Ulrich Matthias

FUNDAMENTOJ DE LINEARA ALGEBRO

Eldonita de la aŭtoro
Neckarhausen, 1995

Contents

Pro multaj valoraj konsiloj kaj korektoj la aŭtoro kore dankas al: Edmund Grimley-Evans, Konrad Hinsen, Horst Holdgrün, Jim Kingdon, Christer Kiselman kaj Marko Rauhamaa.

Matthias, Ulrich: Fundamentoj de lineara algebro. Unua eldono, la aŭtoro, oktobro 1995. Adreso de la aŭtoro: Frhr.-v.-Drais-Str. 53, 68535 Neckarhausen, Germanio; retpoŝto: umatthia@ix.urz.uni-heidelberg.de

---

Antaŭparolo

"Inter la esperantistoj sin trovas proporcie pli da matematikistoj ol da filologoj", konstatis la *Enciklopedio de Esperanto* jam en 1934. Multaj Esperanto-pioniroj estis matematikistoj, kaj same hodiaŭ, kiam junaj esperantistoj konatiĝas, ili ofte konstatas, ke mirige multaj el ili studas, studis aŭ intencas studi matematikon.

Tamen la matematika publikigado en Esperanto neniam vere viglis. La *Katalogo 1994* de la Libroservo de UEA ofertas nur 10 tiajn titolojn, kaj sur la bretoj de la Germana Esperanto-Biblioteko en Aalen sufiĉas 30-centimetra spaco por la kolektitaj matematikaj verkoj. Preskaŭ tute mankas en nia lingvo modernaj enkondukoj en la plej gravajn matematikajn branĉojn. Tio estas tre bedaŭrinda, ĉar jam de almenaŭ du jardekoj Esperanto-aktivuloj precipe el Irano, Ĉinio kaj aliaj aziaj landoj forte pledas por pli abunda scienca publikigado en Esperanto. Ankoraŭ nun mi memoras la vortojn de Saeed Farani el Pakistano, kiu prelegis en la Internacia Junulara Kongreso de la jubilea jaro 1987 en Krakovo pri "Esperanto kaj la tria mondo". "Se vi eŭropaj esperantistoj volas helpi al ni", emfazis Farani, "tiam ne verku aŭ traduku beletron, sed sciencajn publikaĵojn. Eĉ se vi tradukas nur kelkajn paĝojn el matematika faklibro, tio utilas al ni pli ol tuta romano..."

Malfrue, nur 8 jarojn poste, mi akceptis lian instigon, verkante tiun ĉi modestan broŝuron, kiu entenas proksimume tion, kion germanaj studentoj pri matematiko aŭ fiziko lernas en la unuaj ses semajnoj de sia studado en la lekciaro *lineara algebro*. Mi esperas, ke en la ne tro malproksima estonteco mi trovos tempon por pliampleksigi ĝin kaj por verki similan broŝureton pri la alia grava matematika branĉo, pri kiu studentoj okupiĝas ekde sia unua semestro, la *analitiko*. Mi ĝojus, se tiu ĉi broŝuro vere estus uzata ankaŭ en la tria mondo. Estas permesite multobligi ĝin en papera aŭ elektronika formo por nekomercaj celoj.

Kiel celgrupon mi imagas unuavice gejunulojn ĉie en la mondo, kiuj ĵus komencis aŭ baldaŭ komencos studi matematikon aŭ parencan fakon. Enketo de Germana Esperanto-Asocio montris, ke almenaŭ en mia lando homoj eklernas Esperanton precipe en aĝo de 18 ĝis 22 jaroj. Ne malmultaj el ili proksimume samtempe konatiĝas kun la universitatnivela matematiko. Al ili tiu ĉi broŝuro ebligas profundigi siajn sciojn pri Esperanto kaj pri matematiko samtempe.

Fine mi rimarkigu, ke mi verkis tiun ĉi broŝuron ne laste pro tio, ke tio estis plezuro por mi. Esperanto same kiel la matematiko ĉiam ravis kaj plu ravas min pro sia klareco kaj logikeco. Estas agrable vidi ilin kune. Por mi la publikigado en Esperanto krome donas ion, kion hodiaŭ la publikigado de matematika verko en nacia lingvo ne ĉiam povas doni - la senton fari ion utilan al la homaro.

Ulrich Matthias

1 Enkonduko

En lernejoj oni instruas, ke *vektoro* estas "io, kio havas direkton kaj longon". Oni imagas la vektorojn kiel sagojn. En la universitatnivela matematiko oni uzas alian, pli abstraktan difinon: Vektoro estas elemento de vektorspaco. Kompreneble per tio la problemo difini vektoron reduktiĝis nur je la problemo difini vektorspacon. Montriĝas, ke tiu ĉi difino fakte signifas, ke vektoroj estas matematikaj objektoj, kiuj lige kun du operacioj, la adicio kaj la multipliko per "skalaroj", plenumas certajn regulojn, kiujn oni nomas "aksiomoj". Nur en kelkaj tre specialaj kazoj oni vere povas imagi la vektorojn kiel sagojn.

La malfacilaĵoj de multaj studentoj kompreni lekcion pri *lineara algebro* rezultas el la granda abstrakteco kaj ĝeneraleco de ĝiaj difinoj kaj teoremoj. Oni ne tuj vidas la sencon starigi tian abstraktan teorion, kaj tio malpliigas la emon kompreni ĝin. Studkomencanto eble interesiĝas pri la solvoj de lineara ekvaciaro kun reelaj variabloj kaj koeficientoj, sed por tio malpli ĝenerala teorio sufiĉus. La plej multaj aliaj problemoj, pri kiuj okupiĝas la lineara algebro, aspektas iom artefarite. Ilia graveco montriĝos nur poste dum plua studado. Ekzemple vektoroj, kiujn oni ne povas imagi simple kiel sagojn, estas tre utilaj en la teorio de la Furieraj serioj. Tiu ĉi teorio pri la elvolvo de periodaj funkcioj laŭ la funkcioj $\sin kx$ kaj $\cos kx$ ($k \in \mathbf{Z}$) fariĝas esence pli eleganta kaj pli bone travidebla kiam oni konsideras "vektorspacon" de integreblaj funkcioj kaj aplikas rezultojn de la lineara algebro.

La leganto estas invitita simple kompreni la difinojn, rimarkojn, konkludojn, teoremojn kaj korolariojn, eĉ se li aŭ ŝi ankoraŭ ne plene komprenas, por kio tio utilas.

2 Aroj kaj bildigoj

2.1 Aroj

La fondinto de la aroteorio, Georg Cantor, klarigis aron kiel "kunigon de certaj distingitaj objektoj de nia percepto aŭ pensado al tutaĵo". Pli preciza enkonduko de tiu ĉi termino ne estas bezonata en la lineara algebro.

Finiajn arojn ni povas skribi en la formo $X = \{x_1, \ldots, x_n\}$. La plej simpla ekzemplo de *nefinia* aro estas $\mathbf{N} = \{0, 1, 2, \ldots\}$, la aro de la *naturaj nombroj*. Pliaj ekzemploj estas $\mathbf{Z} = \{0, 1, -1, 2, -2, \ldots\}$, la aro de la *entjeroj*, kaj $\mathbf{Q} = \{\frac{p}{q} : p, q \in \mathbf{Z}$ kaj $q \neq 0\}$, la aro de la *racionalaj nombroj*. La aron $\mathbf{R}$ de la *reelaj nombroj* la *EK-vortaro de matematikaj terminoj* enkondukas jene:

Sur la aro F de *koŝiaj vicoj* de racionalaj nombroj oni enkonduku la ekvivalentrilaton R difinitan per $(x_i)R(y_i) \Leftrightarrow \lim_{i\to\infty}(x_i - y_i) = 0$. La *kvocientaro* F/R estas la aro de la reelaj nombroj kiu faras korpon $\mathbf{R}$.

Bonŝance ne necesas kompreni tion por okupiĝi pri lineara algebro. Sufiĉas imagi $\mathbf{R}$ ekzemple kiel aron de "ĉiuj" nombroj, kiuj troviĝas sur rekto tra la entjeroj (aŭ tra la racionalaj nombroj).

Difino 2.1.1 *Se X kaj Y estas aroj, ni difinas*

- *la* intersekcon $X \cap Y$ *per* $X \cap Y := \{x : x \in X \text{ kaj } x \in Y\}$,
- *la* kunigaĵon $X \cup Y$ *per* $X \cup Y := \{x : x \in X \text{ aŭ } x \in Y\}$,
- *la* diferencon $X \backslash Y$ *per* $X \backslash Y := \{x \in X : x \notin Y\}$,
- *la* kartezian produton $X \times Y$ *per* $X \times Y := \{(x, y) : x \in X \text{ kaj } y \in Y\}$.

La kartezia produto de n faktoroj estas aro de n-opoj:

$$X_1 \times \ldots \times X_n := \{(x_1, \ldots, x_n) : x_1 \in X_1, \ldots, x_n \in X_n\}$$

X nomiĝas subaro *de Y se $x \in X \Rightarrow x \in Y$, t.e. se ĉiu elemento de X estas entenata ankaŭ en Y. Oni skribas tiam $X \subset Y$.*

2.2 Bildigoj

Ni komencas tiun ĉi paragrafon per abstrakta, formala difino, kiu tamen rapide fariĝas travidebla.

Difino 2.2.1 *Subaro F de la kartezia produto $X \times Y$ de du aroj X kaj Y nomiĝas* bildigo *se por ĉiu $x \in X$ ekzistas unu kaj nur unu $y \in Y$ tiel ke $(x, y) \in F$.*

Anstataŭ $(x, y) \in F$ oni skribas ankaŭ $y = F(x)$. Bildigo F do atribuas al ĉiu $x \in X$ unu kaj nur unu elementon $F(x) \in Y$. Oni skribas

$$\begin{array}{rccc} F: & X & \to & Y \\ & x & \mapsto & y \end{array}$$

y nomiĝas la *bildo* de x per la bildigo F, dum x nomiĝas *malbildo* de y. La bildo de aro X per F estas $F(X) := \{f(x) : x \in X\}$.

Difino 2.2.2 *Estu $F : X \to Y$ bildigo. F nomiĝas*

- surjekcia*, se $F(X) = Y$, t.e. se por ĉiu $y \in Y$ ekzistas* almenaŭ unu *malbildo x kun $F(x) = y$.*
- enjekcia*, se $F(x) = F(x') \Rightarrow x = x'$, t.e. se por ĉiu $y \in Y$ ekzistas* maksimume unu *malbildo x kun $F(x) = y$.*
- bijekcia*, se ĝi estas surjekcia kaj enjekcia, t.e. se por ĉiu $y \in Y$ ekzistas* unu kaj nur unu *malbildo x kun $F(x) = y$.*

Evidente ĉiu bijekcia bildigo estas *inversigebla*. Tio signifas, ke se F estas bijekcia ni povas difini inversan bildigon $F^{-1} : Y \to X$ per $y \to F^{-1}(y)$, kie $F^{-1}(y)$ estas la (ununura) malbildo de y per F.

3 Grupoj kaj korpoj

3.1 Grupoj

Difino 3.1.1 Grupo *estas paro $(G, \cdot)$, konsistanta el aro G kaj operacio*

$$\begin{array}{rccc} \cdot : & G \times G & \to & G \\ & (a, b) & \mapsto & (a \cdot b) \end{array}$$

tiel ke validas la sekvaj aksiomoj:

G 1 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ por ĉiuj $a, b, c \in G$ (aksiomo de asocieco)

G 2 Ekzistas elemento $e \in G$ tiel ke

$e \cdot a = a$ *por ĉiuj* $a \in G$ (ekzisto de neŭtrala elemento)

G 3 Por ĉiu elemento $a \in G$ ekzistas elemento $a' \in G$ tiel ke $a' \cdot a = e$

(ekzisto de inversaj elementoj)

Grupo nomiĝas abela *aŭ* komuta *se*

$$a \cdot b = b \cdot a \text{ por ĉiuj } a, b \in G$$

(aksiomo de komuteco).

Anstataŭ $(G, \cdot)$ ni nomas ankaŭ G grupo. Anstataŭ $a \cdot b$ ni ofte skribas ab.

Ekzemploj de grupoj

1. $(\mathbf{Z}, +)$, la aro de la entjeroj kun la adicio kiel operacio, estas abela grupo. La neŭtrala elemento estas 0; la inversa elemento de $n \in \mathbf{Z}$ estas $-n \in \mathbf{Z}$.

   Same ankaŭ $(\mathbf{Q}, +)$ kaj $(\mathbf{R}, +)$, la aroj de la racionalaj kaj la reelaj nombroj kun la adicio estas abelaj grupoj.

   Kontraŭe $(\mathbf{N}, +)$, la aro de la naturaj nombroj kun la adicio, ne estas grupo, ĉar por $a \in \mathbf{N}\backslash\{0\}$ la aksiomo G 3 ne estas plenumita.

2. $(\mathbf{R}\backslash\{0\}, \cdot)$ estas abela grupo. La neŭtrala elemento estas 1, kaj la inversa elemento de $a \in \mathbf{R}\backslash\{0\}$ estas $\frac{1}{a}$.

   Sed $(\mathbf{R}, \cdot)$ ne estas grupo, ĉar por la elemento $0 \in \mathbf{R}$ ne ekzistas inversa elemento.

3. Estu M nemalplena aro kaj $S(M)$ la aro de la permutoj de M, t.e. de la bijekciaj bildigoj de M sur ĝin mem. Ni difinas en $S(M)$ operacion $\cdot$ per sinsekva aplikado de la permutoj:

   Por σ, τ estu $\sigma \cdot \tau$ la bildigo

   $$(\sigma \cdot \tau)(x) = \sigma(\tau(x)) \text{ por ĉiuj } x \in M.$$

   Tiam $\sigma \cdot \tau$ estas *bijekcia* bildigo de M sur ĝin mem. Ni montras, ke $(S(M), \cdot)$ estas grupo:

   Neŭtrala elemento estas la *identa* bildigo $id_M : x \to x$ por ĉiu $x \in M$. La inversaj elementoj ekzistas, ĉar bijekciaj bildigoj estas inversigeblaj. La aksiomo de asocieco validas pro

   $$((\sigma \cdot \tau) \cdot \rho)(x) = (\sigma \cdot \tau)(\rho(x)) = \sigma(\tau(\rho(x))) = \sigma((\tau \cdot \rho)(x)) = (\sigma \cdot (\tau \cdot \rho))(x)$$

   Ĝenerale tiu ĉi grupo ne estas abela, kiel montras la sekva ekzemplo sur la aro $M = \{0, 1, 2\}$:

   $$\sigma \cdot \tau = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{bmatrix},$$

   $$\tau \cdot \sigma = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{bmatrix},$$

   kie la subaj elementoj estas la bildoj de la supraj. Notu, ke ni aplikas unue la *dekstran* permuton.

Konkludoj el la grupaj aksiomoj

Rimarko 3.1.2 *El la grupaj aksiomoj ni konkludas:*

(i) El $a'a = e$ sekvas $aa' = e$.

(ii) $ae = a$ por ĉiuj $a \in G$.

(iii) G entenas maksimume unu neŭtralan elementon.

(iv) Por ĉiu $a \in G$ ekzistas maksimume unu inversa elemento $a' \in G$.

Pruvo.

(i) Pro G 3 ekzistas b kun $ba' =$ e. Nun sekvas

$$aa' \overset{G2}{=} e(aa') = (ba')(aa') \overset{G1}{=} ((ba')a)a' \overset{G1}{=} (b(a'a))a' = (be)a' \overset{G2}{=} ba' = e$$

(ii) Estu a' inversa elemento de a. Tiam sekvas

$$ae \overset{G3}{=} a(a'a) \overset{G1}{=} (aa')a \overset{(i)}{=} ea \overset{G2}{=} a$$

(iii) Se e_1 kaj e_2 estas neŭtralaj elementoj, tiam

$$e_1 \overset{(ii)}{=} e_1 \cdot e_2 \overset{G2}{=} e_2$$

(iv) Se a_1 kaj a_2 estas du inversaj elementoj de a, ni havas

$$a_1 \overset{G2}{=} e \cdot a_1 \overset{G3}{=} (a_2a)a_1 \overset{G1}{=} a_2(aa_1) \overset{G3,(i)}{=} a_2e \overset{(ii)}{=} a_2$$

Ni montris, ke por ĉiu elemento a ekzistas unu kaj nur unu inversa elemento. Ni nomas ĝin a^{-1}.

Rimarko 3.1.3

(i) $(ab)^{-1} = b^{-1}a^{-1}$ por ĉiuj $a, b \in G$.

(ii) $(a^{-1})^{-1} = a$ por ĉiu $a \in G$

Pruvo.

(i) Ni devas pruvi, ke $b^{-1}a^{-1}$ estas la inversa elemento de ab. Fakte

$$(b^{-1}a^{-1})ab = ((b^{-1}a^{-1})a)b = (b^{-1}(a^{-1}a))b = (b^{-1}e)b = b^{-1}b = e$$

(ii) Ni devas pruvi, ke la inversa elemento de a^{-1} estas a. Tio ĝustas pro $aa^{-1} = e$.

3.2 Korpoj

Difino 3.2.1 *Korpo estas triopo* $(K, +, \cdot)$ *konsistanta el aro* K *kaj du operacioj, la adicio*

$$\begin{array}{rccc} + : & K \times K & \to & K \\ & (a, b) & \mapsto & (a + b) \end{array}$$

kaj la multipliko

$$\begin{array}{rccc} \cdot : & K \times K & \to & K \\ & (a, b) & \mapsto & (a \cdot b) \end{array}$$

tiel ke validas la sekvaj aksiomoj:

K 1 $(K, +)$ estas abela grupo. (Ĝia neŭtrala elemento estas nomata 0.)

K 2 $(K\backslash\{0\}, \cdot)$ estas abela grupo. (Ĝia neŭtrala elemento estas nomata 1.)

K 3 $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ por ĉiuj $a, b, c \in K$ (aksiomo de distribueco)

Anstataŭ $(K, +, \cdot)$ ni nomas ankaŭ K korpo. Anstataŭ $a \cdot b$ ni ofte skribas ab. La inverso de a rilate la adicion estas nomata $-a$. Ni do skribas a^{-1} nur por la inverso rilate la multiplikon. Anstataŭ $a + (-b)$ ni skribas ankaŭ $a - b$, kaj anstataŭ ab^{-1} ni foje skribas $\frac{a}{b}$. Laŭ kutima konvencio la multipliko $\cdot$ ligas pli forte ol la adicio $+$, kio ŝparigas multe da krampoj.

Simplaj ekzemploj de korpoj

1. $(\mathbf{Q}, +, \cdot)$ estas la korpo de la racionalaj nombroj.
2. $(\mathbf{R}, +, \cdot)$ estas la korpo de la reelaj nombroj.

Konkludoj el la korpaj aksiomoj

Rimarko 3.2.2 *Ni konkludas el la korpaj aksiomoj:*

K 3' $(a + b)c = ac + bc$ (maldekstra distribueco)

kaj krome

(i) $a \cdot 0 = 0$ kaj $0 \cdot a = 0$ por ĉiuj $a \in K$

(ii) El $ab = 0$ sekvas $a = 0$ aŭ $b = 0$.

(iii) $a(-b) = (-a)b = -ab$ por ĉiuj $a, b \in K$

(iv) $(-a)(-b) = ab$ por ĉiuj $a, b \in K$

Pruvo.

K 3' $(a+b)c \overset{K1}{=} c(a+b) \overset{K3}{=} ca + cb$

(i) $a \cdot 0 \overset{K1}{=} a \cdot 0 + (a \cdot 0 - a \cdot 0) \overset{K1,K3}{=} a(0+0) - a \cdot 0 \overset{K1}{=} a \cdot 0 - a \cdot 0 \overset{K1}{=} 0;$
$0 \cdot a \overset{K1}{=} 0 \cdot a + (0 \cdot a - 0 \cdot a) \overset{K1,K3'}{=} (0+0)a - 0 \cdot a \overset{K1}{=} 0 \cdot a - 0 \cdot a \overset{K1}{=} 0.$

(ii) Se $a \neq 0$ kaj $b \neq 0$, tiam pro K 2 ankaŭ $ab \neq 0$.

(iii) $a(-b) = a(0-b) \overset{K3}{=} a \cdot 0 - ab \overset{(i)}{=} 0 - ab = -ab;$
$(-a)b = (0-a)b \overset{K3'}{=} 0 \cdot b - ab \overset{(i)}{=} 0 - ab = -ab.$

(iv) $(-a)(-b) \overset{(iii)}{=} -(a(-b)) \overset{(iii)}{=} -(-ab) \overset{3.1.3}{=} ab$

La korpo de la kompleksaj nombroj

Difino 3.2.3 *Sur la aro* $\mathbf{R} \times \mathbf{R}$ *de la (orditaj) paroj de reelaj nombroj ni difinas adicion kaj multiplikon per*

$$\begin{array}{lcll} (a,b) + (c,d) & = & (a+c, b+d) & kaj \\ (a,b) \cdot (c,d) & = & (ac - bd, ad + bc) & \end{array}$$

Oni facile vidas, ke $(\mathbf{R} \times \mathbf{R}, +, \cdot)$ *estas korpo kun* $(0,0)$ *kiel neŭtrala elemento de la adicio,* $-(a,b) = (-a,-b)$ *kiel negativa elemento de* (a,b) *(t.e. kiel inversa elemento rilate la adicion),* $(1,0)$ *kiel neŭtrala elemento de la multipliko kaj*

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right)$$

kiel inversa elemento de (a,b) *rilate la multiplikon. Tiu ĉi korpo nomiĝas la korpo* $\mathbf{C}$ *de la* kompleksaj nombroj.

Pro $(a,0) + (a',0) = (a+a',0)$ kaj $(a,0) \cdot (a',0) = (aa',0)$ ni rajtas identigi la reelan nombron a kun la kompleksa nombro $(a,0)$. Tiamaniere $\mathbf{R}$ fariĝas subaro de $\mathbf{C}$. Ni nun difinas $i := (0,1)$ kaj ricevas la kutiman skribmanieron de la kompleksaj nombroj:

$$(a,b) = (a,0) + (b,0)(0,1) = a + bi \quad (\text{a,b} \in \mathbf{R})$$

Evidente $i^2 = (0,1)(0,1) = -1$. La reguloj por la adicio kaj multipliko nun aspektas jene:

$$\begin{array}{rcll} (a+bi) + (c+di) & = & (a+c) + (b+d)i & kaj \\ (a+bi) \cdot (c+di) & = & ac - bd + (ad+bc)i & \end{array}$$

Difino 3.2.4 *Por* $\lambda = a + bi$, $\operatorname{re}\lambda := a$ *nomiĝas la* reela parto, $\operatorname{im}\lambda := b$ *la* imaginara parto *kaj* $\bar{\lambda} := a - bi$ *la* konjugaĵo *de* λ. *La* absoluta valoro *de* λ *estas*

$$|\lambda| := \sqrt{\lambda\bar{\lambda}} = \sqrt{(a+bi)(a-bi)} = \sqrt{a^2+b^2}\ ;$$

tiu ĉi radiko ekzistas pro $a^2 + b^2 \geq 0$.

Rimarko 3.2.5 *Por ĉiuj* $\lambda, \mu \in \mathbf{C}$ *ni havas:*

(i) $\overline{\lambda + \mu} = \bar{\lambda} + \bar{\mu}$

(ii) $\overline{\lambda \cdot \mu} = \bar{\lambda} \cdot \bar{\mu}$

(iii) $\bar{\bar{\lambda}} = \lambda$

(iv) $|\lambda \cdot \mu| = |\lambda| \cdot |\mu|$

(v) $\lambda \in \mathbf{R} \Leftrightarrow \lambda = \bar{\lambda}$

Pruvo. La unuaj kvar egalaĵoj montriĝas veraj kiam oni substituas λ kaj μ per $a + bi$ respektive $c + di$ kaj aplikas la difinojn de la adicio, multipliko, konjugo kaj absoluta valoro. Ĉe aserto (v) la direkto "$\Rightarrow$" estas triviala; la alia direkto "$\Leftarrow$" sekvas jene:

$$\begin{array}{rrcl} & a+bi & = & a-bi \\ \Rightarrow & 2bi & = & 0 \\ \Rightarrow & b & = & 0 \end{array}$$

Finiaj korpoj

Sur la aro $M_2 = \{0, 1\}$ ni enkondukas la operaciojn + kaj $\cdot$ per la sekvaj tabeloj:

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Oni facile vidas, ke la korpaj aksiomoj estas plenumitaj. Ni do konstruis korpon kun du elementoj. En ĝi validas la unuavide kurioza egalaĵo $1 + 1 = 0$.

Ni povas konstrui eĉ por ĉiu primo p korpon sur la aro $M_p := \{0, 1, \ldots, p-1\}$: Por $x, y \in M_p$ estu $x + y$ la resto module p de la kutima sumo de x kaj y en $\mathbf{Z}$. Same $x \cdot y$ estu la resto module p de la kutima produto de x kaj y en $\mathbf{Z}$.

Ni nun pruvas, ke M_p kune kun tiuj ĉi du operacioj plenumas la korpajn aksiomojn: La neŭtrala elemento de la adicio estas 0, la negativo de a estas $-a = p - a \in M_p$; la neŭtrala elemento de la multipliko estas 1, kaj la aksiomoj de asocieco, komuteco kaj distribueco validas ĉar ili validas en $\mathbf{Z}$. Netriviala estas nur la aserto, ke por ĉiu $a \in M_p \backslash \{0\}$ ekzistas inverso rilate la multiplikon:

Se iu elemento $a \in M_p \backslash \{0\}$ ne havas inverson en M_p, tiam inter la p produtoj $x \cdot a, x \in M_p$ neniu egalas al la neŭtrala elemento 1. Sekve iu el la p elementoj de M_p aperas plurfoje kiel rezulto. Ekzistas do elementoj $x, y \in M_p, x \neq y$, kun $xa = ya$. Sekve $(x - y)a = 0$. Tio signifas en la aro $\mathbf{Z}$, ke la produto $(x - y)a$ estas dividebla per p. Simpla teoremo el la nombroteorio diras, ke primo dividanta produton dividas unu el ĝiaj faktoroj. Ni signas la dividon per | kaj konkludas: $p|(x-y)$ aŭ $p|a$. Pro $a \in \{1, \ldots, p-1\}$ ni povas malakcepti la duan eblecon. Sekve $p|(x - y)$. Rigardante $x - y$ kiel elementon de M_p, ni ricevas $x - y = 0$ kaj sekve $x = y$; ni do ricevis kontraŭdiron.

Ni nomas la ĵus konstruitan korpon $\mathbf{F_p}$. Evidente $\mathbf{F_2}$ estas la korpo, kiun ni difinis en la komenco de tiu ĉi paragrafo per la du tabeloj por la adicio kaj multipliko. La egalaĵo $1 + 1 = 0$ ne plu surprizas, kiam ni komprenas ĝin kiel konstaton pri restoj module 2: Ĝi tiam signifas, ke la sumo de du neparaj nombroj estas para.

Ni ĵus vidis, ke por ĉiu primo p ekzistas korpo kun p elementoj. Kiel ĝeneraligon de tiu ĉi konstato ni mencias sen pruvo, ke korpo kun n elementoj ekzistas se kaj nur se n estas potenco de primo.

Kiel ekzemplon de korpo kun neprima nombro de elementoj ni nun konstruas korpon kun 4 elementoj: Difinu sur la aro $M_4 = \{0, 1, s, t\}$ la operaciojn + kaj $\cdot$ per la sekvaj tabeloj:

$+$	0	1	s	t
0	0	1	s	t
1	1	0	t	s
s	s	t	0	1
t	t	s	1	0

$\cdot$	1	s	t
1	1	s	t
s	s	t	1
t	t	1	s

Estas facile, kvankam iomete penige, pruvi, ke $(M_4, +, \cdot)$ estas korpo. Oni nomas ĝin kutime $\mathbf{F_4}$.

4 Vektorspacoj

4.1 Difino de vektorspaco kaj ekzemploj

Difino 4.1.1 *V estu aro kaj K estu korpo.* K-vektorspaco *aŭ* vektorspaco super la korpo K *estas triopo* $(V, +, \cdot)$ *konsistanta el aro V kaj du operacioj, la adicio*

$$\begin{array}{rccc} + : & V \times V & \to & V \\ & (v, w) & \mapsto & (v + w) \end{array}$$

kaj la skalara multipliko

$$\begin{array}{rccc} \cdot : & K \times V & \to & V \\ & (\lambda, v) & \mapsto & \lambda \cdot v \end{array}$$

tiel ke (por ĉiuj $\lambda, \mu \in K,\ v, w \in V$) la sekvaj aksiomoj validas:

V 1 $(V, +)$ estas abela grupo.

V 2 $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$

V 3 $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$

V 4 $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$

V 5 $1 \cdot v = v$

La neŭtrala elemento 0 de la abela grupo $(V, +)$ estas nomata *nulvektoro*. Simile kiel ĉe grupoj kaj korpoj, anstataŭ $(V, +, \cdot)$ ni nomas ankaŭ V vektorspaco, kaj anstataŭ $\lambda \cdot v$ $(\lambda \in K, v \in V)$ ni ofte skribas simple λv. Laŭ kutima konvencio la skalara multipliko ligas pli forte ol la adicio en V.

La elementoj de V nomiĝas *vektoroj* kaj la elementoj de K *skalaroj*.

Ekzemploj

Ĉe la sekvaj tri ekzemploj oni facile vidas, ke la aksiomoj de vektorspaco estas plenumitaj.

1. Bazaj ekzemploj de K-vektorspacoj estas la spacoj $V = K^n = \underbrace{K \times \ldots \times K}_{n-foje}$ de la orditaj n-opoj, en kiuj la adicio kaj la skalara multipliko estas enkondukitaj per

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

2. Estu V la aro de ĉiuj polinomoj super korpo K, t.e.

$$V = \{a_n x^n + \ldots + a_1 x + a_0;\ a_0, \ldots, a_n \in K,\ n \geq 0\}.$$

   Ni enkondukas adicion per

$$(a_n x^n + \ldots + a_1 x + a_0) + (b_n x^n + \ldots + b_1 x + b_0) = (a_n + b_n)x^n + \ldots + (a_1 + b_1)x + a_0 + b_0$$

   (se la plej altaj potencoj havas malsamajn gradojn, samigu ilin per adicio de potencoj kun koeficiento 0)

   kaj skalaran multiplikon per

$$\lambda(a_n x^n + \ldots + a_1 x + a_0) = \lambda a_n x^n + \ldots + \lambda a_1 x + \lambda a_0$$

   Evidente $(V, +)$ estas abela grupo kaj $(V, +, \cdot)$ estas vektorspaco.

3. Estu V la aro de ĉiuj reelaj funkcioj, t.e. de ĉiuj bildigoj de $\mathbf{R}$ al ĝi mem. Ni enkondukas adicion $+$ kaj multiplikon $\cdot$ de elementoj de V per reelaj nombroj per

$$\left.\begin{array}{l}(f + g)(x) = f(x) + g(x) \\ (\lambda \cdot f)(x) = \lambda \cdot f(x)\end{array}\right\} \quad \text{por ĉiuj } \lambda, x \in \mathbf{R} \text{ kaj } f, g \in V.$$

   La bildigo $f + g$ do atribuas al ĉiu elemento $x \in \mathbf{R}$ la elementon $f(x) + g(x) \in \mathbf{R}$. Evidente $(V, +)$ estas abela grupo kaj $(V, +, \cdot)$ estas vektorspaco.

Konkludoj el la aksiomoj de vektorspaco

Rimarko 4.1.2 *Se V estas K-vektorspaco, ni havas:*

(i) $0 \cdot v = 0$ por ĉiuj $v \in V$

(ii) $\lambda \cdot 0 = 0$ por ĉiuj $\lambda \in K$

(iii) $(-\lambda)v = -\lambda v$ por ĉiuj $\lambda \in K, v \in V$

(iv) El $\lambda v = 0$ sekvas $\lambda = 0$ aŭ $v = 0$.

Pruvo

(i) $0 \cdot v = 0 \cdot v + 0 \cdot v - 0 \cdot v = (0+0) \cdot v - 0 \cdot v = 0 \cdot v - 0 \cdot v = 0$

(ii) $\lambda \cdot 0 = \lambda \cdot 0 + \lambda \cdot 0 - \lambda \cdot 0 = \lambda \cdot (0+0) - \lambda \cdot 0 = \lambda \cdot 0 - \lambda \cdot 0 = 0$

(iii) $(-\lambda)v = (-\lambda)v + \lambda v - \lambda v = (-\lambda + \lambda)v - \lambda v = 0 - \lambda v = -\lambda v$

(iv) Estu $\lambda v = 0$, $\lambda \neq 0$. Tiam ekzistas $\lambda^{-1} \in K$ kun $v = (\lambda^{-1}\lambda)v = \lambda^{-1}(\lambda v)$ $= \lambda^{-1} \cdot 0 \overset{(ii)}{=} 0$

4.2 Subspacoj

Difino 4.2.1 *$(V, +, \cdot)$ estu K-vektorspaco kaj $U \subset V$ estu subaro de V. $(U, +, \cdot)$ nomiĝas* subspaco *de V se U kune kun la adicio kaj skalara multipliko el $(V, +, \cdot)$ mem estas vektorspaco.*

Rimarko 4.2.2 *Subaro $U \neq \emptyset$ de vektorspaco V estas subspaco se kaj nur se la sekvaj kondiĉoj estas plenumitaj:*

(i) $x, y \in U \Rightarrow x + y \in U$ (fermiteco rilate la adicion)

(ii) $\lambda \in K, x \in U \Rightarrow \lambda x \in U$ (fermiteco rilate la multiplikon)

Pruvo. Se U estas subspaco de V, la du kondiĉoj estas evidente plenumitaj. Inverse, se U estas subaro de V, kiu plenumas (i) kaj (ii), U entenas kun x ankaŭ $-x = -(1x) = (-1)x$; pro (i) ĝi entenas ankaŭ $0 = x + (-x)$. La aliaj aksiomoj de vektorspaco validas simple ĉar ili validas en V.

Ekzemploj de subspacoj

Subspacoj de $\mathbf{R}^2$ estas

- la nulvektoro,
- la rektoj tra 0, t.e. ĉiu aro $\{\lambda v : \lambda \in \mathbf{R}\}$ por fiksita $v \in \mathbf{R}^2 \backslash \{0\}$,
- $\mathbf{R}^2$ mem.

Oni povas pruvi, ke $\mathbf{R}^2$ ne havas pliajn subspacojn.

4.3 Lineara dependeco kaj bazoj

Difino 4.3.1 *Aro de r vektoroj $\{v_1, \ldots, v_r\}$ el K-vektorspaco V nomiĝas* lineare sendependa*, se el $\lambda_1, \ldots, \lambda_r \in K$ kaj $\lambda_1 v_1 + \ldots + \lambda_r v_r = 0$ sekvas $\lambda_1 = \ldots = \lambda_r = 0$.*

Ĝi nomiĝas lineare dependa*, se ĝi ne estas lineare sendependa.*

Ekzemploj

- En la vektorspaco $\mathbf{R}^2$ la aro $\{(1,2),(2,3)\}$ estas lineare sendependa, dum $\{(1,2),(2,4)\}$ estas lineare dependa. Pli ĝenerale, en K-vektorspaco aro {v,w} de *du* vektoroj estas lineare dependa se kaj nur se ekzistas iu $\lambda \in K$ tiel ke $v = \lambda w$ aŭ $w = \lambda v$.
- En la vektorspaco $\mathbf{R}^n$ la aro $\{(1,0,\ldots,0,0),(0,1,\ldots,0,0),\ldots,(0,0,\ldots,0,1)\}$ estas lineare sendependa.

Por povi uzi Difinon 4.3.1 ankaŭ por nefiniaj aroj de vektoroj, ni nun ĝeneraligas ĝin.

Difino 4.3.2 *V estu K-vektorspaco. Subaro $M \subset K$ nomiĝas* lineare sendependa *se ĉiu finia subaro $\{v_1, \ldots, v_r\} \subset M$ estas lineare sendependa. M nomiĝas* lineare dependa *se ĝi ne estas lineare sendependa.*

Rimarko 4.3.3 *Se M estas lineare sendependa subaro de vektorspaco V, tiam ankaŭ ĉiu subaro $M' \subset M$ estas lineare sendependa.* □

Difino 4.3.4 *Vektoro v el K-vektorspaco V nomiĝas* lineara kombinaĵo *de la vektoroj $v_1, \ldots, v_r \in V$ se ekzistas $\lambda_1, ..., \lambda_r \in K$ tiel ke*

$$v = \lambda_1 v_1 + \ldots + \lambda_r v_r$$

Se M estas subaro de K-vektorspaco V, ni difinas

$$\operatorname{Lin} M := \{v \in V : \text{ } v \text{ estas lineara kombinaĵo de finia nombro de vektoroj el } M\}$$

$\operatorname{Lin} M$ *estas nomata la* lineara tegaĵo *de M. (Oni foje skribas anstataŭ* $\operatorname{Lin} M$ *ankaŭ* $\langle M \rangle$*.)*

Generantaroj kaj bazoj

Difino 4.3.5 *Subaro M de K-vektorspaco V nomiĝas* generantaro *de V se* $V = \operatorname{Lin} M$. Bazo *B de vektorspaco V estas lineare sendependa generantaro.*

Teoremo 4.3.6 *La sekvaj asertoj estas ekvivalentaj:*

(i) M estas bazo de V.

(ii) M estas minimuma generantaro de V. (Tio signifas, ke $V = \operatorname{Lin} M$, sed $V \neq \operatorname{Lin}(M \backslash \{v\})$ por ĉiu $v \in M$.)

(iii) M estas maksimuma lineare sendependa subaro de V. (Tio signifas, ke M estas lineare sendependa, sed $M \cup \{v\}$ estas lineare dependa por ĉiu $v \in V \backslash M$.)

(iv) Ĉiu vektoro $v \in V$ estas unike reprezentebla kiel lineara kombinaĵo de finia nombro de malsamaj vektoroj el M.

Pruvo.

1. (i) $\Rightarrow$ (ii) Se M estas lineare sendependa, tiam por ĉiu $v \in M$ la egalaĵo

   $$\lambda v + \lambda_1 v_1 + \ldots + \lambda_r v_r = 0 \text{ kun } v_1, \ldots, v_r \in M, \lambda, \lambda_1, \ldots, \lambda_r \in K$$

   ĝustas nur por $\lambda = \lambda_1, \ldots, \lambda_r = 0$. (Ni supozas, ke $v, v_1, \ldots, v_r$ estas *malsamaj* elementoj de M.) Sekve $v \notin \operatorname{Lin}(M \backslash \{v\})$. Tio signifas, ke M estas *minimuma* generantaro.

2. (ii) $\Rightarrow$ (i) (Nerekta pruvo.) Se M estas *lineare dependa* generantaro de V, tiam ekzistas $v_1, \ldots, v_r \in M$ kaj $\lambda_1, \ldots, \lambda_r \in K$, kiuj ne ĉiuj estas 0, tiel ke

   $$\lambda_1 v_1 + \ldots + \lambda_r v_r = 0$$

   Ni elektas iun $i \in \{1, \ldots, r\}$ kun $\lambda_i \neq 0$. Tiam $v_i = -\frac{1}{\lambda_i}(\lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + \ldots + \lambda_r v_r)$. Sekve ankaŭ $M \backslash \{v_i\}$ estas generantaro de V. (Kontraŭdiro al (ii).)

3. (i) ⇒ (iii) (Nerekta pruvo.) Ni supozu, ke ni povas aldoni al M iun plian vektoron v tiel, ke ankaŭ $M \cup \{v\}$ estas lineare sendependa. Tio signifas, ke por ĉiuj $v_1, \ldots, v_r \in M,\ \lambda, \lambda_1, \ldots, \lambda_r \in K$ validas la implico

$$\lambda v + \lambda_1 v_1 + \ldots + \lambda_r v_r = 0 \Rightarrow \lambda = \lambda_1 = \ldots = \lambda_r = 0$$

Sekve $v \notin \operatorname{Lin} M$, t.e. M ne estas generantaro de V. (Kontraŭdiro al (i).)

4. (iii) ⇒ (i) (Nerekta pruvo.) Ni supozu, ke M ne estas generantaro de V. Tiam ekzistas en V iu vektoro $v \notin \operatorname{Lin} M$. Nun por ĉiuj $v_1, \ldots, v_r \in M,\ \lambda, \lambda_1, \ldots, \lambda_r \in K$ validas la implico

$$\lambda v + \lambda_1 v_1 + \ldots + \lambda_r v_r = 0 \Rightarrow \lambda = \lambda_1 = \ldots = \lambda_r = 0,$$

kion ni konkludas por $\lambda = 0$ el la lineara sendependeco de M kaj por $\lambda \neq 0$ el $v \notin \operatorname{Lin} M$. Sekve ankaŭ $M \cup \{v\}$ estas lineare sendependa. (Kontraŭdiro al (iii).)

5. (i) ⇒ (iv) Pro $v \in \operatorname{Lin} M$ ĉiu vektoro $v \in V$ estas reprezentebla kiel lineara kombinaĵo de vektoroj el M. Se ni havas du reprezentojn $v = \lambda_1 v_1 + \ldots + \lambda_r v_r$ kaj $v = \mu_1 v_1 + \ldots + \mu_r v_r$ (kie $v_1, \ldots, v_r \in M,\ \lambda_1, \ldots, \lambda_r, \mu_1, \ldots, \mu_r \in K$), tiam el la diferenco $0 = (\lambda_1 - \mu_1)v_1 + \ldots + (\lambda_r - \mu_r)v_r$ sekvas pro la lineara sendependeco de $v_1, \ldots, v_r$ ke $\lambda_1 = \mu_1, \ldots, \lambda_r = \mu_r$; la du reprezentoj do estas identaj.

6. (iv) ⇒ (i) Pro (iv) M estas generantaro de V. Ni nun pruvas nerekte, ke M estas lineare sendependa: Se M estus lineare dependa, la vektoro $0 \in V$ havus iun netrivialan reprezenton $v = \lambda_1 v_1 + \ldots + \lambda_r v_r$, kie $v_1, \ldots, v_r \in M$, $\lambda, \lambda_1, \ldots, \lambda_r \in K$ kaj ne ĉiuj λ_i $(i = 1, \ldots, r)$ estas nuloj. Ĉar 0 havas ankaŭ la trivialan reprezenton $0 = 0v_1 + \ldots + 0v_r$, tiu reprezento ne estus la sola. (Kontraŭdiro al (iv).)

Korolario 4.3.7 *Ĉiu vektorspaco kun finia generantaro havas bazon.*

Pruvo. Per forpreno de vektoroj el finia generantaro ni povas trovi *minimuman* generantaron. Pro la ĵus pruvita teoremo tia minimuma generantaro estas bazo. □

Ni notas, ke tiu ĉi korolario validas ankaŭ por vektorspacoj kun nefinia generantaro; la ĝenerala pruvo baziĝas sur aksiomo de la aroteorio.

4.4 Interŝanĝo de bazaj vektoroj

Teoremo 4.4.1 *Estu $w_1, \ldots, w_s$ lineare sendependaj vektoroj el la vektorspaco V kun bazo $\{v_1, \ldots, v_n\}$. Tiam ni povas elekti el la vektoroj $v_1, \ldots, v_n$ vektorojn $v'_1, \ldots, v'_m$ tiel, ke ankaŭ $\{w_1, \ldots, w_s, v'_1, \ldots, v'_m\}$ estas bazo de V.*

Pruvo. Konsideru ĉiujn subarojn de $M = \{w_1, \ldots, w_s, v_1, \ldots, v_n\}$, kiuj entenas $M_1 = \{w_1, \ldots, w_s\}$ kaj estas generantaroj de V. Almenaŭ M mem havas tiujn ĉi ecojn. Elektu tian subaron kun minimuma nombro de vektoroj: $M_2 = \{w_1, \ldots, w_s, v'_1, \ldots, v'_m\}$. Ni nun montras per nerekta pruvo, ke M_2 estas lineare sendependa, kio pruvas la teoremon. Se M_2 estus lineare dependa, ni havus $\lambda_1, \ldots, \lambda_s, \mu_1, \ldots, \mu_m \in K$, kiuj ne ĉiuj estas nuloj, tiel ke

$$\lambda_1 w_1 + \ldots + \lambda_s w_s + \mu_1 v'_1 + \ldots + \mu_m v'_m = 0$$

Nun ekzistas iu $i \in \{1, \ldots, m\}$ kun $\mu_i \neq 0$, ĉar alikaze $\{w_1, \ldots, w_s\}$ estus lineare dependa. Tio signifas, ke ne nur $\mu_i v'_i \in \mathrm{Lin}\{w_1, \ldots, w_s, v'_1, \ldots, v'_{i-1}, v'_{i+1}, \ldots, v'_m\}$, sed eĉ $v'_i \in \mathrm{Lin}\{w_1, \ldots, w_s, v'_1, \ldots, v'_{i-1}, v'_{i+1}, \ldots, v'_m\}$. Tio estas kontraŭdiro al la minimumeco de M_2, ĉar ankaŭ $M_2 \backslash \{v'_i\}$ havas la deziratajn ecojn. □

Korolario 4.4.2 *En vektorspaco kun finia bazo ĉiuj bazoj havas la saman longon. (La longo de bazo estas la nombro de vektoroj entenataj en ĝi.)*

Pruvo. Estu $\{v_1, \ldots, v_r\}$ bazo de V kun minimuma longo. $\{w_1, \ldots, w_n\}$ estu alia bazo de V. Tiam $r \leq n$. Ni devas pruvi, ke $r = n$. Tiucele ni konstatas, ke laŭ Teoremo 4.4.1 ekzistas $v'_1, \ldots, v'_{m_1} \in \{v_1, \ldots, v_r\}$ tiel ke ankaŭ $\{w_1, v'_1, \ldots, v'_{m_1}\}$ estas bazo de V. Nun $m_1 < r$, ĉar $w_1 \in \mathrm{Lin}\{v_1, \ldots, v_r\}$. Krome $m_1 \geq r-1$, ĉar alikaze V havus bazon entenantan malpli ol r vektorojn. Sekve ankaŭ $\{w_1, v'_1, \ldots, v'_{m_1}\}$ estas bazo de V kun longo r.

Ĉar $\{w_1, w_2\}$ estas lineare sendependa, laŭ Teoremo 4.4.1 ekzistas $v''_1, \ldots, v''_{m_2} \in \{w_1, v'_1, \ldots, v'_{m_1}\}$ tiel, ke ankaŭ $\{w_1, w_2, v''_1, \ldots, v''_{m_2}\}$ estas bazo de V. Ni havas eĉ $v''_1, \ldots, v''_{m_2} \in \{v'_1, \ldots, v'_{m_1}\}$, ĉar w_1 ne povas plurfoje aperi en bazo. Nun $m_2 < r-1$, ĉar $w_2 \in \mathrm{Lin}\{w_1, v'_1, \ldots, v'_{m_1}\}$. Krome $m_2 \geq r-2$, ĉar alikaze V havus bazon entenantan malpli ol r vektorojn. Sekve ankaŭ $\{w_1, w_2, v''_1, \ldots, v''_{m_2}\}$ estas bazo de V kun longo r. Aplikante tiun ĉi proceduron r-foje, ni konstatas, ke ankaŭ $\{w_1, \ldots, w_r\}$ estas bazo de V. Ĉar ankaŭ $\{w_1, \ldots, w_n\}$ estas bazo (kaj do *minimuma* lineare sendependa generantaro) de V, ni konkludas, ke $r = n$. □

Tiu ĉi korolario ebligas la sekvan difinon:

Difino 4.4.3 *La* dimensio *de vektorspaco V estas*

$$\dim V := \begin{cases} r, \text{ se } V \text{ havas bazon kun longo } r \\ \infty, \text{ se } V \text{ ne havas finian bazon} \end{cases}$$

4.5 La dimensia formulo

Difino 4.5.1 *Se U, W estas subspacoj de V, ni difinas*

la intersekcon $U \cap W := \{v : v \in U \text{ kaj } v \in W\}$

kaj la sumon $U + W := \{u + w : u \in U \text{ kaj } w \in W\}$

Rimarko 4.5.2 *Ankaŭ $U \cap W$ kaj $U + W$ estas subspacoj de V.*

Pruvo. Ni pruvas nur la duan aserton, ĉar la unua estas eĉ pli facila. Ni aplikas rimarkon 4.2.2. Se $v_1, v_2 \in U + W$, tiam ekzistas $u_1, u_2 \in U$ kaj $w_1, w_2 \in W$ tiel ke $v_1 = u_1 + w_1$ kaj $v_2 = u_2 + w_2$. Sekve $v_1 + v_2 = \underbrace{(u_1 + u_2)}_{\in U} + \underbrace{(w_1 + w_2)}_{\in W} \in U + W$ kaj $\lambda v_1 = \underbrace{\lambda u_1}_{\in U} + \underbrace{\lambda w_1}_{\in W} \in U + W$. □

Se $U \cap W = \{0\}$, la sumo $U + W$ nomiĝas la *rekta sumo* de U kaj W, kaj oni skribas $U \oplus W$.

Rimarko 4.5.3 *Ĉiu vektoro $v \in U \oplus W$ havas ununuran reprezenton en la formo $v = u + w$ kun $u \in U, w \in W$.*

Pruvo. Se $v = u_1 + w_1 = u_2 + w_2$ kun $u_1, u_2 \in U$ kaj $w_1, w_2 \in W$, tiam $\underbrace{u_1 - u_2}_{\in U} = \underbrace{w_2 - w_1}_{\in W}$. El $U \cap W = \{0\}$ nun sekvas $u_1 - u_2 = 0$ kaj $w_2 - w_1 = 0$; la du reprezentoj do samas. □

Teoremo 4.5.4 (Dimensia formulo por subspacoj) *Estu U, W subspacoj de K-vektorspaco V kun finia dimensio. Tiam*

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

Pruvo. Estu $m := \dim U, n := \dim W, r := \dim(U \cap W)$. Estu $\{u_1, \ldots, u_m\}$ bazo de U kaj $\{v_1, \ldots, v_r\}$ bazo de $U \cap W$. Pro Teoremo 4.4.1 ekzistas bazo $\{v_1, \ldots, v_r, w_{r+1}, \ldots, w_n\}$ de W. Ni devas pruvi, ke $\dim(U + W) = m + n - r$. Tiucele sufiĉas montri, ke $\{u_1, \ldots, u_m, w_{r+1}, \ldots, w_n\}$ estas bazo de $U + W$. Ni konkludas tion el du asertoj.

(i) $\{u_1, \ldots, u_m, w_{r+1}, \ldots, w_n\}$ estas generantaro de $U + W$:

Elektu iun ajn $v \in U + W$. Tiam ekzistas $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_n \in K$ tiel ke

$$v = \lambda_1 u_1 + \ldots + \lambda_m u_m + \mu_1 v_1 + \ldots + \mu_r v_r + \mu_{r+1} w_{r+1} + \ldots + \mu_n w_n$$

Pro $\mu_1 v_1 + \ldots + \mu_r v_r \in U \cap W$ ekzistas $\lambda'_1, \ldots, \lambda'_m \in K$ tiel ke

$$\mu_1 v_1 + \ldots + \mu_r v_r = \lambda'_1 u_1 + \ldots + \lambda'_m u_m$$

Sekve $v \in \mathrm{Lin}\{u_1, \ldots, u_m, w_{r+1}, \ldots, w_n\}$.

(ii) $\{u_1, \ldots, u_m, w_{r+1}, \ldots, w_n\}$ estas lineare sendependa:

Ni supozu, ke ekzistas $\lambda_1, \ldots, \lambda_m, \mu_{r+1}, \ldots, \mu_n \in K$ tiel ke

$$\lambda_1 u_1 + \ldots + \lambda_m u_m + \mu_{r+1} w_{r+1} + \ldots + \mu_n w_n = 0$$

Tiam $v := \lambda_1 u_1 + \ldots + \lambda_m u_m = -\mu_{r+1} w_{r+1} - \ldots - \mu_n w_n$. Sekve $v \in U \cap W$. Nun $v \in \mathrm{Lin}\{v_1, \ldots, v_r\}$ kaj $v \in \mathrm{Lin}\{w_{r+1}, \ldots, w_n\}$. Ĉar $\{v_1, \ldots, v_r, w_{r+1}, \ldots, w_n\}$ estas lineare sendependa, ni konkludas ke $v = 0$. Ĉar $\{u_1, \ldots, u_m\}$ kaj $\{w_{r+1}, \ldots, w_n\}$ estas lineare sendependaj aroj (la lasta pro Rimarko 4.3.3), ni ricevas $\lambda_1 = \ldots = \lambda_m = \mu_{r+1} = \ldots = \mu_n = 0$. □

5 Linearaj bildigoj

5.1 Difino de lineara bildigo, bildo kaj kerno

Difino 5.1.1 *Estu V kaj V' vektorspacoj super la sama korpo K. Tiam $F : V \to V'$ nomiĝas* lineara bildigo *aŭ* homomorfio *se*

L 1 $F(v + w) = F(v) + F(w)$ por ĉiuj $v, w \in V$

L 2 $F(\lambda v) = \lambda F(v)$ por ĉiuj $\lambda \in K,\ v \in V$

En la speciala kazo $V = V'$ tia bildigo nomiĝas endomorfio.

Rimarko 5.1.2 *La du kondiĉoj* L 1 *kaj* L 2 *estas ekvivalentaj al la kondiĉo*

L $F(\lambda v + \mu w) = \lambda F(v) + \mu F(w)$ por ĉiuj $\lambda \in K,\ v, w \in V$

Pruvo. La direkto "⇐" estas triviala. La direkto "⇒" sekvas jene: $F(\lambda v + \mu w) \overset{L1}{=} F(\lambda v) + F(\mu w) \overset{L2}{=} \lambda F(v) + \mu F(w)$. □

Rimarko 5.1.3 *Se $F : V \to V'$ estas lineara bildigo kaj $\{v_1, \ldots, v_n\}$ estas lineare dependa subaro de V, tiam $\{F(v_1), \ldots, F(v_n)\}$ estas lineare dependa subaro de V'.*

Pruvo. $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0 \Rightarrow F(\lambda_1 v_1 + \ldots + \lambda_n v_n) = F(0) \overset{L}{\Rightarrow} \lambda_1 F(v_1) + \ldots + \lambda_n F(v_n) = F(0)$; la aserto nun sekvas pro $F(0) = F(0 \cdot 0) \overset{L2}{=} 0 \cdot F(0) = 0$.

Evidente la inversa konkludo de Rimarko 5.1.3 ne validas; ekzemple la 0-bildigo $F : v \to 0$ por ĉiuj $v \in V$ bildigas lineare sendependajn arojn sur la lineare dependan aron $\{0\}$.

Difino 5.1.4 *Por lineara bildigo $F : V \to V'$ ni difinas*

la *kernon* $\operatorname{Ker} F := \{v \in V : F(v) = 0\}$

kaj la *bildon* $\operatorname{Im} F := \{F(v) : v \in V\} = F(V)$

$\operatorname{Ker} F$ do estas la aro de la malbildoj de 0.

Rimarko 5.1.5 *Estu $F : V \to W$ lineara bildigo. Tiam*

(i) $\operatorname{Ker} F$ kaj $\operatorname{Im} F$ estas vektorspacoj.

(ii) $\dim \operatorname{Im} F \leq \dim V$

(iii) F estas surjekcia se kaj nur se $\operatorname{Im} F = W$.

(iv) F estas enjekcia se kaj nur se $\operatorname{Ker} F = \{0\}$.

Pruvo.

(i) $v_1, v_2 \in \operatorname{Ker} F,\ \lambda, \mu \in K \Rightarrow 0 = \lambda F(v_1) + \mu F(v_2) \overset{L}{=} F(\lambda v_1 + \mu v_2) \Rightarrow \lambda v_1 + \mu v_2 \in \operatorname{Ker} F$.

La dua aserto sekvas simile, se ni elektas v_1 kaj v_2 kiel malbildojn de w_1 kaj w_2: $w_1, w_2 \in \operatorname{Im} F,\ \lambda, \mu \in K \Rightarrow \lambda w_1 + \mu w_2 = \lambda F(v_1) + \mu F(v_2) \overset{L}{=} F(\lambda v_1 + \mu v_2) \in \operatorname{Im} F$.

Pro Rimarko 4.2.2 tio pruvas la aserton.

(ii) Se $\{v_1, \ldots, v_n\}$ estas bazo (kaj do generantaro) de V, tiam $\{F(v_1), \ldots, F(v_n)\}$ estas generantaro de $F(V) = \operatorname{Im} F$. Tial bazo (t.e. minimuma generantaro) de $\operatorname{Im} F$ havas maksimume $n = \dim V$ elementojn.

(iii) Tiu ĉi aserto estas triviala.

(iv) "$\Rightarrow$": $F(v) = 0 \Rightarrow F(v) = F(0) \overset{F\ enjekcia}{\Longrightarrow} v = 0$

"$\Leftarrow$": $F(v_1) = F(v_2) \overset{L}{\Rightarrow} F(v_1 - v_2) = 0 \Rightarrow v_1 - v_2 \in \operatorname{Ker} F \Rightarrow v_1 - v_2 = 0$
$\Rightarrow v_1 = v_2$. □

Oni nomas $\dim \operatorname{Im} F$ la rango de la lineara bildigo F.

5.2 La dimensia formulo por linearaj bildigoj

Teoremo 5.2.1 *Estu $F : V \to V'$ lineara bildigo, kaj $\dim V$ estu finia. Tiam*

$$\dim \operatorname{Ker} F + \dim \operatorname{Im} F = \dim V$$

Pruvo. Estu $n := \dim V$. Tiam ankaŭ $k := \dim \operatorname{Ker} F$ estas finia, kaj $k \leq n$. $\{v_1, \ldots, v_k\}$ estu bazo de $\operatorname{Ker} F$. Pro Teoremo 4.4.1 nun ekzistas bazo $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ de V. Ni devas pruvi, ke $\dim \operatorname{Im} F = n - k$, kaj tiucele sufiĉas montri, ke $\{F(v_{k+1}), \ldots, F(v_n)\}$ estas bazo de $\operatorname{Im} F$. Ni konkludas tion el du asertoj:

(i) $\{F(v_{k+1}), \ldots, F(v_n)\}$ estas generantaro de $\operatorname{Im} F$, ĉar:

Elektu iun $w \in \operatorname{Im} F$. Tiam ekzistas iu $v \in V : w = F(v)$, kaj $\lambda_1, \ldots, \lambda_n \in K$ tiel ke $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$. Sekve $w = F(v) = F(\lambda_1 v_1 + \ldots + \lambda_n v_n) = \lambda_1 F(v_1) + \ldots + \lambda_k F(v_k) + \lambda_{k+1} F(v_{k+1}) + \ldots + \lambda_n F(v_n) = \lambda_{k+1} F(v_{k+1}) + \ldots + \lambda_n F(v_n)$.

(ii) $\{F(v_{k+1}), \ldots, F(v_n)\}$ estas lineare sendependa, ĉar:

$$\begin{aligned}
& \lambda_{k+1} F(v_{k+1}) + \ldots + \lambda_n F(v_n) = 0 \\
\Rightarrow \quad & F(\lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n) = 0 \\
\Rightarrow \quad & \lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n \in \operatorname{Ker} F \\
\Rightarrow \quad & \lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n \in \operatorname{Lin}\{v_1, \ldots, v_k\} \\
\Rightarrow \quad & \lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n = 0 \\
\Rightarrow \quad & \lambda_{k+1} = \ldots = \lambda_n = 0
\end{aligned}$$

(Ĉe la du lastaj konkludoj ni uzis la fakton, ke $\{v_1, \ldots, v_n\}$ kaj $\{v_{k+1}, \ldots, v_n\}$ estas lineare sendependaj.) □

5.3 Konkludoj

La ĵus pruvita *dimensia formulo por linearaj bildigoj* estas utila por ekhavi informojn pri la solvaro de lineara ekvaciaro. La ĝenerala formo de lineara ekvaciaro estas $Ax = b$, kie A estas matrico, t.e.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \text{ kun } a_{ij} \in K,\ i = 1, \dots, m,\ j = 1, \dots, n,$$

x, b kaj Ax estas vektoroj el la spaco K^n, t.e.

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \text{ kaj } Ax = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix} \in K^n.$$

Se $b = 0$, la ekvaciaro nomiĝas *homogena*. La bildigo $F : x \to Ax$ estas lineara; sekve la solvaro $\{x : Ax = 0\}$ de homogena ekvaciaro estas subspaco de la vektorspaco K^n, nome $\operatorname{Ker} F$. Teoremo 5.2.1 liveras al ni la dimension de tiu ĉi subspaco:

$$\dim\{x : Ax = 0\} = \dim \operatorname{Ker} F = \dim K^n - \dim \operatorname{Im} F = n - \dim \operatorname{Im} F$$

$\operatorname{Im} F$ estas la rango de la bildigo F; montriĝas, ke tiu ĉi rango estas egala al la *rango de la matrico* A, kiu estas difinita kiel la nombro de la lineare sendependaj *vertikaloj* de A. Oni povas pruvi, ke tiu ĉi nombro estas egala al la nombro de la lineare sendependaj *horizontaloj* de A.

6 Aldonoj

6.1 Fontoj

La strukturo kaj enhavo de tiu ĉi kajero orientiĝas jen kaj jen laŭ diversaj libroj kaj lekciaj manuskriptoj. Menciindas precipe la du nuntempe plej popularaj germanlingvaj enkondukoj en la linearan algebron:

Fischer, Gerd: Lineare Algebra, 9a eldono, Vieweg, Braunschweig 1985.

Lorenz, Falko: Lineare Algebra I, 3a eldono, Bibliographisches Institut, Mannheim 1993.

6.2 Terminaroj

Por la elekto de la terminoj estas uzitaj la sekvaj fakvortaroj:

Holdgrün, Horst S. kaj *Kiselman, Christer O.:* La matematiko en Plena Ilustrita Vortaro. Revizio. Manuskripto de 1992-07-12. *(Ĉiurilate tre profesinivela verko kun pli ol 300 terminoj; pro kopirajtaj kialoj ankoraŭ ne aĉetebla. Ĝi eniros en la novan eldonon de PIV. Eblas tamen ricevi la terminojn - plejparte ankoraŭ sen difinoj - jam nun per anonima* ftp *de* cfgauss.uni-math.gwdg.de, *dosieraro* Ilo/terminaro/matematiko.*)*

Hilgers, R. kaj *Yashovardhan:* EK-vortaro de matematikaj terminoj. Leuchtturm-Verlag, Alsbach 1980. *(8-lingva vortaro kun 460 terminoj; tre utila pro la precizaj esperantlingvaj difinoj.)*

Reiersøl, Olav: Matematika kaj stokastika terminaro. 2a eldono, Universitato de Oslo 1994. *(Vortaro kun ĉ. 650 terminoj kun difinoj, rimarkoj pri ilia elekto kaj vortlistoj angla-esperanta kaj esperanta-angla. Relative skemisma, foje harfende ekzaktema elekto de la terminoj.)*

Werner, Jan: Matematika vortaro esperanta-ĉeĥa-germana. La aŭtoro, Brno 1990. *(La vortaro entenas 3722 terminojn sen difinoj.)*

En tiu ĉi broŝuro la terminoj estas ĉerpitaj plejparte el la "Revizio" de Holdgrün kaj Kiselman, kiu laŭeble estu bazo por ĉiu estonta matematika verkado en Esperanto. Tamen mi (ankoraŭ) ne emis plene sekvi ĝin kaj uzis ekzemple "intersekco" anstataŭ "komunaĵo", "lineare sendependa" anstataŭ "lineare nedependa" kaj "vektorspaco" anstataŭ "vektora spaco". Ankaŭ mian uzon de "triviala" en la senco de "banala" aŭ "tre simpla" mi ne povas pravigi per ĝi. Kie mi malatentas la "Revizion", mi kutime apogis min sur la vortaron de Jan Werner, kiu impresas pro sia amplekso kaj miaopinie ne malpli saĝa elekto de la terminoj.

6.3 Periodaĵoj

Matematikaj artikoloj en Esperanto aperas de tempo al tempo en la sekvaj gazetoj:

Scienca Revuo, 2-foje jare, eldonas ISAE, redaktas Rudi Hauger, Ringstr. 13, CH-8172 Niederglatt, Svislando.

Tutmondaj Sciencoj kaj Teknikoj, 4-foje jare, eldonas Esperanto-Asocio, Academia Sinica, 52 Sanlihe, 100864 Beijing, Ĉinio.

Matematiko Translimen, aperas nur sporade: La lastaj numeroj estas n-ro 6 de 1983 kaj n-ro 7 de 1992.

Cirkulero de IAdEM, aperas unufoje jare, eldonas Internacia Asocio de Esperantistaj Matematikistoj, redaktas Alfred Heiligenbrunner, Vorderdimbach 11, 4371 Dimbach, Aŭstrio.

En la datenbanko de la Faka Informcentro Karlsruhe estas registritaj matematikaj publikaĵoj en ĉirkaŭ 50 lingvoj. Jen iliaj kvantoj laŭ la stato de 1995-09-20: angla 847 966, rusa 110 043, franca 45 100, germana 40 768, ... , Esperanto 11, latina 11, ... Certe la vera nombro de matematikaj libroj kaj artikoloj en Esperanto estas 10- ĝis 30-oble pli alta. En la menciita datenbanko troviĝas krome ĉirkaŭ 100 publikaĵoj verkitaj de esperantistaj matematikistoj en naciaj lingvoj. Publikaĵoj en aliaj planlingvoj krom Esperanto ne estas registritaj.

6.4 Kelkaj terminoj en kvar lingvoj

Jen kelkaj terminoj el la lineara algebro kun tradukoj en la lingvoj angla, franca kaj germana. La nombro en krampoj malantaŭ la termino indikas la paragrafon aŭ difinon, en kiu la termino unuafoje aperas.

aro (2.1) *An* set; *Fr* ensemble *m*; *Ge* Menge *f*

bazo (4.3.5) *An* basis; *Fr* base *f*; *Ge* Basis *f*

bildo (2.2.1) *An* image; *Fr* image *f* ; *Ge* Bild *n*

bildigo (2.2.1) *An* map, mapping; *Fr* application *f*; *Ge* Abbildung *f*

generantaro (4.3.5) *An* generating set; *Fr* partie *f* génératrice; *Ge* Erzeugendensystem *n*

grupo (3.1.1) *An* group; *Fr* groupe *m* ; *Ge* Gruppe *f*

kerno (5.1) *An* kernel; *Fr* noyau *m*; *Ge* Kern *m*

korpo (3.2.1) *An* field; *Fr* corps *m*; *Ge* Körper *m*

lineare sendependa (4.3.1) *An* linearly independent; *Fr* linéairement indépendant; *Ge* linear unabhängig

subspaco (4.2.1) *An* subspace; *Fr* sous-espace *m*; *Ge* Teilraum *m*

vektorspaco (4.1.1) *An* vector space; *Fr* espace *m* vectoriel; *Ge* Vektorraum *m*

La aŭtoro

Ulrich Matthias naskiĝis en 1966 en Bad Pyrmont, Germanio, kaj esperantistiĝis en 1986. Li studis matematikon kun kromfako fiziko en Heidelberg, kie li diplomiĝis en 1992 kaj doktoriĝis en 1994. Enrigardon en lian esplorkampon, la problemojn de ekstremeco en grafoteorio, donas lia esperantlingva artikolo "Rifuto de kombinatorika konjekto de P. Turán" en *Scienca Revuo* Vol. **45** (1994)(2), p. 26-30.

Fundamentoj de lineara algebro

Tiu ĉi kajero entenas la plej bazajn difinojn, konkludojn kaj teoremojn de la *lineara algebro*. El la enhavo: grupoj, korpoj, vektorspacoj, lineara sendependeco, bazoj, interŝanĝo de bazaj vektoroj, la dimensia formulo por subspacoj, linearaj bildigoj, la dimensia formulo por linearaj bildigoj.