - u_m|_p \to 0$ ($n, m \to \infty$ mellett). Mivel u_r minden r pozitív egészre egy p-adikus egység, tehát p-adikus egész szám, és a 2.10. következmény szerinte $\mathbb{Z}_p$ teljes a metrikus topológiával, így az (u_n) sorozatnak van határértéke $\mathbb{Z}_p$-ben, ami határértéke lesz $\mathbb{Q}_p$-ben is. Ennek p^k-szorosa nyilván x_n határértéke lesz $\mathbb{Q}_p$-ben.

q.e.d.

Vegyük észre, hogy a p-adikus abszolútértéket $\mathbb{Q}$-ra megszorítva a következőt kapjuk:

$$|r|_p = e^{-}k, \text{ ahol } r = \frac{a}{b}p^k, \text{ és } a \in \mathbb{Z}\ , b \in \mathbb{Z}\ , p \nmid a, b\ , \text{ tetszőleges } r \text{ racionális számra.}$$

Ez nyilván abszolútérték lesz a racionális számokon (egy abszolútérték megszorítása egy szűkebb gyűrűre mindig abszolútérték marad). A 2.13. állításbanláttuk, hogy $\mathbb{Q}$ sűrű $\mathbb{Q}_p$-ben, és az imént bizonyítottuk, hogy $\mathbb{Q}_p$ teljes. *Vagyis $\mathbb{Q}_p$ pont $\mathbb{Q}$ telítettje (lezártja) lesz, a p-adikus abszolútértékre nézve.* Az pedig nyilvánvaló, hogy $\mathbb{R}$ pont $\mathbb{Q}$ telítettje lesz a hagyományos abszolútértékre nézve. Ezek fényében érdekes a következő tétel:

A.2. Tétel (Ostrowski tétele)**.** *A racionális számok testén ekvivalencia erejéig csak a triviális, a hagyományos és a p-adikus abszolútértékek léteznek.*

A tétel bizonyítása előtt még kell ejtenünk pár szót az abszolútértékekről. A 11. oldalon található megjegyzésben már bevezettük a nemarkhimédészi abszolútérték fogalmát, az ultrametrikus egyenlőtlenség segítségével. Eredetileg a nemarkhimédésziséget nem így definiálták, hanem azzal, hogy az ilyen abszolútértékek felrúgják az arkhimédészi axiómát, vagyis, hogy ezekre az abszolútértékekre nézve az egész számok abszolútértékeinek halmaza korlátos. Most bebizonyítjuk, hogy ez a két feltétel ekvivalens:

A.3. Lemma. *Tetszőleges abszolútérték pontosan akkor nemarkhimédészi (vagyis pontosan akkor teljesül rá az ultrametrikus egyenlőtlenség) ha az egészek abszolútértékeinek halmaza korlátos.*

Bizonyítás. Mivel már láttuk, hogy minden abszolútértékre $|1| = 1$, ezért a nemarkhimédészi abszolútértékekre minden $n \in \mathbb{Z}^+$ esetén:

$$|n| = |1+(n-1)| \leq \max\{|1|, |n-1|\} = \max\{1, |1+(n-2)|\} \leq \max\{1, |n-2|\} \leq \cdots \leq \max\{1, |1|\} = 1,$$

azt pedig már láttuk, hogy egy számnak és az ellentettjének az abszolútértéke ugyanannyi, az abszolútérték definíciójában benne van, hogy $|0| = 0$, tehát $|n| \leq 1$, minden n egészre.

Másfelől, ha x-re és y-ra teljesül $|x| \geq |y|$, és az egészek abszolútértékeinek halmaza korlátos (legyen egy felső korlátja K), akkor minden k pozitív egészre:

$$\begin{aligned} |x+y| &= \sqrt[k]{|x+y|^k} = \sqrt[k]{|(x+y)^k|} = \sqrt[k]{\left|\sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i}\right|} \leq \sqrt[k]{\sum_{i=0}^{k} \left|\binom{k}{i}\right| |x|^i |y|^{k-i}} \leq \\ &\leq \sqrt[k]{(k+1)K |x|^k} = \sqrt[k]{K(k+1)}\,|x| \longrightarrow |x|\,, \text{ ha } k \to \infty. \end{aligned}$$

q.e.d.

A.4. Következmény. A bizonyítás első feléből következik, hogy ha egy abszolútérték nemarkhimédészi, akkor minden egész szám abszolútértéke legfeljebb 1.

Azokat az abszolútértékeket, amik nem elégítik ki az ultrametrikus egyenlőtlenséget, vagyis (mint láttuk) amikre nézve nem korlátos az egész számok abszolútértékeinek halmaza, azokat arkhimédészi abszolútértékeknek nevezzük. Ezekről szól a következő lemma:

A.5. Lemma. *Bármely arkhimédészi abszolútértékre, illetve bármely n és m, 1-től különböző pozitív egészekre $|n|^{\frac{1}{\log n}} = |m|^{\frac{1}{\log m}}$.*

Bizonyítás. Tekintsük m-et n-es számrendszerben felírva – legyenek számjegyei sorban $a_1, a_2, \ldots, a_r$ ($a_r \neq 0$). Ekkor $m \geq n^r$, vagyis $r \leq \frac{\log m}{\log n}$. A háromszög-egyenlőtlenségből, illetve abból, hogy $|1| = 1$ (ezt általában, tetszőleges abszolútértékre láttuk), következik, hogy minden k pozitív egészre $|k| \leq k$, vagyis minden $i = 1, \ldots, r$-re $|a_i| \leq a_i < n$.

Ha $|n| \leq 1$, akkor:

$$|m| = \left|\sum_{i=0}^{r} a_i n^i\right| \leq \sum_{i=0}^{r} |a_i|\,|n|^i \leq (r+1)n \leq n\frac{\log m}{\log n} + n.$$

Mivel m-re nem tettünk semmilyen feltételt, azon kivíül, hogy egy 1-nél nagyobb egész legyen, így mindez elmondható m^k-ra is, amiből $|m|^k \leq nk\frac{\log m}{\log n} + n$ következik. Ha ebből k-adik gyököt vonunk, és tartunk k-val a végtelenbe, akkor $|m| \leq 1$-et kapunk, minden 1-nél nagyobb egészre, amiből következik, hogy az egészek abszolútértékeinke halmaza korlátos, vagyis az abszolútérték nem arkhimédészi, amivel ellentmondásra jutottunk. Vagyis $|n| > 1$.

Ekkor az előzőhöz hasonlóan:

$$|m| = \left|\sum_{i=0}^{r} a_i n^i\right| \leq \sum_{i=0}^{r} |a_i|\,|n|^i \leq (r+1)\,n\,|n|^r \leq |n|^{\frac{\log m}{\log n}}\, n\left(1 + \frac{\log m}{\log n}\right).$$

Az előzőhöz hasonlóan ezt is tekinthetjük m helyett m^k-ra, majd vonhatunk k-adiku gyököt. Az így kapott egyenlőtlenségből ($|m| \leq |n|^{\frac{\log m}{\log n}} \sqrt[k]{n\left(1 + \frac{k\log m}{\log n}\right)}$) k-val végtelenhez tartva $|m| \leq |n|^{\frac{\log m}{\log n}}$ adódik. Mivel n és m szerepe felcserélhető, ezért az állítás valóban igaz lesz.

q.e.d.

Most már bebizonyíthatjuk Ostrowski tételét:

Bizonyítás. Legyen adott egy abszolútérték $\mathbb{Q}$-n. Erről fogjuk látni, hogy vagy a triviális, vagy a hagyományos, vagy valamelyik p-adiku abszolútértékkel ekvivalens.

Ha az abszolútérték nemarkhimédészi, akkor az első lemma szerint minden p prímre $|p| \leq 1$. Ha minden prímre $|p| = 1$, akkor (az abszolútérték szorzattartása, illetve az ellentettek azonos abszolútértéke miatt) nyilván a triviális abszolútértékkel van dolgunk. Amennyiben van egy p prím, amire $|p| < 1$, akkor észrevehetjük, hogy $I := \{n \in Z \mid |n| < 1\}$ egy ideál $\mathbb{Z}$-ben, hiszen nemarkhimédészi abszolútértékről lévén szó teljesül az ultrametrikus egyenlőtlenség, valamint az, hogy minden egész szám abszolútértéke legfeljebb 1. De $p \in I$, $1 \notin I$, és (p) maximális ideál $\mathbb{Z}$-ben – vagyis $I = (p)$, így ha p nem osztja a és b egész számokat, akkor minden n-re $\left|\frac{a}{b}p^n\right| = |p|^n$ teljesül, vagyis az abszolútértékünk ekvivalens a p-adikus abszolútértékkel.

Ha a vizsgált abszolútérték arkhimédészi, akkor vegyünk egy tetszőleges 1-nél nagyobb n egész számot, és tekintsük az $s = \frac{\log|n|}{\log n}$ értéket. A második lemma szerint s nem függ n-től, és a második lemma bizonyítása alapján az is kijelenthető, hogy s pozitív. (Láttuk, hogy $|n| > 1$.) Ekkor minden m, 1-től különböző, pozitív egészre:

$$|m| = \left(|m|^{\frac{1}{\log m}}\right)^{\log m} = (e^s)^{\log m} = m^s.$$

Ebből, az ellentettek abszolútértékének egyenlőségéből, abból, hogy $|1| = 1 = 1^s$, illetve $|0| = 0 = 0^s$, valamint az abszolútérték szorzattartásából látható, hogy minden r racionális számra $|r| = |r|_\infty^s$ (ahol $|.|_\infty$ a hagyományos abszolútérték).

Tehát a tételt bebizonyítottuk.

q.e.d.

Ez az állítás számunkra azért érdekes, mert lehetővé teszi, hogy a Hasse–Minkowski-tételt egy könnyen általánosítható formában fogalmazzuk meg:

A Hasse–Minkowski-tétel. *Vegyük a racionális számtest összes abszolútértékét, és vegyük $\mathbb{Q}$ ezek szerinti telítettjeit. Egy $\mathbb{Q}$ feletti kvadratikus alaknak pontosan akkor van nemtriviális gyöke ($\mathbb{Q}$-ban), ha az így keletkezett telítettek mindegyikében van nemtriviális gyöke.*

Nyilvánvaló, hogy a racionális számtestet bármilyen testre kicserélve egy értelmes állítást kapunk. Ennek ellenére ezt a fajta általánosítást nem nagyon vizsgálták, ugyanis a p-adikus abszolútértékek viszonylag könnyen (bár nem a triviális módon) általánosíthatóak más testekre is (ezek az általánosítások a prímideálok elméletén alapulnak), viszont egy test abszolútértékeiről általában nem sokat tudunk mondani. Ezért a téma kutatói inkább olyan általánosításokkal foglalkoztak, ahol csak a p-adikus (helyesebb lenne úgy mondanunk, $\mathfrak{p}$-adikus) abszolútértékekre követeljük meg a megfelelő telítettben való nemtriviális gyökök létezését. Ezen általánosítások eredményeiről a bevezetőben emlékeztünk meg.

Irodalomjegyzék

[1] J. S. Hsia: On the Hasse principle for quadratic forms, *Proceedings of the American Mathematical Society* Vol. 39. No. 3. (1973. augusztus), 468-470.

[2] J. S. Milne: *Algebraic Number Theory (v3.04)*. Kiadatlan, letölthető: `http://www.jmilne.org/math/CourseNotes/ANT.pdf`, 2012. 04. 16.

[3] R. Scharlau: Martin Kneser's work on quadratic forms and algebraic groups, *Quadratic Forms – Algebra, Arithmetic, and Geometry*. Contemporary Mathematics 493., 339-358. American Mathematical Society, 2009.

[4] J.-P. Serre: *A Course in Arithmetic*. Graduate Texts in Mathematics Vol. 7. Springer, 1973. Corrected fifth printing: Springer, 1996.

[5] Zábrádi G.: *Értékelések, telítés és a p-adikus számok teste*. Kiadatlan, letölthető: `http://www.cs.elte.hu/~zger/Algebra3_2012/p-adikus.pdf`, 2012. 10. 02.