

ALGEBRA II

Sügis 2024

Loengukonspekt

Lektor: Kristo Väljako

15. jaanuar 2025. a.

Sisukord

1	Üldise algebra põhimõisted ja -konstruktsioonid	4
1.1	Ω -algebra	4
1.2	Homomorfism	5
1.3	Alamalgebra	9
1.4	Cayley teoreem	12
1.5	Kongruents ja faktoralgebra	13
1.6	Kõrvalklassid, Lagrange'i teoreem	16
1.7	Faktorrihm	17
1.8	Faktoring	21
1.9	Faktorruum	23
1.10	Ω -algebrate otsekorrutis	23
1.11	Moodul üle ringi	25
1.12	R -moodulite otsesummad	26
1.13	Vektorruumide otsesumma	30
2	Polünoomid, algebra põhiteoreem	34
2.1	Mitme muutuja polünoomide ringid	34
2.2	Sümmeetrilised polünoomid	37
2.3	Polünoomi lahutuskorpus	40
2.4	Algebra põhiteoreem	44
3	Lineaarteisenduse kanooniline baas	48
3.1	Probleemi püstitus ja põhitulemuse sõnastus	48
3.2	Invariantsed alamruumid	49
3.3	Nilpotentse lineaarteisenduse kanooniline baas	50
3.4	Nilpotentse maatriksi Jordani normaalkuju leidmine	56
3.5	Piisav tingimus kanoonilise baasi olemasoluks	57
3.6	Cayley-Hamiltoni teoreem	61
3.7	Kanoonilise baasi ja Jordani normaalkuju leidmine	65
4	Funktsionaalid ja vormid	68
4.1	Lineaarsed funktsionaalid ja lineaarvormid	68
4.2	Bilineaarsed funktsionaalid ja bilineaarvormid	72
4.3	Ruutfunktsionaalid ja ruutvormid	74
4.4	Ruutfunktsionaalid vektorruumidel üle $\mathbb{C}$ ja $\mathbb{R}$	78
5	Abeli rühmad	84
5.1	Tsüklilised rühmad	84
5.2	Rühma elemendi järk	86
5.3	Perioodilised Abeli rühmad	87
5.4	Lõplikud Abeli p -rühmad	89
5.5	Vabad Abeli rühmad	92

Sissejuhatus

Tegemist on 2022. aasta sügisel Tartu Ülikoolis loetud kursuse “Algebra II” loengukonspektiga.

Seda kursust võib vaadelda kursuse “Algebra I” jätkuna. Kui kursuses “Algebra I” on põhiliselt juttu lineaaralgebrast (maatriksid, determinandid, lineaarvõrrandisüsteemid, vektorruumid, ühe muutuja polünoomid) ja pisut ka algebralistest struktuuridest, siis kursuses “Algebra II” vaatleme neid olulisi lineaaralgebra teemasid, mis kursusesse “Algebra I” ära ei mahtunud (mitme muutuja polünoomid, lineaarteisenduse kanooniline baas, funktsionaalid ja vormid) ning süvendame teadmisi algebraliste struktuuride kohta (homomorfismid, alamstruktuurid, faktorstruktuurid, otsesummad, Abeli rühmade ehitus).

Konspekti on koostanud prof. Valdis Laan ja täiendanud Kristo Väljako. Konspekti parandamisele ja täiendamisele on kaasa aidanud mitmed üliõpilased: **Jaagup Kirme, Indrek Pertman, Tähvend Uustalu, Nikita Leo, Stefan Ehin, Erki Külaots.** Tänud neile!

1 Üldise algebra põhimõisted ja -konstruktsioonid

Selles peatükis vaatleme algebralisi struktuure üldise algebra vaatepunktist. Me anname üldise Ω -algebra definitsiooni ja näeme, et varem vaadeldud konkreetset struktuurid (nt. rühm, ring, vektorruum) on selle erijuhtudeks. Samuti tutvume üldise homomorfismi ja alamstruktuuri mõistega ning uurime, kuidas saab moodustada faktorstruktuure.

1.1 Ω -algebra

Abstraktses algebras uuritakse algebralisi struktuure, need on hulgad, millel on defineeritud üks või mitu algebralist tehet. Kursuses “Algebra I” me vaatlesime põhiliselt kahekojalisi algebralisi tehteid, s.t. tehteid, millel on kaks argumenti. Üldiselt võib argumentide arv olla suvaline mittenegatiivne täisarv.

Definitsioon 1.1 Olgu A hulk ja $n \in \{0, 1, 2, \dots\}$. Kujutust

$$\omega : A^n \rightarrow A$$

nimetatakse n -aarseks ehk n -kohaliseks algebraliseks tehteks hulgal A .

Kui $n = 0$, siis A^0 on üheelemendiline hulk ja kujutus $\omega : A^0 \rightarrow A$ on ära määratud selle ainsa elemendi kujutisega. Seda kujutist tähistame sümboliga 0_A^ω .

Definitsioon 1.2 Hulka Ω nimetatakse **tüübiks**, kui ta on esitatud mittelõikuvate alamhulkade $\Omega_0, \Omega_1, \Omega_2, \dots$ ühendina.

Rõhutame, et selles definitsioonis võivad hulgad Ω_i olla lõplikud või lõpmatud või isegi tühjad. Me mõtleme tüübist kui tehtemärkide hulgast, kusjuures Ω_i all peame silmas kõigi i -kohaliste tehete märkide hulka.

Definitsioon 1.3 Olgu Ω tüüp. Hulka A nimetatakse Ω -algebraks, kui iga arvu $n \in \{0, 1, 2, \dots\}$ ja iga $\omega \in \Omega_n$ jaoks on hulgal A defineeritud üks n -kohaline tehe $\omega_A : A^n \rightarrow A$.

Seega kui A on Ω -algebra, siis iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, \dots, a_n \in A$ korral on olemas üheselt määratud element $\omega_A(a_1, \dots, a_n) \in A$.

Kui tahetakse rõhutada, mis tüüpi algebraga on tegemist, siis tähistatakse Ω -algebrat A paarina $(A; \Omega)$.

Mõnikord lubatakse definitsioonis ka tühje Ω -algebraid. Selles kursuses lähtume siiski pisut levinumast praktikast, kus nõutakse, et Ω -algebra on mittetühi. Niipea kui Ω sisaldab mõnda nullkohalise tehete märki, peab ka Ω -algebra A olema kindlasti mittetühi.

Märgime, et sõna algebra võib matemaatikas tähendada väga paljusid erinevaid asju (näiteks teadusharu või teatavat hulkade kogumit mõõduteoorias). Definitsioonis 1.3 toodud algebra mõistet nimetatakse ka **universaalalgebraks**. Kuid kuna too termin on natuke kohmakas, siis tihti lühendatakse ta lihtsalt algebraks.

Näide 1.4 Rühmi on otstarbekas vaadelda kui Ω -algebraid, kus $\Omega = \Omega_0 \cup \Omega_1 \cup \Omega_2$, $\Omega_0 = \{1\}$, $\Omega_1 = \{-1\}$, $\Omega_2 = \{\cdot\}$ ja $\Omega_n = \emptyset$ iga $n \geq 3$ korral. Selliste tehete korral kirjutatakse harilikult $^{-1}(x)$ asemel x^{-1} ja $\cdot((x, y))$ asemel $x \cdot y$ või isegi xy . Rühma A tehted $\cdot$, $^{-1}$ ja 1 peavad rahuldama järgmisi samasusi: iga $x, y, z \in A$ korral

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
2. $x \cdot 1 = x = 1 \cdot x$,
3. $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

Ring on Ω -algebra, kus $\Omega = \Omega_0 \cup \Omega_1 \cup \Omega_2$, $\Omega_0 = \{0, 1\}$, $\Omega_1 = \{-\}$ ja $\Omega_2 = \{+, \cdot\}$. Niisiis ringil on kaks nullkohalist tehet (üks neist fikseerib nullelemendi ja teine ühikelemendi), ühekohaline vastandelemendi võtmise tehe ning kahekohalised liitmise ja korrutamise tehted.

Vektorruumi V üle korpuse K võib vaadelda kui Ω -algebrat, kus $\Omega = \Omega_0 \cup \Omega_1 \cup \Omega_2$, $\Omega_0 = \{0\}$, $\Omega_1 = \{k \cdot \mid k \in K\}$ ja $\Omega_2 = \{+\}$. Seega vektorruumil on nullkohaline tehe, mis fikseerib nullelemendi, ühekohaline skalaariga korrutamise tehe iga $k \in K$ jaoks (neid on lõpmata palju, kui K on lõpmatu) ja kahekohaline liitmistehe. Vastandelemendi võtmise tehet ei ole vaja eraldi vaadelda, sest see tehe on kujutusena $V \rightarrow V$ sama, mis skalaariga -1 korrutamine.

1.2 Homomorfism

Homomorfismid on tehteid säilitavad kujutused sama tüüpi algebrate vahel. Need mängivad algebrate uurimisel sama tähtsat rolli kui kujutused hulkadega tegelemisel.

Definitsioon 1.5 Olgu Ω mingi tüüp ning A ja B Ω -algebrad. Kujutust $\varphi : A \rightarrow B$ nimetatakse **homomorfismiks**, kui iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes $a_1, \dots, a_n \in A$ korral kehtib võrdus

$$\varphi(\omega_A(a_1, \dots, a_n)) = \omega_B(\varphi(a_1), \dots, \varphi(a_n))$$

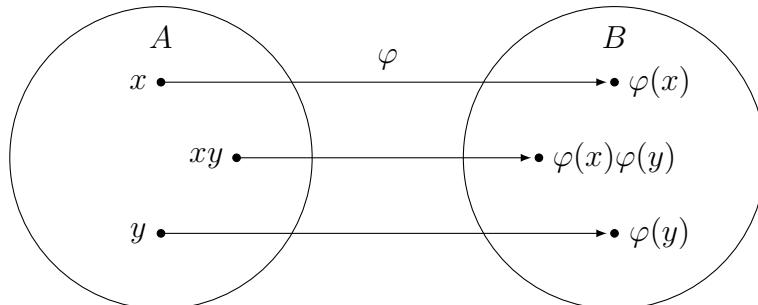
(selle võrduse poolt esitatavat tingimust väljendatakse sõnadega: *kujutus φ säilitab tehet ω*) ja iga nullkohalise tehte $\omega \in \Omega_0$ korral

$$\varphi(0_A^\omega) = 0_B^\omega.$$

Kõigi homomorfismide hulka Ω -algebrast A Ω -algebrasse B tähistame selles kursuses sümboliga $\text{Hom}(A, B)$.

Näide 1.6 Olgu A ja B rühmad. Definitsiooni kohaselt on kujutus $\varphi : A \rightarrow B$ rühmade homomorfism, kui ta rahuldab järgmisi tingimusi:

- $\varphi(1) = 1$, s.t. φ säilitab nullkohalist tehet, mis fikseerib rühma ühikelemendi;
- iga $x \in A$ korral $\varphi(x^{-1}) = (\varphi(x))^{-1}$, s.t. φ säilitab ühekohalist pöördelemendi võtmise tehet;
- iga $x, y \in A$ korral $\varphi(xy) = \varphi(x)\varphi(y)$, s.t. φ säilitab kahekohalist korrutamistehet.



Märkus 1.7 Kui meil on kaks rühma A ja B , siis formaalselt võttes peaksime nullkohalise tehete poolt fikseeritud elemente tähistama erinevalt, näiteks 1_A ja 1_B . Harilikult seda praktikas siiski ei tehta ja tähistatakse mõlema rühma ühikelementi lihtsalt sümboliga 1 . Ka $x \cdot_A y$ asemel kirjutatakse lihtsalt $x \cdot y$ või isegi xy , nagu tegime ka eelmises näites.

Algebrate puhul võib olla nii, et mingite tehete säilitamisest järeldub mingite teiste tehete säilitamine. Näiteks rühmade korrutamise säilitamisest järeldub nii ühikelemendi säilitamine kui ka pöördelementide säilitamine.

Lause 1.8 Olgu A ja B rühmad. Kujutus $\varphi : A \rightarrow B$ on rühmade homomorfism parajasti siis, kui iga $x, y \in A$ korral

$$\varphi(xy) = \varphi(x)\varphi(y).$$

TÕESTUS. Tarvilikkus on definitsiooni põhjal ilmne. Piisavuse tõestamiseks peame näitama, et korrutamise säilitamisest järeldub ühikelemendi ja pöördelemendi võtmise säilitamine. Eeldame, et kujutus $\varphi : A \rightarrow B$ säilitab korrutamist. Kuna rühmas A kehtib võrdus $1 \cdot 1 = 1$, siis rühmas B kehtib tänu eeldusele võrdus $\varphi(1)\varphi(1) = \varphi(1)$. Korrutades selle võrduse mõlemaid pooli elementidega $\varphi(1)^{-1}$ ja kasutades rühma tehete omadusi saame võrduse $\varphi(1) = 1$. Seega φ säilitab ühikelemendi fikseerimise tehet. Kui nüüd $x \in A$, siis

$$\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(1) = 1.$$

Analoogiliselt $\varphi(x)\varphi(x^{-1}) = 1$. Seega $\varphi(x^{-1}) = (\varphi(x))^{-1}$. □

Näide 1.9 Selles kursuses tähistame sümboliga K^* korpuse K nullist erinevate elementide hulka. Nagu teame, on hulk K^* rühm korpuse korrutamistehte suhtes. Muuhulgas võime vaadelda rühma $\mathbb{R}^*$.

Kujutus

$$\varphi : \mathbb{R}^* \rightarrow \mathbb{R}^*, \quad x \mapsto x^2,$$

on rühmade homomorfism, sest

$$\varphi(xy) = xyxy = xxyy = \varphi(x)\varphi(y).$$

Vaatleme regulaarsete maatriksite rühma $GL_n(\mathbb{R})$ korrutamise suhtes. Kujutus

$$\psi : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*, \quad A \mapsto \det(A)$$

on rühmade homomorfism, sest $\det(AB) = \det(A)\det(B)$ mistahes $A, B \in GL_n(\mathbb{R})$ korral.

Abeli rühmade korral räägitakse korrutamise asemel harilikult liitmistest ja seega lause 1.8 saab järgmise kuju.

Lause 1.10 Olgu A ja B Abeli rühmad. Kujutus $\varphi : A \rightarrow B$ on Abeli rühmade homomorfism parajasti siis, kui iga $x, y \in A$ korral

$$\varphi(x + y) = \varphi(x) + \varphi(y).$$

Näide 1.11 Olgu A ja B ringid. Tänu lausele 1.10 võime öelda, et kujutus $\varphi : A \rightarrow B$ on ringide homomorfism parajasti siis, kui

- $\varphi(1) = 1$;

- iga $x, y \in A$ korral $\varphi(xy) = \varphi(x)\varphi(y)$;
- iga $x, y \in A$ korral $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Näide 1.12 Olgu A ja B vektorruumid üle korpuse K . Arvestades jällegi lauset 1.10 võime öelda, et kujutus $\varphi : A \rightarrow B$ on vektorruumide homomorfism (ehk lineaarkujutus) parajasti siis, kui

- iga $k \in K$ ja iga $x \in A$ korral $\varphi(kx) = k\varphi(x)$;
- iga $x, y \in A$ korral $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Näide 1.13 Vektorruumide homomorfismidest (lineaarkujutustest) oleme vaadelnud hulgaliselt näiteid kursuses “Algebra I”. Näiteks on lihtne kontrollida, et kujutus

$$\varphi : \mathbb{R}^3 \rightarrow \mathbb{R}^4, \quad (x, y, z) \mapsto (z, x + y, 0, x),$$

on lineaarkujutus.

Kas kahe homomorfismi järjestrakendamisel (kui see on võimalik) saame ka homomorfismi? Olgu antud Ω -algebrad A, B ja C ning nende homomorfismid $\varphi : A \rightarrow B$ ja $\psi : B \rightarrow C$. Siis nende kujutuste korrutis (ehk kompositsioon) $\psi \circ \varphi : A \rightarrow C$ on defineeritud eeskirjaga

$$(\psi \circ \varphi)(a) := \psi(\varphi(a))$$

iga $a \in A$ korral. Osutub, et see kujutus $\psi \circ \varphi$ on samuti homomorfism.

Lause 1.14 Kui kahe Ω -algebrate homomorfismi korrutis on olemas, siis see korrutis on ise ka Ω -algebrate homomorfism.

TÕESTUS. Olgu A, B ja C Ω -algebrad ning $\varphi : A \rightarrow B$ ja $\psi : B \rightarrow C$ nende homomorfismid. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $a_1, \dots, a_n \in A$. Siis

$$\begin{aligned} (\psi \circ \varphi)(\omega_A(a_1, \dots, a_n)) &= \psi(\varphi(\omega_A(a_1, \dots, a_n))) && (\psi \circ \varphi \text{ def.}) \\ &= \psi(\omega_B(\varphi(a_1), \dots, \varphi(a_n))) && (\varphi \text{ on hom.}) \\ &= \omega_C(\psi(\varphi(a_1)), \dots, \psi(\varphi(a_n))) && (\psi \text{ on hom.}) \\ &= \omega_C((\psi \circ \varphi)(a_1), \dots, (\psi \circ \varphi)(a_n)). && (\psi \circ \varphi \text{ def.}) \end{aligned}$$

Samuti iga $\omega \in \Omega_0$ korral

$$(\psi \circ \varphi)(0_A^\omega) = \psi(0_B^\omega) = 0_C^\omega.$$

□

Definitsioon 1.15 Homomorfismi mingist Ω -algebrast iseendasse nimetatakse selle algebra **endomorfismiks**.

Ω -algebra A kõigi endomorfismide hulka tähistatakse sümboliga $\text{End}(A)$. On selge, et Ω -algebra A samasusteisendus id_A (või 1_A) on selle algebra endomorfism ja et kahe endomorfismi korrutis on alati defineeritud.

Meenutame, et **monoid** on Ω -algebra S , kus $\Omega = \Omega_0 \cup \Omega_2$, $\Omega_0 = \{1\}$, $\Omega_2 = \{\cdot\}$, mis rahuldab tingimusi

1. $(\forall s, t, u \in S)((s \cdot t) \cdot u = s \cdot (t \cdot u)),$
2. $(\forall s \in S)(s \cdot 1 = s = 1 \cdot s).$

Lause 1.16 Iga Ω -algebra A korral on hulk $\text{End}(A)$ monoid kujutuste korrutamise (s.t. järjest rakendamise) suhtes.

TÕESTUS. Selle lihtsa tõestuse jätame läbimõtlemiseks lugejale. $\square$

Definitsioon 1.17 Bijektiivset homomorfismi nimetatakse **isomorfismiks**.

Definitsioon 1.18 Ω -algebrad A ja B nimetatakse **isomorfseteks**, kui leidub isomorfism $\varphi : A \rightarrow B$.

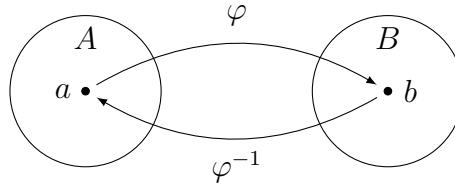
Asjaolu, et Ω -algebrad A ja B on isomorfsed, tähistatakse sümboliga $A \simeq B$ või $A \cong B$.

Nii nagu ei saa rääkida kõigi hulkade hulgast, ei saa rääkida ka kõigi Ω -algebrate hulgast. Küll aga saab rääkida kõigi Ω -algebrate klassist.

Lause 1.19 Isomorfisusseos on ekvivalentsiseos kõigi Ω -algebrate klassil, s.t. ta on reflekstiivne, sümmeetriline ja transitiivne.

TÕESTUS. On selge, et Ω -algebra A korral on samasusteisendus $\text{id}_A : A \rightarrow A$ isomorfism ja seega $A \simeq A$. Samuti on selge, et kahe isomorfismi korrutis on isomorfism ja seega on isomorfisusseos transitiivne. Veendume, et seos $\simeq$ on sümmeetriline. Olgu $A \simeq B$ ja leidugu Ω -algebrate isomorfism $\varphi : A \rightarrow B$. Kuna φ on bijektiivne, siis on tal olemas pöördkujutus $\varphi^{-1} : B \rightarrow A$, kusjuures mistahes $b \in B$ ja $a \in A$ korral

$$\varphi^{-1}(b) = a \iff \varphi(a) = b. \quad (1)$$



Hulgateooriast teame, et kujutus φ^{-1} on bijektiivne. Jääb veel näidata, et ta on homomorfism. Olgu nüüd $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $b_1, \dots, b_n \in B$. Kujutuse φ sürjektiivsuse tõttu leiduvad sellised elemendid $a_1, \dots, a_n \in A$, et $\varphi(a_i) = b_i$ iga $i \in \{1, \dots, n\}$ korral. Siis

$$\begin{aligned}
\varphi^{-1}(\omega_B(b_1, \dots, b_n)) &= \varphi^{-1}(\omega_B(\varphi(a_1), \dots, \varphi(a_n))) \\
&= \varphi^{-1}(\varphi(\omega_A(a_1, \dots, a_n))) && (\varphi \text{ on homomorfism}) \\
&= (\varphi^{-1} \circ \varphi)(\omega_A(a_1, \dots, a_n)) && (\varphi^{-1} \circ \varphi \text{ def.}) \\
&= \text{id}_A(\omega_A(a_1, \dots, a_n)) && (\varphi^{-1} \circ \varphi = \text{id}_A) \\
&= \omega_A(a_1, \dots, a_n) && (\text{id}_A \text{ def.}) \\
&= \omega_A(\varphi^{-1}(b_1), \dots, \varphi^{-1}(b_n)). && (\text{omadus (1)})
\end{aligned}$$

Samuti

$$\varphi^{-1}(0_B^\omega) = 0_A^\omega$$

iga $\omega \in \Omega_0$ korral, sest $\varphi(0_A^\omega) = 0_B^\omega$. Seega $\varphi^{-1} : B \rightarrow A$ on Ω -algebrate homomorfism ja kokkuvõttes isomorfism. Viimane tähendab, et $B \simeq A$, mida oligi tarvis tõestada. $\square$

Definitsioon 1.20 Bijektiivset endomorfismi nimetatakse **automorfismiks**.

Ω -algebra A kõigi automorfismide hulka tähistatakse sümboliga $\text{Aut}(A)$.

Lause 1.21 Iga Ω -algebra A korral on hulk $\text{Aut}(A)$ rühm kujutuste korrutamise (s.t. järjest rakendamise) suhtes.

TÕESTUS. Ka selle tõestuse jätame lugejale läbimõtlemiseks. $\square$

1.3 Alamalgebra

Vektorruumide alamalgebrate ehk alamruumidega oleme tutvunud kursuses “Algebra I”. Vaatame nüüd, kuidas üldjuhul defineeritakse Ω -algebra alamalgebra.

Definitsioon 1.22 Ω -algebra A alamhulka B nimetatakse algebra A **alamalgebraks** (ja kirjutatakse $B \leq A$), kui iga $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $b_1, \dots, b_n \in B$ korral

$$\omega_A(b_1, \dots, b_n) \in B$$

ja iga $\omega \in \Omega_0$ korral

$$0_A^\omega \in B.$$

Sama definitsiooni sõnastatakse mõnikord lühemalt öeldes: alamhulk B on Ω -algebra A alamalgebra, kui ta on kinnine kõigi tehete suhtes.

Selles kursuses (mõnevõrra ebatraditsiooniliselt) me lubame ka tühjasid alamalgebraid. Näiteks poolrühmal on olemas tühi alampoolrühm. Samas kui Ω sisaldab nullkohalisi tehtemärke (nagu näiteks monoidi, rühma või ringi korral), siis peab iga alamalgebra olema kindlasti mittetühi.

Ω -algebra A kõigi alamalgebrate hulka tähistatakse $\text{Sub}(A)$.

Järgmine väide on ilmne.

Lemma 1.23 Kui B on Ω -algebra A (mittetühi) alamalgebra, siis on B ise ka Ω -algebra algebra A tehete poolt indutseeritud tehete suhtes, s.t. tehete suhtes, mis on iga $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $b_1, \dots, b_n \in B$ korral defineeritud võrdusega

$$\omega_B(b_1, \dots, b_n) := \omega_A(b_1, \dots, b_n)$$

ja iga $\omega \in \Omega_0$ korral võrdusega

$$0_B^\omega := 0_A^\omega.$$

Kui me räägime A alamalgebrast B kui Ω -algebrast, siis peamegi alati silmas just nimelt selliseid tehteid, mis on defineeritud lemmas 1.23.

Lemma 1.24 Seos $\leq$ on järjestusseos kõigi Ω -algebrate klassil.

TÕESTUS. On selge, et iga algebra on iseenda alamalgebra, s.t. $A \leq A$.

Kui $A \leq B$ ja $B \leq A$, siis hulkadena $A \subseteq B$ ja $B \subseteq A$, seega $A = B$, mis tähendab, et seos $\leq$ on antisümmeetriline.

Tõestame, et seos $\leq$ on transitiivne. Eeldame, et $C \leq B$ ja $B \leq A$. Näitame, et $C \leq A$. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $c_1, \dots, c_n \in C$. Kuna $B \leq A$ ja $c_1, \dots, c_n \in B$, siis

$$\omega_A(c_1, \dots, c_n) \in B.$$

Alamalgebra B tehted defineeritakse samamoodi nagu A tehted, järelikult

$$\omega_B(c_1, \dots, c_n) = \omega_A(c_1, \dots, c_n).$$

Kuna $C \leq B$, siis $\omega_B(c_1, \dots, c_n) \in C$ ja seega ka $\omega_A(c_1, \dots, c_n) \in C$. Lisaks sellele $0_A^\omega \in B$ ja

$$0_A^\omega = 0_B^\omega \in C.$$

□

Näide 1.25 Definiitsiooni järgi on alamhulk $B \subseteq A$ rühma A alamrühm, kui

- rühma A ühikelement kuulub hulka B ;
- hulk B on kinnine pöördelemendi võtmise suhtes;
- hulk B on kinnine korrutamise suhtes.

Lause 1.26 Rühma mittetühi alamhulk on selle rühma alamrühm parajasti siis, kui see alamhulk on kinnine pöördelemendi võtmise ja korrutamise suhtes.

TÕESTUS. Tarvilikkus on ilmne. Piisavuse tõestamiseks eeldame, et rühma A mittetühi alamhulk B on kinnine pöördelemendi võtmise ja korrutamise suhtes. Peame veenduma, et rühma A ühikelement 1 kuulub hulka B . Kuna $B \neq \emptyset$, siis leidub mingi element $b \in B$. Eelduste põhjal ka $b^{-1} \in B$ ja $1 = bb^{-1} \in B$. □

Näide 1.27 On lihtne veenduda, et hulk

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$$

on rühma $GL_n(\mathbb{R})$ alamrühm.

Kui $B \leq A$, siis saab vaadelda sisestuskujutust $\iota : B \rightarrow A$, mis on defineeritud võrdusega

$$\iota(b) = b$$

iga $b \in B$ korral. On lihtne aru saada, et selline kujutus on alati üksühene homomorfism. Seega iga alamalgebra tekitab teatud kanoonilise homomorfismi. Teatud mõttes kehtib ka vastupidine, s.t. iga homomorfismiga on seotud teatud alamalgebra.

Kui $\varphi : B \rightarrow A$ on homomorfism, siis võime vaadelda φ kujutist, s.t. hulka

$$\varphi(B) = \{\varphi(b) \mid b \in B\} \subseteq A.$$

Tihti kirjutatakse $\varphi(B)$ asemel ka $\text{im}(\varphi)$. Tuleb välja, et $\varphi(B)$ on A alamalgebra.

Lause 1.28 Kui $\varphi : B \rightarrow A$ on Ω -algebrate homomorfism, siis $\varphi(B)$ on A alamalgebra. Kui φ on üksühene, siis

$$B \simeq \varphi(B).$$

TÕESTUS. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $\varphi(b_1), \dots, \varphi(b_n) \in \varphi(B)$, kus $b_1, \dots, b_n \in B$. Kuna φ on homomorfism, siis

$$\omega_A(\varphi(b_1), \dots, \varphi(b_n)) = \varphi(\omega_B(b_1, \dots, b_n)) \in \varphi(B).$$

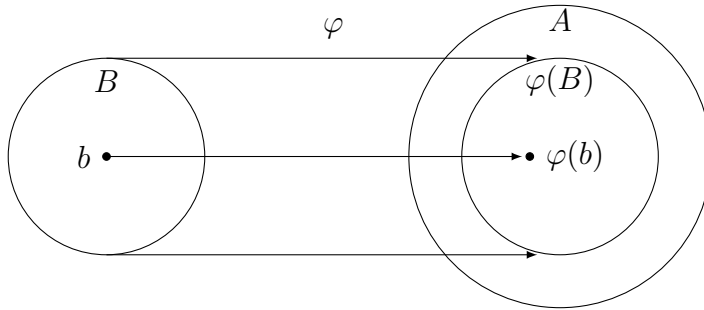
Samuti

$$0_A^\omega = \varphi(0_B^\omega) \in \varphi(B)$$

iga $\omega \in \Omega_0$ korral. Seega $\varphi(B)$ on algebra A alamalgebra. Kui φ on üksühene, siis kujutus

$$B \rightarrow \varphi(B), \quad b \mapsto \varphi(b)$$

on bijektiivne ja seega Ω -algebrate isomorfism.



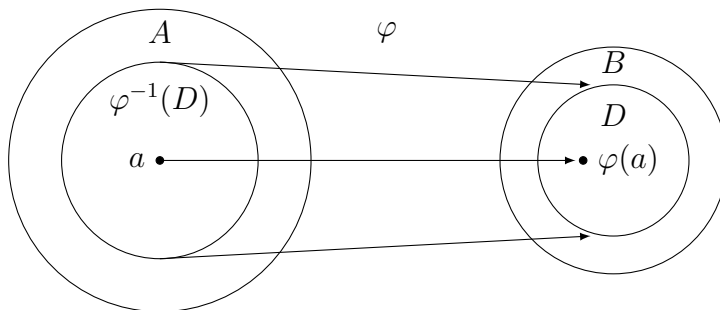
□

Näide 1.29 Seda tüüpi isomorfisme nagu esines eelmises lauses oleme kohanud juba mitmes kohas kursuses “Algebra I”.

Vaatleme näiteks reaalarvuliste kordajatega polünoomide ringi $\mathbb{R}[X]$ ja reaalarvude ringi $\mathbb{R}$. Siis kujutus $\varphi : \mathbb{R} \rightarrow \mathbb{R}[X]$, mis viib reaalarvu r konstantseks polünoomiks r (formaalselt jadaks $(r, 0, 0, \dots)$), on üksühene ringide homomorfism. Seega $\mathbb{R}[X]$ sisaldab alamringi, mis on isomorfne reaalarvude ringiga.

Alamalgebrate ja homomorfismide vahel on veel järgmine seos.

Lause 1.30 Olgu antud Ω -algebrate homomorfism $\varphi : A \rightarrow B$ ning olgu antud alamalgebra $D \leq B$. Siis $\varphi^{-1}(D) \leq A$, kus $\varphi^{-1}(D) = \{a \in A \mid \varphi(a) \in D\}$.



TÕESTUS. Vaatleme tehet $\omega \in \Omega_n$ ($n \in \mathbb{N}$) ja elemente $a_1, \dots, a_n \in \varphi^{-1}(D)$. Siis $\varphi(a_1), \dots, \varphi(a_n) \in D$ ning kuna D on alamalgebra ja φ homomorfism, siis ka

$$\varphi(\omega_A(a_1, \dots, a_n)) = \omega_B(\varphi(a_1), \dots, \varphi(a_n)) \in D.$$

See tähendab, et $\omega_A(a_1, \dots, a_n) \in \varphi^{-1}(D)$. Kuna $\varphi(0_A^\omega) = 0_B^\omega = 0_D^\omega$ (viimane võrdus kehtib tänu lemmale 1.23), siis

$$0_A^\omega \in \varphi^{-1}(D)$$

iga $\omega \in \Omega_0$ korral. □

Osutub, et alamalgebrate ühisosa on samuti alamalgebra.

Lause 1.31 *Olgu antud Ω -algebra A alamalgebrate hulk $\{B_i \mid i \in I\}$ ja $B = \bigcap_{i \in I} B_i$. Siis $B \leq A$.*

TÕESTUS. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $b_1, \dots, b_n \in B$. Siis $b_1, \dots, b_n \in B_i$ iga $i \in I$ korral. Kuna B_i , $i \in I$, on Ω -algebra A alamalgebrad, siis $\omega_A(b_1, \dots, b_n) \in B_i$ iga $i \in I$ korral. See aga tähendab, et $\omega_A(b_1, \dots, b_n) \in B$. On ka selge, et $0_A^\omega \in B$ iga $\omega \in \Omega_0$ korral. □

Sellest lausest järeldub, et kui X on Ω -algebra A mittetühi alamhulk, siis leidub algebra A vähim alamalgebra, mis sisaldab hulka X . Tõepoolest: vaatleme kõikvõimalikke alamalgebrad, mis sisaldavad hulka X (selliseid on kindlasti vähemalt üks: A ise), ja võtame nende ühisosa. Seda vähimat alamalgebrat nimetatakse algebra A **alamhulga X poolt tekitatud alamalgebraks** ja tähistatakse $\langle X \rangle$. Kui $\langle X \rangle = A$, siis öeldakse, et X on A **tekitajate süsteem** (ehk moodustajate süsteem).

Saab näidata, et $\langle X \rangle$ koosneb täpselt neist algebra A elementidest, mis on saadavad hulga X elementidest, kui neile rakendada lõplik arv kordi algebra A tehteid. Näiteks kui A on vektorruum, siis $\langle X \rangle$ on alamhulga $X \subseteq A$ lineaarne kate.

1.4 Cayley teoreem

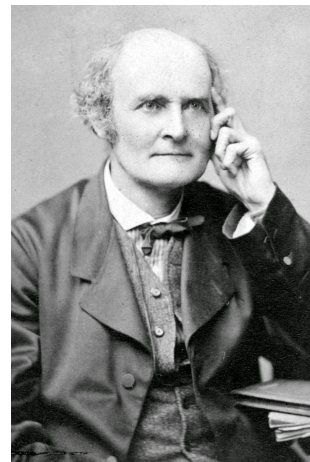
Selles paragrahvis tõestame ühe olulise teoreemi rühmade kohta, mis demonstreerib substitutsioonirühmade erilist rolli rühmateoorias.

Tuletame meelde, et iga mittetühja hulga M bijektiivsete teisenduste ehk **substitutsioonide** hulk $\mathcal{S}(M)$ on rühm teisenduste järjestrakendamise suhtes. Sellest rühmast oli kursuses “Algebra I” juttu erijuhul, kus

$$M = \{1, 2, \dots, n\},$$

ja vastavat rühma tähistasime siis sümboliga S_n . Tuleb välja, et iga rühma saab sisestada alamrühmana mingisse substitutsioonirühma.

Järgmise teoreemi osalise tõestuse andis inglise matemaatik Arthur Cayley (1821–1895) oma 1854. aastal ilmunud teadusartiklis.



Arthur Cayley

Teoreem 1.32 (Cayley teoreem) *Iga rühm on isomorfne mingi substitutsioonirühma alamrühmaga.*

TÕESTUS. Tõestuse idee on kasutada lauset 1.28.

Olgu G suvaline rühm. Iga elemendi $g \in G$ korral võime vaadelda kujutust

$$L_g : G \rightarrow G, \quad x \mapsto gx.$$

Kui $x, y \in G$ ja $gx = gy$, siis korrutades seda võrdust vasakult elemendiga g^{-1} saame võrduse $x = y$. Seega kujutus L_g on injektiivne. Ta on ka sürjektiivne, sest iga $x \in G$ korral

$$L_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = 1x = x.$$

Seega L_g on bijektiivne kujutus ehk $L_g \in \mathcal{S}(G)$. See lubab meil defineerida kujutuse

$$\varphi : G \rightarrow \mathcal{S}(G), \quad g \mapsto L_g.$$

Näitame, et φ on rühmade homomorfism. Lause 1.8 tõttu piisab, kui näitame, et φ säilitab korrumist. Selleks tuleb veenduda, et mistahes $g, g' \in G$ korral $\varphi(gg') = \varphi(g) \circ \varphi(g')$ ehk $L_{gg'} = L_g \circ L_{g'}$. Viimane võrdus kehtib, sest iga $x \in G$ korral

$$\begin{aligned} L_{gg'}(x) &= (gg')x && (L_{gg'} \text{ def.}) \\ &= g(g'x) && (\text{assotsiatiivsus}) \\ &= L_g(g'x) && (L_g \text{ def.}) \\ &= L_g(L_{g'}(x)) && (L_{g'} \text{ def.}) \\ &= (L_g \circ L_{g'})(x). && (\text{järjestrakendamise def.}) \end{aligned}$$

Kujutus φ on ka üksühene, sest kui $L_g = L_{g'}$, siis $g = L_g(1) = L_{g'}(1) = g'$. Lause 1.28 põhjal

$$G \simeq \varphi(G) = \{L_g \mid g \in G\} \leq \mathcal{S}(G).$$

□

1.5 Kongruents ja faktoralgebra

Faktoralgebraid saab moodustada kongruentside järgi. Kongruentsid on ekvivalentsiseosed, mis on kooskõlas vaadeldava algebra tehetege.

Definitsioon 1.33 Ekvivalentsiseost ρ Ω -algebral A nimetatakse selle algebra **kongruentsiks**, kui iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes $x_1, \dots, x_n, y_1, \dots, y_n \in A$ korral sellest, et

$$x_1 \rho y_1, \dots, x_n \rho y_n$$

järeldub, et

$$\omega_A(x_1, \dots, x_n) \rho \omega_A(y_1, \dots, y_n).$$

Ω -algebra A kõigi kongruentside hulka tähistatakse $\text{Con}(A)$.

Näide 1.34 Poolrühma A kongruents on ekvivalentsiseos ρ , mis rahuldab tingimust

$$x_1 \rho y_1 \wedge x_2 \rho y_2 \implies (x_1 x_2) \rho (y_1 y_2)$$

mistahes $x_1, x_2, y_1, y_2 \in A$ korral. Rühma kongruentsi korral lisandub sellele tingimusele implikatsioon

$$x \rho y \implies x^{-1} \rho y^{-1}.$$

Veel konkreetsemalt: poolrühmal $(\mathbb{N}, \cdot)$ võib vaadelda kongruentsi ρ , mis on defineeritud järgmiselt:

$$x \rho y \iff x = y \text{ või } x \text{ ja } y \text{ on paarisarvud.}$$

Kui ρ on ekvivalentsiseos hulgal A , siis iga element $a \in A$ määrab ära ekvivalentsiklassi $\{x \in A \mid x \rho a\}$, mida me hakkame tähistama sümboliga a/ρ . Meenutame hulgateooriast, et

$$a/\rho = a'/\rho \iff a \rho a'.$$

Kõigi ρ -klasside hulka nimetatakse hulga A **faktorhulgaks** seose ρ järgi ja tähistatakse A/ρ . Niisiis

$$A/\rho = \{a/\rho \mid a \in A\}.$$

Definitsioon 1.35 Ω -algebra A **faktoralgebraks** kongruentsi ρ järgi nimetatakse faktorhulka A/ρ , millel tehked $\omega \in \Omega_n$ ($n \in \mathbb{N}$) on defineeritud võrdusega

$$\omega_{A/\rho}(a_1/\rho, \dots, a_n/\rho) := (\omega_A(a_1, \dots, a_n))/\rho$$

ja nullkohalised tehked $\omega \in \Omega_0$ võrdusega

$$0_{A/\rho}^\omega := 0_A^\omega/\rho.$$

Tänu sellele, kuidas on defineeritud kongruentsid, on faktoralgebra tehked korrektselt defineeritud, s.t.

$$a_1/\rho = b_1/\rho \wedge \dots \wedge a_n/\rho = b_n/\rho \implies (\omega_A(a_1, \dots, a_n))/\rho = (\omega_A(b_1, \dots, b_n))/\rho.$$

Kui ρ on ekvivalentsiseos hulgal A , siis kujutust $\pi : A \rightarrow A/\rho$, mis on defineeritud võrdusega

$$\pi(a) := a/\rho,$$

$a \in A$, nimetatakse **loomulikuks kujutuseks faktorhulgale** ehk **loomulikuks projektisooniks**. On selge, et see kujutus on sürjektiivne.

Lause 1.36 *Kui ρ on Ω -algebra A kongruents, siis loomulik kujutus $\pi : A \rightarrow A/\rho$ on sürjektiivne Ω -algebrate homomorfism.*

TÕESTUS. Veendume, et π on homomorfism. Kui $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $a_1, \dots, a_n \in A$, siis

$$\begin{aligned} \pi(\omega_A(a_1, \dots, a_n)) &= \omega_A(a_1, \dots, a_n)/\rho && (\pi \text{ def.}) \\ &= \omega_{A/\rho}(a_1/\rho, \dots, a_n/\rho) && (\omega_{A/\rho} \text{ def.}) \\ &= \omega_{A/\rho}(\pi(a_1), \dots, \pi(a_n)). && (\pi \text{ def.}) \end{aligned}$$

Nullkohalise tehte ω korral

$$\pi(0_A^\omega) = 0_A^\omega/\rho = 0_{A/\rho}^\omega.$$

□

Ka järgmine definitsioon peaks lugejale olema tuttav hulgateooriast.

Definitsioon 1.37 Kujutuse $\varphi : A \rightarrow B$ **tuumaks** nimetatakse binaarset seost $\ker \varphi$ hulgal A , mis on defineeritud võrdusega

$$\ker \varphi = \{(x, y) \in A^2 \mid \varphi(x) = \varphi(y)\}.$$

On lihtne näha, et kujutuse $\varphi : A \rightarrow B$ tuum on ekvivalentsiseos hulgal A .

Lause 1.38 Kui $\varphi : A \rightarrow B$ on Ω -algebrate homomorfism, siis $\ker \varphi$ on algebra A kongruents.

TÕESTUS. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja eeldame, et elemendid $x_1, \dots, x_n, y_1, \dots, y_n \in A$ on sellised, et

$$(x_1, y_1) \in \ker \varphi, \dots, (x_n, y_n) \in \ker \varphi.$$

Siis $\varphi(x_1) = \varphi(y_1), \dots, \varphi(x_n) = \varphi(y_n)$ ja

$$\begin{aligned} \varphi(\omega_A(x_1, \dots, x_n)) &= \omega_B(\varphi(x_1), \dots, \varphi(x_n)) && (\varphi \text{ on homomorfism}) \\ &= \omega_B(\varphi(y_1), \dots, \varphi(y_n)) && (\text{eeldus}) \\ &= \varphi(\omega_A(y_1, \dots, y_n)). && (\varphi \text{ on homomorfism}) \end{aligned}$$

Seega $(\omega_A(x_1, \dots, x_n), \omega_A(y_1, \dots, y_n)) \in \ker \varphi$. $\square$

Lause 1.39 Kui ρ on Ω -algebra A kongruents ja $\pi : A \rightarrow A/\rho$ on loomulik homomorfism, siis $\ker \pi = \rho$.

TÕESTUS. Kuna iga $(a, b) \in A \times A$ korral

$$(a, b) \in \ker \pi \iff \pi(a) = \pi(b) \iff a/\rho = b/\rho \iff (a, b) \in \rho,$$

siis hulgad $\ker \pi$ ja ρ koosnevad täpselt samadest paaridest, järelikult $\ker \pi = \rho$. $\square$

Järgmine teoreem on üks enimkasutatavaid mistahes algebraliste struktuuride puhul.

Teoreem 1.40 (Homomorfismiteoreem) Kui $\varphi : A \rightarrow B$ on Ω -algebrate sürjektiivne homomorfism, siis

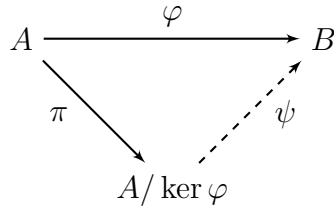
$$A/\ker \varphi \simeq B.$$

TÕESTUS. Tähistame iga $a \in A$ korral $\bar{a} := a/\ker \varphi$. Siis

$$\bar{a} = \bar{b} \iff \varphi(a) = \varphi(b). \quad (2)$$

Defineerime kujutuse $\psi : A/\ker \varphi \rightarrow B$ võrdusega

$$\psi(\bar{a}) := \varphi(a).$$



Tänu seosele (2) on kujutus ψ korrektselt defineeritud ja üksühene. Kuna φ on sürjektiivne, siis ka ψ on sürjektiivne. Kui $n \in \mathbb{N}$, $\omega \in \Omega_n$, $a_1, \dots, a_n \in A$, siis

$$\begin{aligned} \psi(\omega_{A/\ker \varphi}(\bar{a}_1, \dots, \bar{a}_n)) &= \psi(\overline{\omega_A(a_1, \dots, a_n)}) && (\omega_{A/\ker \varphi} \text{ def.}) \\ &= \varphi(\omega_A(a_1, \dots, a_n)) && (\psi \text{ def.}) \\ &= \omega_B(\varphi(a_1), \dots, \varphi(a_n)) && (\varphi \text{ on homomorfism}) \\ &= \omega_B(\psi(\bar{a}_1), \dots, \psi(\bar{a}_n)). && (\psi \text{ def.}) \end{aligned}$$

Kui $\omega \in \Omega_0$, siis

$$\psi(0_{A/\ker \varphi}^\omega) = \psi(\overline{0_A^\omega}) = \varphi(0_A^\omega) = 0_B^\omega.$$

Seega ψ on homomorfism. Kokkuvõttes ψ on isomorfism. $\square$

Järgnevates paragrahvides vaatleme faktoralgebrate moodustamise iseärasusi mõnede tähtsamate algebraliste struktuuride puhul.

1.6 Kõrvalklassid, Lagrange'i teoreem

Tuleb välja, et rühmade faktoriseerimisel võib kongruentsiklasside asemel kasutada niinimetatud kõrvalklasse. Selles paragrahvis uurime kõrvalklasside omadusi ja tõestame nende abil teoreemi, mis on nime saanud prantsuse matemaatiku Joseph-Louis Lagrange'i (1736–1813) järgi. See teoreem annab seose lõpliku rühma alamrühma elementide arvu ja terve rühma elementide arvu vahel.



Joseph-Louis Lagrange

Definitsioon 1.41 Olgu G (multiplikatiivne) rühm ja H tema alamrühm. Siis hulki

$$aH = \{ah \mid h \in H\}$$

($Ha = \{ha \mid h \in H\}$), kus $a \in G$, nimetatakse alamrühma H **vasakpoolseteks (parempoolseteks) kõrvalklassideks** rühmas G .

Kui G on rühm ühikelemendiga 1, siis $1 \cdot H = H = H \cdot 1$, s.t. alamrühm H on ise nii vasakpoolne kui parempoolne kõrvalklass.

Näide 1.42 Vaatleme Abeli rühma $(\mathbb{Z}; 0, -, +)$. Lihtne on veenduda, et hulk

$$5\mathbb{Z} = \{5z \mid z \in \mathbb{Z}\} = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

on selle rühma alamrühm. Kommutatiivsuse tõttu ei ole vahet vasakpoolsetel ja parempoolsetel kõrvalklassidel. Üheks kõrvalklassiks on näiteks hulk

$$2 + 5\mathbb{Z} = \{2 + 5z \mid z \in \mathbb{Z}\} = \{\dots, -8, -3, 2, 7, 12, \dots\},$$

s.t. arvu 2 jäägiklass mooduli 5 järgi.

Lause 1.43 Olgu G rühm, $H \leq G$ ja $a, b \in G$. Siis

$$aH = bH \iff a^{-1}b \in H.$$

Analoogiliselt $Ha = Hb$ parajasti siis, kui $ab^{-1} \in H$.

TÕESTUS. Me tõestame ainult esimese väite. Teise väite tõestus on sarnane.

TARVILIKKUS. Kehtigu võrdus $aH = bH$. Kuna $b = b \cdot 1 \in bH = aH$, siis leidub selline element $h \in H$, et $b = ah$. Korrutades seda võrdust vasakult elemendiga a^{-1} saame, et $a^{-1}b = h \in H$.

PIISAVUS. Oletame, et $a^{-1}b \in H$ ja tähistame $h := a^{-1}b$. Siis $b = ah$, millest järeldub, et $bH \subseteq aH$. Samuti $a^{-1} = hb^{-1}$ ja seega

$$a = (hb^{-1})^{-1} = (b^{-1})^{-1}h^{-1} = bh^{-1} \in bH,$$

millest järeldub sisalduvus $aH \subseteq bH$. Kokkuvõttes $aH = bH$. □

Võttes eelmises lauses $a = 1$ saame järgmise tulemuse.

Järeldus 1.44 Kui H on rühma G alamrühm ja $b \in G$, siis $H = bH$ parajasti siis, kui $b \in H$.

Järgnev lause ütleb, et rühmas on kõik kõrvalklassid sama võimsusega.

Lause 1.45 Olgu G rühm ja $H \leq G$. Siis iga $a \in G$ korral $|aH| = |H| = |Ha|$.

TÕESTUS. Defineerime kujutuse $f : H \rightarrow aH$ võrdusega

$$f(h) := ah$$

iga $h \in H$ korral. On selge, et f on surjektiivne. Kui $ah = ah'$, $h, h' \in H$, siis korrutades selle võrduse mõlemaid pooli vasakult elemendiga a^{-1} saame võrduse $h = h'$. See tähendab, et kujutus f on injektiivne. Järelikult f on bijektiivne ja $|H| = |aH|$. Analogiliselt saab tõestada võrduse $|H| = |Ha|$. $\square$

Definitsioon 1.46 Lõpliku rühma **järguks** nimetatakse tema elementide arvu.

Teoreem 1.47 (Lagrange'i teoreem) Lõpliku rühma iga alamrühma järk jagab selle rühma järku.

TÕESTUS. Olgu G lõplik rühm ja $H \leq G$. Näitame, et vasakpoolsete kõrvalklasside hulk $\{aH \mid a \in G\}$ annab klassijaotuse hulgal G . Kuna $a = a \cdot 1 \in aH$ iga $a \in G$ korral, siis hulga aH on mittetühjad. Samuti on selge, et

$$G = \bigcup_{a \in G} aH.$$

Veendume, et kui hulga aH ja bH lõikuvad, siis on nad võrdsed. Selleks oletame, et leidub element $g = ah_1 = bh_2 \in aH \cap bH$, kus $h_1, h_2 \in H$. Siis $h_1 = a^{-1}bh_2$ ja $a^{-1}b = h_1h_2^{-1} \in H$, sest H on alamrühm. Lause 1.43 põhjal $aH = bH$. Sellega oleme näidanud, et tegemist on klassijaotusega. Lause 1.45 põhjal teame, et kõik vasakpoolsed kõrvalklassid on sama võimsusega (täpsemalt võimsusega $|H|$). Seega kui neid kõrvalklasse on m tükki, siis

$$|G| = m \cdot |H|$$

ehk naturaalarv $|H|$ jagab naturaalarvu $|G|$. $\square$

1.7 Faktorrühm

Nii nagu mistahes Ω -algebrate korral võib ka rühmade korral faktorrühmi moodustada kongruentside järgi. Tuleb aga välja, et rühmade kongruentsid on ära määratud teatud eriomadusega alamrühmade poolt.

Definitsioon 1.48 Rühma G alamrühma H nimetatakse **normaalseks alamrühmaks** ehk **normaaljagajaks**, kui iga $g \in G$ ja iga $h \in H$ korral $g^{-1}hg \in H$.

Rühma G kõigi normaalsete alamrühmade hulka tähistame $\mathcal{N}(G)$.

Näide 1.49 Iga rühma G korral on alamrühmad G ja $\{1\}$ normaalsed.

Näide 1.50 Kommutatiivse rühma (ehk Abeli rühma) kõik alamrühmad on normaalsed, sest $g^{-1}hg = g^{-1}gh = h \in H$.

Näide 1.51 Rühma $GL_n(\mathbb{R})$ alamrühm $SL_n(\mathbb{R})$ on normaalne.

Lause 1.52 Rühma G alamrühm H on normaalne parajasti siis, kui iga $g \in G$ korral $gH = Hg$.

TÕESTUS. TARVILIKKUS. Olgu H rühma G normaalne alamrühm. Kui $g \in G$ ja $h \in H$, siis $gh = (g^{-1})^{-1}hg^{-1} \cdot g \in Hg$, sest $(g^{-1})^{-1}hg^{-1} \in H$. Seega $gH \subseteq Hg$. Samuti $hg = g \cdot g^{-1}hg \in gH$ ja seega $Hg \subseteq gH$. Kokkuvõttes $gH = Hg$ iga $g \in G$ korral.

PIISAVUS. Eeldame, et $gH = Hg$ iga $g \in G$ korral. Kui $h \in H$, siis $hg \in gH$ ja seega leidub selline $h' \in H$, et $hg = gh'$. Järelikult $g^{-1}hg = h' \in H$. $\square$

Niisiis alamrühma normaalsus tähendab seda, et vasakpoolsed ja parempoolsed kõrvalklassid tema järgi langevad kokku.

Teoreem 1.53 Iga rühma G korral leidub üksühene vastavus hulkade $\text{Con}(G)$ ja $\mathcal{N}(G)$ vahel.

TÕESTUS. Olgu $\rho \in \text{Con}(G)$. Näitame, et $1/\rho \in \mathcal{N}(G)$. Kuna $1\rho 1$, siis $1 \in 1/\rho$ ja hulk $1/\rho$ on mittetühi. Kui $x, y \in 1/\rho$, siis $x\rho 1, y\rho 1$ ja kongruentsi definitsiooni põhjal $xy\rho 1$ ehk $xy \in 1/\rho$. Kui $x \in 1/\rho$, siis $x\rho 1$, millest saame, et $x^{-1}\rho 1^{-1}$ ehk $x^{-1}\rho 1$ ehk $x^{-1} \in 1/\rho$. Seega $1/\rho$ on rühma G alamrühm. Kontrollime normaalsust. Olgu $g \in G$ ja $x \in 1/\rho$. Kuna $g^{-1}\rho g^{-1}, x\rho 1, g\rho g$, siis kongruentsi definitsiooni tõttu ka $(g^{-1}xg)\rho(g^{-1}1g)$ ehk $(g^{-1}xg)\rho 1$ ehk $g^{-1}xg \in 1/\rho$. Sellega oleme näidanud, et $1/\rho \in \mathcal{N}(G)$. See fakt lubab meil defineerida kujutuse

$$\nu : \text{Con}(G) \rightarrow \mathcal{N}(G), \quad \rho \mapsto 1/\rho.$$

Olgu nüüd $H \in \mathcal{N}(G)$. Defineerime binaarse seose ρ_H rühmal G järgmise eeskirjaga:

$$x\rho_H y \iff xH = yH \iff x^{-1}y \in H.$$

On lihtne veenduda, et ρ_H on ekvivalentsiseos. Näitame, et ρ_H on rühma G kongruents (vt. näidet 1.34). Selleks oletame, et $x\rho_H y$ ja $z\rho_H w$ ehk $x^{-1}y, z^{-1}w \in H$. Kuna H on normaalne alamrühm, siis $z^{-1}(x^{-1}y)z \in H$. Järelikult

$$(xz)^{-1}(yw) = z^{-1}x^{-1}yw = (z^{-1}x^{-1}yz)(z^{-1}w) \in H$$

ehk $(xz)\rho_H(yw)$. Kui $x\rho_H y$ ehk $x^{-1}y \in H$, siis ka

$$yx^{-1} = xx^{-1}yx^{-1} = (x^{-1})^{-1}(x^{-1}y)x^{-1} \in H,$$

sest H on normaalne alamrühm. Kuna H on kinnine pöördlemendi võtmise suhtes, siis saame, et $(x^{-1})^{-1}y^{-1} = (yx^{-1})^{-1} \in H$. Järelikult ρ_H definitsiooni põhjal $x^{-1}\rho_H y^{-1}$. See tähendab, et ρ_H on rühma G kongruents.

Defineerime kujutuse

$$\kappa : \mathcal{N}(G) \rightarrow \text{Con}(G), \quad H \mapsto \rho_H.$$

Tõestuse lõpetamiseks näitame, et ν ja κ on teineteise pöördkujutused. Olgu $\rho \in \text{Con}(G)$. Paneme tähele, et $x^{-1}y\rho 1$ ($x, y \in G$) parajasti siis, kui $x\rho y$. Tähistades nüüd $H := 1/\rho$ võime väita, et

$$x\rho_H y \iff x^{-1}y \in 1/\rho \iff x^{-1}y\rho 1 \iff x\rho y,$$

s.t. $\rho_H = \rho$. Järelikult

$$(\kappa \circ \nu)(\rho) = \kappa(1/\rho) = \kappa(H) = \rho_H = \rho.$$

Sellega oleme tõestanud võrduse $\kappa \circ \nu = \text{id}_{\text{Con}(G)}$.

Tõestamaks võrdust $\nu \circ \kappa = \text{id}_{\mathcal{N}(G)}$ vaatleme suvalist normaalset alamrühma $H \in \mathcal{N}(G)$. Siis

$$(\nu \circ \kappa)(H) = \nu(\rho_H) = 1/\rho_H = H,$$

sest $y \in 1/\rho_H$ parajasti siis, kui $1/\rho_H y$ ehk $y \in H$. □

Olgu H rühma G normaalne alamrühm. Teoreemi 1.53 tõestuses nägime, et ν bijektiivsuse tõttu leidub täpselt üks G kongruents ρ , mille korral $1/\rho = H$. Täpsemalt öeldes $\rho = \rho_H$. Paneme tähele, et mistahes $a \in G$ korral

$$a/\rho = \{b \in G \mid a\rho_H b\} = \{b \in G \mid aH = bH\} = aH.$$

Viimase võrduse puhul on sisalduvus $\{b \in G \mid aH = bH\} \subseteq aH$ ilmne. Vastupidi, kui $ah \in aH$, siis $a^{-1}ah = h \in H$ ja lauset 1.43 kasutades saame võrduse $aH = ahH$. Seega $ah \in \{b \in G \mid aH = bH\}$. Niisiis ρ -klassid on täpselt H (vasakpoolsed) kõrvalklassid rühmas G : iga $a \in G$ korral

$$a/\rho = aH.$$

Seega faktorühma G/ρ elementideks on kõrvalklassid $aH, a \in G$, ja faktorühma korrutamistehte definitsiooni

$$a/\rho \cdot b/\rho = (ab)/\rho$$

võib esitada kujul

$$(aH) \cdot (bH) = (ab)H.$$

Sellest tulenevalt võib faktorühma defineerida järgmiselt (ja rühmateoorias seda harilikult nii ka tehakse).

Definitsioon 1.54 Rühma G **faktorrühmaks** normaalse alamrühma H järgi nimetatakse rühma, mille elementideks on kõrvalklassid $aH, a \in G$, ja mille korrutamine toimub eeskirja

$$(aH) \cdot (bH) = (ab)H$$

kohaselt. Seda rühma tähistatakse G/H . Selle rühma ühikelement on $H = 1H$ ja elemendi aH pöördelament on $a^{-1}H$.

Olgu $\varphi : G \rightarrow G'$ rühmade homomorfism. Tänu lausele 1.38 on selle tuum rühma G kongruents. Rakendades kongruentsile $\ker \varphi \in \text{Con}(G)$ teoreemi 1.53 tõestuses kasutatud kujutust ν saame normaalse alamrühma

$$\nu(\ker \varphi) = 1/\ker \varphi = \{g \in G \mid (g, 1) \in \ker \varphi\} = \{g \in G \mid \varphi(g) = \varphi(1) = 1\}.$$

Tähistame seda normaalset alamrühma sümboliga

$$\text{Ker } \varphi := \{g \in G \mid \varphi(g) = 1\}$$

ja nimetame ka seda homomorfismi φ **tuumaks**.

Tänu eespoolöeldule võime väita, et

$$G/\ker \varphi = G/\text{Ker } \varphi$$

rühmadena. Seega võib rühmade homomorfismiteoreemi sõnastada järgmisel kujul.

Teoreem 1.55 Kui $\varphi : G \rightarrow G'$ on surjektiivne rühmade homomorfism, siis $G' \simeq G/\text{Ker } \varphi$.

Näide 1.56 Vaatleme rühmade homomorfismi

$$\psi : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*, \quad A \mapsto \det(A).$$

See homomorfism on surjektiivne. Kui $r \in \mathbb{R}^*$, siis tema üheks originaaliks ψ suhtes on näiteks n -ndat järku diagonaalmaatriks, mille peadiagonaalil on $r, 1, 1, \dots, 1$. Lisaks sellele

$$\text{Ker } \psi = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\} = SL_n(\mathbb{R}).$$

Homomorfismiteoreem ütleb meile, et

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

Lause 1.57 Kui H on rühma G normaalne alamrühm, siis loomuliku homomorfismi

$$\pi : G \rightarrow G/H, \quad a \mapsto aH,$$

tuum on H .

TÕESTUS. Tänu järeldusele 1.44

$$\text{Ker } \pi = \{a \in G \mid aH = H\} = H.$$

□

Abeli rühma kõik alamrühmad on normaalsed. Kui A on aditiivne Abeli rühm (s.t. tema kahekohalist tehet tähistame sümboliga $+$ ja nimetatakse liitmiseks) ja H tema alamrühm, siis faktorrühma A/H elementideks on kõrvalklassid $a + H = \{a + h \mid h \in H\}$, $a \in A$, ja kõrvalklasside liitmine on defineeritud võrdusega

$$(a + H) + (b + H) := (a + b) + H.$$

Kuna pöördelementide osas on vastandelemendid, siis lause 1.43 põhjal mistahes elementide $a, b \in A$ korral

$$a + H = b + H \iff -a + b \in H \iff a - b \in H. \quad (3)$$

On selge, et Abeli rühma faktorrühm on ka kommutatiivne. Kui $\varphi : A \rightarrow B$ on Abeli rühmade homomorfism, siis

$$\text{Ker } \varphi = \{x \in A \mid \varphi(x) = 0\}.$$

Näide 1.58 Vaatleme Abeli rühma $(\mathbb{Z}; +)$. Lihtne on veenduda, et kui $n \geq 2$ on naturaalarv, siis alamhulk

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z}$$

on alamrühm rühmas $(\mathbb{Z}; +)$. Kõrvalklassid on kujul

$$a + n\mathbb{Z} = \{a + nx \mid x \in \mathbb{Z}\},$$

$a \in \mathbb{Z}$. Tähistame sellist kõrvalklassi sümboliga $\bar{a}$. Tähistame faktorrühma

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\}.$$

Faktorrühma liitmine on defineeritud võrdusega

$$\bar{a} + \bar{b} = \overline{a + b},$$

$a, b \in \mathbb{Z}$. On võimalik näidata, et $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. Selle faktorrühma puhul on tegemist hästituntud jäägiklasside aditiivse rühmaga mooduli n järgi.

1.8 Faktoring

Selles paragrahvis uurime ringide faktoriseerimist. Käesolevas kursuses peame ringide all silmas ühikelemendiga assotsiatiivseid ringe. Meenutame definitsiooni.

Definitsioon 1.59 Ring on hulk R koos kahe kahekohalise algebralise tehtega $+$ ja $\cdot$, mille korral on rahuldatud järgmised tingimused:

1. $(R, +)$ on Abeli rühm,
2. $(R, \cdot)$ on monoid,
3. $(\forall a, b, c \in R) \quad a(b + c) = ab + ac \quad \text{ja} \quad (a + b)c = ac + bc$.

Vaadeldes ringi Ω -algebrana nii nagu näites 1.4 võime üldist kongruentsi definitsiooni kohandada ringide juhu jaoks.

Ekvivalentsiseos ρ on **ringi R kongruents**, kui ta rahuldab tingimusi

1. $(\forall x, y, z, w \in R) \quad x\rho y \wedge z\rho w \implies (x + z)\rho(y + w)$,
2. $(\forall x, y, z, w \in R) \quad x\rho y \wedge z\rho w \implies (xz)\rho(yw)$,
3. $(\forall x, y \in R) \quad x\rho y \implies (-x)\rho(-y)$.

Paneme tähele, et kui tingimus 2 kehtib ρ korral, siis

$$(-1)\rho(-1) \wedge x\rho y \implies (-1)x\rho(-1)y \implies (-x)\rho(-y).$$

See tähendab, et tingimus 3 järeldub tingimusest 2 ja ringis alati kehtivast omadusest $(-1)x = -x$.

Sarnaselt rühmadega saab ka faktoringide moodustamiseks kongruentside asemel kasutada teatud alamhulki, mida kutsutakse ideaalideks. Ideaali mõiste võeti algselt kasutusele arvuteoorias (Ernst Kummer, Richard Dedekind). Abstraktsete ringide jaoks hakkas 1920-ndatel ideaale kasutama saksa matemaatik Emmy Noether (1882-1935).



Emmy Noether

Definitsioon 1.60 Ringi R **ideaaliks** nimetatakse rühma $(R; +)$ alamrühma I , mis on kinnine R elementidega vasakult ja paremalt korrutamise suhtes, s.t. iga $x \in I$ ja $r \in R$ korral $xr, rx \in I$.

Ringi R kõigi ideaalide hulka tähistame $\text{Id}(R)$.

Näide 1.61 1. Alati $\{0\}$ ja R on ringi R ideaalid.

2. Kui R on kommutatiivne ring, siis hulk $aR = \{ar \mid r \in R\}$ on ideaal.

Teoreem 1.62 Iga ringi R korral leidub üksühene vastavus hulkade $\text{Con}(R)$ ja $\text{Id}(R)$ vahel.

TÕESTUS. Olgu $\rho \in \text{Con}(R)$. Näitame, et $0/\rho \in \text{Id}(R)$. Kuna ρ on muuhulgas rühma $(R; +)$ kongruents, siis teoreemi 1.53 tõestuse põhjal teame, et $0/\rho$ on selle rühma alamrühm. Kui $x \in 0/\rho$ ja $r \in R$, siis $x\rho 0$ ja järelikult $xr\rho 0r = 0$, $rx\rho r0 = 0$ ehk $xr, rx \in 0/\rho$. Seega $0/\rho$ on ringi R ideaal ja võime defineerida kujutuse

$$\nu : \text{Con}(R) \rightarrow \text{Id}(R), \quad \rho \mapsto 0/\rho.$$

Olgu nüüd $I \in \text{Id}(R)$. Defineerime binaarse seose ρ_I ringil R järgmise eeskirjaga:

$$x\rho_I y \iff x + I = y + I \iff x - y \in I.$$

On selge, et ρ_I on ekvivalentsiseos ja teoreemi 1.53 tõestuse põhjal on ta ka ringi aditiivse rühma $(R; +)$ kongruents. Näitame, et ρ_I on ringi R kongruents. Selleks oletame, et $x\rho_I y$ ja $z\rho_I w$ ehk $x - y, z - w \in I$. Kuna I on ideaal, siis ka $xz - yz = (x - y)z \in I$ ja $yz - yw = y(z - w) \in I$. Et I on kinnine liitmise suhtes, siis

$$xz - yw = (xz - yz) + (yz - yw) \in I$$

ehk $(xz)\rho_I(yw)$. Sellega oleme tõestanud, et ρ_I on ringi R kongruents.

Defineerime kujutuse

$$\kappa : \text{Id}(R) \rightarrow \text{Con}(R), \quad I \mapsto \rho_I.$$

Võrdused $\kappa \circ \nu = \text{id}_{\text{Con}(R)}$ ja $\nu \circ \kappa = \text{id}_{\text{Id}(R)}$ järelduvad täpselt samamoodi nagu teoreemi 1.53 tõestuses.

□

Definitsioon 1.63 Ringi R **faktorringiks** ideaali I järgi nimetatakse ringi, mille elementideks on ideaali I kõrvalklassid rühmas $(R; +)$ ning mille liitmine ja korrutamine on defineeritud võrdustega

$$\begin{aligned} (x + I) + (y + I) &= (x + y) + I, \\ (x + I) \cdot (y + I) &= (xy) + I, \end{aligned}$$

$x, y \in R$. Seda ringi tähistatakse R/I .

Analoogiliselt rühmade juhuga saab tõestada järgmised tulemused.

Teoreem 1.64 Kui $\varphi : R \rightarrow R'$ on surjektiivne ringide homomorfism, siis $R' \simeq R/\text{Ker } \varphi$.

Lause 1.65 Kui I on ringi R ideaal, siis loomuliku homomorfismi

$$\pi : R \rightarrow R/I, \quad x \mapsto x + I,$$

tuum on I .

Näide 1.66 Lihtne on veenduda, et alamhulk $n\mathbb{Z}$ ($n \geq 2$) on ringi $(\mathbb{Z}; +, \cdot)$ ideaal (kuid mitte alamring). Faktorringiks $\mathbb{Z}/n\mathbb{Z}$ on jäägiklassiring $\mathbb{Z}_n$ mooduli n järgi, milles liitmine ja korrutamine on defineeritud võrdustega

$$\begin{aligned} \bar{a} + \bar{b} &= \overline{a + b}, \\ \bar{a} \cdot \bar{b} &= \overline{a \cdot b}. \end{aligned}$$

1.9 Faktorruum

Kui faktoriseeritavaks Ω -algebraks on vektorruum, siis faktoralgebrat nimetatakse lihtsalt **faktorruumiks** (mitte faktorvektorruumiks).

Analoogiliselt rühmade ja ringide juhtumiga saab tõestada järgmise teoreemi.

Teoreem 1.67 Iga vektorruumi V korral leidub üksühene vastavus hulkade $\text{Con}(V)$ ja $\text{Sub}(V)$ vahel.

Definitsioon 1.68 Vektorruumi V (üle korpuse K) **faktorruumiks** alamruumi W järgi nimetatakse vektorruumi, mille elementideks on alamruumi W kõrvalklassid rühmas $(V; +)$ ja mille liitmine ja skalaaridega korrutamine on defineeritud võrdustega

$$\begin{aligned}(x + W) + (y + W) &= (x + y) + W, \\ k \cdot (x + W) &= (kx) + W,\end{aligned}$$

$x, y \in V, k \in K$. Seda faktorruumi tähistatakse V/W .

Meenutame, et vektorruumide homomorfisme nimetatakse lineaarkujutusteks.

Teoreem 1.69 Kui $\varphi : V \rightarrow V'$ on sürjektiivne lineaarkujutus, siis $V' \simeq V / \text{Ker } \varphi$.

Lause 1.70 Kui W on vektorruumi V alamruum, siis loomuliku homomorfismi

$$\pi : V \rightarrow V/W, \quad x \mapsto x + W,$$

tuum on W .

1.10 Ω -algebrate otsekorutis

Alamalgebra võtmist ja faktoralgebra moodustamist võib vaadelda kui teatud konstruktsioone, mille abil saab etteantud Ω -algebratest tekitada uusi algebraid. Selles paragrahvis tutvume veel kolmanda olulise konstruktsiooniga — otsekorutiste moodustamisega.

Meenutame, kuidas defineeritakse hulkade otsekorutis. Lõpliku arvu mittetühjade hulkade $A_1, \dots, A_n$ ($n \in \mathbb{N}$) otsekorutis on hulk $A_1 \times \dots \times A_n$, mille elementideks on kõik lõplikud jadad (ehk järjendid ehk korteežid) $(a_1, \dots, a_n)$, kus $a_1 \in A_1, \dots, a_n \in A_n$. Seda otsekorutist tähistatakse ka $\prod_{i=1}^n A_i$.

Loenduva hulga mittetühjade hulkade $A_1, A_2, \dots$ otsekorutis on kõigi selliste jadade $(a_1, a_2, \dots)$ hulk, kus $a_i \in A_i$ iga indeksi $i \in \mathbb{N}$ korral. Seda jadade hulka tähistatakse kas $A_1 \times A_2 \times \dots$ või $\prod_{i=1}^{\infty} A_i$ või $\prod_{i \in \mathbb{N}} A_i$. Jada $(a_1, a_2, \dots)$ tähistatakse ka $(a_i)_{i \in \mathbb{N}}$.

Paneme tähele, et jada $(a_i)_{i \in \mathbb{N}}$ võib vaadelda kui kujutust $a : \mathbb{N} \rightarrow \bigcup_{i \in \mathbb{N}} A_i$, mis rahuldab tingimust $a(i) \in A_i$ iga $i \in \mathbb{N}$ korral ja mille puhul on tähistatud $a_i := a(i)$.

Analoogiliselt defineeritakse suvalise mittetühjade hulkade pere $A_i, i \in I$, otsekorutis kui kõigi kujutuste $a : I \rightarrow \bigcup_{i \in I} A_i$ hulk, mis rahuldavad tingimusi $a(i) \in A_i$ iga $i \in I$ korral. Seda hulka tähistatakse $\prod_{i \in I} A_i$. Tema elemente võib ette kujutada kui “üldistatud jadasid” ja me hakkame neid tähistama analoogiliselt harilike jadadega $(a_i)_{i \in I}$.

Kui $A = \prod_{j \in I} A_j$, siis kujutust $\pi_i : A \rightarrow A_i, i \in I$, mis on defineeritud võrdusega

$$\pi_i((a_j)_{j \in I}) := a_i$$

nimetatakse otsekorutise A i -ndaks projektsiooniks. On selge, et mittetühjade hulkade otsekorutise kõik projektsioonid on sürjektiivsed.

Definitsioon 1.71 Ω -algebrate A_i , $i \in I$, **otsekorrutiseks** nimetatakse hulkade A_i , $i \in I$, otsekorrutist $A = \prod_{i \in I} A_i$, millel tehted on defineeritud komponenthaaval. See tähendab, et kui $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $a^1 = (a_i^1)_{i \in I}, \dots, a^n = (a_i^n)_{i \in I} \in A$, siis

$$\omega_A(a^1, \dots, a^n) = (\omega_{A_i}(a_i^1, \dots, a_i^n))_{i \in I}$$

ja kui $\omega \in \Omega_0$, siis

$$0_A^\omega = (0_{A_i}^\omega)_{i \in I}.$$

Näide 1.72 Olgu $A_1, \dots, A_m$ rühmad. Siis otsekorrutisel

$$A = A_1 \times \dots \times A_m$$

defineeritakse kahekohaline korrumisteste võrdusega

$$(a_1, \dots, a_m) \cdot (a'_1, \dots, a'_m) = (a_1 \cdot a'_1, \dots, a_m \cdot a'_m),$$

ühikohaline pöördelemendi võtmise tehe võrdusega

$$(a_1, \dots, a_m)^{-1} = (a_1^{-1}, \dots, a_m^{-1})$$

ja ühikelemendiks loetakse jada $(1_1, 1_2, \dots, 1_m)$, kus 1_i ($i \in \{1, \dots, m\}$) on rühma A_i ühikelement.

Veelgi konkreetsemalt: näiteks rühmade $(\mathbb{Z}_3; +)$ ja $(\mathbb{Z}_7; +)$ otsekorrutises $\mathbb{Z}_3 \times \mathbb{Z}_7$ võib arvutada

$$(\bar{2}, \bar{4}) + (\bar{1}, \bar{5}) = (\bar{2} + \bar{1}, \bar{4} + \bar{5}) = (\bar{3}, \bar{9}) = (\bar{0}, \bar{2}).$$

Lause 1.73 Kui A on Ω -algebrate A_i , $i \in I$, otsekorrutis, siis kõik projektsioonid $\pi_i : A \rightarrow A_i$, $i \in I$, on Ω -algebrate homomorfismid.

TÕESTUS. Kui $i \in I$, $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $a^1 = (a_j^1)_{j \in I}, \dots, a^n = (a_j^n)_{j \in I} \in A$, siis

$$\begin{aligned} \pi_i(\omega_A(a^1, \dots, a^n)) &= \pi_i\left((\omega_{A_j}(a_j^1, \dots, a_j^n))_{j \in I}\right) && (\omega_A \text{ def.}) \\ &= \omega_{A_i}(a_i^1, \dots, a_i^n) && (\pi_i \text{ def.}) \\ &= \omega_{A_i}(\pi_i(a^1), \dots, \pi_i(a^n)) && (\pi_i \text{ def.}) \end{aligned}$$

ja kui $\omega \in \Omega_0$, siis

$$\pi_i(0_A^\omega) = \pi_i\left((0_{A_j}^\omega)_{j \in I}\right) = 0_{A_i}^\omega.$$

□

Algebralised struktuurid defineeritakse tihti teatud samasuste abil (näiteks assotsiatiivsuse samasus $(x * y) * z = x * (y * z)$, kommutatiivsuse samasus $x * y = y * x$ jne.). Kuna tehted defineeritakse otsekorrutisel komponenthaaval, siis kehtivad Ω -algebrate A_i , $i \in I$, otsekorrutisel kõik samasused, mis kehtivad kõigil neil algebratel. Teisisõnu, kui mingi Ω -algebrate klass on defineeritav samasuste abil, siis see klass on kinnine otsekorrutiste moodustamise suhtes. Nii näiteks rühmade otsekorrutis on rühm, Abeli rühmade otsekorrutis on Abeli rühm, ringide otsekorrutis on ring ja üle korpuse K vaadeldavate vektorruumide otsekorrutis on vektorruum üle korpuse K . Küll aga kahe korpuse otsekorrutis ei ole korpus.

1.11 Moodul üle ringi

Vaatleme nüüd veel ühte tüüpi algebralisi struktuure — mooduleid üle ringi. Moodul saadakse, kui vektorruumi definitsioonis asendatakse korpus ringiga, aga kõik muud nõuded jäetakse samaks.

Definitsioon 1.74 Olgu R ring. **Vasakpoolseks mooduliks üle ringi R ehk vasakpoolseks R -mooduliks** nimetatakse Abeli rühma $(A; +)$, kui iga elemendi $r \in R$ jaoks on defineeritud ühekohaline tehe

$$A \rightarrow A, \quad a \mapsto ra,$$

nii et mistahes $a, b \in A$ ja $r, s \in R$ korral

1. $(r + s)a = ra + sa$;
2. $r(a + b) = ra + rb$;
3. $(rs)a = r(sa)$;
4. $1a = a$.

Analoogiliselt saab defineerida parempoolse R -mooduli. Edasises vaatleme ainult vasakpoolseid mooduleid ja kutsume neid lihtsalt mooduliteks.

Näide 1.75 1. Iga vektorruum üle korpuse on moodul.

2. Nii nagu iga korpus on vektorruum üle iseenda on ka iga ring moodul üle iseenda.

3. Osutub, et Abeli rühmi saab vaadelda moodulitena üle täisarvude ringi $\mathbb{Z}$. Olgu $(A; +)$ Abeli rühm. Iga $n \in \mathbb{N}$ ja $a \in A$ korral defineerime

$$\begin{aligned} na &:= a + \dots + a, \\ (-n)a &:= -(a + \dots + a) \end{aligned}$$

(kus summades on n liidetavat) ja

$$0a = 0$$

(võrduse vasakul poolel on täisarv 0 ja paremal poolel on Abeli rühma A nullelement). Sellega on iga täisarvu z ja iga $a \in A$ jaoks defineeritud element $za \in A$. Saab näidata, et A rahuldab vasakpoolse $\mathbb{Z}$ -mooduli nõudeid.

4. Vaatleme maatriksringi $R = \text{Mat}_n(K)$, kus K on korpus. Olgu $A = \text{Mat}_{n,1}(K)$, s.t. A on üheveeruliste maatriksite hulk. Ühekohalised tehted $A \rightarrow A$ on defineeritud maatriksite korrutamise abil. Siis A on vasakpoolne R -moodul.

Järgmised väited tõestatakse täpselt samamoodi nagu vastavad väited vektorruumide jaoks (vt. [1], lause 2.3.9).

Lause 1.76 Olgu A moodul üle ringi R . Mistahes $a, b \in A$ ja $r, s \in R$ korral

1. $r0 = 0$;
2. $0a = 0$;
3. $(-r)a = -ra = r(-a)$;

$$4. \quad r(a - b) = ra - rb;$$

$$5. \quad (r - s)a = ra - sa.$$

Erinevalt vektorruumide juhust on moodulite korral võimalik, et $ra = 0$, kuigi $r \neq 0$ ja $a \neq 0$. Selline olukord on näiteks moodulis $\mathbb{Z}_4$ üle ringi $\mathbb{Z}_4$, kui võtame $r = \bar{2}$ ja $a = \bar{2}$.

R -moodulid on Ω -algebrad samasuguse tüüpi Ω jaoks nagu vektorruumidki (vaata näidet 1.4). See võimaldab kasutada eespool esitatud definitsioone alamalgebra (alam-mooduli), homomorfismi, isomorfismi ja otsekorrutise jaoks. Me ei hakka kõiki neid definitsioone siin moodulite jaoks lahti kirjutama. Mainime vaid, et kui A ja B on vasakpoolsed R -moodulid, siis kujutus $\varphi : A \rightarrow B$ on R -moodulite homomorfism parajasti siis, kui

$$\varphi(a + a') = \varphi(a) + \varphi(a') \quad \text{ja} \quad \varphi(ra) = r\varphi(a)$$

mistahes $a, a' \in A$ ja $r \in R$ korral. Sellest jäeldub, et $\varphi(0) = 0$.

Lause 1.77 R -moodulite homomorfism $\varphi : A \rightarrow B$ on injektiivne parajasti siis, kui $\text{Ker } \varphi = \{0\}$.

TÕESTUS. TARVILIKKUS. Kui $a \in \text{Ker } \varphi$, siis $\varphi(a) = 0 = \varphi(0)$. Injektiivsuse tõttu $a = 0$ ja seega $\text{Ker } \varphi \subseteq \{0\}$. Vastupidine sisalduvus on ilmne.

PIISAVUS. Eeldame, et $\text{Ker } \varphi = \{0\}$. Kui $\varphi(a) = \varphi(a')$, kus $a, a' \in A$, siis $0 = \varphi(a) - \varphi(a') = \varphi(a - a')$. Järelikult $a - a' \in \text{Ker } \varphi = \{0\}$, kust $a - a' = 0$ ja $a = a'$. Seega φ on injektiivne. $\square$

1.12 R -moodulite otsesummad

Moodulite korral võib rääkida kahte tüüpi otsesummadest — välistest ja sisemistest. Väliste otsesumma konstruktsioon on tihedalt seotud otsekorrutisega.

Definitsioon 1.78 Olgu R ring. R -moodulite A_i , $i \in I$, **väliseks otsesummaks** nimetatakse nende moodulite otsekorrutise $\prod_{i \in I} A_i$ alam-moodulit $\oplus \sum_{i \in I} A_i$, mis koosneb kõigist neist üldistatud jadadest $(a_i)_{i \in I}$, millel on ainult lõplik arv nullist erinevaid komponente.

Seega

$$\oplus \sum_{i \in I} A_i = \left\{ (a_i)_{i \in I} \in \prod_{i \in I} A_i \mid |\{j \in I \mid a_j \neq 0\}| < \infty \right\}.$$

Kui $I = \{1, \dots, n\}$, siis kirjutame $\oplus \sum_{i \in I} A_i$ asemel $A_1 \oplus \dots \oplus A_n$.

On selge, et lõpliku arvu R -moodulite väline otsesumma on võrdne nende otsekorrutisega, s.t.

$$A_1 \oplus \dots \oplus A_n = A_1 \times \dots \times A_n.$$

Selleks, et rääkida sisemisest otsesummast, on vaja alam-moodulite summa mõistet.

Definitsioon 1.79 R -mooduli A alam-moodulite A_i , $i \in I$, **summaks** nimetatakse R -mooduli A kõigi nende elementide hulka, mis esituvad alam-moodulitesse A_i kuuluvate elementide lõpliku summana.

R -mooduli A alammodulite A_i , $i \in I$, summat tähistatakse $\sum_{i \in I} A_i$. Lõpliku arvu alammodulite $A_1, \dots, A_n$ summat tähistatakse $A_1 + \dots + A_n$. Seega alammodulite summa $\sum_{i \in I} A_i$ elementideks on kõikvõimalikud summad

$$a_{i_1} + a_{i_2} + \dots + a_{i_n}, \quad (4)$$

kus $n \in \mathbb{N}$, $i_1, i_2, \dots, i_n \in I$ ja iga $j = 1, \dots, n$ korral $a_{i_j} \in A_{i_j}$. Kui $n = 1$, siis summa (4) võrdub elemendiga a_{i_1} . See tähendab, et summa $\sum_{i \in I} A_i$ sisaldab kõiki alammoduleid A_i , $i \in I$.

Lause 1.80 R -mooduli A alammodulite A_i , $i \in I$, summa on mooduli A vähim alammodul, mis sisaldab kõiki alammoduleid A_i , $i \in I$.

TÕESTUS. Lihtne on näha, et summade (4) hulk on alammodul (s.t. kinnine liitmise ja R elementidega korrutamise suhtes). Seega $\sum_{i \in I} A_i$ on A alammodul.

Kui B on mooduli A alammodul, mis sisaldab kõiki alammoduleid A_i , $i \in I$, siis peab B sisaldama kõiki summasid (4) (sest B peab olema kinnine liitmise suhtes), seega $\sum_{i \in I} A_i \subseteq B$. $\square$

Näide 1.81 Vaatleme moodulit $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ üle ringi $\mathbb{Z}$ koos komponenthaaval defineeritud tehete. Siis

$$\begin{aligned} A_1 &= \{(a, 0, a) \mid a \in \mathbb{Z}\}, \\ A_2 &= \{(b, b, b) \mid b \in \mathbb{Z}\} \end{aligned}$$

on A alammodulid. Lihtne on kontrollida, et nende summa on

$$A_1 + A_2 = \{(c, d, c) \mid c, d \in \mathbb{Z}\} \subset A.$$

Definitsioon 1.82 R -mooduli A alammodulite $A_1, \dots, A_n$ summat nimetatakse (**sisesummaks**) **otsesummaks** ja tähistatakse $A_1 + \dots + A_n$, kui iga element $a \in A_1 + \dots + A_n$ esitub üheselt summana

$$a = a_1 + \dots + a_n,$$

kus $a_i \in A_i$ iga $i = 1, \dots, n$ korral.

Esituse ühesus selles definitsioonis tähendab, et kui

$$a_1 + \dots + a_n = b_1 + \dots + b_n,$$

kus $a_i, b_i \in A_i$ iga $i = 1, \dots, n$ korral, siis

$$a_1 = b_1, \dots, a_n = b_n.$$

Teoreem 1.83 Olgu $A_1, \dots, A_n$ R -mooduli A alammodulid. Siis järgmised tingimused on samaväärsed:

1. alammodulite $A_1, \dots, A_n$ summa on otsesumma;
2. iga $i = 1, \dots, n$ korral kehtib võrdus

$$A_i \cap (A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_n) = \{0\}; \quad (5)$$

3. kui $a_1 + \dots + a_n = 0$, kus $a_i \in A_i$ iga $i = 1, \dots, n$ korral, siis $a_1 = \dots = a_n = 0$.

TÕESTUS. 1. $\Rightarrow$ 2. Eeldame, et $A_1 + \dots + A_n = A_1 \dot{+} \dots \dot{+} A_n$. Olgu

$$a \in A_i \cap (A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_n).$$

Siis leiduvad $a_1 \in A_1, \dots, a_{i-1} \in A_{i-1}, a_{i+1} \in A_{i+1}, \dots, a_n \in A_n$ nii, et

$$a = a_1 + \dots + a_{i-1} + a_{i+1} + \dots + a_n.$$

Tänu esituse ühesusele $a = 0$. Sellega oleme näidanud, et

$$A_i \cap (A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_n) \subseteq \{0\}.$$

Vastupidine sisalduvus on ilmne.

2. $\Rightarrow$ 3. Eeldame, et iga $i = 1, \dots, n$ korral kehtib võrdus (5) ning et $a_1 + \dots + a_n = 0$, kus $a_i \in A_i$ iga $i = 1, \dots, n$ korral. Siis iga $i = 1, \dots, n$ korral

$$-a_i = a_1 + \dots + a_{i-1} + a_{i+1} + \dots + a_n \in A_i \cap (A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_n) = \{0\}$$

ja seega $-a_i = 0$, kust $a_i = 0$.

3. $\Rightarrow$ 1. Eeldame, et kehtib tingimus 3. Oletame, et

$$a_1 + \dots + a_n = b_1 + \dots + b_n,$$

kus $a_i, b_i \in A_i$ iga $i = 1, \dots, n$ korral. Siis

$$(a_1 - b_1) + \dots + (a_n - b_n) = 0,$$

kus $a_i - b_i \in A_i$ iga $i = 1, \dots, n$ korral. Eelduse põhjal

$$a_1 - b_1 = 0, \dots, a_n - b_n = 0$$

ehk $a_1 = b_1, \dots, a_n = b_n$. □

Näide 1.84 Näites 1.81 vaadeldud alammodulite summa $A_1 + A_2$ on otsesumma, sest kui $(x, y, z) \in A_1 \cap A_2$, siis $y = 0$ ja $x = y = z$, kust ka $x = z = 0$. Seega $A_1 \cap A_2 = \{(0, 0, 0)\}$.

Näide 1.85 Vaatleme jälle moodulit $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ üle ringi $\mathbb{Z}$. Lihtne on veenduda, et

$$\begin{aligned} A_1 &= \{(a, 0, 0) \mid a \in \mathbb{Z}\}, \\ A_2 &= \{(0, b, 0) \mid b \in \mathbb{Z}\}, \\ A_3 &= \{(0, 0, c) \mid c \in \mathbb{Z}\} \end{aligned}$$

on selle mooduli alammodulid ja et $A = A_1 + A_2 + A_3$. Samuti on selge, et

$$A_1 \cap (A_2 + A_3) = \{0\}, \quad A_2 \cap (A_1 + A_3) = \{0\}, \quad \text{ja} \quad A_3 \cap (A_1 + A_2) = \{0\}.$$

Kuna teoreemi 1.83 tingimus 2 on rahuldatud, siis võime öelda, et

$$A = A_1 \dot{+} A_2 \dot{+} A_3.$$

Näide 1.86 Vaatleme ringi $\mathbb{Z}_{12}$ moodulina üle iseenda. Siis

$$\begin{aligned}\bar{2}\mathbb{Z}_{12} &= \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}, \\ \bar{3}\mathbb{Z}_{12} &= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}\end{aligned}$$

on alammodulid. Kuna $\bar{1} = \bar{10} + \bar{3}$, siis iga $\mathbb{Z}_{12}$ element on esitatav summana $a + b$, kus $a \in \bar{2}\mathbb{Z}_{12}$ ja $b \in \bar{3}\mathbb{Z}_{12}$. Seega

$$\bar{2}\mathbb{Z}_{12} + \bar{3}\mathbb{Z}_{12} = \mathbb{Z}_{12}.$$

See summa ei ole otsesumma, sest $\bar{0} \neq \bar{6} \in \bar{2}\mathbb{Z}_{12} \cap \bar{3}\mathbb{Z}_{12}$.

Alammodulite sisemise otsesumma saab defineerida ka siis, kui neid alammoduleid on lõpmata palju.

Definitsioon 1.87 R -mooduli A alammodulite A_i , $i \in I$, summat nimetatakse (**sisemiseks**) **otsesummaks** ja tähistatakse $\sum_{i \in I} A_i$, kui iga lõpliku hulga paarikaupa erinevate indeksite $i_1, \dots, i_n \in I$ korral alammodulite $A_{i_1}, \dots, A_{i_n}$ summa on otsesumma.

Teoreem 1.83 kandub samuti üle üldjuhule, s.t. juhule, kui alammoduleid ei pruugi olla lõplik arv.

Teoreem 1.88 Olgu A_i , $i \in I$, R -mooduli A alammodulid. Siis järgmised tingimused on samaväärsed:

1. alammodulite A_i , $i \in I$, summa on otsesumma;
2. iga $i \in I$ korral kehtib võrdus

$$A_i \cap \left(\sum_{j \in I \setminus \{i\}} A_j \right) = \{0\};$$

3. kui $a_1 + \dots + a_n = 0$, kus $a_j \in A_{i_j}$ iga $j = 1, \dots, n$ korral ning $i_1, \dots, i_n \in I$ on paarikaupa erinevad, siis $a_1 = \dots = a_n = 0$.

Selle teoreemi tõestust me käesolevas kursuses ei anna.

Osutub, et sisemiste ja väliste otsesummade vahel on väga tihe seos.

Teoreem 1.89 Kui $A = \sum_{i \in I} A_i$, kus A_i , $i \in I$, on mooduli A alammodulid, siis $A \simeq \sum_{i \in I}^{\oplus} A_i$. Vastupidi, kui B_i , $i \in I$, on R -moodulid ja $A = \sum_{i \in I}^{\oplus} B_i$, siis leiduvad mooduli A alammodulid A_i , $i \in I$, nii et $A = \sum_{i \in I} A_i$ ja $A_i \simeq B_i$ iga $i \in I$ korral.

TÕESTUS. Tõestame esimese väite. Eeldame, et $A = \sum_{i \in I} A_i$ ja defineerime kujutuse $\varphi : \sum_{i \in I}^{\oplus} A_i \rightarrow A$ võrdusega

$$\varphi((a_i)_{i \in I}) := \sum_{i \in I} a_i.$$

Selle võrduse paremat poolt mõistame kui üldistatud jada $(a_i)_{i \in I}$ nullist erinevate komponentide summat. Kuna neid nullist erinevaid komponente on lõplik arv, siis on selline summa olemas ja $\sum_{i \in I} a_i \in \sum_{i \in I} A_i = A$.

Veendume, et φ on moodulite homomorfism. Tõepoolest, mistahes $(a_i)_{i \in I}, (b_i)_{i \in I} \in \sum_{i \in I}^{\oplus} A_i$ ja $r \in R$ korral

$$\begin{aligned}
\varphi((a_i)_{i \in I} + (b_i)_{i \in I}) &= \varphi((a_i + b_i)_{i \in I}) && (\text{otsekorrutise + def.}) \\
&= \sum_{i \in I} (a_i + b_i) && (\varphi \text{ def.}) \\
&= \sum_{i \in I} a_i + \sum_{i \in I} b_i && (\text{mooduli + kommutatiivsus}) \\
&= \varphi((a_i)_{i \in I}) + \varphi((b_i)_{i \in I}), && (\varphi \text{ def.}) \\
\varphi(r(a_i)_{i \in I}) &= \varphi((ra_i)_{i \in I}) && (r\text{-ga korr. def. otsekorrutises}) \\
&= \sum_{i \in I} (ra_i) && (\varphi \text{ def.}) \\
&= r \sum_{i \in I} a_i && (\text{mooduli def.}) \\
&= r\varphi((a_i)_{i \in I}). && (\varphi \text{ def.})
\end{aligned}$$

On selge, et φ on surjektiivne. Oletame, et $\varphi((a_i)_{i \in I}) = 0 \in A$. Siis $\sum_{i \in I} a_i = 0$, kusjuures summas on lõplik arv nullist erinevaid liidetavaid. Kuna A on alammodulite A_i , $i \in I$, otsesumma, siis peab $a_i = 0$ iga $i \in I$ korral. Seega $(a_i)_{i \in I} = (0)_{i \in I}$ ja φ on injektiivne lause 1.77 tõttu. Kokkuvõttes φ on moodulite isomorfism.

Tõestame teise väite. Eeldame, et B_i , $i \in I$, on R -moodulid ja $A = \sum_{i \in I}^{\oplus} B_i$. Tähistame

$$A_i := \{(b_j)_{j \in I} \in A \mid b_j = 0 \text{ iga } j \in I \setminus \{i\} \text{ korral}\}.$$

Seega A_i elementideks on üldistatud jadad, mille ainuke nullist erinev komponent (kui see leidub) on i -ndal kohal. On lihtne aru saada, et A_i on mooduli A alammodul ja $A_i \simeq B_i$ iga $i \in I$ korral. Olgu $(b_j)_{j \in I} \in A$ üldistatud jada, mille nullist erinevad komponendid on $b_{j_1}, \dots, b_{j_n}$. Tähistades sümboliga β_{j_i} , $i = 1, \dots, n$, üldistatud jada, mille j_i -s komponent on b_{j_i} ja ülejäänud komponendid on 0-d, võime öelda, et

$$(b_j)_{j \in I} = \beta_{j_1} + \dots + \beta_{j_n},$$

kusjuures $\beta_{j_i} \in A_{j_i}$ iga $i = 1, \dots, n$ korral. Seega A on alammodulite A_i , $i \in I$, summa.

Kui nüüd $j_1, \dots, j_n \in I$ on paarikaupa erinevad indeksid, $\alpha_{j_1} \in A_{j_1}, \dots, \alpha_{j_n} \in A_{j_n}$ ja $\alpha_{j_1} + \dots + \alpha_{j_n}$ on nullidest koosnev üldistatud jada, siis ka $\alpha_{j_1}, \dots, \alpha_{j_n}$ on nulljadad, sest liitmine on defineeritud komponenthaval. Seega teoreemi 1.88 kolmas tingimus on täidetud ning järelikult A on alammodulite A_i , $i \in I$, sisemine otsesumma. $\square$

Näide 1.90 Näites 1.85 vaadeldud mooduli puhul $A = B_1 \times B_2 \times B_3 = B_1 \oplus B_2 \oplus B_3$, kus $B_1 = B_2 = B_3 = \mathbb{Z}$. Mooduli A alammodulid A_1, A_2, A_3 on konstrueeritud täpselt samamoodi nagu alammodulid A_i teoreemi 1.89 tõestuses.

1.13 Vektorruumide otsesumma

Nagu mainitud, iga vektorruum on moodul, seega saab ka vektorruumide korral rääkida nende alamruumide summadest ja sisemistest otsesummadest. Tõestame nende kohta mõned tulemused, mis kasutavad vektorruumi baasi ja mõõtme mõistet. Esimese asjana näitame, kuidas konstrueerida alamruumide summa baasi.

Lause 1.91 Olgu V_1 ja V_2 vektorruumi V (üle korpuse K) lõplikumõõtmelised alamruumid, B alamruumi $V_1 \cap V_2$ mingi baas (kui $V_1 \cap V_2 = \{0\}$, siis loeme, et $B = \emptyset$) ja B_i , $i = 1, 2$, alamruumi V_i baas, mis sisaldab hulka B . Siis $B_1 \cup B_2$ on alamruumi $V_1 + V_2$ baas.

TÕESTUS. Olgu

$$\begin{aligned} B &= \{e_1, \dots, e_r\}, \\ B_1 &= \{e_1, \dots, e_r, a_{r+1}, \dots, a_s\}, \\ B_2 &= \{e_1, \dots, e_r, b_{r+1}, \dots, b_t\}. \end{aligned}$$

Peame näitama, et

$$B_1 \cup B_2 = \{e_1, \dots, e_r, a_{r+1}, \dots, a_s, b_{r+1}, \dots, b_t\}$$

on alamruumi $V_1 + V_2$ baas. (Märgime, et juhul kui üks alamruum sisaldub teises, nt. $V_1 \subseteq V_2$, siis $V_1 \cap V_2 = V_1$, $B_1 = B$, $B_1 \cup B_2 = B_2$ ja $V_1 + V_2 = V_2$. Kuna B_2 on V_2 baas, siis sellisel erijuhul väide kehtib.)

On selge, et iga vektor $x = x_1 + x_2 \in V_1 + V_2$, kus $x_1 \in V_1$ ja $x_2 \in V_2$, on esitatav hulka $B_1 \cup B_2$ kuuluvate vektorite lineaarkombinatsioonina. Seega $B_1 \cup B_2$ on alamruumi $V_1 + V_2$ moodustajate süsteem.

Tõestuse lõpetamiseks peame näitama, et $B_1 \cup B_2$ vektorid on lineaarselt sõltumatud. Selleks oletame, et mingite korpuse elementide $k_1, \dots, k_r, l_{r+1}, \dots, l_s, j_{r+1}, \dots, j_t \in K$ korral

$$k_1 e_1 + \dots + k_r e_r + l_{r+1} a_{r+1} + \dots + l_s a_s + j_{r+1} b_{r+1} + \dots + j_t b_t = 0. \quad (6)$$

Tähistame

$$c := k_1 e_1 + \dots + k_r e_r + l_{r+1} a_{r+1} + \dots + l_s a_s \in V_1.$$

Siis võrdusest (6) saame, et

$$c = -j_{r+1} b_{r+1} - \dots - j_t b_t \in V_2.$$

Seega $c \in V_1 \cap V_2$. Kuna B on alamruumi $V_1 \cap V_2$ baas, siis leiduvad sellised $h_1, \dots, h_r \in K$, et

$$c = h_1 e_1 + \dots + h_r e_r.$$

Järelikult

$$h_1 e_1 + \dots + h_r e_r + j_{r+1} b_{r+1} + \dots + j_t b_t = 0,$$

kust B_2 lineaarse sõltumatuse tõttu järeldub, et

$$h_1 = \dots = h_r = j_{r+1} = \dots = j_t = 0.$$

Võrdus (6) lihtsustub nüüd kujule

$$k_1 e_1 + \dots + k_r e_r + l_{r+1} a_{r+1} + \dots + l_s a_s = 0.$$

Kuna B_1 on lineaarselt sõltumatu, siis

$$k_1 = \dots = k_r = l_{r+1} = \dots = l_s = 0.$$

Sellega oleme näidanud, et $B_1 \cup B_2$ on lineaarselt sõltumatu. $\square$

Meenutame, et vektorruumi **mõõde** (ehk dimensioon) on vektorite arv selle vektorruumi mistahes baasis. Nullalamruumi mõõtmeks loetakse arv 0. Mõõtmete kohta saame eelmisest lausest järgmise tulemuse.

Lause 1.92 Olgu V_1 ja V_2 vektorruumi V lõplikumõõtmelised alamruumid. Siis

$$\dim(V_1 + V_2) = \dim(V_1) + \dim(V_2) - \dim(V_1 \cap V_2).$$

Kuna alamruumi mõõde on 0 parajasti siis, kui see alamruum on nullalamruum, siis kehtib järgmine väide.

Järeldus 1.93 Olgu V_1 ja V_2 vektorruumi V lõplikumõõtmelised alamruumid. Siis

$$V_1 + V_2 = V_1 \dot{+} V_2 \iff \dim(V_1 + V_2) = \dim(V_1) + \dim(V_2).$$

Alamruumide summa mõõde ei saa olla suurem kui nende alamruumide mõõtmete summa.

Lause 1.94 Kui $V_1, \dots, V_m$ on vektorruumi V lõplikumõõtmelised alamruumid, siis

$$\dim(V_1 + \dots + V_m) \leq \dim(V_1) + \dots + \dim(V_m).$$

TÕESTUS. Olgu iga $i \in \{1, \dots, m\}$ korral B_i alamruumi V_i baas. Siis $\cup_{i \in I} B_i$ on summa $V_1 + \dots + V_m$ lõplik moodustajate süsteem. Teame, et igast lõplikust moodustajate süsteemist saab välja eraldada baasi. Seega

$$\dim(V_1 + \dots + V_m) \leq |B_1| + \dots + |B_m| = \dim(V_1) + \dots + \dim(V_m).$$

□

Osutub, et mõõtmete põhjal saab otsustada, kas alamruumide summa on otsesumma või mitte.

Teoreem 1.95 Olgu $V_1, \dots, V_m$ ($m \geq 2$) vektorruumi V lõplikumõõtmelised alamruumid. Siis

$$V_1 + \dots + V_m = V_1 \dot{+} \dots \dot{+} V_m$$

parajasti siis, kui

$$\dim(V_1 + \dots + V_m) = \dim(V_1) + \dots + \dim(V_m).$$

TÕESTUS. Tõestame väite induktsiooniga m järgi. Juhul kui $m = 2$ kehtib vaadeldav väide tänu järeldusele 1.93. Olgu $m > 2$ ja oletame, et väide kehtib, kui liidetavaid alamruume on vähem kui m . Tõestame väite m alamruumi jaoks.

TARVILIKKUS. Olgu alamruumide $V_1, V_2, \dots, V_m$ summa nende alamruumide otsesumma. Siis teoreemi 1.83 punkti 2 põhjal $V_1 \cap (V_2 + \dots + V_m) = \{0\}$. Teoreemi 1.83 punkti 3 abil on lihtne näha, et $V_2 + \dots + V_m = V_2 \dot{+} \dots \dot{+} V_m$. Induktsiooni eelduse põhjal peab kehtima võrdus $\dim(V_2 + \dots + V_m) = \dim(V_2) + \dots + \dim(V_m)$. Kasutades lauset 1.92 ja eelnevaid tähelepanekuid saame, et

$$\begin{aligned} \dim(V_1 + V_2 + \dots + V_m) &= \dim(V_1 + (V_2 + \dots + V_m)) \\ &= \dim(V_1) + \dim(V_2 + \dots + V_m) - \dim(V_1 \cap (V_2 + \dots + V_m)) \\ &= \dim(V_1) + \dim(V_2 + \dots + V_m) - \dim(\{0\}) \\ &= \dim(V_1) + \dim(V_2) + \dots + \dim(V_m). \end{aligned}$$

PIISAVUS. Eeldame, et kehtib võrdus $\dim(V_1 + \dots + V_m) = \dim(V_1) + \dots + \dim(V_m)$. Siis lause 1.92 tõttu

$$\begin{aligned}\dim(V_1) + \dots + \dim(V_m) &= \dim(V_1 + V_2 + \dots + V_m) \\ &= \dim(V_1) + \dim(V_2 + \dots + V_m) - \dim(V_1 \cap (V_2 + \dots + V_m)).\end{aligned}$$

Lahutades selle võrduse mõlemast poolest arvu $\dim(V_1)$ saame

$$\dim(V_2) + \dots + \dim(V_m) = \dim(V_2 + \dots + V_m) - \dim(V_1 \cap (V_2 + \dots + V_m)),$$

kust järeldub võrratus $\dim(V_2) + \dots + \dim(V_m) \leq \dim(V_2 + \dots + V_m)$. Vastupidine võrratus kehtib tänu lausele 1.94. Seega $\dim(V_2) + \dots + \dim(V_m) = \dim(V_2 + \dots + V_m)$. Induktsiooni eelduse põhjal

$$V_2 + \dots + V_m = V_2 \dot{+} \dots \dot{+} V_m. \quad (7)$$

Kuna

$$\begin{aligned}\dim(V_1 + (V_2 + \dots + V_m)) &= \dim(V_1 + V_2 + \dots + V_m) \\ &= \dim(V_1) + \dim(V_2) + \dots + \dim(V_m) \\ &= \dim(V_1) + \dim(V_2 + \dots + V_m),\end{aligned}$$

siis

$$\begin{aligned}V_1 + V_2 + \dots + V_m &= V_1 \dot{+} (V_2 + \dots + V_m) && (\text{järeldus 1.93}) \\ &= V_1 \dot{+} V_2 \dot{+} \dots \dot{+} V_m. && (\text{võrdus (7)})\end{aligned}$$

□

Järgmine lause ütleb, et vektorruumi baasi mistahes tükeldus tekitab teatud alamruumide otsesumma.

Lause 1.96 Olgu B lõplikumõõtmelise vektorruumi V baas, olgu $\{B_1, \dots, B_m\}$ klassijao- tus hulgal B ja olgu V_i , $i = 1, \dots, m$, hulga B_i poolt tekitatud alamruum (s.t. lineaarne kate). Siis

$$V = V_1 \dot{+} \dots \dot{+} V_m.$$

TÕESTUS. On selge, et $V = V_1 + \dots + V_m$. Kui $m = 1$, siis $B = B_1$, $V = V_1$ ja väide kehtib. Kui $m \geq 2$, siis väide järeldub teoreemist 1.95, sest

$$\begin{aligned}\dim(V_1 + \dots + V_m) &= \dim(V) = |B| = |\sqcup_{i=1}^m B_i| = |B_1| + \dots + |B_m| \\ &= \dim(V_1) + \dots + \dim(V_m).\end{aligned}$$

□

Lause 1.97 Olgu $V_1, \dots, V_m$ lõplikumõõtmelise vektorruumi V alamruumid,

$$V = V_1 \dot{+} \dots \dot{+} V_m$$

ja olgu B_i , $i = 1, \dots, m$, alamruumi V_i baas. Siis $\bigcup_{i=1}^m B_i$ on vektorruumi V baas.

TÕESTUS. Tänu teoreemile 1.83 on $(V_1 + \dots + V_{i-1}) \cap V_i = \{0\}$ iga $i = 2, \dots, m$ korral. Kuna $V_1 \cap V_2 = \{0\}$, siis $B_1 \cup B_2$ on $V_1 + V_2$ baas lause 1.91 põhjal. Et $(V_1 + V_2) \cap V_3 = \{0\}$, siis $B_1 \cup B_2 \cup B_3$ on $V_1 + V_2 + V_3$ baas. Analoogiliselt jätkates saame, et $B_1 \cup \dots \cup B_m$ on vektorruumi $V_1 + \dots + V_m = V$ baas. □

2 Polünoomid, algebra põhiteoreem

2.1 Mitme muutuja polünoomide ringid

Olgu R ring, milles on vähemalt kaks elementi (muuhulgas $1 \neq 0$). Siis võib vaadelda polünoomide ringi $R[X]$ üle ringi R muutuja X suhtes. Võib vaadelda ka polünoomide ringi $R[X][Y]$ üle ringi $R[X]$ muutuja Y suhtes. Seda ringi tähistatakse $R[X, Y]$ ja nimetatakse **kahe muutuja polünoomide ringiks üle ringi R** . Selle ringi elemendid on polünoomid

$$f = a_0 Y^n + a_1 Y^{n-1} + \dots + a_{n-1} Y + a_n,$$

kus $a_i \in R[X]$ iga $i = 0, 1, \dots, n$ korral. Seega saab polünoomi f esitada summana, kus liidetavaiks on avaldised kujul $aX^k Y^l$, kus $a \in R$ ja $k, l \in \mathbb{N} \cup \{0\}$. Seda protsessi võib jätkata ja vaadelda nt. polünoomide ringi $R[X, Y, Z] = R[X, Y][Z]$.

Kui R on ring, siis kasutades eelpoolkirjeldatud meetodit võib eeskirja

$$R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$$

abil defineerida ringid

$$R[X_1, X_2], R[X_1, X_2, X_3], \dots, R[X_1, \dots, X_n], \dots$$

Definitsioon 2.1 Ringi $R[X_1, \dots, X_n]$ nimetatakse **n -muutuja polünoomide ringiks üle ringi R** ja tema elemente nimetatakse **n -muutuja polünoomideks üle ringi R** .

Seega n -muutuja polünoom üle ringi R on summa liidetavatest kujul

$$aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n},$$

kus $a \in R$ ja $k_1, \dots, k_n \in \mathbb{N} \cup \{0\}$ ja $X_1, \dots, X_n$ on muutujad.

Kui n on väike (nt. 2 või 3), siis kasutatakse muutujate tähistamiseks tihti erinevaid tähti, harilikult $X, Y, Z, \dots$. Näiteks $XY^2 - 5X^3 + 2XY - 7$ on üks polünoom ringist $\mathbb{Z}[X, Y]$.

Märkus. Meenutame, kuidas konstrueeriti ring $R[X]$ kursuses Algebra I. Hulga $R[X]$ elementideks loetakse R elementide jadad $(a_0, a_1, \dots, a_n, 0, 0, \dots)$, milles on lõplik arv nullist erinevaid komponente. Sobival viisil defineeritakse jadade liitmine ja korrutamine. Ringi R element a samastatakse jadaga $(a, 0, 0, \dots)$ ja muutuja X defineeritakse kui jada $X = (0, 1, 0, 0, \dots)$. Arvutades välja korrutised $1 \cdot X$ ja $X \cdot 1$ näeme, et

$$1 \cdot X = (1, 0, 0, \dots)(0, 1, 0, \dots) = (0, 1, 0, \dots) = (0, 1, 0, \dots)(1, 0, 0, \dots) = X \cdot 1$$

ehk $1 \cdot X = X = X \cdot 1$ ringis $R[X]$. Vaatleme polünoomide ringi $R[X][Y]$ üle ringi $R[X]$. Selle elementideks on jadad $(b_0, b_1, \dots, b_n, 0, 0, \dots)$, kus $b_i \in R[X]$. Muuhulgas $Y = (0, 1, 0, 0, \dots)$, kus

$$1 = \text{ringi } R[X] \text{ ühikelement} = \text{ringi } R \text{ ühikelement}.$$

Ringi $R[X]$ element X samastatakse jadaga $(X, 0, 0, \dots)$. Nüüd

$$\begin{aligned} XY &= (X, 0, 0, \dots)(0, 1, 0, 0, \dots) = (0, X \cdot 1, 0, 0, \dots) = (0, 1 \cdot X, 0, 0, \dots) \\ &= (0, 1, 0, 0, \dots)(X, 0, 0, \dots) = YX, \end{aligned}$$

s.t. muutujad X ja Y kommuteeruvad ringis $R[X, Y]$. Paneme tähele, et võrduse $XY = YX$ tõestamisel ei ole oluline, et ring R oleks kommutatiivne. Samamoodi jätkates näeme, et ringis $R[X_1, \dots, X_n]$ muutujad kommuteeruvad.

Polünoomi, milles on üksainus nullist erineva kordajaga liidetav, nimetatakse **üksliikmeks**.

Üksliikmeid nimetatakse **sarnasteks**, kui nad on võrdsed või nende kordajad (ringi R elemendid) on erinevad, aga muidu on nad samad.

Iga nullist erinev polünoom on üheselt esitatav paarikaupa mittesarnaste üksliikmete summana. Neid üksliikmeid nimetatakse vaadeldava polünoomi **liikmeteks**. Näiteks polünoomi $2X^2Y + 4Y - 5X^2Y = -3X^2Y + 4Y \in \mathbb{Z}[X, Y]$ liikmed on $-3X^2Y$ ja $4Y$.

Kaks nullist erinevat polünoomi on **võrdsed**, kui nad on samade liikmete summad.

Definitsioon 2.2 Üksliikme $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ **astmeks** nimetatakse mittenegatiivset täisarvu $k_1 + \dots + k_n$. Nullist erineva polünoomi **astmeks** nimetatakse suurimat tema liikmete astmetest. Nullpolünoomi aste ei ole määratud, sest temas ei ole liikmeid. Polünoomi f astet tähistatakse $\deg(f)$.

Näiteks $\deg(XY^2 - 5X^3 + 2XY - 7) = 3$.

Järgmisena tahame defineerida ühe järjestusseose üksliikmete hulgal. Selleks peame fikseerima ka muutujate järjestuse. Me loeme, et X_1 on esimene muutuja, X_2 on teine muutuja jne.

Definitsioon 2.3 Ringi $R[X_1, \dots, X_n]$ kuuluvate üksliikmete hulgal saab defineerida nn. **leksikograafilise järjestuse** järgmiselt. Öeldakse, et üksliige $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ on **kõrgem** kui üksliige $bX_1^{l_1}X_2^{l_2}\dots X_n^{l_n}$, kui

- $l_1 < k_1$ või
- leidub selline $i \in \{1, \dots, n-1\}$, et $k_1 = l_1, \dots, k_i = l_i$, kuid $l_{i+1} < k_{i+1}$.

Üksliikmete m ja m' korral tähistame

$$m <_{\text{lex}} m' \iff m' \text{ on kõrgem kui } m$$

ja

$$m \leq_{\text{lex}} m' \iff m <_{\text{lex}} m' \text{ või } m \text{ ja } m' \text{ on sarnased.}$$

Lemma 2.4 Seos $\leq_{\text{lex}}$ on järjestusseos kõigi üksliikmete hulgal.

TÕESTUS. Refleksiivsus on ilmne. Transitiivsus on lihtne kontrollida. Veendume, et see seos on antisümmeetriline.

Olgu $m = bX_1^{l_1}X_2^{l_2}\dots X_n^{l_n}$ ja $m' = aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$. Oletame vastuväiteliselt, et $m \leq_{\text{lex}} m'$ ja $m' \leq_{\text{lex}} m$, kuid $m \neq m'$. Siis $m <_{\text{lex}} m'$ ja $m' <_{\text{lex}} m$. Võrratuse $m <_{\text{lex}} m'$ jaoks on kaks võimalust:

1. $l_1 < k_1$ või
2. leidub selline $i \in \{1, \dots, n-1\}$, et $k_1 = l_1, \dots, k_i = l_i$, kuid $l_{i+1} < k_{i+1}$.

Kummalgi juhul ei saa olla $m' <_{\text{lex}} m$. Saadud vastuolu näitab, et

$$m \leq_{\text{lex}} m' \wedge m' \leq_{\text{lex}} m \implies m = m'.$$

□

Tuleb välja, et seos $<_{\text{lex}}$ on kooskõlas korrutamisega.

Lemma 2.5 *Kui R on nullitegureita ring ja m_1, m_2, m on üksliikmed ringist $R[X_1, \dots, X_n]$ ning $m_1 <_{\text{lex}} m_2$, siis ka $m_1 m <_{\text{lex}} m_2 m$ ja $m m_1 <_{\text{lex}} m m_2$.*

TÕESTUS. Tõestame neist väidetest esimese (teine on analoogiline). Olgu

$$m_1 = bX_1^{l_1} X_2^{l_2} \dots X_n^{l_n}, \quad m_2 = aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n}, \quad m = cX_1^{j_1} X_2^{j_2} \dots X_n^{j_n}, \quad m_1 <_{\text{lex}} m_2.$$

Siis

$$m_1 m = bcX_1^{l_1+j_1} X_2^{l_2+j_2} \dots X_n^{l_n+j_n}, \quad m_2 m = acX_1^{k_1+j_1} X_2^{k_2+j_2} \dots X_n^{k_n+j_n}$$

on üksliikmed, sest $bc, ac \neq 0$ tänu nullitegurite puudumisele ringis R . Kui $l_1 < k_1$, siis $l_1 + j_1 < k_1 + j_1$ ja seega $m_1 m <_{\text{lex}} m_2 m$. Kui $k_1 = l_1, \dots, k_i = l_i$, kuid $l_{i+1} < k_{i+1}$, siis

$$k_1 + j_1 = l_1 + j_1, \dots, k_i + j_i = l_i + j_i, \quad \text{kuid} \quad l_{i+1} + j_{i+1} < k_{i+1} + j_{i+1}.$$

Järelikult jällegi $m_1 m <_{\text{lex}} m_2 m$. □

Kui meil on mingi n muutuja polünoom f , siis selle liikmeid on lõplik arv ja me saame nad lineaarselt järjestada, s.t. f mistahes liikmete m ja m' korral kas $m = m'$, $m <_{\text{lex}} m'$ või $m' <_{\text{lex}} m$. Seega f liikmete hulgast saab alati leida kõrgeima liikme (s.t. suurima elemendi järjestusseose $\leq_{\text{lex}}$ suhtes). Näiteks polünoomi

$$3X_2X_3^3 - 5X_1X_2X_3 + 2X_1X_3^7$$

kõrgeim liige on $-5X_1X_2X_3$.

Lause 2.6 *Kui R on nullitegureita ring ning f ja g on nullist erinevad n muutuja polünoomid üle R , siis korrutise fg kõrgeim liige on polünoomide f ja g kõrgeimate liikmete korrutis.*

TÕESTUS. Olgu polünoomide f ja g kõrgeimad liikmed vastavalt m_f ja m_g . Polünoomide korrutise fg leidmist võib ette kujutada nii, et avame sulud ja siis koondame sarnased üksliikmed, mille tulemusena jäävad järgi fg liikmed. Näitame kõigepealt, et fg arvutamisel ei teki teisi üksliikmega $m_f m_g$ sarnaseid liikmeid. (Siis $m_f m_g$ ei saa välja koonduda ja ta peab olema korrutise fg liige.)

Vaatleme sulgude avamisel tekkivat üksliiget mm' , kus m on f liige ja m' on g liige. Kui $m \neq m_f$, siis $m <_{\text{lex}} m_f$. Lisaks sellele $m' \leq_{\text{lex}} m_g$. Lemma 2.5 tõttu

$$mm' <_{\text{lex}} m_f m' \leq_{\text{lex}} m_f m_g.$$

Seega mingi X_i astendaja üksliikmes mm' peab olema väiksem kui X_i astendaja üksliikmes $m_f m_g$. Järelikult mm' ja $m_f m_g$ ei ole sarnased üksliikmed. Samale järeldusele jõuame siis, kui $m' \neq m_g$. Niisiis üksliikmega $m_f m_g$ sarnaseid üksliikmeid ei teki ja $m_f m_g$ on fg liige.

Jääb üle veel näidata, et $m_f m_g$ on fg kõrgeim liige. Korrutise fg iga liige m avaldub lõpliku summana

$$m = m_1 m'_1 + \dots + m_k m'_k,$$

kus $m_1, \dots, m_k$ on f liikmed, $m'_1, \dots, m'_k$ on g liikmed ja üksliikmed $m_1m'_1, \dots, m_km'_k$ on sarnased. Kuna iga $i \in \{1, \dots, k\}$ korral $m_i \leq_{\text{lex}} m_f$ ja $m'_i \leq_{\text{lex}} m_g$, siis lemma 2.5 põhjal

$$m_im'_i \leq_{\text{lex}} m_fm'_i \leq_{\text{lex}} m_fm_g.$$

Transitiivsuse tõttu $m_im'_i \leq_{\text{lex}} m_fm_g$. Sarnaseid üksliikmeid kokku liites saame, et ka $m \leq_{\text{lex}} m_fm_g$. Seega m_fm_g on polünoomi fg kõrgeim liige. $\square$

Järeldus 2.7 Kui ring R on nullitegureita, siis iga naturaalarvu n korral on ka polünoomide ring $R[X_1, \dots, X_n]$ nullitegureita.

TÕESTUS. Kui f ja g on nullist erinevad polünoomid, siis nende kõrgeimad liikmed m_f ja m_g on nullist erineva kordajaga. Siis ka fg liige m_fm_g on nullist erineva kordajaga ning $fg \neq 0$. $\square$

Definitsioon 2.8 Mitme muutuja polünoomi nimetatakse **homogeenseks**, kui tema kõigi liikmete astmed on võrdsed.

Kuna nullpolünoomil liikmed puuduvad, siis on ta homogeenne, kuigi tema aste pole määratud.

Lihtne on aru saada, et kahe homogeense polünoomi korrutis on homogeenne. Iga polünoom on esitatav homogeensete polünoomide summana.

Näide 2.9 Polünoom

$$f(X, Y) = 2X^2Y + XY + 5XY^2 + X^2 - Y^2 + 3$$

on homogeensete polünoomide $2X^2Y + 5XY^2$, $XY + X^2 - Y^2$ ja 3 summa.

2.2 Sümmeetrilised polünoomid

Definitsioon 2.10 Mitme muutuja polünoomi nimetatakse **sümmeetriliseks**, kui ta ei muutu muutujate mistahes substituutsiooni korral. Kõigi sümmeetriliste polünoomide alamhulka ringis $R[X_1, \dots, X_n]$ tähistatakse $S[X_1, \dots, X_n]$.

Teiste sõnadega, polünoom $f \in R[X_1, \dots, X_n]$ on sümmeetriline, kui iga $\sigma \in S_n$ korral

$$f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_1, \dots, X_n).$$

Näide 2.11 Polünoom $f(X, Y) = X^2Y + X + 3$ ei ole sümmeetriline, sest $f(Y, X) = Y^2X + Y + 3 \neq f(X, Y)$. Polünoom

$$f(X, Y, Z) = X^2 + Y^2 + Z^2 - 4XYZ + 13$$

on sümmeetriline.

Lause 2.12 Hulk $S[X_1, \dots, X_n]$ on ringi $R[X_1, \dots, X_n]$ alamring.

TÕESTUS. Iga $\sigma \in S_n$ korral võime vaadelda teisendust

$$h_\sigma : R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n], \quad f(X_1, \dots, X_n) \mapsto f(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

See teisendus on bijektiivne, sest $h_{\sigma^{-1}}$ on tema pöördteisendus. Ta on ka ringide homomorfism, sest

$$\begin{aligned} h_\sigma(f(X_1, \dots, X_n) + g(X_1, \dots, X_n)) &= f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) + g(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \\ &= h_\sigma(f(X_1, \dots, X_n)) + h_\sigma(g(X_1, \dots, X_n)), \\ h_\sigma(f(X_1, \dots, X_n)g(X_1, \dots, X_n)) &= f(X_{\sigma(1)}, \dots, X_{\sigma(n)})g(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \\ &= h_\sigma(f(X_1, \dots, X_n))h_\sigma(g(X_1, \dots, X_n)), \\ h_\sigma(1) &= 1. \end{aligned}$$

Hulk

$$S_\sigma[X_1, \dots, X_n] := \{f \in R[X_1, \dots, X_n] \mid h_\sigma(f) = f\}$$

on alamring, sest mistahes $f, g \in S_\sigma[X_1, \dots, X_n]$ korral

$$\begin{aligned} h_\sigma(f + g) &= h_\sigma(f) + h_\sigma(g) = f + g, \\ h_\sigma(-f) &= -h_\sigma(f) = -f, \\ h_\sigma(fg) &= h_\sigma(f)h_\sigma(g) = fg, \\ h_\sigma(1) &= 1 \end{aligned}$$

ja seega $f + g, -f, fg, 1 \in S_\sigma[X_1, \dots, X_n]$. Kuna alamringide ühisosa on alati alamring, siis ka

$$S[X_1, \dots, X_n] := \bigcap_{\sigma \in S_n} S_\sigma[X_1, \dots, X_n]$$

on ringi $R[X_1, \dots, X_n]$ alamring. □

On olemas üks kogum sümmeetrilisi polünoome, mida loetakse teistest teatud mõttes lihtsamateks.

Definitsioon 2.13 Sümmeetrilisi polünoome

$$\begin{aligned} \sigma_1 &= X_1 + X_2 + \dots + X_n, \\ \sigma_2 &= X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n, \\ &\dots \\ \sigma_n &= X_1X_2 \dots X_n \end{aligned}$$

nimetatakse n **muutuja sümmeetrilisteks põhipolünoomideks**.

Sümmeetriliste põhipolünoomide abil saab kirjelda seoseid unitaarse ühe muutuja polünoomi kordajate ja juurte vahel. Meenutame, et polünoomi unitaarsus tähendab seda, et tema pealiikme kordaja on 1.

Teoreem 2.14 Olgu

$$f(X) = X^n + a_1X^{n-1} + a_2X^{n-2} + \dots + a_{n-1}X + a_n$$

ühe muutuja polünoom üle nullitegureita kommutatiivse ringi R ning olgu $c_1, \dots, c_n$ tema juured. Siis kehtivad nn. Viète'i valemid:

$$a_k = (-1)^k \sigma_k(c_1, \dots, c_n), \quad k = 1, \dots, n.$$



François Viète (1540–1603)

TÕESTUS. Meenutame kursusest Algebra I, et kui n -nda astme unitaarsel polünoomil $f(X)$ on n juurt $c_1, \dots, c_n$, siis on ta esitatav korrutisena

$$f(X) = (X - c_1)(X - c_2) \dots (X - c_n).$$

Seega kehtib võrdus

$$X^n + a_1 X^{n-1} + a_2 X^{n-2} + \dots + a_{n-1} X + a_n = (X - c_1)(X - c_2) \dots (X - c_n).$$

Kuna X vastavate astmete kordajad selle võrduse mõlemal poolel peavad olema võrdsed, siis neid omavahel võrreldes saamegi valemid

$$\begin{aligned} a_1 &= -c_1 - c_2 - \dots - c_n = (-1)^1 \sigma_1(c_1, \dots, c_n), \\ a_2 &= c_1 c_2 + c_1 c_3 + \dots + c_{n-1} c_n = (-1)^2 \sigma_2(c_1, \dots, c_n), \\ &\dots \\ a_n &= (-c_1) \cdot (-c_2) \cdot \dots \cdot (-c_n) = (-1)^n \sigma_n(c_1, \dots, c_n). \end{aligned}$$

□

Lemma 2.15 *Kui $aX_1^{k_1} \dots X_n^{k_n}$ on sümmeetrilise n muutuja polünoomi kõrgeim liige, siis $k_1 \geq k_2 \geq \dots \geq k_n$.*

TÕESTUS. Oletame vastuväiteliselt, et polünoomi $f \in S[X_1, \dots, X_n]$ kõrgeima liikme $m = aX_1^{k_1} \dots X_n^{k_n}$ korral leidub $i \in \{2, \dots, n\}$ nii, et $k_1 \geq k_2 \geq \dots \geq k_{i-1} < k_i$. Vahetades omavahel ära muutujad X_{i-1} ja X_i saame polünoomi f liikme

$$aX_1^{k_1} \dots X_i^{k_{i-1}} X_{i-1}^{k_i} \dots X_n^{k_n} = aX_1^{k_1} \dots X_{i-1}^{k_i} X_i^{k_{i-1}} \dots X_n^{k_n},$$

mis on kõrgem kui m , sest $k_i > k_{i-1}$. See on vastuolu.

□

Teoreem 2.16 (Põhiteoreem sümmeetriliste polünoomide kohta) *Iga n muutuja sümmeetriline polünoom üle nullitegureita ringi R on esitatav polünoomina n muutuja sümmeetrilistest põhipolünoomidest.*

TÕESTUS. Olgu $f \in S[X_1, \dots, X_n]$ ja olgu

$$m = aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$$

tema kõrgeim liige leksikograafilise järjestuse mõttes. Tänu lemmale 2.15 teame, et $k_1 \geq k_2 \geq \dots \geq k_n$. Seega saame moodustada üksliikme

$$g_1 = a\sigma_1^{k_1-k_2} \sigma_2^{k_2-k_3} \dots \sigma_{n-1}^{k_{n-1}-k_n} \sigma_n^{k_n}$$

sümmeetrilistest põhipolünoomidest, sest arvud $k_1 - k_2, k_2 - k_3, \dots, k_{n-1} - k_n, k_n$ on mittenegatiivsed. Kuna sümmeetriliste põhipolünoomide $\sigma_1, \sigma_2, \dots, \sigma_n$ kõrgeimad liikmed on vastavalt $X_1, X_1 X_2, X_1 X_2 X_3, \dots, X_1 X_2 \dots X_n$, siis lause 2.6 põhjal on polünoomi g_1 (vaadelduna muutujate $X_1, \dots, X_n$ suhtes) kõrgeim liige

$$aX_1^{k_1-k_2} (X_1 X_2)^{k_2-k_3} (X_1 X_2 X_3)^{k_3-k_4} \dots (X_1 X_2 \dots X_n)^{k_n} = aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n} = m.$$

Seega g_1 kõrgeim liige on sama, mis f kõrgeim liige. Kuna g_1 on sümmeetriliste polünoomide korrutis, siis on ta ise ka sümmeetriline polünoom $X_1, \dots, X_n$ suhtes.

Olgu nüüd

$$f_1 := f - g_1.$$

Tänu lausele 2.12 on see polünoom sümmeetriline polünoom muutujate $X_1, \dots, X_n$ suhtes ja selle polünoomi kõrgeim liige on madalam kui polünoomi f kõrgeim liige. Lähtudes polünoomi f_1 kõrgeimast liikmest moodustame uue üksliikme g_2 sümmeetrilistest põhipolünoomidest, millel (kui polünoomil $X_1, \dots, X_n$ suhtes) on sama kõrgeim liige kui polünoomil f_1 . Olgu

$$f_2 := f_1 - g_2.$$

Selle polünoomi f_2 kõrgeim liige on madalam kui polünoomi f_1 kõrgeim liige. Lähtudes polünoomi f_2 kõrgeimast liikmest moodustame samal viisil üksliikme g_3 sümmeetrilistest põhipolünoomidest jne. Kuna polünoomi liikmete astmed ei saa lõpmatult kahaneda, siis niimoodi jätkates jõuame mingil sammul olukorrani, kus vahe

$$f_{r-1} - g_r = 0$$

mingi $r \in \mathbb{N}$ jaoks. See aga tähendab, et

$$f = g_1 + f_1 = g_1 + g_2 + f_2 = \dots = g_1 + g_2 + \dots + g_{r-1} + f_{r-1} = g_1 + g_2 + \dots + g_{r-1} + g_r.$$

Nii oleme avaldanud polünoomi f polünoomina sümmeetrilistest põhipolünoomidest. $\square$

Formaalsemalt võib selle teoreemi sõnastada nii: *iga* $f(X_1, \dots, X_n) \in S[X_1, \dots, X_n]$ *jaoks leidub polünoom* $g(Y_1, \dots, Y_n) \in R[Y_1, \dots, Y_n]$ *nii, et*

$$f(X_1, \dots, X_n) = g(\sigma_1, \dots, \sigma_n).$$

2.3 Polünoomi lahutuskorpus

Selles paragrahvis vaatleme ühe muutuja polünoome üle korpuse. Selles kursuses peame **korpuse** all silmas kommutatiivset ringi, mille nullist erinevad elemendid moodustavad korrutamise suhtes rühma. On olemas polünoome, mis ei lahutu linearpolünoomide korrutiseks (näiteks $X^2 + 2X + 7 \in \mathbb{R}[X]$ on selline). Selle paragrahvi eesmärgiks on näidata, et polünoomi kordajate korpust saab nii “laiendada”, et üle suurema korpuse lahutub vaadeldav polünoom lineaartegurite korrutiseks. Meil läheb vaja järgmisi definitsioone.

Definitsioon 2.17 Korpuse L alamringi K nimetatakse korpuse L **alamkorpuseks**, kui iga $k \in K \setminus \{0\}$ korral $k^{-1} \in K$. Kui K on L alamkorpus, siis öeldakse, et L on korpuse K **laiend**.

Definitsioon 2.18 Korpuse K ja K' nimetatakse **isomorfseteks**, kui nad on isomorfsete ringidena.

Definitsioon 2.19 Mittekonstantset polünoomi üle korpuse K nimetatakse **taandumatuks**, kui teda ei saa esitada kahe mittekonstantse polünoomi korrutisena.

Näide 2.20 1. Linearpolünoomid $aX + b \in K[X]$ on alati taandumatud.

2. Polünoom $X^2 + 2X + 7 \in \mathbb{R}[X]$ on taandumatu.

3. Polünoom $X^2 + 2X + 7 \in \mathbb{C}[X]$ ei ole taandumatu.

Lause 2.21 Olgu K korpus ja $p \in K[X]$ vähemalt teise astme taandumatu polünoom. Vaatleme faktoringi

$$K_p = K[X]/pK[X].$$

Siis

1. K_p on korpus,
2. K_p sisaldab korpusega K isomorfset alamkorpust,
3. kui vaadelda polünoomi p üle korpuse K_p , siis tal leidub juur korpuses K_p .

TÕESTUS. 1. Teame, et hulk

$$pK[X] = \{pg \mid g \in K[X]\} \subseteq K[X]$$

on polünoomide ringi $K[X]$ ideaal (vt. näidet 1.61). Seega saame moodustada faktoringi K_p . Kuna ring $K[X]$ on kommutatiivne, siis ka tema faktoring K_p on kommutatiivne. Tuleb veel näidata, et ringi K_p nullist erinevad elemendid on pööratavad. Tähistame kõrvalklasse ideaali $pK[X]$ järgi lühidalt

$$\bar{f} := f + pK[X] = \{f + pg \mid g \in K[X]\}.$$

Siis

$$K_p = \{\bar{f} \mid f \in K[X]\}.$$

Meenutame, et faktoringis

$$\bar{f} = \bar{h} \iff f - h \in pK[X] \iff p \mid f - h.$$

Muuhulgas $\bar{f} = \bar{0}$ parajasti siis, kui $p \mid f$, ning faktoringis kehtib võrdus $\bar{p} = \bar{0}$.

Vaatleme nüüd elementi $\bar{0} \neq \bar{f} \in K_p$. Olgu $d := \text{SÜT}(f, p)$. Siis $d \mid f$ ja $d \mid p$. Oletame vastuväiteliselt, et d ei ole konstantne polünoom. Kuna $d \mid p$, siis leidub polünoom $h \in K[X]$ nii, et $dh = p$. Polünoomi p taandumatuse tõttu h peab olema konstantne polünoom, $h \in K$. Järelikult

$$p \mid ph^{-1} = d \mid f,$$

kust $\bar{f} = \bar{0}$, vastuolu. Seega d on konstantne polünoom ja võime kirjutada $\text{SÜT}(f, p) = 1$. Viimasest asjaolust järeldub (vt. [1], lause 6.13.3), et leiduvad polünoomid $u, v \in K[X]$ nii, et $fu + pv = 1$. Faktoringis K_p saame siis arvutada

$$\bar{1} = \overline{fu + pv} = \overline{fu} + \overline{pv} = \bar{f}\bar{u} + \bar{p}\bar{v} = \bar{f}\bar{u} + \bar{0}\bar{v} = \bar{f}\bar{u}.$$

See tähendab, et $\bar{f} \in K_p$ pöördelemendiks on $\bar{u} \in K_p$. Sellega oleme näidanud, et K_p on korpus.

2. Vaatleme kujutust

$$\varphi : K \rightarrow K_p, \quad k \mapsto \bar{k}$$

(φ viib korpuse elemendi k konstantse polünoomi k kõrvalklassiks $\bar{k}$). Kuna

$$\begin{aligned} \varphi(k + l) &= \overline{k + l} = \bar{k} + \bar{l} = \varphi(k) + \varphi(l), \\ \varphi(kl) &= \overline{kl} = \bar{k}\bar{l} = \varphi(k)\varphi(l), \\ \varphi(1) &= \bar{1}, \end{aligned}$$

siis φ on ringide homomorfism. Näitame, et φ on injektiivne. Selleks oletame, et $\varphi(k) = \varphi(l)$, $k, l \in K$. Siis $\bar{k} = \bar{l}$ ehk $p \mid k - l$. Kuna $k - l$ on konstantne polünoom, aga $\deg(p) \geq 2$, siis ainus võimalus on, et $k - l = 0$ ehk $k = l$. Seega φ on injektiivne.

Lause 1.28 põhjal

$$K \simeq \varphi(K) = \{\bar{k} \mid k \in K\} \leq K_p,$$

s.t. ring K on isomorfne korpuse K_p alamringiga $\varphi(K)$. See alamring on ka K_p alamkorpus, sest kui $\bar{k} \in \varphi(K) \setminus \{\bar{0}\}$, siis $\bar{k} \cdot \bar{k}^{-1} = \overline{kk^{-1}} = \bar{1}$ ehk

$$\bar{k}^{-1} = \overline{k^{-1}} = \varphi(k^{-1}) \in \varphi(K).$$

Niisiis korpus K_p sisaldab korpusega K isomorfset alamkorpust $\{\bar{k} \mid k \in K\}$. Edaspidi samastame korpuse K elemendi k temaga isomorfse korpuse elemendiga $\bar{k}$. See lubab meil muuhulgas vaadelda iga polünoomi üle korpuse K polünoomina üle korpuse K_p .

3. Olgu

$$p = p(X) = a_0X^m + \dots + a_{m-1}X + a_m,$$

kus $a_0, a_1, \dots, a_m \in K$ ja $m \geq 2$. Kuna X on ka polünoom üle K , siis võime vaadelda faktoringi K_p elementi $\bar{X} = X + pK[X]$. Vaadeldes polünoomi p üle korpuse K_p näeme, et

$$\begin{aligned} p(\bar{X}) &= a_0\bar{X}^m + \dots + a_{m-1}\bar{X} + a_m \\ &= \bar{a}_0\bar{X}^m + \dots + \bar{a}_{m-1}\bar{X} + \bar{a}_m && (a_i \text{ ja } \bar{a}_i \text{ on samastatud}) \\ &= \overline{a_0X^m + \dots + a_{m-1}X + a_m} && (\text{korrutamise def. faktoringis}) \\ &= \overline{a_0X^m + \dots + a_{m-1}X + a_m} && (\text{liitmise def. faktoringis}) \\ &= \bar{p} = \bar{0}. \end{aligned}$$

See tähendab, et element $\bar{X} \in K_p$ on polünoomi p juur. □

Meil läheb veel vaja järgmist hästi tuntud fakti (vt. [1], järeldus 7.1.5).

Lause 2.22 Korpuse K element c on polünoomi $f(X) \in K[X]$ juur parajasti siis, kui $X - c \mid f(X)$ ringis $K[X]$.

Teoreem 2.23 Olgu K korpus ja olgu $f(X) \in K[X]$ mittekonstantne polünoom. Siis leidub selline korpus $\bar{K}$, et

1. K on isomorfne korpuse $\bar{K}$ alamkorpusega;
2. $f(X)$ lahutub lineaarpolünoomide korrutiseks ringis $\bar{K}[X]$.

Selles korpuses $\bar{K}$ on polünoomil $f(X)$ samapalju juuri, kui on tema aste.

TÕESTUS. Vaatleme mittekonstantset polünoomi $f(X) \in K[X]$ ja esitame ta taandumatute polünoomide korrutisena

$$f = p_1 p_2 \dots p_s \tag{8}$$

(selline esitus leidub tänu järeldusele 6.13.5 raamatust [1]). Kui polünoomid $p_1, p_2, \dots, p_s$ on lineaarpolünoomid, siis võime võtta $\bar{K} = K$ ja vajalik lahutus f jaoks on olemas. Vastasel korral leidub nende polünoomide hulgas mõni, mille aste on vähemalt 2, olgu see

näiteks p_1 (vajaduse korral võime tegureid esituses (8) ümber järjestada). Konstrueerime korpuse

$$K_{p_1} = K[X]/p_1 K[X]$$

ja samastame korpuse K korpuse K_{p_1} teatud alamkorpusega nii nagu tegime seda lause 2.21 tõestuses. Siis polünoomil p_1 leidub mingi juur c_1 korpuses K_{p_1} . Lause 2.22 põhjal leidub mingi polünoom $p'_1 \in K_{p_1}[X]$ nii, et $p_1 = (X - c_1)p'_1$ ja $\deg(p'_1) \geq 1$. Seega

$$f = (X - c_1)p'_1 p_2 \dots p_s.$$

Võib juhtuda, et ka polünoomidest $p'_1, p_2, \dots, p_s$ mõni lahutub mittekonstantsete tegurite korrutiseks üle K_{p_1} . Esitades polünoomi $p'_1 p_2 \dots p_s$ taandumatute polünoomide korrutise-na üle korpuse K_{p_1} saame f jaoks lahutuse

$$f = (X - c_1)q_1 q_2 \dots q_t,$$

kus lineaartegureid on vähemalt ühe võrra rohkem kui lahutuses (8). Kui nüüd $q_1, q_2, \dots, q_t$ on kõik lineaartegurid, siis on meil vajalik olukord saavutatud. Vastasel juhul leidub nende polünoomide hulgas vähemalt üks — olgu see q_1 —, mille aste on vähemalt 2. Konstrueerime korpuse

$$K_{q_1} = K_{p_1}[X]/q_1 K_{p_1}[X],$$

milles polünoomil q_1 leidub mingi juur c_2 . Siis q_1 jagub lineaarpolünoomiga $X - c_2$. Paneme tähele, et c_1 ja c_2 on ka polünoomi f juured. Analooiliselt jätkates peame hiljemalt $n = \deg(f)$ sammuga jõudma olukorrani, kus f on n lineaarteguri korrutis. See tähendab, et leiduvad elemendid $a_1, \dots, a_n, b_1, \dots, b_n \in \overline{K}$ nii, et

$$f(X) = (a_1 X + b_1)(a_2 X + b_2) \dots (a_n X + b_n).$$

Seega kordsusi arvestades on polünoomil $f(X)$ korpuses $\overline{K}$ n juurt: $-a_i^{-1}b_i, i \in \{1, \dots, n\}$. $\square$

Mõnikord kutsutakse teoreemis 2.23 esinevat korpust $\overline{K}$ **polünoomi $f(X)$ lahutuskorpuseks**.

Näide 2.24 Polünoom $p(X) = X^2 + 1 \in \mathbb{R}[X]$ on taandumatu. Vaatleme faktoringi

$$\mathbb{R}_p = \mathbb{R}[X]/p\mathbb{R}[X].$$

Kuna iga polünoomi üle $\mathbb{R}$ saab jäägiga jagada polünoomiga $X^2 + 1$ nii, et jäägi aste on ülimalt 1, siis saab näidata, et

$$\mathbb{R}_p = \{\overline{f} \mid f \in \mathbb{R}[X]\} = \{\overline{bX + a} \mid b, a \in \mathbb{R}\}.$$

Paneme tähele, et faktoringis $\mathbb{R}_p$ kehtib võrdus $\overline{X^2 + 1} = \overline{0}$ ehk $\overline{X^2} = \overline{-1}$ ehk $\overline{X^2} = -\overline{1}$, s.t. ringis $\mathbb{R}_p$ leidub element $\overline{X}$, mille ruut on ühikelemendi $\overline{1}$ vastandelement. Lisaks sellele

$$\begin{aligned} \overline{a_1 + b_1 X} + \overline{a_2 + b_2 X} &= \overline{(a_1 + a_2) + (b_1 + b_2)X}, \\ \overline{a_1 + b_1 X} \cdot \overline{a_2 + b_2 X} &= \overline{a_1 a_2 + a_1 b_2 X + b_1 a_2 X + b_1 b_2 \cdot (-1)} \\ &= \overline{(a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)X}. \end{aligned}$$

Lihtne on aru saada, et $\mathbb{R}_p$ on isomorfne kompleksarvude korpusega $\mathbb{C}$. Seega $\mathbb{C}$ võib konstrueerida polünoomi $X^2 + 1 \in \mathbb{R}[X]$ lahutuskorpusena.

Ka lõplikud korpused konstrueeritakse harilikult teatud taandumatute polünoomide lahutuskorpusena (vt. [3]). Lõplikel korpustel on väga oluline roll krüptograafias ja kodeerimisteoorias.

2.4 Algebra põhiteoreem

Selle paragrahvi eesmärgiks on tõestada teoreem, mida tuntakse algebra põhiteoreemi nime all. See käsitleb kompleksarvuliste kordajatega polünoomide juuri. Teoreemi saab sõnastada mitmel erineval viisil. Üks võimalik sõnastus on selline, et igal kompleksarvuliste kordajatega mittekonstant-sel polünoomil peab leiduma vähemalt üks kompleksarvuline juur.

Algebra põhiteoreemi on aegade jooksul tõestanud ja tõestada üritanud paljud nimekad matemaatikud. Esimese täielikult korrektse tõestuse andis saksa matemaatik Carl Friedrich Gauss (1777–1855) aastal 1816. Ta ise kutsus seda “algebraaliste võrrandite teooria põhiteoreemiks”. Ülevaate algebra põhiteoreemi ajaloost võib leida raamatust [1], lk. 229–231.

Me alustame abitulemusega, mille kehtivus peaks olema üsna ilmne.

Lemma 2.25 *Olgu K korpus ja*

$$f(X) = a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in K[X],$$

kusjuures $a_0 \neq 0$. Polünoomil $f(X)$ ja unitaarsel polünoomil

$$a_0^{-1} \cdot f(X) = X^n + (a_1a_0^{-1})X^{n-1} + \dots + (a_{n-1}a_0^{-1})X + a_na_0^{-1}$$

on ühed ja samad juured.

Lause 2.26 *Igal paaritu arvulise astmega reaalarvuliste kordajatega polünoomil leidub reaalarvuline juur.*

TÕESTUS. Tänu lemmale 2.25 võime eeldada, et vaadeldav polünoom on unitaarne. Olgu

$$f(X) = X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in \mathbb{R}[X]$$

selline polünoom, et $n = \deg(f(X))$ on paaritu arv. Vaatleme selle polünoomi poolt määratud funktsiooni $f : \mathbb{R} \rightarrow \mathbb{R}$, mis reaalarvule r seab vastavusse reaalarvu $f(r)$. On teada, et see funktsioon on pidev. Iga nullist erineva r korral

$$f(r) = r^n \left(1 + \frac{a_1}{r} + \frac{a_2}{r^2} + \dots + \frac{a_n}{r^n} \right),$$

ja funktsioonid $f(r)$ ja r^n on ekvivalentssed protsessis $r \rightarrow -\infty$ ja protsessis $r \rightarrow \infty$, s.t. nende jagatise piirväärtus on 1. Järelikult

$$\lim_{r \rightarrow -\infty} f(r) = \lim_{r \rightarrow -\infty} r^n = -\infty \quad \text{ja} \quad \lim_{r \rightarrow \infty} f(r) = \lim_{r \rightarrow \infty} r^n = \infty.$$

Seega leiduvad sellised reaalarvud a ja b , et $f(a) < 0$ ja $f(b) > 0$. Lõigus $[a, b]$ pideval funktsioonil, mille väärtused lõigu otspunktides on erimärgilised, leidub tänu Bolzano-Cauchy teoreemile vahemikus (a, b) nullkoht. Seega leidub selline $c \in \mathbb{R}$, et $f(c) = 0$. Teiste sõnadega, polünoomil $f(X)$ leidub reaalarvuline juur c . $\square$



Carl Friedrich Gauss

Lause 2.27 *Polünoomi*

$$f(X) = X^2 + pX + q \in \mathbb{C}[X]$$

juurteks on kompleksarvud

$$-\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q},$$

kus $\sqrt{\left(\frac{p}{2}\right)^2 - q}$ on mingi ruutjuur kompleksarvust $\left(\frac{p}{2}\right)^2 - q$.

TÕESTUS. Olgu z selline kompleksarv, et $z^2 = \left(\frac{p}{2}\right)^2 - q$ (me teame, et selline leidub). Vahetu kontroll näitab, et $w_1 = -\frac{p}{2} + z$ ja $w_2 = -\frac{p}{2} - z$ on polünoomi $f(X)$ juured. Rohkem juuri sellel polünoomil olla ei saa. $\square$

Lause 2.28 *Igal reaalarvuliste kordajatega mittekonstantsel polünoomil leidub kompleksarvuline juur.*

TÕESTUS. Tänu lemmale 2.25 võime eeldada, et vaadeldav polünoom on unitaarne. Olgu

$$f(X) = X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in \mathbb{R}[X]$$

ja olgu $n = \deg(f(X)) = 2^k q$, kus $k \in \mathbb{N} \cup \{0\}$ ja q on paaritu arv. Viime tõestuse läbi induktiooniga k järgi. Kui $k = 0$, siis leidub polünoomil $f(X)$ lause 2.26 põhjal isegi reaalarvuline juur. Eeldame nüüd, et $k > 0$ ja et väide kehtib kõigi reaalarvuliste kordajatega polünoomide korral, mille aste on $2^l m$, kus $l \in \{0, 1, \dots, k-1\}$ ja $m \in \mathbb{N}$ on paaritu. Näitame, et polünoomil $f(X)$ astmega $2^k q$ leidub kompleksarvuline juur.

Kuna $f(X) \in \mathbb{C}[X]$, siis teoreemi 2.23 põhjal leidub korpus F , mis sisaldab korpust $\mathbb{C}$ alamkorpuseks ja milles polünoomil $f(X)$ on n juurt $c_1, \dots, c_n$. Me tõestame, et vähemalt üks elementidest $c_1, \dots, c_n \in F$ on tegelikult kompleksarv.

Olgu r mingi reaalarv. Vaatleme korpuse F elemente

$$a_{ij} := c_i c_j + r(c_i + c_j), \quad i, j \in \{1, 2, \dots, n\}, \quad i < j. \quad (9)$$

Vaatleme polünoomi

$$f_r(X) := \prod_{1 \leq i < j \leq n} (X - a_{ij}) \in F[X].$$

Siis

$$\deg(f_r(X)) = \binom{n}{2} = \frac{n(n-1)}{2} = \frac{2^k q(2^k q - 1)}{2} = 2^{k-1} q(2^k q - 1) = 2^{k-1} q_0,$$

kus $q_0 := q(2^k q - 1)$ on paaritu arv ning polünoomi $f_r(X)$ juured korpuses F on elemendid a_{ij} , $i, j \in \{1, 2, \dots, n\}$, $i < j$, ja ainult nemad. Tähistame $n_0 := 2^{k-1} q_0$.

Olgu polünoomi $f_r(X)$ kordajad $b_1, \dots, b_{n_0} \in F$, s.t.

$$f_r(X) = X^{n_0} + b_1 X^{n_0-1} + \dots + b_{n_0-1} X + b_{n_0}.$$

Näitame, et need kordajad on tegelikult reaalarvud. Viete'i valemitel põhjal

$$b_k = (-1)^k \sigma_k(a_{12}, a_{13}, \dots, a_{n-1,n}), \quad k = 1, \dots, n_0. \quad (10)$$

Tänu võrdustele (9) võime öelda, et

$$b_k = g_k(c_1, \dots, c_n),$$

kus $g_k(c_1, \dots, c_n)$ on mingi reaalarvuliste kordajatega polünoom $c_1, \dots, c_n$ suhtes. Veelgi enam, me võime öelda, et $g_k(c_1, \dots, c_n)$ on sümmeetriline polünoom, sest muutujate $c_1, \dots, c_n$ substitutsioon tekitab muutujate $a_{12}, a_{13}, \dots, a_{n-1,n}$ substitutsiooni ja viimase käigus b_k ei muutu, sest b_k on sümmeetriline polünoom muutujate a_{ij} suhtes (tänu võrdusele (10)). Teoreemi 2.16 põhjal leidub sümmeetrilise polünoomi $g_k(c_1, \dots, c_n)$ jaoks reaalarvuliste kordajatega polünoom $h(Y_1, \dots, Y_n) \in \mathbb{R}[Y_1, \dots, Y_n]$ nii, et

$$g_k(c_1, \dots, c_n) = h(\sigma_1(c_1, \dots, c_n), \dots, \sigma_n(c_1, \dots, c_n)).$$

Viete'i valemitest polünoomi $f(X)$ jaoks järeldub, et

$$\begin{aligned} \sigma_1(c_1, \dots, c_n) &= -a_1 \in \mathbb{R}, \\ \sigma_2(c_1, \dots, c_n) &= a_2 \in \mathbb{R}, \\ &\dots \\ \sigma_n(c_1, \dots, c_n) &= (-1)^n a_n \in \mathbb{R}. \end{aligned}$$

Seega $b_k = h(-a_1, a_2, \dots, (-1)^n a_n) \in \mathbb{R}$, s.t. $b_1, \dots, b_{n_0}$ on reaalarvud ehk $f_r(X) \in \mathbb{R}[X]$.

Kuna iga reaalarvu r korral $f_r(X) \in \mathbb{R}[X]$ ja $\deg(f_r(X)) = n_0 = 2^{k-1}q_0$, siis induktsiooni eelduse põhjal omab $f_r(X)$ vähemalt üht kompleksarvulist juurt, mis peab olema üks elementidest a_{ij} . See tähendab, et

$$(\forall r \in \mathbb{R})(\exists i, j \in \{1, \dots, n\})(i < j \text{ ja } c_i c_j + r(c_i + c_j) \in \mathbb{C}).$$

Et reaalarve r on lõpmata palju, aga indeksite paare (i, j) , kus $i < j$ ja $i, j \in \{1, \dots, n\}$, on lõplik arv, siis peab leiduma indeksite paar (i, j) , millele vastab kaks erinevat reaalarvu r_1, r_2 , mille korral arvud

$$\begin{aligned} m_1 &= c_i c_j + r_1(c_i + c_j), \\ m_2 &= c_i c_j + r_2(c_i + c_j) \end{aligned}$$

on kompleksarvud. Lahutades ülemise võrduse vastavatest pooltest alumise võrduse vastavad pooled saame $m_1 - m_2 = (r_1 - r_2)(c_i + c_j)$, millest $r_1 \neq r_2$ tõttu

$$c_i + c_j = \frac{m_1 - m_2}{r_1 - r_2} \quad (11)$$

ja

$$c_i c_j = m_1 - r_1(c_i + c_j). \quad (12)$$

Võrdustest (11) ja (12) näeme, et $c_i + c_j$ ja $c_i c_j$ on kompleksarvud. Seega c_i ja c_j on kompleksarvuliste kordajatega ruutpolünoomi

$$(X - c_i)(X - c_j) = X^2 - (c_i + c_j)X + c_i c_j$$

juured. Lause 2.27 kohaselt on

$$\{c_i, c_j\} = \left\{ \frac{c_i + c_j}{2} \pm \sqrt{\left(\frac{c_i + c_j}{2}\right)^2 - c_i c_j} \right\}.$$

Kuna võrduse paremal poolel olevas hulgas on kompleksarvud, siis ka $c_i, c_j \in \mathbb{C}$. Seega c_i, c_j on polünoomi $f(X)$ kaks kompleksarvulist juurt (mis võivad küll olla ka võrdsed). $\square$

Teoreem 2.29 (Algebra põhiteoreem) *Igal kompleksarvuliste kordajatega mittekonstanttsel polünoomil leidub kompleksarvuline juur.*

TÕESTUS. Arvestades lauset 2.25 piisab vaadelda unitaarseid polünoome. Olgu

$$f(X) = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in \mathbb{C}[X],$$

kus $n \geq 1$ ning vaatleme ka polünoomi

$$\bar{f}(X) = X^n + \bar{a}_1 X^{n-1} + \dots + \bar{a}_{n-1} X + \bar{a}_n \in \mathbb{C}[X],$$

kus $\bar{a}_i$ on a_i kaaskompleksarv iga $i = 1, \dots, n$ korral. Korrutades need polünoomid saame polünoomi

$$g(X) = f(X)\bar{f}(X) = X^{2n} + b_1 X^{2n-1} + \dots + b_{2n-1} X + b_{2n},$$

kus

$$b_k = \sum_{i+j=k} a_i \bar{a}_j$$

iga $k = 1, 2, \dots, 2n$ korral ja loeme, et $a_0 = \bar{a}_0 = 1$. Kasutades kaaskompleksarvude omadusi ja vahetades summeerimisindekseid saame, et

$$\bar{b}_k = \overline{\sum_{i+j=k} a_i \bar{a}_j} = \sum_{i+j=k} \overline{a_i \bar{a}_j} = \sum_{i+j=k} \bar{a}_i \overline{\bar{a}_j} = \sum_{i+j=k} \bar{a}_i a_j = \sum_{i+j=k} a_j \bar{a}_i = \sum_{i+j=k} a_i \bar{a}_j = b_k.$$

Võrdus $\bar{b}_k = b_k$ tähendab, et b_k on reaalarv. Järelikult $g(X) \in \mathbb{R}[X]$. Lause 2.28 põhjal leidub selline kompleksarv c , et $0 = g(c) = f(c)\bar{f}(c)$. Järelikult $f(c) = 0$ või $\bar{f}(c) = 0$. Esimesel juhul on c polünoomi $f(X)$ juur. Kui $\bar{f}(c) = 0$, siis

$$\begin{aligned} f(\bar{c}) &= \bar{c}^n + a_1 \bar{c}^{n-1} + \dots + a_{n-1} \bar{c} + a_n \\ &= \bar{c}^n + \overline{\bar{a}_1} \bar{c}^{n-1} + \dots + \overline{\bar{a}_{n-1}} \bar{c} + \overline{\bar{a}_n} \\ &= \overline{c^n + \bar{a}_1 c^{n-1} + \dots + \bar{a}_{n-1} c + \bar{a}_n} \\ &= \overline{f(c)} = \bar{0} = 0 \end{aligned}$$

ja $\bar{c} \in \mathbb{C}$ on polünoomi $f(X)$ juur. $\square$

Definitsioon 2.30 Korpust K nimetatakse **algebraiselt kinniseks**, kui iga mittekonstantne polünoom ringist $K[X]$ lahutub selles ringis lineaartegurite korrutiseks.

Järeldus 2.31 *Igal kompleksarvuliste kordajatega mittekonstanttsel polünoomil on (kordust arvestades) n kompleksarvulist juurt, kus n on selle polünoomi aste. Teiste sõnadega, korpus $\mathbb{C}$ on algebraiselt kinnine.*

3 Lineaarteisenduse kanooniline baas

3.1 Probleemi püstitus ja põhitulemuse sõnastus

Olgu V lõplikumõõtmeline vektorruum üle korpuse K ja φ selle vektorruumi lineaarteisendus. Kui vektorruumis V on valitud mingi baas $e = \{e_1, \dots, e_n\}$, siis tekib selle teisenduse maatriks baasi e suhtes $A_\varphi^e \in \text{Mat}_n(K)$. Maatriksi A_φ^e i -ndas veerus on vektori $\varphi(e_i)$ koordinaadid baasi e suhtes. See maatriks sõltub baasi valikust. Eesmärk on leida antud lineaarteisenduse jaoks selline baas, mille suhtes oleks teisenduse maatriks võimalikult lihtne. Käesolevas peatükis anname sellele probleemile ühe lahenduse juhul, kui K on algebraliselt kinnine korpus.



Camille Jordan (1838–1922)

Selles peatükis eeldame vaikinisi, et *kõik vaadeldavad vektorruumid on lõplikumõõtmelised*.

Definitsioon 3.1 Maatriksit $J_m(\lambda) \in \text{Mat}_m(K)$ nimetatakse **m -ndat järku Jordani¹ kastiks**, kui selle kõik peadiagonaali elemendid on võrdsed elemendiga λ , igas reas on peadiagonaali elemendile järgnev element võrdne korpuse ühikelemendiga ja kõik ülejäänud elemendid on nullid.

Seega

$$J_m(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}.$$

Definitsioon 3.2 Ruutmaatriksit, mille peadiagonaalil asuvad Jordani kastid ja mille ülejäänud elemendid on nullid, nimetatakse **Jordani maatriksiks**.

Ruutmaatriksit, mille peadiagonaalil asuvad ruudukujulised alammaatriksid $B_1, \dots, B_s$ ja mille ülejäänud elemendid on nullid, tähistame $\text{diag}(B_1, \dots, B_s)$ ja nimetame **plokk-diagonaalseks maatriksiks**. Seega Jordani maatriks on kujul

$$\text{diag}(J_{m_1}(\lambda_1), \dots, J_{m_s}(\lambda_s)) = \begin{pmatrix} \boxed{J_{m_1}(\lambda_1)} & & & 0 \\ & \boxed{J_{m_2}(\lambda_2)} & & \\ & & \ddots & \\ 0 & & & \boxed{J_{m_s}(\lambda_s)} \end{pmatrix}.$$

Näide 3.3 Kastide

$$J_2(4) = \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix}, \quad J_3(7) = \begin{pmatrix} 7 & 1 & 0 \\ 0 & 7 & 1 \\ 0 & 0 & 7 \end{pmatrix} \quad \text{ja} \quad J_1(0) = (0)$$

¹Marie Ennemond Camille Jordan (1838–1922) — prantsuse matemaatik

abil saab moodustada Jordani maatriksi

$$\text{diag}(J_2(4), J_3(7), J_1(0)) = \begin{pmatrix} \boxed{\begin{matrix} 4 & 1 \\ 0 & 4 \end{matrix}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 7 & 1 & 0 \\ 0 & 7 & 1 \\ 0 & 0 & 7 \end{matrix}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{0} \end{pmatrix}.$$

Definitsioon 3.4 Vektorruumi V lineaarteisenduse **kanooniliseks baasiks** nimetatakse sellist V baasi, mille suhtes selle teisenduse maatriks on Jordani maatriks.

Meie eesmärgiks on tõestada järgmine teoreem.

Teoreem. Kui $V \neq \{0\}$ on vektorruum üle algebraliselt kinnise korpuse, siis selle vektorruumi iga lineaarteisenduse jaoks leidub kanooniline baas.

Meenutame, et sama järku ruutmaatrikseid A ja B nimetatakse **sarnasteks**, kui leidub regulaarne maatriks C nii, et $B = C^{-1}AC$. Kui φ on vektorruumi V lineaarteisendus ning e, e' on V baasid, siis $A_{\varphi}^{e'} = T^{-1}A_{\varphi}^e T$, kus T on üleminekumaatriks baasilt e baasile e' .

Definitsioon 3.5 Antud ruutmaatriksiga sarnast Jordani maatriksit nimetatakse selle maatriksi **Jordani normaalkujuks**.

Eelmise teoreemi maatrikskuju kõlab järgmiselt.

Teoreem. Iga ruutmaatriks üle algebraliselt kinnise korpuse omab Jordani normaalkuju.

3.2 Invariantseid alamruumid

Definitsioon 3.6 Olgu φ vektorruumi V lineaarteisendus. Vektorruumi V alamruumi U nimetatakse **φ -invariantseks** (ehk **invariantseks φ suhtes**), kui $\varphi(U) \subseteq U$ (teiste sõnadega, $\varphi(u) \in U$ iga $u \in U$ korral).

Näide 3.7 Alamruumid V , $\{0\}$, $\text{Ker}(\varphi)$ ja $\text{Im}(\varphi)$ on iga lineaarteisenduse $\varphi \in \text{End}(V)$ korral φ -invariantseid alamruumid.

Tähistagu $\langle a_1, \dots, a_n \rangle$ vektorite süsteemi $a_1, \dots, a_n$ lineaarset katet, s.t

$$\langle a_1, \dots, a_n \rangle = \{k_1 a_1 + \dots + k_n a_n \mid k_1, \dots, k_n \in K\}.$$

Lause 3.8 Olgu φ vektorruumi V lineaarteisendus ja $U = \langle a_1, \dots, a_n \rangle$ vektorruumi V alamruum. Siis U on φ -invariantne parajasti siis, kui $\varphi(a_i) \in U$ iga $i \in \{1, \dots, n\}$ korral.

TÕESTUS. Tarvilikkus on ilmne.

Piisavuse tõestamiseks võtame suvalise vektori $a = k_1 a_1 + \dots + k_n a_n \in U$, kus $k_1, \dots, k_n \in K$. Siis

$$\varphi(a) = k_1 \varphi(a_1) + \dots + k_n \varphi(a_n) \in U,$$

sest $\varphi(a_1), \dots, \varphi(a_n) \in U$ ja U on alamruum. □

Lause 3.9 Vektorruumi V lineaarteisenduse φ omavektori lineaarne kate on vektorruumi V ühemõõtmeline φ -invariantne alamruum. Vastupidi, kui U on vektorruumi V ühemõõtmeline φ -invariantne alamruum, siis alamruumi U iga nullist erinev vektor on φ omavektor.

TÕESTUS. Oletame, et $a \in V \setminus \{0\}$ on lineaarteisenduse φ omavektor, mis vastab omaväärtusele $\lambda \in K$. Siis $\varphi(a) = \lambda a \in \langle a \rangle$. Lause 3.8 põhjal on $\langle a \rangle$ φ -invariantne alamruum.

Olgu nüüd U vektorruumi V ühemõõtmeline φ -invariantne alamruum, mille baasivektori on e . Siis $U = \{ke \mid k \in K\}$. Et U on φ -invariantne, siis leidub selline $l \in K$, et $\varphi(e) = le$. Iga $k \in K \setminus \{0\}$ korral

$$\varphi(ke) = k\varphi(e) = kle = lke,$$

mis tähendab, et ke on φ omavektor, mis vastab omaväärtusele l . Seega U nullist erinevad vektorid on φ omavektorid. $\square$

Lause 3.10 Olgu φ vektorruumi V lineaarteisendus ja olgu vektorruum V oma φ -invariantsete alamruumide otsesumma

$$V = U_1 \dot{+} \dots \dot{+} U_m.$$

Kui B_i on alamruumi U_i baas iga $i \in \{1, \dots, m\}$ korral, siis $B = B_1 \cup \dots \cup B_m$ on vektorruumi V baas, mille korral

$$A_\varphi^B = \text{diag}(A_{\varphi_1}^{B_1}, \dots, A_{\varphi_m}^{B_m}), \quad (13)$$

kus φ_i ($i \in \{1, \dots, m\}$) on lineaarteisendus

$$\varphi_i : U_i \rightarrow U_i, \quad a \mapsto \varphi(a).$$

TÕESTUS. Hulk $B = B_1 \cup \dots \cup B_m$ on vektorruumi V baas lause 1.97 tõttu. Tänu alamruumi U_i φ -invariantsusele on olemas lineaarteisendused $\varphi_i : U_i \rightarrow U_i$. Võrdus (13) tuleneb vahetult lineaarteisenduse maatriksi definitsioonist, sest

$$\varphi_i(b) \in U_i = \langle B_i \rangle$$

iga $b \in B_i$ korral. $\square$

3.3 Nilpotentse lineaarteisenduse kanooniline baas

Definitsioon 3.11 Ringi R elementi x nimetatakse **nilpotentseks**, kui leidub selline $n \in \mathbb{N}$, et $x^n = 0$. Vähimat naturaalarvu r , mille korral $x^r = 0$, nimetatakse elemendi x **nilpotentsuse indeksiks**.

Näide 3.12 1. Element $\bar{2}$ on nilpotentne indeksiga 4 ringis $\mathbb{Z}_{16}$.

2. Element $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ on nilpotentne indeksiga 2 ringis $\text{Mat}_2(\mathbb{R})$.

Muuhulgas võib rääkida näiteks **nilpotentsetest lineaarteisendustest** (s.t. ringi $\text{End}(V)$, kus V on vektorruum, nilpotentsetest elementidest) ja **nilpotentsetest ruutmaatriksitest** (s.t. ringi $\text{Mat}_n(K)$ nilpotentsetest elementidest).

Meenutame, et ringi $\text{End}(V)$ elementideks on vektorruumi V lineaarteisendused, liitmine on defineeritud punktiivisiliselt, korrutamine on defineeritud järjestakendamise abil, ühikelemendiks on vektorruumi V samasusteisendus ja nullelemendiks on nullteisendus. Rääkides lineaarteisenduse φ astmetest loeme, et $\varphi^0 = \text{id}_V$. Muuhulgas $\varphi^2(a) = \varphi(\varphi(a))$, $\varphi^3(a) = \varphi(\varphi(\varphi(a)))$ jne.

Niisiis $\varphi \in \text{End}(V)$, kus $V \neq \{0\}$, on nilpotentne lineaarteisendus indeksiga r parajasti siis, kui

$$(\forall a \in V)(\varphi^r(a) = 0) \quad \text{ja} \quad (\exists b \in V)(\varphi^{r-1}(b) \neq 0).$$

Näide 3.13 1. Mistahes vektorruumi nullteisendus on nilpotentne indeksiga 1.

2. Olgu n fikseeritud naturaalarv ja vaatleme polünoomide vektorruumi

$$V = \{f(X) \in \mathbb{R}[X] \mid \deg(f(X)) \leq n\}$$

üle korpuse $\mathbb{R}$. Selle vektorruumi diferentseerimisteisendus

$$\varphi : V \rightarrow V, \quad f(X) \mapsto f'(X)$$

on nilpotentne indeksiga $n + 1$.

Lause 3.14 Vektorruumi $V \neq \{0\}$ nilpotentsel lineaarteisendusel on täpselt üks omaväärtus, milleks on 0.

TÕESTUS. Olgu φ vektorruumi V nilpotentne lineaarteisendus indeksiga r . Siis leidub vektor $b \in V$, et $\varphi^{r-1}(b) \neq 0$. See aga tähendab, et

$$\varphi(\varphi^{r-1}(b)) = \varphi^r(b) = 0 = 0 \cdot \varphi^{r-1}(b),$$

kust näeme, et 0 on teisenduse φ omaväärtus, millele vastab omavektor $\varphi^{r-1}(b)$.

Näitame, et teisi omaväärtusi teisendusel φ ei ole. Selleks oletame vastuväiteliselt, et $\varphi(a) = \lambda a$, kus $a \in V \setminus \{0\}$ ja $\lambda \in K \setminus \{0\}$. Siis

$$0 = \varphi^r(a) = \varphi^{r-1}(\varphi(a)) = \varphi^{r-1}(\lambda a) = \lambda \varphi^{r-1}(a) = \dots = \lambda^r a.$$

Kuna $\lambda \neq 0$ ja korpuses pole nullitegureid, siis ka $\lambda^r \neq 0$. Korrutades võrduse $0 = \lambda^r a$ mõlemaid pooli korpuse elemendiga $(\lambda^r)^{-1}$ saame võrduse $a = 0$, mis on vastuolus eeldustega. $\square$

Lause 3.15 Olgu φ vektorruumi $V \neq \{0\}$ nilpotentne lineaarteisendus indeksiga r . Iga $i \in \{0, 1, \dots, r\}$ korral tähistame

$$H_i := \text{Ker}(\varphi^i) = \{a \in V \mid \varphi^i(a) = 0\}.$$

Siis

$$\{0\} = H_0 \subset H_1 \subset H_2 \subset \dots \subset H_{r-1} \subset H_r = V. \quad (14)$$

TÕESTUS. Võrdused $\{0\} = \text{Ker}(1_V) = \text{Ker}(\varphi^0) = H_0$ ja $H_r = \text{Ker}(\varphi^r) = \text{Ker}(0) = V$ on ilmsed.

Kui $\varphi^{i-1}(a) = 0$, siis ka $\varphi^i(a) = \varphi(\varphi^{i-1}(a)) = \varphi(0) = 0$ ja seega $H_{i-1} \subseteq H_i$ iga $i \in \{1, \dots, r\}$ korral. Kuna teisenduse φ nilpotentsuse indeks on r , siis leidub selline vektor $b \in V$, et $\varphi^{r-1}(b) \neq 0$. Nüüd $\varphi^{r-i}(b) \in H_i \setminus H_{i-1}$, sest

$$\varphi^i(\varphi^{r-i}(b)) = \varphi^{i+r-i}(b) = \varphi^r(b) = 0$$

ja

$$\varphi^{i-1}(\varphi^{r-i}(b)) = \varphi^{i-1+r-i}(b) = \varphi^{r-1}(b) \neq 0.$$

Seega kõik sisalduvused alamruumide ahelas (14) on ranged. $\square$

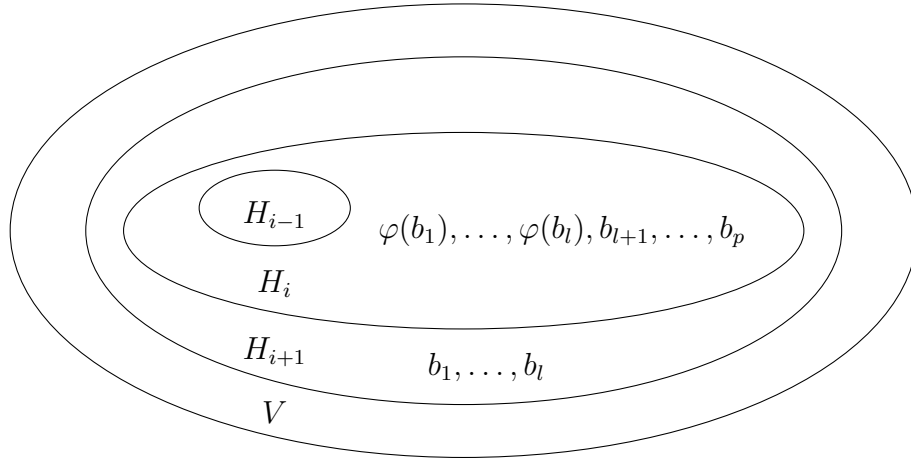
Meenutame, et lõplikumõõtmelise vektorruumi iga lineaarselt sõltumatu vektorite süsteemi saab vektoreid vajaduse korral lisades täiendada baasiks. Seda fakti läheb meil vaja järgmistes tõestustes.

Lemma 3.16 *Kasutame eelmise lause eeldusi ja tähistusi. Kui $i \in \{1, \dots, r-1\}$ ja $b_1, \dots, b_l \in H_{i+1}$ on sellised lineaarselt sõltumatud vektorid, et*

$$H_{i+1} = H_i \dot{+} \langle b_1, \dots, b_l \rangle, \quad (15)$$

siis leiduvad vektorid $b_{l+1}, \dots, b_p \in H_i$ nii, et süsteem $\varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p$ on lineaarselt sõltumatu ja

$$H_i = H_{i-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle.$$



TÕESTUS. Kõigepealt näitame, et vektorid $\varphi(b_1), \dots, \varphi(b_l)$ on lineaarselt sõltumatud. Selleks oletame, et $k_1\varphi(b_1) + \dots + k_l\varphi(b_l) = 0$ ehk $\varphi(k_1b_1 + \dots + k_lb_l) = 0$, kus $k_1, \dots, k_l \in K$. Siis

$$k_1b_1 + \dots + k_lb_l \in \text{Ker}(\varphi) = H_1 \subset H_2 \subset \dots \subset H_i.$$

Et $k_1b_1 + \dots + k_lb_l \in H_i \cap \langle b_1, \dots, b_l \rangle = \{0\}$ (vt. võrdust (15)), siis saame järeldada, et $k_1b_1 + \dots + k_lb_l = 0$. Kuna $b_1, \dots, b_l$ on lineaarselt sõltumatud, siis $k_1 = \dots = k_l = 0$.

Teiseks veendume, et

$$H_{i-1} \cap \langle \varphi(b_1), \dots, \varphi(b_l) \rangle = \{0\}.$$

Selleks oletame, et $a = k_1\varphi(b_1) + \dots + k_l\varphi(b_l) \in H_{i-1}$, kus $k_1, \dots, k_l \in K$. Siis

$$0 = \varphi^{i-1}(a) = \varphi^i(k_1b_1 + \dots + k_lb_l)$$

ehk

$$k_1b_1 + \dots + k_lb_l \in H_i \cap \langle b_1, \dots, b_l \rangle = \{0\}.$$

Kuna $k_1b_1 + \dots + k_lb_l = 0$, siis $a = \varphi(k_1b_1 + \dots + k_lb_l) = 0$.

Teoreemi 1.83 põhjal

$$H_{i-1} + \langle \varphi(b_1), \dots, \varphi(b_l) \rangle = H_{i-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l) \rangle \subseteq H_i.$$

Vaatleme kahte juhtu.

1) $i > 1$. Siis $H_{i-1} \neq \{0\}$. Olgu B alamruumi H_{i-1} suvaline baas. Siis süsteem $B' = B \cup \{\varphi(b_1), \dots, \varphi(b_l)\}$ on lause 1.97 põhjal vektorruumi H_i alamruumi $H_{i-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l) \rangle$ baas. Muuhulgas on B' lineaarselt sõltumatu süsteem. Kui B' ei ole H_i baas, siis täiendame ta alamruumi H_i baasiks mingite vektoritega $b_{l+1}, \dots, b_p \in H_i$. Siis on selge, et vektorid $\varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p$ on lineaarselt sõltumatud ning lause 1.96 põhjal

$$H_i = \langle B \rangle \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle = H_{i-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle.$$

2) $i = 1$. Kuna $\varphi(b_1), \dots, \varphi(b_l)$ on lineaarselt sõltumatu süsteem alamruumis H_1 , siis saab selle mingite vektoritega $b_{l+1}, \dots, b_p \in H_1$ täiendada alamruumi H_1 baasiks. Järelikult

$$H_1 = \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle = H_0 \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle.$$

□

Teoreem 3.17 Iga vektorruumi $V \neq \{0\}$ igal nilpotentsel lineaarteisendusel on olemas kanooniline baas.

TÕESTUS. Olgu φ vektorruumi $V \neq \{0\}$ nilpotentne lineaarteisendus indeksiga r . Kui $B = b_1, \dots, b_m$ on vektorruumi V mingi vektorite süsteem, siis tähistagu $\varphi(B)$ vektorite süsteemi $\varphi(b_1), \dots, \varphi(b_m)$. Vaatleme V alamruumide jada

$$\{0\} = H_0 \subset H_1 \subset H_2 \subset \dots \subset H_{r-1} \subset H_r = V.$$

Kui $r = 1$, siis $\varphi^1 = \varphi$ on nullteisendus ja selle maatriks iga baasi suhtes on nullmaatriks, mis on $\text{diag}(J_1(0), \dots, J_1(0))$. Niisiis iga V baas on nullteisenduse kanooniline baas. Edasises vaatleme olukorda, kus $r \geq 2$.

Kuna H_{r-1} ei ole nullalamruum, siis temas leidub mingi baas B' . Olgu $a_1, \dots, a_{p_1} \in V$ vektorid, mis täiendavad selle baasi $H_r = V$ baasiks. Siis $a_1, \dots, a_{p_1}$ on lineaarselt sõltumatud ja lause 1.96 põhjal

$$V = H_r = \langle B' \rangle \dot{+} \langle a_1, \dots, a_{p_1} \rangle = H_{r-1} \dot{+} \langle a_1, \dots, a_{p_1} \rangle.$$

Kasutades lemmat 3.16 saame leida sellised vektorid $a_{p_1+1}, \dots, a_{p_2} \in H_{r-1}$, et süsteem $\varphi(a_1), \dots, \varphi(a_{p_1}), a_{p_1+1}, \dots, a_{p_2}$ on lineaarselt sõltumatu ja

$$H_{r-1} = H_{r-2} \dot{+} \langle \varphi(a_1), \dots, \varphi(a_{p_1}), a_{p_1+1}, \dots, a_{p_2} \rangle. \quad (16)$$

Tähistades $S_1 = a_1, \dots, a_{p_1}$ ja $S_2 = a_{p_1+1}, \dots, a_{p_2}$ võime lühidalt kirjutada

$$\begin{aligned} V &= H_r = H_{r-1} \dot{+} \langle S_1 \rangle, \\ H_{r-1} &= H_{r-2} \dot{+} \langle \varphi(S_1), S_2 \rangle. \end{aligned}$$

Seega

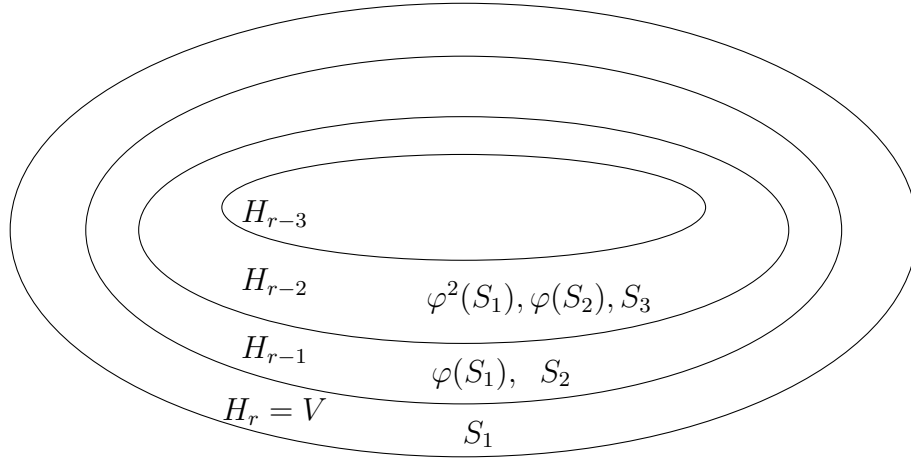
$$V = H_{r-2} \dot{+} \langle \varphi(S_1), S_2 \rangle \dot{+} \langle S_1 \rangle$$

ja alamruumi H_{r-1} süsteem $\varphi(S_1), S_2$ on lineaarselt sõltumatu. Järgmine lemma 3.16 rakendamine annab süsteemi S_3 alamruumnis H_{r-2} nii, et $\varphi^2(S_1), \varphi(S_2), S_3$ on lineaarselt sõltumatu,

$$H_{r-2} = H_{r-3} \dot{+} \langle \varphi^2(S_1), \varphi(S_2), S_3 \rangle$$

ja

$$\begin{aligned} V &= H_{r-3} \dot{+} \langle \varphi^2(S_1), \varphi(S_2), S_3 \rangle \\ &\quad \dot{+} \langle \varphi(S_1), S_2 \rangle \\ &\quad \dot{+} \langle S_1 \rangle. \end{aligned}$$



Analoogiliselt jätkates jõuame lõpuks selleni, et

$$\begin{aligned} V &= H_0 \dot{+} \langle \varphi^{r-1}(S_1), \varphi^{r-2}(S_2), \dots, \varphi^1(S_{r-1}), S_r \rangle \\ &\quad \dot{+} \langle \varphi^{r-2}(S_1), \varphi^{r-3}(S_2), \dots, S_{r-1} \rangle \\ &\quad \dots \\ &\quad \dot{+} \langle \varphi(S_1), S_2 \rangle \\ &\quad \dot{+} \langle S_1 \rangle. \end{aligned}$$

Tähistame $S_i = a_{p_{i-1}+1}, \dots, a_{p_i}$ iga $i \in \{1, \dots, r\}$ korral (loeme, et $p_0 = 0$). Võib juhtuda, et mõni süsteemidest $S_1, \dots, S_r$ on tühi. Kui S_i on tühi, siis loeme, et $p_{i-1} = p_i$. Arvestades, et $H_0 = \{0\}$, võime kirjutada

$$\begin{aligned} V &= \\ &\langle \varphi^{r-1}(a_1), \dots, \varphi^{r-1}(a_{p_1}), \varphi^{r-2}(a_{p_1+1}), \dots, \varphi^{r-2}(a_{p_2}), \dots, \varphi(a_{p_{r-2}+1}), \dots, \varphi(a_{p_{r-1}}), a_{p_{r-1}+1}, \dots, a_{p_r}, \\ &\quad \varphi^{r-2}(a_1), \dots, \varphi^{r-2}(a_{p_1}), \varphi^{r-3}(a_{p_1+1}), \dots, \varphi^{r-3}(a_{p_2}), \dots, a_{p_{r-2}+1}, \dots, a_{p_{r-1}}, \\ &\quad \dots, \dots \\ &\quad \varphi(a_1), \dots, \varphi(a_{p_1}), a_{p_1+1}, \dots, a_{p_2}, \\ &\quad a_1, \dots, a_{p_1} \rangle, \end{aligned}$$

kusjuures siin esinev vektorite süsteem (mida edaspidi tähistame sümboliga B) on lineaarselt sõltumatu tänu lausele 1.97. Seega on see süsteem vektorruumi V baas. Veendume, et B on vektorruumi V kanooniline baas.

Järjestame baasi B vektorid nii, et kõigepealt on esimese veeru vektorid ülevalt alla, siis teise veeru vektorid ülevalt alla jne. Olgu B_i , $i \in \{1, \dots, p_r\}$, selle vektorite tabeli i -nda veeru vektorite süsteem ja U_i selle süsteemi lineaarne kate. Näitame, et

$$U_1 = \langle B_1 \rangle = \langle \varphi^{r-1}(a_1), \varphi^{r-2}(a_1), \dots, \varphi(a_1), a_1 \rangle$$

on φ -invariantne alamruum (suvalise U_i korral on tõestus analoogiline). Tõepoolest, kui

$$x = k_1 \varphi^{r-1}(a_1) + k_2 \varphi^{r-2}(a_1) + \dots + k_{r-1} \varphi(a_1) + k_r a_1 \in U_1,$$

kus $k_1, \dots, k_r \in K$, siis $k_1 \varphi^r(a_1) = 0$ (sest $a_1 \in H_r = \text{Ker}(\varphi^r)$) ja seega

$$\varphi(x) = k_2 \varphi^{r-1}(a_1) + k_3 \varphi^{r-2}(a_1) + \dots + k_{r-1} \varphi^2(a_1) + k_r \varphi(a_1) \in U_1.$$

Lause 3.10 põhjal

$$A_\varphi^B = \text{diag} \left(A_{\varphi_1}^{B_1}, \dots, A_{\varphi_{p_r}}^{B_{p_r}} \right),$$

kus φ_i ($i \in \{1, \dots, p_r\}$) on lineaarteisendus

$$\varphi_i : U_i \rightarrow U_i, \quad a \mapsto \varphi(a).$$

Kuna

$$\begin{aligned} \varphi_1(\varphi^{r-1}(a_1)) &= \varphi^r(a_1) = 0, \\ \varphi_1(\varphi^{r-2}(a_1)) &= \varphi^{r-1}(a_1), \\ &\dots \\ \varphi_1(\varphi(a_1)) &= \varphi^2(a_1), \\ \varphi_1(a_1) &= \varphi(a_1), \end{aligned}$$

siis lineaarteisenduse maatriksi definitsiooni põhjal

$$A_{\varphi_1}^{B_1} = J_r(0).$$

Analoogiliselt saab veenduda, et ka kõik ülejäänud maatriksid $A_{\varphi_i}^{B_i}$ on Jordani kastid, mille peadiagonaalil on 0. Näeme, et A_φ^B on Jordani maatriks, milles on

- p_1 kasti $J_r(0)$,
- $p_2 - p_1$ kasti $J_{r-1}(0)$,
- $p_3 - p_2$ kasti $J_{r-2}(0)$ jne.

□

Teoreem 3.18 *Igal nilpotentsel ruutmaatriksil üle mistahes korpuse on olemas Jordani normaalkuju.*

TÕESTUS. Olgu $A \in \text{Mat}_n(K)$ nilpotentne matriks. Siis leidub mingi vektorruum V üle K , selle baas $e = \{e_1, \dots, e_n\}$ ja lineaarteisendus $\varphi \in \text{End}(V)$ nii, et

$$A = A_\varphi^e.$$

Kuna matriks A on nilpotentne, siis ka teisendus φ on nilpotentne. Teoreemi 3.17 põhjal leidub teisendusel φ kanooniline baas B . Seega

$$A_\varphi^B = T^{-1} A_\varphi^e T = T^{-1} A T$$

on Jordani matriks, kus $T = T^{e,B}$ on üleminekumatriks baasilt e baasile B . Kuna matriks A on sarnane Jordani matriksiga A_φ^B , siis viimane on A Jordani normaalkuju. $\square$

Teoreemi 3.17 tõestus annab meile ka meetodi nilpotentse lineaarteisenduse kanoonilise baasi leidmiseks. Olgu φ vektorruumi V nilpotentne lineaarteisendus, mis on antud oma matriksiga $A = A_\varphi^e$ mingi baasi $e = \{e_1, \dots, e_n\}$ suhtes.

- Kõigepealt leiame teisenduse φ nilpotentsuse indeksi r , mis on ühtlasi matriksi A nilpotentsuse indeks. Selleks tuleb leida vähim naturaalarv r , mille korral $A^r = 0$. See tähendab, et arvutame $A^2, A^3, \dots$ kuni A mingi aste on nullmatriks.
- Iga $k \in \{1, \dots, r-1\}$ jaoks leiame V alamruumi $H_k := \text{Ker}(\varphi^k)$ baasi. Selleks leiame sellise homogeense lineaarvõrrandisüsteemi lahendite alamruumi baasi (fundamentalsüsteemi) B_k , mille matriks on A^k .
- Vaatleme baasi B_{r-1} . Täiendame selle baasi mingite vektoritega vektorruumi V baasiks. Rakendame saadud vektoritele teisendust φ . Saadud vektorid kuuluvad alamruumi H_{r-1} . Täiendame nad H_{r-1} baasiks. Rakendame neile vektoreile jälle teisendust φ . Saadud vektorid kuuluvad alamruumi H_{r-2} . Täiendame nad H_{r-2} baasiks. Niimoodi jätkame kuni jõuame alamruumini H_1 .

3.4 Nilpotentse matriksi Jordani normaalkuju leidmine

Lihtne on veenduda, et kehtivad järgmised kaks lauset.

Lause 3.19 *Mistahes ruutmatriksite $A_1, \dots, A_m$ korral*

- $\text{rank}(\text{diag}(A_1, \dots, A_m)) = \text{rank}(A_1) + \dots + \text{rank}(A_m)$;
- $(\text{diag}(A_1, \dots, A_m))^k = \text{diag}(A_1^k, \dots, A_m^k)$.

Lause 3.20 *Kui $k, m \in \mathbb{N}$, siis*

$$\text{rank}((J_k(0))^m) = \begin{cases} k - m, & \text{kui } m < k; \\ 0, & \text{kui } m \geq k. \end{cases}$$

Meil läheb veel vaja järgmist lauset.

Lause 3.21 *Sarnaste matriksite astakud on võrdsed.*

TÕESTUS. Olgu matriksid A ja B sarnased. Siis leidub regulaarne matriks C nii, et $B = C^{-1}AC$. On teada (vt. [1], lause 4.6.6), et matriksite korrutise astak on väiksem või võrdne tegurite astakuga. Järelikult $\text{rank}(B) \leq \text{rank}(A)$. Kuna aga $CBC^{-1} = A$, siis ka $\text{rank}(A) \leq \text{rank}(B)$. Seega $\text{rank}(A) = \text{rank}(B)$. $\square$

Me teame, et n -ndat järku nilpotentse matriksi Jordani normaalkujus saavad esineda ainult Jordani kastid $J_k(0)$, kus $k \in \{1, \dots, n\}$. Kui me saaksime teada, kui palju mingit järku kaste peab olema, siis olekski Jordani normaalkuju käes. Tuleb välja, et kastide arvud saab leida teatud lineaarvõrrandisüsteemi lahendamise teel.

Teoreem 3.22 *Olgu $A \in \text{Mat}_n(K)$ nilpotentne matriks ja olgu $J(A)$ matriksi A Jordani normaalkuju. Olgu s_k , $k = 1, \dots, n$, Jordani kastide $J_k(0)$ arv matriksis $J(A)$. Siis arvud s_k saab leida lineaarvõrrandisüsteemist*

$$\begin{cases} s_1 + s_2 + s_3 + s_4 + \dots + s_n &= n - u_1 \\ s_2 + s_3 + s_4 + \dots + s_n &= u_1 - u_2 \\ s_3 + s_4 + \dots + s_n &= u_2 - u_3 \\ &\dots \\ s_n &= u_{n-1} - u_n, \end{cases}$$

kus $u_i = \text{rank}(A^i)$ iga $i = 1, \dots, n$ korral.

TÕESTUS. Kuna matriksid A ja $J(A)$ on sarnased, siis leidub regulaarne matriks C nii, et $J(A) = C^{-1}AC$. Järelikult

$$J(A)^i = (C^{-1}AC)(C^{-1}AC) \dots (C^{-1}AC) = C^{-1}A^iC,$$

s.t. A^i ja $J(A)^i$ on ka sarnased iga $i = 1, \dots, n$ korral. Et sarnaste matriksite astakud on võrdsed, siis

$$u_i = \text{rank}(A^i) = \text{rank}(J(A)^i).$$

On selge, et $n - u_1 = n - \text{rank}(J(A))$ on võrdne kõigi Jordani kastide arvuga $s_1 + s_2 + \dots + s_n$. Matriksi $J(A)$ astak on matriksi $J(A)^2$ astakust nii palju suurem, kui palju on kaste, mille järk on vähemalt 2, s.o. $u_1 - u_2 = s_2 + s_3 + \dots + s_n$. Analoogiliselt jätkates saame kätte kõik vaadeldavad võrrandid. $\square$

3.5 Piisav tingimus kanoonilise baasi olemasoluks

Hakkame nüüd vaatlema suvalisi lineaarteisendusi (mis ei pruugi olla nilpotentsed). Meie eesmärgiks selles paragrahvis on anda piisav tingimus selleks, et lineaarteisendus omaks kanoonilist baasi. See tingimus on sõnastatud polünoomide keeles.

Definitsioon 3.23 Olgu V vektorruum üle korpuse K , $\varphi \in \text{End}(V)$ ja

$$g(X) = k_0 + k_1X + k_2X^2 + \dots + k_nX^n \in K[X].$$

Polünoomi $g(X)$ **väärtuseks** kohal φ nimetatakse vektorruumi V lineaarteisendust

$$g(\varphi) = k_0 \text{id}_V + k_1\varphi + k_2\varphi^2 + \dots + k_n\varphi^n.$$

Analoogiliselt defineeritakse polünoomi $g(X)$ väärtus kohal $A \in \text{Mat}_n(K)$.

Näide 3.24 Olgu $K = \mathbb{R}$, olgu V vektorruum üle $\mathbb{R}$, $\varphi \in \text{End}(V)$ ja $g(X) = 3 - 2X + 5X^2$. Siis $g(\varphi)$ on vektorruumi V selline lineaar teisendus, mis viib vektori $a \in V$ vektoriks

$$g(\varphi)(a) = (3 \text{id}_V - 2\varphi + 5\varphi^2)(a) = 3a - 2\varphi(a) + 5\varphi(\varphi(a)).$$

Definitsioon 3.25 Olgu V vektorruum üle korpuse K ja $\varphi \in \text{End}(V)$. Nullist erinevat polünoomi $g(X) \in K[X]$ nimetatakse lineaar teisenduse φ **annulleerivaks polünoomiks**, kui $g(\varphi)$ on null teisendus. Analoogiliselt defineeritakse maatriksi $A \in \text{Mat}_n(K)$ annulleeriv polünoom.

Näide 3.26 Olgu tasandi vabavektorite vektorruumis $\mathbb{E}_2$ fikseeritud mingi ristbaas ja vaatleme lineaar teisendust φ , mis peegeldab vektoreid x -telje suhtes. Siis $\varphi^2 = \text{id}_{\mathbb{E}_2}$ ehk $\varphi^2 - \text{id}_{\mathbb{E}_2}$ on null teisendus. Siit näeme, et $g(X) = X^2 - 1 \in \mathbb{R}[X]$ on teisenduse φ annulleeriv polünoom.

Lause 3.27 Olgu V vektorruum üle korpuse K , $\varphi \in \text{End}(V)$ ning olgu A lineaar teisenduse φ maatriks mingi baasi suhtes. Polünoom $g(X) \in K[X]$ annulleerib lineaar teisenduse φ parajasti siis, kui ta annulleerib maatriksi A .

TÕESTUS. Olgu $g(X) = k_0 + k_1X + \dots + k_nX^n$, olgu e vektorruumi V baas ja $A = A_\varphi^e$. Peame näitama, et $g(A)$ on nullmaatriks. Meenutame, et kujutus

$$f : \text{End}(V) \rightarrow \text{Mat}_n(K), \quad \psi \mapsto A_\psi^e$$

on nii ringide isomorfism kui ka vektorruumide isomorfism ([1], teoreemid 4.1.12 ja 4.2.12). Järelikult

$$\begin{aligned} f(g(\varphi)) &= f(k_0 \text{id}_V + k_1\varphi + \dots + k_n\varphi^n) && (\text{def. 3.23}) \\ &= k_0f(\text{id}_V) + k_1f(\varphi) + \dots + k_nf(\varphi^n) && (f \text{ on lineaarkujutus}) \\ &= k_0f(\text{id}_V) + k_1f(\varphi) + \dots + k_nf(\varphi^n) && (f \text{ on ringide homomorfism}) \\ &= k_0E + k_1A + \dots + k_nA^n && (f \text{ def.}) \\ &= g(A). && (\text{def. 3.23}) \end{aligned}$$

Et f on muuhulgas injektiivne lineaarkujutus, siis

$$g(\varphi) = 0 \text{ vektorruumis } \text{End}(V) \iff f(g(\varphi)) = 0 \text{ vektorruumis } \text{Mat}_n(K) \iff g(A) = 0.$$

□

Lause 3.28 Igal ruutmaatriksil üle korpuse on olemas annulleeriv polünoom. Iga vektorruumi igal lineaar teisendusel on olemas annulleeriv polünoom.

TÕESTUS. Tõestame selle väite maatriksite jaoks. Vastav tulemus lineaar teisenduste kohta järel dub siis lausest 3.27.

Olgu $A \in \text{Mat}_n(K)$. Teatavasti $\dim(\text{Mat}_n(K)) = n^2$. Järelikult vektorruumi $\text{Mat}_n(K)$ vektorite süsteem

$$E = A^0, A^1, A^2, \dots, A^{n^2}$$

on lineaarselt sõltuv, mis tähendab, et leiduvad skalaarid $k_0, k_1, \dots, k_{n^2} \in K$, mis ei ole kõik korraga nullid, nii et

$$k_0E + k_1A + k_2A^2 + \dots + k_{n^2}A^{n^2} = 0.$$

See tähendab, et $g(X) = k_0 + k_1X + k_2X^2 + \dots + k_{n^2}X^{n^2} \in K[X]$ on maatriksi A annulleeriv polünoom. □

Lause 3.29 Olgu V vektorruum üle korpuse K ning eeldame, et lineaarteisenduse $\varphi \in \text{End}(V)$ annulleeriv polünoom $g(X) \in K[X]$ lahutub paarikaupa ühistegurita polünoomide $g_1(X), \dots, g_m(X)$ korrutiseks:

$$g(X) = g_1(X) \dots g_m(X).$$

Siis

$$V = \text{Ker}(g_1(\varphi)) \dot{+} \dots \dot{+} \text{Ker}(g_m(\varphi)),$$

kusjuures otseliidetavad on φ -invariantseid alamruumid.

TÕESTUS. Tõestame lause vaid juhul, kui $m = 2$ (üldjuhul on tõestus analoogiline). Niisiis eeldame, et $g(X) = g_1(X)g_2(X)$, $\text{SÜT}(g_1(X), g_2(X)) = 1$ ja $g(\varphi)$ on nullteisendus. Siis leiduvad polünoomid $u(X), v(X) \in K[X]$ nii, et

$$1 = g_1(X)u(X) + g_2(X)v(X)$$

(vaata [1], lause 6.13.3). Järelikult $\text{id}_V = g_1(\varphi)u(\varphi) + g_2(\varphi)v(\varphi)$ ehk iga $a \in V$ korral

$$a = (g_1(\varphi) \circ u(\varphi))(a) + (g_2(\varphi) \circ v(\varphi))(a). \quad (17)$$

Kuna

$$g_2(\varphi)((g_1(\varphi) \circ u(\varphi))(a)) = (g_2(\varphi) \circ g_1(\varphi))(u(\varphi)(a)) = (g(\varphi))(u(\varphi)(a)) = 0(u(\varphi)(a)) = 0,$$

siis $(g_1(\varphi) \circ u(\varphi))(a) \in \text{Ker}(g_2(\varphi))$. Analoogiliselt $(g_2(\varphi) \circ v(\varphi))(a) \in \text{Ker}(g_1(\varphi))$. Seega võrdust (17) arvestades saame, et

$$V = \text{Ker}(g_1(\varphi)) + \text{Ker}(g_2(\varphi)).$$

Veendume, et see summa on otsesumma. Selleks oletame, et $b \in \text{Ker}(g_1(\varphi)) \cap \text{Ker}(g_2(\varphi))$. Kuna $u(X)g_1(X) = g_1(X)u(X)$, siis ka $g_1(\varphi) \circ u(\varphi) = u(\varphi) \circ g_1(\varphi)$. Analoogiliselt kehtib võrdus $g_2(\varphi) \circ v(\varphi) = v(\varphi) \circ g_2(\varphi)$. Järelikult

$$\begin{aligned} b &= (g_1(\varphi) \circ u(\varphi))(b) + (g_2(\varphi) \circ v(\varphi))(b) = (u(\varphi) \circ g_1(\varphi))(b) + (v(\varphi) \circ g_2(\varphi))(b) \\ &= u(\varphi)(g_1(\varphi)(b)) + v(\varphi)(g_2(\varphi)(b)) = u(\varphi)(0) + v(\varphi)(0) = 0 + 0 = 0. \end{aligned}$$

Seega $\text{Ker}(g_1(\varphi)) \cap \text{Ker}(g_2(\varphi)) = \{0\}$ ja

$$V = \text{Ker}(g_1(\varphi)) \dot{+} \text{Ker}(g_2(\varphi)).$$

Näitamaks, et $\text{Ker}(g_i(\varphi))$ on φ -invariantne, võtame $a \in \text{Ker}(g_i(\varphi))$. Siis $g_i(\varphi)(a) = 0$ ja

$$g_i(\varphi)(\varphi(a)) = (g_i(\varphi) \circ \varphi)(a) = (\varphi \circ g_i(\varphi))(a) = \varphi(g_i(\varphi)(a)) = \varphi(0) = 0.$$

Seega $\varphi(a) \in \text{Ker}(g_i(\varphi))$. □

Järgmine teoreem annab piisava tingimuse selleks, et lineaarteisendusel leiduks kanooniline baas.

Teoreem 3.30 Kui V on vektorruum üle korpuse K ja lineaarteisendusel $\varphi \in \text{End}(V)$ leidub selline annulleeriv polünoom, mis lahutub lineaartegurite korrutiseks, siis on lineaarteisendusel φ olemas kanooniline baas.

TÕESTUS. Olgu $g_1(X)$ lineaarteisenduse annulleeriv polünoom, mis lahutub n lineaarteguri korrutiseks ($n = \deg(g_1(X))$), ja olgu $a \in K$ tema pealiikme kordaja. Siis polünoom $g(X) := a^{-1} \cdot g_1(X)$ on unitaarne annulleeriv polünoom φ jaoks, kusjuures polünoomidel $g_1(X)$ ja $g(X)$ on samad juured ja sama aste. Seega saame unitaarse polünoomi $g(X)$ esitada kujul

$$g(X) = (X - \lambda_1)^{r_1} \cdot \dots \cdot (X - \lambda_m)^{r_m},$$

kus $r_1, \dots, r_m \in \mathbb{N}$ ja elemendid $\lambda_1, \dots, \lambda_m \in K$ on paarikaupa erinevad. Siis on selge, et $S\ddot{U}T(X - \lambda_i, X - \lambda_j) = 1$, kui $i \neq j$. Lause 3.29 põhjal

$$V = \text{Ker}(\varphi - \lambda_1 \text{id}_V)^{r_1} \dot{+} \dots \dot{+} \text{Ker}(\varphi - \lambda_m \text{id}_V)^{r_m},$$

kusjuures otseliidetavad on φ -invariantsed alamruumid. Tähistame

$$U_i := \text{Ker}(\varphi - \lambda_i \text{id}_V)^{r_i},$$

$i = 1, \dots, m$. Kui $a \in U_i$, siis ka $\varphi(a) \in U_i$, $\lambda_i a \in U_i$ ja $\varphi(a) - \lambda_i a \in U_i$. Seega võib vaadelda vektorruumi U_i lineaarteisendusi

$$\begin{aligned} \varphi_{U_i} &: a \mapsto \varphi(a), \\ (\lambda_i \text{id}_V)_{U_i} &: a \mapsto \lambda_i a, \\ (\varphi - \lambda_i \text{id}_V)_{U_i} &: a \mapsto \varphi(a) - \lambda_i a. \end{aligned}$$

Kuna iga $a \in U_i$ korral

$$((\varphi - \lambda_i \text{id}_V)_{U_i})^{r_i}(a) = (\varphi - \lambda_i \text{id}_V)^{r_i}(a) = 0,$$

siis $((\varphi - \lambda_i \text{id}_V)_{U_i})^{r_i}$ on nullteisendus. Seega lineaarteisendus $(\varphi - \lambda_i \text{id}_V)_{U_i} \in \text{End}(U_i)$ on nilpotentne. Teoreemi 3.17 põhjal leidub selle teisenduse jaoks kanooniline baas B_i vektorruumis U_i . Et $\varphi = (\varphi - \lambda_i \text{id}_V) + \lambda_i 1_V$, siis ka

$$\varphi_{U_i} = (\varphi - \lambda_i \text{id}_V)_{U_i} + (\lambda_i \text{id}_V)_{U_i}$$

ja

$$A_{\varphi_{U_i}}^{B_i} = A_{(\varphi - \lambda_i \text{id}_V)_{U_i}}^{B_i} + A_{(\lambda_i \text{id}_V)_{U_i}}^{B_i}.$$

Teame, et $A_{(\varphi - \lambda_i \text{id}_V)_{U_i}}^{B_i}$ on Jordani maatriks, mille peadiagonaalil on nullid, ja $A_{(\lambda_i \text{id}_V)_{U_i}}^{B_i}$ on diagonaalmaatriks, mille kõik peadiagonaali elemendid on võrdsed elemendiga λ_i . Järelikult $A_{\varphi_{U_i}}^{B_i}$ on Jordani maatriks, mille peadiagonaalil on kõikjal λ_i . Tähistades

$$B := B_1 \cup \dots \cup B_m$$

võime lause 3.10 põhjal väita, et

$$A_{\varphi}^B = \text{diag} \left(A_{\varphi_{U_1}}^{B_1}, \dots, A_{\varphi_{U_m}}^{B_m} \right),$$

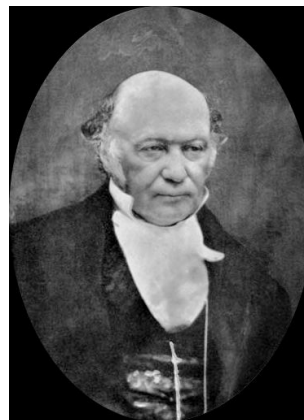
mis on Jordani maatriks. Seega B on teisenduse φ kanooniline baas. $\square$

Järeldus 3.31 *Olgu V vektorruum üle korpuse $\mathbb{C}$. Siis igal lineaarteisendusel $\varphi \in \text{End}(V)$ leidub kanooniline baas.*

TÕESTUS. Tänu lausele 3.28 leidub lineaarteisendusel φ annulleeriv polünoom $g(X) \in \mathbb{C}[X]$. Vastavalt järeldusele 2.31 leidub sellel polünoomil s juurt, kus $s = \deg(g(X))$. Seega polünoom $g(X)$ esitub s lineaarteguri korrutisena ([1], lause 7.1.8) ja kanooniline baas φ jaoks leidub teoreemi 3.30 põhjal. $\square$

3.6 Cayley-Hamiltoni teoreem

Selles paragrahvis on meie eesmärgiks tõestada tulemus, mida tänapäeval tuntakse Cayley-Hamiltoni teoreemina, ja mis ütleb, et lineaarteisenduse karakteristik polünoom on tema annulleeriv polünoom. Inglise matemaatik Arthur Cayley (1821–1895) ja iiri matemaatik William Rowan Hamilton (1805–1865) tõestasid selle väite teatud erijuhtude jaoks, üldjuhul andis esimese tõestuse saksa matemaatik Ferdinand Georg Frobenius aastal 1878.



Georg Frobenius ja William Rowan Hamilton

Eespool nägime, et kui lineaarteisendusel leidub mingi n -nda astme annulleeriv polünoom, siis tal leidub ka unitaarne n -nda astme annulleeriv polünoom.

Definitsioon 3.32 Lineaarteisenduse **minimaalseks polünoomiks** nimetatakse selle lineaarteisenduse minimaalse astmega unitaarset annulleerivat polünoomi. Analoogiliselt defineeritakse ruutmaatriksi minimaalne polünoom.

Tänu lausele 3.28 on igal lineaarteisendusel olemas nii annulleeriv kui ka minimaalne polünoom.

Lause 3.33 Olgu V vektorruum üle korpuse K ja $\varphi \in \text{End}(V)$. Nullist erinev polünoom $g(X)$ on lineaarteisenduse φ annulleeriv polünoom parajasti siis, kui ta jagub selle lineaarteisenduse minimaalse polünoomiga. Sama kehtib ruutmaatriksite jaoks üle korpuse K .

TÕESTUS. Tõestame väite lineaarteisenduste jaoks. Maatriksite korral on tõestus analoogiline.

TARVILIKKUS. Olgu $g(X) \in K[X]$ lineaarteisenduse φ annulleeriv polünoom. Jagades polünoomi $g(X)$ jäägiga teisenduse φ minimaalse polünoomiga $m(X)$ saame leida sellised polünoomid $q(X), r(X) \in K[X]$, et

$$g(X) = m(X)q(X) + r(X) \quad \text{ja} \quad \deg(r(X)) < \deg(m(X)).$$

Järelikult

$$0 = g(\varphi) = m(\varphi)q(\varphi) + r(\varphi) = 0 \cdot q(\varphi) + r(\varphi) = r(\varphi).$$

Kui $r(X)$ ei oleks nullpolünoom, siis ta oleks annulleeriv polünoom, mille aste on väiksem $m(X)$ astmest. See annaks vastuolu sellega, et $m(X)$ on minimaalne polünoom. Järelikult $r(X)$ peab olema nullpolünoom, $r(X) = 0$. See aga tähendab, et $g(X) = m(X)q(X)$ ehk polünoom $g(X)$ jagub polünoomiga $m(X)$.

PIISAVUS. Oletame, et mingi polünoom $g(X) \in K[X]$ jagub teisenduse φ minimaalse polünoomiga $m(X)$, s.t. $g(X) = m(X)q(X)$, kus $q(X) \in K[X]$. Siis

$$g(\varphi) = m(\varphi)q(\varphi) = 0 \cdot q(\varphi) = 0.$$

□

Järeldus 3.34 *Igal lineaarteisendusel ja igal ruutmaatriksil üle korpuse leidub üheselt määratud minimaalne polünoom.*

TÕESTUS. Olgu $m_1(X)$ ja $m_2(X)$ lineaarteisenduse $\varphi \in \text{End}(V)$ minimaalsed polünoomid. Siis peab neil olema sama aste. Kuna $m_1(\varphi) = 0$ ja $m_2(X)$ on minimaalne polünoom, siis lause 3.33 põhjal $m_2(X) \mid m_1(X)$. Et nende polünoomide aste on sama, siis peab leiduma $k \in K$ nii, et $km_2(X) = m_1(X)$. Kuna $m_1(X)$ ja $m_2(X)$ on unitaarsed polünoomid, siis $k = 1$ ehk $m_1(X) = m_2(X)$. Maatriksite jaoks on tõestus täpselt samasugune. $\square$

Lause 3.35 *Olgu V vektorruum üle korpuse K , $\varphi \in \text{End}(V)$ ning olgu A lineaarteisenduse φ maatriks mingi baasi suhtes. Polünoom $f(X) \in K[X]$ on lineaarteisenduse φ minimaalne polünoom parajasti siis, kui ta on maatriksi A minimaalne polünoom.*

TÕESTUS. Lause 3.27 põhjal on teisendusel φ ja maatriksil A samad annulleerivad polünoomid, s.t.

$$\{g(X) \in K[X] \setminus \{0\} \mid g(\varphi) = 0\} = \{g(X) \in K[X] \setminus \{0\} \mid g(A) = 0\}.$$

Järelduse 3.34 põhjal peab mõlemas hulgas leiduma täpselt üks minimaalse astmega unitaarne polünoom. Seega φ minimaalne polünoom võrdub A minimaalse polünoomiga. $\square$

Järeldus 3.36 *Sarnastel maatriksitel on samad annulleerivad polünoomid ja võrdsed minimaalsed polünoomid.*

TÕESTUS. Olgu $A, B \in \text{Mat}_n(K)$ sarnased maatriksid. Siis (vt. [1], järeldus 8.2.6) leidub vektorruum V üle korpuse K , selle baasid e ja e' ning lineaarteisendus $\varphi \in \text{End}(V)$ nii, et $A = A_\varphi^e$ ja $B = A_\varphi^{e'}$. Lause 3.27 põhjal

$$\begin{aligned} \{g(X) \in K[X] \setminus \{0\} \mid g(A) = 0\} &= \{g(X) \in K[X] \setminus \{0\} \mid g(\varphi) = 0\} \\ &= \{g(X) \in K[X] \setminus \{0\} \mid g(B) = 0\}, \end{aligned}$$

seega A ja B omavad samu annulleerivaid polünoome. Järelduse 3.34 põhjal leidub esimeses ja kolmandas hulgas täpselt üks minimaalse astmega unitaarne polünoom. Järelikult maatriksite A ja B minimaalsed polünoomid on võrdsed. $\square$

Lemma 3.37 *Olgu K korpus, $\lambda \in K$ ja $n \in \mathbb{N}$. Polünoomi $(X - \lambda)^n$ unitaarsed jagavad polünoomide ringis $K[X]$ on kujul $(X - \lambda)^k$, kus $k \leq n$.*

TÕESTUS. Olgu $f(X)$ polünoomi $(X - \lambda)^n$ unitaarne jagaja ringis $K[X]$. Siis leidub polünoom $h(X) \in K[X]$ nii, et

$$f(X) \cdot h(X) = (X - \lambda)^n.$$

Olgu

$$k \in \mathbb{N} \cup \{0\} \text{ suurim selline arv, et } (X - \lambda)^k \mid f(X), \quad (18)$$

$$l \in \mathbb{N} \cup \{0\} \text{ suurim selline arv, et } (X - \lambda)^l \mid h(X). \quad (19)$$

Siis

$$k + l \leq \deg(f(X)) + \deg(h(X)) = \deg((X - \lambda)^n) = n$$

ning leiduvad polünoomid $f_1(X), h_1(X) \in K[X]$ nii, et $(X - \lambda)^k \cdot f_1(X) = f(X)$ ja $(X - \lambda)^l \cdot h_1(X) = h(X)$. Järelikult

$$(X - \lambda)^{k+l} \cdot f_1(X) \cdot h_1(X) = (X - \lambda)^n.$$

Polünoomide ring $K[X]$ on nullitegureita ja iga nullitegureita ring on taandamisega. Seega viimasest võrdusest saame võrduse

$$f_1(X) \cdot h_1(X) = (X - \lambda)^{n-k-l}.$$

Oletame vastuväiteliselt, et $k + l < n$ ehk $n - k - l > 0$. Siis

$$0 = (\lambda - \lambda)^{n-k-l} = f_1(\lambda) \cdot h_1(\lambda).$$

Kuna korpuses K ei ole nullitegureid, siis kas $f_1(\lambda) = 0$ või $h_1(\lambda) = 0$. Kui $f_1(\lambda) = 0$, siis λ on polünoomi $f_1(X)$ juur. Siis aga $(X - \lambda) \mid f_1(X)$ ja $(X - \lambda)^{k+1} \mid f(X)$, mis on vastuolus eeldusega (18). Analoogiliselt saame vastuolu, kui $h_1(\lambda) = 0$. Seega

$$k + l = n = \deg(f(X)) + \deg(h(X)).$$

Kuna $k \leq \deg(f(X))$ ja $l \leq \deg(h(X))$, siis tegelikult peavad kehtima võrdused $k = \deg(f(X))$ ja $l = \deg(h(X))$. Tänu unitaarsusele $(X - \lambda)^k = f(X)$. $\square$

Lause 3.38 Jordani kasti $J_n(\lambda) \in \text{Mat}_n(K)$ minimaalne polünoom on $(X - \lambda)^n \in K[X]$, mis märgi täpsusega on võrdne selle kasti karakteristliku polünoomiga.

TÕESTUS. Vahetu maatriksite korrutamine annab, et $J_n(0)^n$ on nullmaatriks. Kuna

$$0 = J_n(0)^n = (J_n(\lambda) - \lambda E)^n,$$

siis $(X - \lambda)^n \in K[X]$ on maatriksi $J_n(\lambda)$ annuleeriv polünoom. Tänu lausele 3.33 jagub see polünoom maatriksi $J_n(\lambda)$ minimaalse polünoomiga. Lemma 3.37 tõttu on maatriksi $J_n(\lambda)$ minimaalne polünoom kujul $(X - \lambda)^k$, kus $k \leq n$. Kui $k < n$, siis $J_n(0)^k \neq 0$, seega peab kehtima võrdus $k = n$. Niisiis $J_n(\lambda)$ minimaalne polünoom on $(X - \lambda)^n$. Teisest küljest maatriksi $J_n(\lambda)$ karakteristlik polünoom (muutuja X suhtes) on

$$\begin{aligned} \det(J_n(\lambda) - XE) &= \begin{vmatrix} \lambda - X & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda - X & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda - X & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda - X & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda - X \end{vmatrix} \\ &= (\lambda - X)^n = ((-1)(X - \lambda))^n = (-1)^n (X - \lambda)^n. \end{aligned}$$

$\square$

Lemma 3.39 Kui $A = \text{diag}(A_1, \dots, A_s)$ on plokk-diagonaalne maatriks üle korpuse K ja $g(X) \in K[X]$, siis

$$g(A) = \text{diag}(g(A_1), \dots, g(A_s)).$$

TÕESTUS. Maatriksit A astendades näeme, et

$$(\forall r \in \mathbb{N}) \quad A^r = \text{diag}(A_1^r, \dots, A_s^r).$$

Samuti on selge, et iga $k \in K$ korral $kA = \text{diag}(kA_1, \dots, kA_s)$. Kui vaadeldav polünoom on $g(X) = b_n X^n + \dots + b_1 X + b_0$, siis

$$\begin{aligned} g(A) &= b_n A^n + \dots + b_1 A + b_0 E \\ &= \text{diag}(b_n A_1^n, \dots, b_n A_s^n) + \dots + \text{diag}(b_1 A_1, \dots, b_1 A_s) + \text{diag}(b_0 E_1, \dots, b_0 E_s) \\ &= \text{diag}(b_n A_1^n + \dots + b_1 A_1 + b_0 E_1, \dots, b_n A_s^n + \dots + b_1 A_s + b_0 E_s) \\ &= \text{diag}(g(A_1), \dots, g(A_s)), \end{aligned}$$

kus $E_1, \dots, E_s$ on sobivat järku ühikmaatriksid. □

Lause 3.40 *Jordani maatriksi minimaalne polünoom on tema kastide minimaalsete polünoomide vähim ühiskordne.*

TÕESTUS. Vaatleme Jordani maatriksit

$$J = \text{diag}(J_1, \dots, J_s),$$

kus $J_1, \dots, J_s$ on Jordani kastid. Kui $g(X) \in K[X]$, siis

$$g(J) = \text{diag}(g(J_1), \dots, g(J_s)).$$

Seega $g(X)$ on maatriksi J annulleeriv polünoom parajasti siis, kui $g(X)$ on iga $i \in \{1, \dots, s\}$ korral maatriksi J_i annulleeriv polünoom. Olgu $m(X)$ maatriksi J minimaalne polünoom ja $m_i(X)$, $i \in \{1, \dots, s\}$, maatriksi J_i minimaalne polünoom. Siis $m(X)$ on ka iga maatriksi J_i annulleeriv polünoom. Lause 3.33 põhjal $m_i(X) \mid m(X)$ iga $i \in \{1, \dots, s\}$ korral, mis tähendab, et $m(X)$ on polünoomide $m_1(X), \dots, m_s(X)$ ühine kordne.

Olgu nüüd $p(X) \in K[X]$ selline polünoom, et $m_i(X) \mid p(X)$ iga $i \in \{1, \dots, s\}$ korral. Siis $p(X)$ on maatriksite $J_1, \dots, J_s$ annulleeriv polünoom. Seega $p(X)$ on maatriksi J annulleeriv polünoom ja $m(X) \mid p(X)$. Sellega oleme tõestanud, et $m(X)$ on polünoomide $m_1(X), \dots, m_s(X)$ vähim ühiskordne. □

Teoreem 3.41 (Cayley-Hamiltoni teoreem) *Lineaarteisenduse karakteristlik polünoom on tema annulleeriv polünoom.*

TÕESTUS. Tõestame samaväärse väite, et iga maatriksi $A \in \text{Mat}_n(K)$ karakteristlik polünoom $\det(A - XE)$ annulleerib selle maatriksi.

Olgu K korpus, $A \in \text{Mat}_n(K)$ ja olgu $g(X) \in K[X]$ maatriksi A annulleeriv polünoom (selline polünoom leidub tänu lausele 3.28). Teoreemi 2.23 põhjal leidub selline korpus $\overline{K}$, et K on $\overline{K}$ alamkorpus ja $g(X)$ lahutub lineaarpolünoomide korrutiseks ringis $\overline{K}[X]$. Teoreemi 3.30 analoog maatriksite jaoks ütleb, et leidub Jordani maatriks $J \in \text{Mat}_n(\overline{K})$ nii, et maatriksid A ja J on sarnased. Järelikult on neil samad karakteristlikud polünoomid ([1], lause 8.2.9) ja samad annulleerivad polünoomid (tänu lausele 3.27). Seega tõestuse lõpetamiseks piisab näidata, et J karakteristlik polünoom annulleerib maatriksi J .

Olgu

$$J = \text{diag}(J_1, \dots, J_s),$$

kus $J_1, \dots, J_s$ on Jordani kastid. Siis maatriksi J karakteristlik polünoom on

$$\det(J - XE) = \det(J_1 - XE) \cdot \dots \cdot \det(J_s - XE).$$

Rakendades lemmat 3.39 olukorras, kus $g(X) := \det(J - XE)$ näeme, et

$$g(J) = \text{diag}(g(J_1), \dots, g(J_s)).$$

Lause 3.38 põhjal iga $i \in \{1, \dots, s\}$ korral Jordani kasti J_i karakteristlik polünoom $g_i(X) = \det(J_i - XE)$ annuleerib selle Jordani kasti, s.t. $g_i(J_i) = 0$. Kuna

$$g(X) = g_1(X) \cdot \dots \cdot g_s(X),$$

siis $g(J_1) = \dots = g(J_s) = 0$. Seega $g(J)$ on plokk-diagonaalne maatriks, mille kõik blokid on nullmaatriksid. Seega J karakteristlik polünoom annuleerib maatriksi J . $\square$

Teoreem 3.42 *Olgu $V \neq \{0\}$ vektorruum üle korpuse K ja $\varphi \in \text{End}(V)$. Lineaarteisendusel φ leidub kanooniline baas parajasti siis, kui tema karakteristlik polünoom lahutub lineaarpolünoomide korrutiseks üle korpuse K .*

TÕESTUS. TARVILIKKUS. Oletame, et lineaarteisendusel φ leidub kanooniline baas, mille suhtes tema maatriks on Jordani maatriks

$$J = \text{diag}(J_{n_1}(\lambda_1), \dots, J_{n_s}(\lambda_s)).$$

Nii teisenduse φ kui maatriksi J karakteristlik polünoom on siis

$$\det(J - XE) = (\lambda_1 - X)^{n_1} \cdot \dots \cdot (\lambda_s - X)^{n_s},$$

mis on lineaarpolünoomide korrutis.

PIISAVUS. Kui lineaarteisenduse φ karakteristlik polünoom lahutub lineaartegurite korrutiseks, siis Cayley-Hamiltoni teoreemi tõttu on teisendusel φ olemas lineaartegureiks lahutuv annuleeriv polünoom. Seega teoreemi 3.30 tõttu on tal olemas kanooniline baas. $\square$

Järeldus 3.43 *Kui $V \neq \{0\}$ on vektorruum üle algebralise kinnise korpuse, siis selle vektorruumi iga lineaarteisenduse jaoks leidub kanooniline baas.*

3.7 Kanoonilise baasi ja Jordani normaalkuju leidmine

Olgu φ vektorruumi V lineaarteisendus, mis on antud oma maatriksiga $A = A_\varphi^e$ mingi baasi $e = \{e_1, \dots, e_n\}$ suhtes.

- Kõigepealt leiame maatriksi A karakteristliku polünoomi $f(X) = \det(A - XE)$ ja selle juured (A omaväärtused). Kanooniline baas leidub siis ja ainult siis, kui $f(X)$ juurte arv, arvestades kordsusi, võrdub $f(X)$ astmega, s.t. vektorruumi V mõõtmega n . Sel juhul on $f(X)$ esitatav kujul

$$f(X) = (\lambda_1 - X)^{n_1} \cdot \dots \cdot (\lambda_s - X)^{n_s}.$$

- Iga $i \in \{1, \dots, s\}$ korral tähistame $U_i := \text{Ker}(\varphi - \lambda_i 1_V)^{n_i}$ ja $\psi_i := (\varphi - \lambda_i 1_V)_{U_i}$. Siis ψ_i on vektorruumi U_i nilpotentne lineaarteisendus ja $V = U_1 \dot{+} \dots \dot{+} U_s$. Nilpotentsus tuleb sellest, et iga $a \in U_i$ korral

$$\psi_i^{n_i}(a) = (\varphi - \lambda_i 1_V)^{n_i}(a) = 0.$$

- Leiame iga teisenduse ψ_i , $i \in \{1, \dots, s\}$, jaoks kanoonilise baasi B_i . Siis nende kanooniliste baaside ühend $B = B_1 \cup \dots \cup B_s$ ongi φ kanooniline baas.

Tõepoolest, kuna $A_{\psi_i}^{B_i}$ on Jordani maatriks, mille peadiagonaalil on nullid, ja $\varphi_{U_i} = \psi_i + (\lambda_i 1_V)_{U_i}$, siis

$$\begin{aligned} A_{\varphi_{U_i}}^{B_i} &= A_{\psi_i}^{B_i} + A_{(\lambda_i 1_V)_{U_i}}^{B_i} = A_{\psi_i}^{B_i} + \lambda_i E \\ &= \begin{pmatrix} 0 & ? & & 0 \\ & 0 & \ddots & \\ & & \ddots & ? \\ 0 & & & 0 \end{pmatrix} + \begin{pmatrix} \lambda_i & 0 & & 0 \\ & \lambda_i & \ddots & \\ & & \ddots & 0 \\ 0 & & & \lambda_i \end{pmatrix} = \begin{pmatrix} \lambda_i & ? & & 0 \\ & \lambda_i & \ddots & \\ & & \ddots & ? \\ 0 & & & \lambda_i \end{pmatrix} \end{aligned}$$

on Jordani maatriks, mille peadiagonaalil on kõikjal λ_i . (Siin iga küsimärgi asemel on kas 1 või 0, sõltuvalt sellest, millised on Jordani kastide järgud.) Järelikult

$$A_{\varphi}^B = \text{diag} \left(A_{\varphi_{U_1}}^{B_1}, \dots, A_{\varphi_{U_s}}^{B_s} \right) = \begin{pmatrix} \boxed{A_{\varphi_{U_1}}^{B_1}} & & & 0 \\ & \boxed{A_{\varphi_{U_2}}^{B_2}} & & \\ & & \ddots & \\ 0 & & & \boxed{A_{\varphi_{U_s}}^{B_s}} \end{pmatrix}$$

on Jordani maatriks ja seega B on φ kanooniline baas.

Kui on vaja leida ainult ruutmaatriksi A Jordani normaalkuju $J(A)$ (ja meid ei huvita C , mille korral $J(A) = C^{-1}AC$), siis tuleb iga i , $i \in \{1, \dots, s\}$, jaoks koostada ja lahendada lineaarvõrrandisüsteem, mis on sarnane sellele, mis on antud teoreemis 3.22. Selleks arvutame kõigepealt iga $j = 1, \dots, n_i$ korral välja arvu

$$u_j = \text{rank} \left((A - \lambda_i E)^j \right).$$

Olgu s_k Jordani kastide $J_k(\lambda_i)$ arv maatriksis $J(A)$. Siis arvud s_k saab leida lineaarvõrrandisüsteemist

$$\begin{cases} s_1 + s_2 + s_3 + s_4 + \dots + s_{n_i} &= n - u_1 \\ s_2 + s_3 + s_4 + \dots + s_{n_i} &= u_1 - u_2 \\ s_3 + s_4 + \dots + s_{n_i} &= u_2 - u_3 \\ &\dots \\ s_{n_i} &= u_{n_i-1} - u_{n_i}. \end{cases}$$

Selle väite saab tõestada analoogiliselt teoreemiga 3.22. Muuhulgas saab näidata, et

$$u_j = \text{rank} \left((A - \lambda_i E)^j \right) = \text{rank} \left((J(A) - \lambda_i E)^j \right).$$

Range tõestuse andmise asemel illustreerime seda väidet järgmise näite abil.

Näide 3.44 Olgu $K = \mathbb{R}$, $n = 6$, $\lambda_1 = 2$, $\lambda_2 = 7$ ja

$$J(A) = \begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ 0 & 2 \end{matrix}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{matrix}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{7} \end{pmatrix}.$$

Vaatleme omaväärtusele 2 vastavate kastide arve

$$s_1 = 0, \quad s_2 = 1, \quad s_3 = 1, \quad s_4 = 0, \quad s_5 = 0.$$

Näeme, et peadiagonaalist 2 lahutamisel tekitab iga omaväärtusele 2 vastav Jordani kast juurde ühe nullrea ja seega astak kahaneb kõigi Jordani kastide arvu $s_1 + \dots + s_5$ võrra:

$$u_1 = \text{rank} \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{matrix}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{5} \end{pmatrix} = 4 = 6 - 0 - 1 - 1 - 0 - 0 = n - s_1 - \dots - s_5.$$

Ruutu võttes saame

$$u_2 = \text{rank} \begin{pmatrix} \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{5^2} \end{pmatrix} = 2 = u_1 - s_2 - s_3 - s_4 - s_5,$$

s.t. iga kast, mille järk on ≥ 2 , vähendab eelmise maatriksi astakut 1 võrra. Kuubi korral

$$u_3 = \text{rank} \begin{pmatrix} \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{5^3} \end{pmatrix} = 1 = u_2 - s_3 - s_4 - s_5.$$

Antud olukorras $1 = u_3 = u_4 = u_5$, aga üldjuhul peaksime samamoodi jätkama. Siit on näha, et arvud $s_1, \dots, s_5$ tõepoolest rahuldavad eespool toodud lineaarvõrrandisüsteemi.

4 Funktsionaalid ja vormid

4.1 Lineaarsed funktsionaalid ja lineaarvormid

Meenutame, et iga korpust K võib loomulikult viisil vaadelda vektorruumina üle iseenda.

Definitsioon 4.1 Olgu V vektorruum üle korpuse K . Lineaarkujutust vektorruumist V korpusesse K nimetatakse **lineaarseks funktsionaaliks** vektorruumil V .

Kõigi lineaarsete funktsionaalide hulka vektorruumil V üle korpuse K tähistame sümboliga $\text{Hom}(V, K)$ või lühidalt V^* . Sellel hulgal saab tehted defineerida niiöelda punkti-
viisiliselt:

$$\begin{aligned}(\varphi + \psi)(a) &:= \varphi(a) + \psi(a), \\ (k\varphi)(a) &:= k\varphi(a)\end{aligned}$$

mistahes $\varphi, \psi \in \text{Hom}(V, K)$ ja $a \in V$ korral. On teada, et nende tehete suhtes on $\text{Hom}(V, K)$ vektorruum ([1], lause 2.5.24).

Definitsioon 4.2 Vektorruumi $\text{Hom}(V, K)$ nimetatakse vektorruumi V **kaasruumiks**.

Lineaarsed funktsionaalid mängivad tähtsat rolli näiteks geomeetrias, funktsionaalanalüüsis ja kvantmehaanikas.

Näide 4.3 1. Kui $\vec{a} \in \mathbb{E}_3$ on mingi fikseeritud vabavektor, siis kujutus

$$\varphi : \mathbb{E}_3 \rightarrow \mathbb{R}, \quad \vec{x} \mapsto \langle \vec{x}, \vec{a} \rangle,$$

on lineaarne funktsionaal vektorruumil $\mathbb{E}_3$.

2. Kui $a < b$ on mingid fikseeritud reaalarvud, siis kujutus

$$\varphi : C[a, b] \rightarrow \mathbb{R}, \quad f(x) \mapsto \int_a^b f(x) dx,$$

on lineaarne funktsionaal lõigus $[a, b]$ pidevate funktsioonide vektorruumil $C[a, b]$.

3. Kui K on kommutatiivne korpus, $a \in K$ üks fikseeritud element ja $K[X]$ on polünoomide vektorruum, siis kujutus

$$\varphi : K[X] \rightarrow K, \quad f(X) \mapsto f(a),$$

on lineaarne funktsionaal vektorruumil $K[X]$.

Definitsioon 4.4 Homogeenseid mitme muutuja polünoome nimetatakse **vormideks**. Esimese astme vorme nimetatakse **lineaarvormideks**, teise astme vorme **ruutvormideks**.

Näide 4.5 1. Polünoom $3X - 2Y + Z \in \mathbb{R}[X, Y, Z]$ on lineaarvorm.

2. Polünoom $5X^2 + Y^2 - 3Z^2 + XZ - 6YZ \in \mathbb{R}[X, Y, Z]$ on ruutvorm.

Kui $e = \{e_1, \dots, e_n\}$ on mingi baas vektorruumis V üle korpuse K , siis iga vektor $x \in V$ avaldub üheselt kujul $x = x_1e_1 + \dots + x_ne_n$, kus $x_1, \dots, x_n$ on korpuse K elemendid, mida nimetatakse vektori x **koordinaatideks** baasi e suhtes ([1], lause 3.2.12). Tähistame

$$\bar{x}_e := \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} \in \text{Mat}_{n,1}(K)$$

ja nimetame seda üheveerulist maatriksit vektori x **koordinaatide veeruks** baasi e suhtes. Olgu φ lineaarne funktsionaal vektorruumil V . Tähistades

$$\varphi(e_i) =: a_i \in K$$

võime kirjutada

$$\varphi(x) = \varphi\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i \varphi(e_i) = \sum_{i=1}^n a_i x_i. \quad (20)$$

Definitsioon 4.6 Homogeenset polünoomi $\sum_{i=1}^n a_i X_i$ nimetatakse lineaarsele funktsionaalile φ vastavaks **lineaarvormiks** baasi e suhtes.

Lause 4.7 Olgu V n -mõõtmeline vektorruum üle korpuse K . Vektorruumi V baasi fikseerimine tekitab üksühese vastavuse selle vektorruumi lineaarsete funktsionaalide ja n muutuja lineaarvormide vahel, mille kordajad on korpusest K .

TÕESTUS. Kasutame eelnevaid tähistusi ja tähistame sümboliga $K_1[X_1, \dots, X_n]$ kõigi n muutuja lineaarvormide hulka üle korpuse K . Olgu

$$\alpha : \text{Hom}(V, K) \rightarrow K_1[X_1, \dots, X_n]$$

kujutus, mis seab lineaarsele funktsionaalile φ vastavusse talle vastava lineaarvormi $\sum_{i=1}^n a_i X_i$, ja olgu

$$\beta : K_1[X_1, \dots, X_n] \rightarrow \text{Hom}(V, K)$$

defineeritud kui kujutus, mis viib lineaarvormi $k_1 X_1 + \dots + k_n X_n$ lineaarseks funktsionaaliks $\beta(k_1 X_1 + \dots + k_n X_n) : V \rightarrow K$, mis on antud võrdusega

$$\beta(k_1 X_1 + \dots + k_n X_n)(x) := k_1 x_1 + \dots + k_n x_n$$

iga $x \in V$ korral. Kuna $\beta(k_1 X_1 + \dots + k_n X_n)(e_i) = k_i$ iga $i \in \{1, \dots, n\}$ korral, siis

$$\alpha(\beta(k_1 X_1 + \dots + k_n X_n)) = k_1 X_1 + \dots + k_n X_n.$$

Samuti

$$\beta(\alpha(\varphi))(x) = \beta(a_1 X_1 + \dots + a_n X_n)(x) = a_1 x_1 + \dots + a_n x_n = \varphi(x)$$

iga $\varphi \in \text{Hom}(V, K)$ ja $x \in V$ korral. Seega $\alpha \circ \beta$ ja $\beta \circ \alpha$ on samasusteisendused. $\square$

Tähistame $\bar{a} = (a_1 \dots a_n) \in \text{Mat}_{1,n}(K)$. Paneme tähele, et kui ühemõõtmelises vektorruumis K (üle K) valida baas, mille ainsaks vektoriks on korpuse K ühikelement, siis $\bar{a}$ on lineaarkujutuse $\varphi : V \rightarrow K$ maatriks baaside e ja 1 suhtes. Harilikult nimetatakse seda üherealist maatriksit $\bar{a}$ lihtsalt **lineaarse funktsionaali** φ **maatriksiks** baasi e suhtes.

Arvestades võrdust (20) ja samastades ühe-elementilise maatriksi tema ainsa elemendiga võime lineaarse funktsionaali esitada maatriksite korrutamise abil:

$$\varphi(x) = \bar{a} \bar{x}_e. \quad (21)$$

Kuidas sõltub lineaarsele funktsionaalile φ vastav lineaarvorm vektorruumi V baasi valikust?

Lause 4.8 Üleminekul ühelt baasilt teisele korrutub lineaarse funktsionaali maatriks paremalt üleminekumaatriksiga.

TÕESTUS. Kasutame eelnevaid tähistusi. Olgu vektorruumis V antud veel baas $e' = \{e'_1, \dots, e'_n\}$. Siis vektor x avaldub ka kujul $x = x'_1 e'_1 + \dots + x'_n e'_n$, $x'_1, \dots, x'_n \in K$, kusjuures

$$\bar{x}_e = T \bar{x}_{e'},$$

kus $T = T^{e, e'}$ on üleminekumaatriks baasilt e baasile e' , s.t. T veergudes on baasi e' vektorite koordinaadid baasi e suhtes. Kui tähistame $a'_i := \varphi(e'_i)$, siis lineaarse funktsionaali φ maatriks baasi e' suhtes on $\bar{a}' = (a'_1 \dots a'_n)$. Seega

$$\varphi(x) = \bar{a} \bar{x}_e = \bar{a} (T \bar{x}_{e'}) = (\bar{a} T) \bar{x}_{e'}.$$

Paneme tähele, et $\bar{a}T$ on üherealine maatriks. Olgu ta $\bar{a}T = (b_1 \dots b_n)$. Võtame nüüd x ossa baasivektori e'_i . Märgime, et $(\bar{e}'_i)_{e'}$ on üheveeruline maatriks, mille i -ndas reas on 1 ja ülejäänud elemendid on 0-d. Kasutades omadust (21) saame, et iga $i \in \{1, \dots, n\}$ korral

$$a'_i = \varphi(e'_i) = (\bar{a}T)(\bar{e}'_i)_{e'} = (b_1 \dots b_n)(\bar{e}'_i)_{e'} = b_i.$$

Seega kehtib maatriksite võrdus

$$\bar{a}' = \bar{a}T,$$

s.t. φ maatriks e' suhtes on tema maatriks e suhtes korda T . Seda oligi tarvis tõestada. $\square$

Lause 4.9 Olgu V vektorruum üle korpuse K baasiga $e = \{e_1, \dots, e_n\}$. Iga $i \in \{1, \dots, n\}$ korral vaatleme kujutust $e^i : V \rightarrow K$, mis on defineeritud võrdusega

$$e^i \left(\sum_{j=1}^n x_j e_j \right) := x_i.$$

Siis $\{e^1, \dots, e^n\}$ on baas vektorruumis $\text{Hom}(V, K)$.

TÕESTUS. Niisiis e^i seab vektorile x vastavusse tema i -nda koordinaadi baasi e suhtes. Kuna

$$e^i \left(\sum_{j=1}^n x_j e_j + \sum_{j=1}^n y_j e_j \right) = e^i \left(\sum_{j=1}^n (x_j + y_j) e_j \right) = x_i + y_i = e^i \left(\sum_{j=1}^n x_j e_j \right) + e^i \left(\sum_{j=1}^n y_j e_j \right),$$

siis e^i on kooskõlas liitmisega. Analoogiliselt saab näidata, et e^i on kooskõlas skalaariga korrutamise. Seega $e^i \in \text{Hom}(V, K)$.

Kui $k_1 e^1 + \dots + k_n e^n = 0$ (ehk $k_1 e^1 + \dots + k_n e^n : V \rightarrow K$ on nullkujutus), siis

$$k_i = k_1 e^1(e_i) + \dots + k_n e^n(e_i) = (k_1 e^1 + \dots + k_n e^n)(e_i) = 0(e_i) = 0$$

iga $i \in \{1, \dots, n\}$ korral. Järelikult süsteem $e^1, \dots, e^n$ on lineaarselt sõltumatu.

Jääb veel näidata, et $e^1, \dots, e^n$ on moodustajate süsteem. Olgu $\varphi \in \text{Hom}(V, K)$ ja vaatleme suvalist vektorit $x = \sum_{j=1}^n x_j e_j \in V$. Siis

$$\varphi(x) = \sum_{i=1}^n x_i \varphi(e_i) = \sum_{i=1}^n \varphi(e_i) x_i = \sum_{i=1}^n \varphi(e_i) e^i(x) = \left(\sum_{i=1}^n \varphi(e_i) e^i \right) (x),$$

mis tähendab, et

$$\varphi = \sum_{i=1}^n \varphi(e_i) e^i = \varphi(e_1) e^1 + \dots + \varphi(e_n) e^n.$$

Seega $e^1, \dots, e^n$ on V kaasruumi moodustajate süsteem ja kokkuvõttes baas. $\square$

Järeldus 4.10 Iga vektorruum on isomorfne oma kaasruumiga.

TÕESTUS. Kaks lõplikumõõtmelist vektorruumi üle sama korpuse on isomorfsed parajasti siis, kui nende mõõtmed on samad ([1], teoreem 3.4.5). Lause 4.9 põhjal on vektorruumi kaasruumi mõõde sama, mis selle vektorruumi mõõde. Seega $V \simeq V^*$. $\square$

Definitsioon 4.11 Lauses 4.9 defineeritud kaasruumi V^* baasi $\{e^1, \dots, e^n\}$ nimetatakse baasi e **kaasbaasiks** ja tähistatakse sümboliga e^* .

Definitsioon 4.12 Vektorruumi V teiseks kaasruumiks nimetatakse vektorruumi

$$V^{**} = (V^*)^* = \text{Hom}(\text{Hom}(V, K), K).$$

Järeldust 4.10 kaks korda kasutades saame, et

$$V \simeq V^* \simeq V^{**}.$$

Isomorfsusseose transitiivsuse tõttu $V \simeq V^{**}$, mis tähendab, et leidub *mingi* isomorfism $V \rightarrow V^{**}$. Järgmine teoreem ütleb meile, et vektorruumide V ja V^{**} vahel leidub teatud loomulikult viisil defineeritud isomorfism. Mõnikord öeldakse: vektorruum on loomulikult isomorfne oma teise kaasruumiga.

Teoreem 4.13 Olgu V vektorruum üle korpuse K . Siis kujutus $\Phi : V \rightarrow V^{**}$, mille puhul

$$(\Phi(x))(\varphi) = \varphi(x)$$

suvaliste $x \in V$ ja $\varphi \in V^*$ korral, on vektorruumide isomorfism.

TÕESTUS. Definitsiooni põhjal $\Phi(x) : \text{Hom}(V, K) \rightarrow K$. Veendume, et $\Phi(x)$ on lineaarkujutus. Kui $\varphi, \psi \in \text{Hom}(V, K)$, $k \in K$ ja $x \in V$, siis

$$\begin{aligned} \Phi(x)(\varphi + \psi) &= (\varphi + \psi)(x) = \varphi(x) + \psi(x) = (\Phi(x))(\varphi) + (\Phi(x))(\psi), \\ \Phi(x)(k\varphi) &= (k\varphi)(x) = k\varphi(x) = k((\Phi(x))(\varphi)). \end{aligned}$$

Seega $\Phi(x) \in V^{**}$. Mistahes $\varphi \in \text{Hom}(V, K)$, $k \in K$ ja $x, y \in V$ korral

$$\begin{aligned} \Phi(x + y)(\varphi) &= \varphi(x + y) = \varphi(x) + \varphi(y) = (\Phi(x))(\varphi) + (\Phi(y))(\varphi) = (\Phi(x) + \Phi(y))(\varphi), \\ \Phi(kx)(\varphi) &= \varphi(kx) = k\varphi(x) = k((\Phi(x))(\varphi)) = (k\Phi(x))(\varphi), \end{aligned}$$

ja seega $\Phi : V \rightarrow V^{**}$ on lineaarkujutus.

Olgu nüüd $e = \{e_1, \dots, e_n\}$ baas vektorruumis V ja $e^* = \{e^1, \dots, e^n\}$ talle vastav kaasbaas kaasruumis V^* . Näitame, et Φ on üksühene. Olgu $x \in \text{Ker}(\Phi)$. Siis $\Phi(x) : \text{Hom}(V, K) \rightarrow K$ on nullkujutus ja seega iga $\varphi \in V^*$ korral $\varphi(x) = \Phi(x)(\varphi) = 0$. Muuhulgas $e^i(x) = 0$ iga $i \in \{1, \dots, n\}$ korral. Kuna vektori x kõik koordinaadid baasi e suhtes on nullid, siis $x = 0$. Seega $\text{Ker}(\Phi) = \{0\}$ ja Φ on üksühene ([1], lause 4.1.10).

Teame, et $\dim(V) = n = \dim(V^{**})$. Kuna Φ on üksühene, siis viib ta baasi e lineaarselt sõltumatuks vektorite süsteemiks $\Phi(e_1), \dots, \Phi(e_n)$ vektorruumis V^{**} . Selle süsteemi saab täiendada baasiks vektorruumis V^{**} ([1], lause 3.2.14). Kuna $\dim(V^{**}) = n$, siis lisatavaid vektoreid saab olla ainult 0 tükki. Järelikult $\Phi(e_1), \dots, \Phi(e_n)$ on vektorruumi V^{**} baas. Kui $f \in V^{**}$ on suvaline, siis leiduvad $k_1, \dots, k_n \in K$ nii, et

$$f = k_1\Phi(e_1) + \dots + k_n\Phi(e_n) = \Phi(k_1e_1 + \dots + k_ne_n).$$

See näitab, et Φ on pealekujutus ja seega kokkuvõttes isomorfism. $\square$

4.2 Bilineaarsed funktsionaalid ja bilineaarvormid

Definitsioon 4.14 Olgu V vektorruum üle korpuse K . Kujutust $f : V \times V \rightarrow K$ nimetatakse **bilineaarseks funktsionaaliks** vektorruumil V , kui on täidetud järgmised tingimused:

1. $f(x + z, y) = f(x, y) + f(z, y)$;
2. $f(kx, y) = kf(x, y)$;
3. $f(x, y + z) = f(x, y) + f(x, z)$;
4. $f(x, ky) = kf(x, y)$

mistahes $x, y, z \in V$ ja $k \in K$ korral.

Näide 4.15 Skalaarkorrutamine mistahes eukleidilisel ruumil on bilineaarne funktsionaal.

Definitsioon 4.16 Olgu V vektorruum üle korpuse K , olgu f bilineaarne funktsionaal vektorruumil V ja olgu $e = \{e_1, \dots, e_n\}$ vektorruumi V baas. Siis f **maatriksiks baasi e suhtes** nimetatakse maatriksit $A = A_f^e = (a_{ij}) \in \text{Mat}_n(K)$, kus

$$a_{ij} = f(e_i, e_j)$$

iga $i, j \in \{1, \dots, n\}$ korral.

Kui f on bilineaarne funktsionaal vektorruumil V ja A on f maatriks baasi e suhtes, siis iga $x, y \in V$ korral

$$\begin{aligned} f(x, y) &= f(x_1e_1 + \dots + x_ne_n, y_1e_1 + \dots + y_ne_n) = \sum_{i,j=1}^n f(x_ie_i, y_je_j) \\ &= \sum_{i,j=1}^n x_iy_jf(e_i, e_j) = \sum_{i,j=1}^n f(e_i, e_j)x_iy_j \end{aligned}$$

kus $x_1, \dots, x_n$ ja $y_1, \dots, y_n$ on vastavalt vektorite x ja y koordinaadid baasi e suhtes. Seega

$$f(x, y) = \sum_{i,j=1}^n a_{ij}x_iy_j. \quad (22)$$

Definitsioon 4.17 Polünoomi

$$\sum_{i,j=1}^n a_{ij} X_i Y_j,$$

kus $a_{ij} = f(e_i, e_j)$ iga $i, j \in \{1, \dots, n\}$ korral, nimetatakse bilineaarsele funktsionaalile f vastavaks **bilineaarvormiks** muutujate $X_1, \dots, X_n, Y_1, \dots, Y_n$ suhtes.

Analoogiliselt lausega 4.7 saab tõestada järgmise lause.

Lause 4.18 Olgu V n -mõõtmeline vektorruum üle korpuse K . Vektorruumi V baasi fikseerimine tekitab üksühese vastavuse selle vektorruumi bilineaarsete funktsionaalide ja $2n$ muutuja bilineaarvormide vahel.

Lause 4.19 Üleminekul ühelt baasilt teisele korrutub bilineaarse funktsionaali maatriks paremalt üleminekumaatriksiga ja vasakult üleminekumaatriksi transponeeritud maatriksiga.

TÕESTUS. Olgu f bilineaarne funktsionaal vektorruumil V , olgu e ja e' kaks baasi selles vektorruumis ja olgu $T = T^{e,e'}$ üleminekumaatriks baasilt e baasile e' . Arvestades võrdust (22) ja samastades jällegi ühe-elementilise maatriksi tema ainsa elementiga võime bilineaarse funktsionaali esitada maatrikskujul

$$f(x, y) = \bar{x}_e^t A_f^e \bar{y}_e, \quad (23)$$

kus $\bar{x}_e$ ja $\bar{y}_e$ on vektorite $x, y \in V$ koordinaatide veerud baasi e suhtes. Lisaks sellele $\bar{x}_e = T \bar{x}_{e'}$, $\bar{y}_e = T \bar{y}_{e'}$ ja

$$(\bar{x}_{e'})^t A_f^{e'} (\bar{y}_{e'}) = f(x, y) = \bar{x}_e^t A_f^e \bar{y}_e = (T \bar{x}_{e'})^t A_f^e (T \bar{y}_{e'}) = (\bar{x}_{e'})^t (T^t A_f^e T) (\bar{y}_{e'}).$$

Võttes $x = e'_i$ ja $y = e'_j$, $i, j \in \{1, \dots, n\}$, saame muuhulgas võrduse

$$(\bar{e}'_i)^t A_f^{e'} (\bar{e}'_j)_{e'} = (\bar{e}'_i)^t_{e'} (T^t A_f^e T) (\bar{e}'_j)_{e'}.$$

See võrdus annab meile, et maatriksites $A_f^{e'}$ ja $T^t A_f^e T$ on kohal (i, j) sama element iga $i, j \in \{1, \dots, n\}$ korral. Järelikult

$$A_f^{e'} = T^t A_f^e T,$$

mida oligi tarvis tõestada. □

Definitsioon 4.20 Bilineaarset funktsionaali f vektorruumil V nimetatakse **sümmeetriliseks**, kui

$$f(x, y) = f(y, x)$$

iga $x, y \in V$ korral.

Lause 4.21 Sümmeetrilise bilineaarse funktsionaali maatriks mistahes baasi suhtes on sümmeetriline. Kui mingi bilineaarse funktsionaali maatriks mingi baasi suhtes on sümmeetriline, siis see funktsionaal on ka sümmeetriline.

TÕESTUS. Kasutame varasemaid tähistusi. Kui f on sümmeetriline, siis $a_{ij} = f(e_i, e_j) = f(e_j, e_i) = a_{ji}$, s.t. A_f^e on sümmeetriline maatriks.

Vastupidi, eeldame, et $f(e_i, e_j) = f(e_j, e_i)$ iga $i, j \in \{1, \dots, n\}$ korral. Siis

$$f(x, y) = \sum_{i,j=1}^n f(e_i, e_j) x_i y_j = \sum_{i,j=1}^n f(e_j, e_i) y_j x_i = \sum_{i,j=1}^n f(e_i, e_j) y_i x_j = f(y, x).$$

□

4.3 Ruutfunktsionaalid ja ruutvormid

Selles paragrahvis uurime ruutfunktsionaale ja ruutvorme. Need leiavad kasutust arvu-teoorias, rühmateoorias, matemaatilises statistikas ja mujal.

Definitsioon 4.22 Olgu V vektorruum üle korpuse K . Kujutust $F : V \rightarrow K$ nimetatakse **ruutfunktsionaaliks** vektorruumil V , kui leidub selline sümmeetriline bilineaarne funktsionaal f vektorruumil V , et

$$F(x) = f(x, x)$$

iga $x \in V$ korral.

Et tõestada järgmine lause, peab enne pisut rääkima korpuse karakteristikast.

Definitsioon 4.23 Öeldakse, et korpuse K **karakteristika on 2**, kui selles korpuses $1 + 1 = 0$ (ühikelemendi liitmisel iseendale saame nullelemendi).

Näiteks korpuse $\mathbb{Z}_2$ karakteristik on 2, aga korpuse $\mathbb{Z}_3$ karakteristik ei ole 2.

Sümboliga **2** tähistame korpuse elementi $1 + 1$. Paneme tähele, et iga $k \in K$ korral

$$k + k = 1 \cdot k + 1 \cdot k = (1 + 1)k = 2k.$$

Kui korpuse karakteristik ei ole 2, siis tema element **2** on pööratav ja saame rääkida elemendiga **2** jagamisest. Nimelt loeme, et

$$\frac{k}{2} = k \cdot 2^{-1},$$

kus $k \in K$.

Lause 4.24 Kui F on ruutfunktsionaal vektorruumil V üle korpuse K , mille karakteristik ei ole 2, siis sümmeetriline bilineaarne funktsionaal f , mis määrab ära F , on üheselt määratud.

TÕESTUS. Olgu $F(x) = f(x, x)$ iga $x \in V$ korral, kus f on sümmeetriline bilineaarne funktsionaal. Siis mistahes $x, y \in V$ korral

$$\begin{aligned} F(x + y) &= f(x + y, x + y) = f(x, x) + f(x, y) + f(y, x) + f(y, y) \\ &= f(x, x) + f(x, y) + f(x, y) + f(y, y) = F(x) + 2f(x, y) + F(y), \end{aligned}$$

millest

$$f(x, y) = \frac{F(x + y) - F(x) - F(y)}{2}.$$

Kui leiduks veel mingi sümmeetriline bilineaarne funktsionaal g nii, et $F(x) = g(x, x)$ iga $x \in V$ korral, siis $g(x, y)$ oleks võrdne samasuguse jagatisega, järelikult $f = g$. $\square$

Edaspidi eeldame selle peatüki jooksul, et korpuse K karakteristik ei ole 2. Seda tingimust rahuldavad näiteks korpused $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ja $\mathbb{Z}_p$, kus $p \neq 2$.

Definitsioon 4.25 Ruutfunktsionaali maatriksiks mingi baasi suhtes nimetatakse teda määrava sümmeetrilise bilineaarse funktsionaali maatriksit selle baasi suhtes.

Lause 4.26 Olgu F ruutfunktsionaal vektorruumil V , mille maatriks baasi $e = \{e_1, \dots, e_n\}$ suhtes on $A_F^e = (a_{ij})$ ning olgu vektori $x \in V$ koordinaadid baasi e suhtes $x_1, \dots, x_n$. Siis

$$F(x) = \sum_{i,j=1}^n a_{ij} x_i x_j.$$

TÕESTUS. Kui ruutfunktsionaal F on määratud sümmeetrilise bilineaarse funktsionaali f poolt, siis $a_{ij} = f(e_i, e_j)$ ja

$$F(x) = f(x, x) = f\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n x_j e_j\right) = \sum_{i,j=1}^n x_i x_j f(e_i, e_j) = \sum_{i,j=1}^n a_{ij} x_i x_j.$$

□

Definitsioon 4.27 Olgu F sümmeetrilise bilineaarse funktsionaali f poolt määratud ruutfunktsionaal. Siis n muutuja polünoom

$$\sum_{i,j=1}^n a_{ij} X_i X_j,$$

kus $a_{ij} = f(e_i, e_j)$ iga $i, j \in \{1, \dots, n\}$ korral, nimetatakse ruutfunktsionaalile F vastavaks **ruutvormiks** baasi $e = \{e_1, \dots, e_n\}$ suhtes. Maatriksit $A = (a_{ij})$ nimetatakse ka vastava **ruutvormi maatriksiks**.

Seega ruutvorm üle korpuse K on teise astme homogeenne polünoom $\sum_{i,j=1}^n a_{ij} X_i X_j \in K[X_1, \dots, X_n]$, kus $X_i X_j$ kordaja on võrdne $X_j X_i$ kordajaga iga $i, j, i \neq j$ korral.

Näide 4.28 Ruutvormide kirja panemisel harilikult ei näidata üksliikmeid $a_{ij} X_i X_j$ ja $a_{ji} X_j X_i$ ($i \neq j$) eraldi vaid esitatakse nende kahe üksliikme summa kujul $2a_{ij} X_i X_j$. Seda asjaolu tuleb arvestada ruutvormi maatriksi koostamisel. Näiteks ruutvormi

$$3X_1^2 + 4X_2^2 - X_3^2 + 2X_1 X_2 - 4X_1 X_3 + 10X_2 X_3$$

(üle korpuse $\mathbb{R}$) maatriks on

$$A = \begin{pmatrix} 3 & 1 & -2 \\ 1 & 4 & 5 \\ -2 & 5 & -1 \end{pmatrix}.$$

Kui A on ruutfunktsionaali F maatriks baasi e suhtes, siis arvestades võrdust (23) võime selle ruutfunktsionaali esitada maatrikskujul järgmiselt:

$$F(x) = \bar{x}_e^t A \bar{x}_e.$$

Lause 4.29 Olgu V n -mõõtmeline vektorruum üle korpuse K . Vektorruumi V baasi fikseerimine tekitab üksühesed vastavused sellel vektorruumil defineeritud ruutfunktsionaalide, n muutuja ruutvormide (üle K) ja n -ndat järku sümmeetriliste ruutmaatriksite (üle K) vahel.

TÕESTUS. On selge, et

$$\sum_{i,j=1}^n a_{ij} X_i X_j \longleftrightarrow A = (a_{ij})$$

on üksühene vastavus n muutuja ruutvormide ja n -ndat järku sümmeetriliste ruutmaatrik-site vahel. Tähistame sümbooliga $RF(V)$ vektorruumil V defineeritud ruutfunktsionaalide hulga ja

$$\text{SMat}_n(K) = \{A \in \text{Mat}_n(K) \mid A^t = A\}.$$

Sümmeetrilise maatriksi $A \in \text{SMat}_n(K)$ korral vaatleme kujutust $f_A : V \times V \rightarrow K$, mis on defineeritud võrdusega

$$f_A(x, y) := \bar{x}_e^t A \bar{y}_e.$$

Kuna $\bar{y}_e^t A \bar{x}_e$ on (1×1) -maatriks, siis ta transponeerimisel ei muutu, seega

$$f_A(x, y) = \bar{x}_e^t A \bar{y}_e = (\bar{y}_e^t A^t \bar{x}_e)^t = (\bar{y}_e^t A \bar{x}_e)^t = \bar{y}_e^t A \bar{x}_e = f_A(y, x).$$

Lisaks sellele

$$\begin{aligned} f_A(x + z, y) &= \overline{x + z}_e^t A \bar{y}_e = (\bar{x}_e^t + \bar{z}_e^t) A \bar{y}_e = \bar{x}_e^t A \bar{y}_e + \bar{z}_e^t A \bar{y}_e = f_A(x, y) + f_A(z, y), \\ f_A(kx, y) &= \overline{kx}_e^t A \bar{y}_e = k \bar{x}_e^t A \bar{y}_e = k f_A(x, y) \end{aligned}$$

mistahes $x, y, z \in V$ ja $k \in K$ korral. Järelikult f_A on sümmeetriline bilineaarne funktsionaal. Ta määrab ära ruutfunktsionaali F_A , mille korral $F_A(x) := \bar{x}_e^t A \bar{x}_e$, $x \in V$. Defineerime kujutuse $\beta : \text{SMat}_n(K) \rightarrow RF(V)$ võrdusega

$$\beta(A) := F_A.$$

Olgu $\alpha : RF(V) \rightarrow \text{SMat}_n(K)$ kujutus, mis seab ruutfunktsionaalile vastavusse tema maatriksi baasi e suhtes.

Kui nüüd F on ruutfunktsionaal maatriksiga $A = (a_{ij})$, siis

$$\beta(\alpha(F)) = \beta(A) = F_A = F,$$

sest $F_A(x) = \bar{x}_e^t A \bar{x}_e = F(x)$ iga $x \in V$ korral. Kui aga $A \in \text{SMat}_n(K)$, siis

$$\alpha(\beta(A)) = \alpha(F_A) = A,$$

sest $F_A(x) = f_A(x, x)$ ja $f_A(e_i, e_j) = (\bar{e}_i)_e^t A (\bar{e}_j)_e = a_{ij}$. □

Lause 4.30 Üleminekul ühelt baasilt teisele korrutatud ruutfunktsionaali maatriks paremalt üleminekumaatriksiga ja vasakult üleminekumaatriksi transponeeritud maatriksiga.

TÕESTUS. Kui F on sümmeetrilisele bilineaarsele funktsionaalile f vastav ruutvorm, e, e' on vektorruumi V baasid ja $T = T^{e, e'}$ on üleminekumaatriks, siis lause 4.19 põhjal $A_F^{e'} = A_F^{e'} = T^t A_F^e T = T^t A_F^e T$ ehk

$$A_F^{e'} = T^t A_F^e T.$$

□

Definitsioon 4.31 Öeldakse, et ruutvorm on **kanoonilisel kujul**, kui temas puuduvad liikmed erinevate muutujate korrutistega.

On selge, et ruutvorm on kanoonilisel kujul parajasti siis, kui tema maatriks on diagonaalmaatriks.

Näide 4.32 Ruutvorm

$$3X_1^2 - 5X_2^2 + 2X_4^2$$

üle $\mathbb{R}$ muutujate X_1, X_2, X_3, X_4 suhtes on kanoonilisel kujul.

Definitsioon 4.33 Baasi, mille suhtes ruutfunktsionaalile vastab kanoonilisel kujul olev ruutvorm, nimetatakse selle ruutfunktsionaali **kanooniliseks baasiks**.

Teoreem 4.34 *Igal ruutfunktsionaalil on olemas kanooniline baas.*

TÕESTUS. Olgu $A \in \text{Mat}_n(K)$ ruutfunktsionaali F maatriks baasi e suhtes. Siis iga regulaarne maatriks T on üleminekumaatriks baasilt e mingile baasile e' . Tänu lausele 4.30 piisab näidata, et leidub selline regulaarne maatriks T , mille korral $T^t A T$ on diagonaalmaatriks.

Selle eesmärgiga teeme elementaarteisendusi maatriksiga A nii, et kohe pärast mingit teisendust maatriksi ridadega teeme samasuguse teisenduse veergudega. Näiteks pärast i -nda ja j -nda rea äravahetamist vahetame kohe ära ka i -nda ja j -nda veeru. Teatavasti elementaarteisenduse ridadega võib sooritada vastava elementaarmaatriksiga antud maatriksit vasakult korrutades ([1], lause 4.7.6). Et sooritada samasugune elementaarteisendus veergudega, tuleb maatriks korrutada sellesama elementaarmaatriksi transposeeritud maatriksiga paremalt. Seega maatrikskujul sõnastatuna tuleb meil leida sellised elementaarmaatriksid $E_1, \dots, E_m$, et

$$D = E_m \dots E_1 A E_1^t \dots E_m^t$$

oleks diagonaalmaatriks. Kuna elementaarmaatriksid on regulaarsed ja regulaarmaatriksite korrutis on regulaarne, siis on ka maatriks

$$T := E_1^t E_2^t \dots E_m^t$$

regulaarne. Et $T^t = E_m \dots E_2 E_1$, siis $D = T^t A T$.

Veendume, et tõesti sellised elementaarteisendused leiduvad. Võime eeldada, et A ei ole nullmaatriks (nullmaatriks on diagonaalmaatriks). Kui element a_{11} ei ole 0, siis lahutades i -ndast reast esimese rea, mis on korrutatud elemendiga $a_{11}^{-1} a_{i1}$, saame maatriksi, kus kohal $(i, 1)$ on 0. Analoogilise veergude teisendusega saab nulliks muuta elemendi kohal $(1, i)$. Nii saab nulliks muuta kõik elemendid (välja arvatud esimene) esimeses reas ja veerus.

Mida teha siis, kui $a_{11} = 0$? Kui leidub selline $i \neq 1$, et $a_{ii} \neq 0$, siis vahetame ära esimese ja i -nda rea ning esimese ja i -nda veeru. Selle tulemusena tekib kohale $(1, 1)$ nullist erinev element, mille abil saame edasi tegutseda nii nagu enne. Kui aga kõik peadiagonaali elemendid on nullid, kuid $a_{ij} \neq 0$, kus $i \neq j$, siis liidame j -ndale reale i -nda rea ja j -ndale veerule i -nda veeru. Nii tekib kohale (j, j) nullist erinev element $a_{ij} + a_{ji} = 2a_{ij}$ (sest A on sümmeetriline ja korpuse karakteristika ei ole 2). Edasi saame toimida kasutades eelnevat mõttekäiku.

Kui esimeses reas ja veerus on kõik elemendid (välja arvatud esimene) nullideks muudetud, siis kordame protseduuri alammaatriksis, mis asub ridades ja veergudes numbritega $2, \dots, n$. $\square$

Meenutame, et **eukleidiliseks ruumiks** nimetatakse vektorruumi üle korpuse $\mathbb{R}$ koos mingi skalaarkorrutamise sellel vektorruumil ([1], def. 9.1.1).

Teoreem 4.35 *Igal eukleidilise ruumi ruutfunktsionaalil on olemas ortonormeeritud kanooniline baas.*

TÕESTUS. Olgu E eukleidiline ruum, olgu e suvaline ortonormeeritud baas ruumis E (selle saab konstrueerida näiteks ortogonaliseerimisprotsessi abil) ja olgu F ruutfunktsionaal ruumil E . Siis maatriks $A := A_F^e$ on sümmeetriline. Olgu $\varphi : E \rightarrow E$ lineaarteisendus, mille korral $A = A_\varphi^e$ (selline lineaarteisendus leidub tänu teoreemile 4.1.12 raamatust [1]). Siis φ on eukleidilise ruumi E sümmeetriline lineaarteisendus ([1], teoreem 9.3.3) ning järelikult leidub φ omavektoreist koosnev ortonormeeritud baas e' ruumis E ([1], teoreem 9.3.6). Selle baasi e' suhtes on φ maatriks $A_\varphi^{e'}$ diagonaalmaatriks. Olgu T üleminekumaatriks baasilt e baasile e' . Siis T on ortogonaalmaatriks ([1], lause 9.2.4), s.t. $T^t = T^{-1}$, ja $A_\varphi^{e'} = T^{-1}A_\varphi^e T$ ([1], lause 8.2.5). Seega

$$A_\varphi^{e'} = T^{-1}A_\varphi^e T = T^{-1}AT = T^t A_F^e T = A_F^{e'},$$

kus viimane võrdus tuleb lausest 4.30. See tähendab, et ruutfunktsionaali F maatriks ortonormeeritud baasi e' suhtes on diagonaalmaatriks $A_\varphi^{e'}$. $\square$

4.4 Ruutfunktsionaalid vektorruumidel üle $\mathbb{C}$ ja $\mathbb{R}$

Selles paragrahvis uurime ruutfunktsionaale ja ruutvorme üle korpuste $\mathbb{C}$ ja $\mathbb{R}$. Nende kohta saab öelda pisut enam kui ruutvormide kohta üle suvalise korpuse K .

Definitsioon 4.36 Kahte n muutuja ruutvormi nimetatakse **ekvivalentseteks**, kui nad vastavad samale ruutfunktsionaalile mingite baaside suhtes.

Seega ruutvormid $\sum_{i,j=1}^n a_{ij}X_iX_j$ ja $\sum_{i,j=1}^n b_{ij}X_iX_j$ üle K on ekvivalentsed, kui leidub vektorruum V üle K , selle baasid $e = \{e_1, \dots, e_n\}$ ja $e' = \{e'_1, \dots, e'_n\}$ ning sümmeetriline bilineaarne funktsionaal $f : V \times V \rightarrow K$ nii, et $a_{ij} = f(e_i, e_j)$ ja $b_{ij} = f(e'_i, e'_j)$.

Maatriksite keeles: ruutvormid maatriksitega $A = (a_{ij})$ ja $B = (b_{ij})$ on ekvivalentsed, kui leidub regulaarne maatriks T nii, et $B = T^t A T$.

On selge, et ruutvormide ekvivalentsuse seos on tõepoolest refleksiivne, sümmeetriline ja transitiivne.

Teoreemi 4.34 silmas pidades võime öelda, et iga ruutvorm on ekvivalentne kanoonilisel kujul oleva ruutvormiga. Antud ruutvormi jaoks ekvivalentse kanoonilisel kujul oleva ruutvormi leidmist kutsutakse selle **ruutvormi kanoonilisele kujule viimiseks**.

Lause 4.37 *Iga n muutuja ruutvormi üle $\mathbb{C}$ saab viia kanoonilisele kujule $X_1^2 + \dots + X_r^2$, kus $r \leq n$.*

TÕESTUS. Olgu antud ruutvorm maatriksiga A . Viies kanoonilisele kujule saame leida regulaarse maatriksi T nii, et $D = T^t A T$ on diagonaalmaatriks. Olgu selle diagonaalmaatriksi peadiagonaalil r nullist erinevat elementi. Siis ridade ja veergude vahetamise teisenduse abil on maatriks D võimalik viia kujule C , kus need nullist erinevad elemendid asuvad kohtadel $(1, 1), \dots, (r, r)$. Olgu need elemendid $c_{11}, \dots, c_{rr}$. Olgu z_{ii} selline kompleksarv, et $z_{ii}^2 = c_{ii}$, $i = 1, \dots, r$. Siis korrutades maatriksi C i -ndat rida ja i -ndat veergu ($i = 1, \dots, r$) arvuga $\frac{1}{z_{ii}}$ saame maatriksi, mille kohtadel $(1, 1), \dots, (r, r)$ on 1 ja mujal nullid. Sellega oleme ruutvormi viinud kujule $X_1^2 + \dots + X_r^2$. $\square$

Definitsioon 4.38 Üle korpuse $\mathbb{C}$ vaadeldava n muutuja ruutvormi **normaalkujuks** nimetatakse temaga ekvivalentset ruutvormi $X_1^2 + \dots + X_r^2$.

Teoreem 4.39 *Kaks n muutuja ruutvormi üle $\mathbb{C}$ on ekvivalentsed parajasti siis, kui nende maatriksite astakud on võrdsed.*

TÕESTUS. Olgu vaadeldavate ruutvormide maatriksid $A = (a_{ij}), B = (b_{ij}) \in \text{Mat}_n(\mathbb{C})$.

TARVILIKKUS. Kui ruutvormid on ekvivalentsed, siis leidub regulaarne maatriks T nii, et $B = T^t A T$. Kuna korrutamisel regulaarse maatriksiga maatriksi astak ei muutu, siis $\text{rank}(B) = \text{rank}(A)$.

PIISAVUS. Eeldame, et $\text{rank}(A) = \text{rank}(B)$. Leiame nende ruutvormide normaalkujud

$$X_1^2 + \dots + X_r^2 \quad \text{ja} \quad X_1^2 + \dots + X_s^2,$$

millele vastavad maatriksid on A' ja B' . Siis $A' = T^t A T$ ja $B' = U^t B U$, kus T, U on regulaarsed maatriksid. Järelikult

$$r = \text{rank}(A') = \text{rank}(A) = \text{rank}(B) = \text{rank}(B') = s$$

ehk $A' = B'$. Seega mõlemad ruutvormid on ekvivalentsed ruutvormiga $X_1^2 + \dots + X_r^2$ ning järelikult on nad ka omavahel ekvivalentsed. $\square$

Vaatleme nüüd reaalarvuliste kordajatega ruutvorme. Me saame sellise ruutvormi viia kanoonilisele kujule, mis tähendab, et tema maatriks on diagonaalmaatriks. Siis tehakse ridade ja veergude vahetamise teisendusi saame maatriksit teisendada nii, et peadiagonaalil oleks alguses positiivsed reaalarvud, siis negatiivsed reaalarvud ja lõpuks nullid (kui neid on). Nii saadud maatriks annab samuti esialgse ruutvormi kanoonilise kuju.

Kuigi kanoonilisi kujusid võib ruutvormil olla palju, on neis kõigis midagi ühist. Järgmise teoreemi tõestas inglise matemaatik James Joseph Sylvester aastal 1852.



James Joseph Sylvester

Teoreem 4.40 (Ruutvormide inertsiseadus) *Reaalarvuliste kordajatega ruutvormi positiivsete (negatiivsete) kordajate arv tema kanoonilises kujus ei sõltu kanoonilisest baasist.*

TÕESTUS. Olgu V n -mõõtmeline vektorruum üle $\mathbb{R}$ ja F ruutfunktsionaal vektorruumil V . Olgu $e = \{e_1, \dots, e_n\}$ ja $e' = \{e'_1, \dots, e'_n\}$ ruutfunktsionaali F sellised kanoonilised baasid, millele vastavad ruutvormid on

$$a_{11}X_1^2 + \dots + a_{nn}X_n^2 \quad \text{ja} \quad b_{11}X_1^2 + \dots + b_{nn}X_n^2.$$

Kõigepealt näitame, et kui esimeses ruutvormis leidub mõni positiivne kordaja, siis ka teises ruutvormis leidub vähemalt üks positiivne kordaja. Olgu $a_{jj} > 0$. Oletame vastuväiteliselt, et teises ruutvormis ei ole positiivseid kordajaid, s.t. $b_{ii} \leq 0$ iga $i \in \{1, \dots, n\}$ korral. Kuna e' on baas, siis leiduvad $k_1, \dots, k_n \in \mathbb{R}$ nii, et $e_j = k_1 e'_1 + \dots + k_n e'_n$. Siis

$$F(e_j) = a_{jj} > 0 \quad \text{ja} \quad F(e_j) = b_{11}k_1^2 + \dots + b_{nn}k_n^2 \leq 0,$$

mis on omavahel vastuolus. Niisiis ka $b_{11}, \dots, b_{nn}$ hulgas leidub positiivseid arve.

Olgu nüüd $a_{11}, \dots, a_{rr}$ esimese ruutvormi positiivsed kordajad ja $b_{11}, \dots, b_{ss}$ teise ruutvormi positiivsed kordajad (me saame kanoonilised baasid nii valida). Oletame vastuväiteliselt, et $r > s$. (Kui $r < s$, siis on tõestus analoogiline.) Vaatleme vektorruumi V alamruume

$$\begin{aligned} V_1 &= \langle e_1, \dots, e_r \rangle, \\ V_2 &= \langle e'_{s+1}, \dots, e'_n \rangle. \end{aligned}$$

Siis

$$\dim(V_1) + \dim(V_2) = r + n - s = n + (r - s) > n,$$

mis tähendab, et $\dim(V_1) + \dim(V_2) \neq \dim(V_1 + V_2)$. Järelduse 1.93 põhjal summa $V_1 + V_2$ ei ole otsesumma ja teoreemi 1.83 tõttu $V_1 \cap V_2 \neq \{0\}$. Seega leidub nullist erinev vektor $x \in V_1 \cap V_2$. Olgu

$$x = k_1 e_1 + \dots + k_r e_r = l_{s+1} e'_{s+1} + \dots + l_n e'_n,$$

kus $k_1, \dots, k_r, l_{s+1}, \dots, l_n \in \mathbb{R}$. Siis

$$F(x) = a_{11}k_1^2 + \dots + a_{rr}k_r^2 > 0,$$

kuid samas ka

$$F(x) = b_{s+1,s+1}l_{s+1}^2 + \dots + b_{nn}l_n^2 \leq 0,$$

mis on vastuolus eelmise võrratusega. Seega $r = s$.

Väite negatiivsete kordajate kohta saab tõestada analoogiliselt. $\square$

Järgmine teoreem annab tarviliku ja piisava tingimuse selleks, et kaks ruutvormi oleks ekvivalentsed üle $\mathbb{R}$.

Teoreem 4.41 *Kaks ruutvormi üle $\mathbb{R}$ on ekvivalentsed parajasti siis, kui nende kanoonilises kujus on ühepalju positiivseid kordajaid ja ühepalju negatiivseid kordajaid.*

TÕESTUS. TARVILIKKUS. Oletame, et kaks ruutvormi on ekvivalentsed. Siis nad vastavad samale ruutfunktsionaalile F . Kui leiame F jaoks kanoonilised baasid e ja e' , siis saame ruutvormide jaoks kaks kanoonilist kuju. Teoreemi 4.40 tõttu on neil ühepalju positiivseid kordajaid ja ühepalju negatiivseid kordajaid.

PIISAVUS. Vaatleme ruutvormi, mille kanooniline kuju on

$$a_{11}X_1^2 + \dots + a_{rr}X_r^2 - a_{r+1,r+1}X_{r+1}^2 - \dots - a_{ss}X_s^2,$$

kus $a_{11}, \dots, a_{ss} > 0$. (Iga ruutvorm üle $\mathbb{R}$ on võimalik sellisele kujule viia.) Korrutades kanoonilisele kujule vastava maatriksi i -ndat rida ja i -ndat veergu ($i = 1, \dots, s$) positiivse reaalarvuga $\frac{1}{\sqrt{a_{ii}}}$ saame ruutvormi viia kanoonilisele kujule

$$X_1^2 + \dots + X_r^2 - X_{r+1}^2 - \dots - X_s^2.$$

Seda kuju nimetatakse üle korpuse $\mathbb{R}$ vaadeldava ruutvormi **normaalkujuks**. On selge, et ruutvormi normaalkuju on üheselt määratud.

Oletame nüüd, et kahe ruutvormi kanoonilises kujus on ühepalju positiivseid kordajaid ja ühepalju negatiivseid kordajaid. Siis on neil sama normaalkuju. Kumbki neist ruutvormidest on ekvivalentne selle normaalkujuga, seega on ka need kaks ruutvormi omavahel ekvivalentsed. $\square$

Definitsioon 4.42 Ruutfunktsionaali F vektorruumil V üle $\mathbb{R}$ nimetatakse

- **positiivselt määratuks**, kui $F(x) > 0$ iga nullist erineva vektori $x \in V$ korral;
- **negatiivselt määratuks**, kui $F(x) < 0$ iga nullist erineva vektori $x \in V$ korral.

Öeldakse, et ruutvorm on **positiivselt (negatiivselt) määratud**, kui talle vastav ruutfunktsionaal on positiivselt (negatiivselt) määratud.

Näide 4.43 Olgu V vektorruum üle $\mathbb{R}$ baasiga $e = \{e_1, e_2, e_3\}$. Vaatleme ruutfunktsionaali $F : V \rightarrow \mathbb{R}$, mis on defineeritud võrdusega

$$F(x) := 4x_1^2 + 3x_2^2 + x_3^2,$$

kus $x = x_1e_1 + x_2e_2 + x_3e_3$. Kui $x \neq 0$, siis vähemalt üks liidetav summas $4x_1^2 + 3x_2^2 + x_3^2$ on positiivne ja seega $F(x) > 0$. Järelikult F on positiivselt määratud ruutfunktsionaal ja talle vastav ruutvorm

$$4X_1^2 + 3X_2^2 + X_3^2$$

on samuti positiivselt määratud.

Lause 4.44 *Ruutvorm on positiivselt määratud parajasti siis, kui tema normaalkuju maatriks on ühikmaatriks. Ruutvorm on negatiivselt määratud parajasti siis, kui tema normaalkuju maatriks on ühikmaatriksi vastandmaatriks.*

TÕESTUS. Tõestame esimese väite (teise väite tõestus on analoogiline).

TARVILIKKUS. Olgu ruutvormile vastav ruutfunktsionaal F positiivselt määratud. Siis leidub kanooniline baas $e = \{e_1, \dots, e_n\}$ nii, et $A_F^e = (a_{ij})$ on diagonaalmaatriks, kus $a_{ii} \in \{1, -1, 0\}$ iga $i \in \{1, \dots, n\}$ korral. Et $a_{ii} = F(e_i) > 0$, siis $a_{ii} = 1$ ja seega $A_F^e = E$. **PIISAVUS.** Olgu ruutvormi normaalkuju maatriks $A_F^e = E = (\delta_{ij})$. Siis iga vektori $x = x_1e_1 + \dots + x_ne_n \neq 0$ korral

$$F(x) = \sum_{i,j=1}^n \delta_{ij} x_i x_j = x_1^2 + x_2^2 + \dots + x_n^2 > 0.$$

See tähendab, et ruutvorm on positiivselt määratud. □

Järgnevalt tahame näidata, et positiivselt määratuse kontrollimiseks piisab n miinori arvutamisest.

Definitsioon 4.45 n -ndat järku ruutmaatriksi $A = (a_{ij})$ **peamiinoriteks** nimetatakse miinoreid

$$M_k = \begin{vmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} \end{vmatrix},$$

kus $k = 1, \dots, n$.

Nagu definitsioonist näha, peamiinorid asuvad maatriksi A ülemises vasakpoolses nurgas.

Teoreem 4.46 *Ruutfunktsionaal vektorruumil üle $\mathbb{R}$ on positiivselt määratud parajasti siis, kui tema maatriksi kõik peamiinorid on positiivsed.*

TÕESTUS. TARVILIKKUS. Olgu F positiivselt määratud ruutfunktsionaal n -mõõtmelisel vektorruumil V üle $\mathbb{R}$, mille maatriks baasi $e = \{e_1, \dots, e_n\}$ suhtes on

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

Asume maatriksit A teisendama teoreemis 4.34 kirjeldatud meetodil. Kuna F on positiivselt määratud, siis $a_{11} = F(e_1) > 0$ ja me saame esimese rea ja veeru ülejäänud elemendid muuta nullideks liites vastavale reale (veerule) sobiva elemendiga korrutatud esimese rea (veeru). Tulemuseks saame maatriksi

$$\begin{pmatrix} b_{11} & 0 & 0 & \dots & 0 \\ 0 & b_{22} & b_{23} & \dots & b_{2n} \\ 0 & b_{32} & b_{33} & \dots & b_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & b_{n2} & b_{n3} & \dots & b_{nn} \end{pmatrix}.$$

See on jällegi ruutfunktsionaali F maatriks mingi baasi $e' = \{e'_1, \dots, e'_n\}$ suhtes. Seega $b_{22} = F(e'_2) > 0$ ja selle elemendi abil saame muuta nulliks ülejäänud elemendid teises reas ja veerus. Tulemuseks on maatriks kujul

$$\begin{pmatrix} c_{11} & 0 & 0 & \dots & 0 \\ 0 & c_{22} & 0 & \dots & 0 \\ 0 & 0 & c_{33} & \dots & c_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & c_{n3} & \dots & c_{nn} \end{pmatrix}.$$

Analoogiliselt jätkates jõuame diagonaalmaatriksini

$$\begin{pmatrix} d_{11} & 0 & 0 & \dots & 0 \\ 0 & d_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & d_{nn} \end{pmatrix},$$

kus $d_{11}, \dots, d_{nn} > 0$. Tehtud teisendused on sellised, mis on muutnud küll maatriksit, kuid mitte tema peamiinoreid. Seega

$$M_k = d_{11}d_{22} \dots d_{kk},$$

$k \in \{1, \dots, n\}$, mis kõik on positiivsed.

PIISAVUS. Olgu F ruutfunktsionaal n -mõõtmelisel vektorruumil V üle $\mathbb{R}$, mille maatriks baasi $e = \{e_1, \dots, e_n\}$ suhtes on

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

Eeldame, et matriksi A kõik peamiinorid $M_1, \dots, M_n$ on positiivsed. Hakkame matriksit A teisendama samamoodi nagu tarvilikkuse tõestuses. Selle käigus jällegi peamiinorid ei muutu.

Kasutades seda, et $a_{11} = M_1 > 0$, saame esimese rea ja veeru ülejäänud elemendid muuta nullideks. Seega saame matriksi

$$\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & b_{22} & b_{23} & \dots & b_{2n} \\ 0 & b_{32} & b_{33} & \dots & b_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & b_{n2} & b_{n3} & \dots & b_{nn} \end{pmatrix}.$$

Kuna

$$M_2 = \begin{vmatrix} a_{11} & 0 \\ 0 & b_{22} \end{vmatrix} = a_{11}b_{22} = M_1b_{22} > 0,$$

siis $b_{22} > 0$. Elementi b_{22} kasutades saame teise rea ja veeru ülejäänud elemendid muuta nullideks, see annab meile matriksi

$$\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & b_{22} & 0 & \dots & 0 \\ 0 & 0 & c_{33} & \dots & c_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & c_{n3} & \dots & c_{nn} \end{pmatrix}.$$

Kuna

$$\begin{vmatrix} a_{11} & 0 & 0 \\ 0 & b_{22} & 0 \\ 0 & 0 & c_{33} \end{vmatrix} = a_{11}b_{22}c_{33} = M_2c_{33} > 0,$$

siis $c_{33} > 0$. Niiviisi jätkates jõuame diagonaalmaatriksini

$$\begin{pmatrix} d_{11} & 0 & 0 & \dots & 0 \\ 0 & d_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & d_{nn} \end{pmatrix},$$

kus $d_{11}, \dots, d_{nn} > 0$. See diagonaalmaatriks on ruutfunktsionaali F matriks mingi baasi suhtes. Siit on näha, et F on positiivselt määratud. $\square$

5 Abeli rühmad

Selles peatükis käsitleme Abeli rühmi (kommutatiivseid rühmi). Need on oma nime saanud Niels Henrik Abeli² järgi. Põhitähelepanu on perioodilistel, lõplikel ja vabadel Abeli rühmadel. Üheks olulisemaks Abeli rühmade näiteks on tsüklilised rühmad, mille vaatlemisest alustamegi.



Niels Henrik Abel

5.1 Tsüklilised rühmad

Olgu $(G, \cdot)$ rühm, $k \in \mathbb{N}$ ja $g \in G$. Tähistame

$$g^k := \underbrace{g \cdot \dots \cdot g}_k, \quad g^{-k} := (g^{-1})^k = \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_k, \quad g^0 := 1.$$

Lihtne on veenduda, et selliselt defineeritud rühma elemendi astmete jaoks kehtivad harilikud astendamise reeglid: mistahes $k, l \in \mathbb{Z}$ korral $g^{k+l} = g^k \cdot g^l$, $(g^k)^l = g^{kl}$ jne.

Kui tegemist on aditiivse rühmaga $(A, +)$, siis defineeritakse analoogiliselt elemendi $a \in A$ kordsed ka , kus $k \in \mathbb{Z}$.

Multiplikatiivse rühma $(G, \cdot)$ elemendi g korral tähistame sümboliga $\langle g \rangle$ hulga G alamhulka, mis koosneb elemendi g kõigist astmetest:

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

On lihtne näha, et hulk $\langle g \rangle$ on rühma G alamrühm. Seda alamrühma nimetatakse elemendi g poolt **tekitatud** (või **moodustatud**) **alamrühmaks**.

Definitsioon 5.1 Rühma $(G, \cdot)$ nimetatakse **tsükliliseks**, kui leidub selline element $g \in G$, et $G = \langle g \rangle$. Seda elementi g nimetatakse tsüklilise rühma **tekitajaks** (või **moodustajaks**).

Teisisõnu rühm $(G, \cdot)$ on tsükliline, kui temas leidub selline element g , mille astmetena esituvad kõik selle rühma elemendid: $G = \{g^k \mid k \in \mathbb{Z}\}$.

Aditiivne rühm $(A, +)$ on tsükliline, kui leidub selline $a \in A$, et $A = \{ka \mid k \in \mathbb{Z}\}$.

Näide 5.2 • Rühm $(\{1, -1\}, \cdot)$ on tsükliline rühm moodustajaga -1 .

- Rühm $(\mathbb{Z}, +)$ on tsükliline rühm moodustajaga 1 või -1 .
- Rühm $(\mathbb{Z}_n, +)$ on tsükliline rühm moodustajaga $\bar{1}$ (aga sellel rühmal võib olla teisigi moodustajaid).

Meil läheb vaja järgmisi arvuteoreetilisi tulemusi.

Lause 5.3 Kui $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$, siis leiduvad $q, r \in \mathbb{Z}$ nii, et $a = bq + r$ ja $0 \leq r < b$.

²Niels Henrik Abel (1802–1829) — norra matemaatik

Lause 5.4 Mistahes $a, b \in \mathbb{Z}$ korral $S\ddot{U}T(a, b) = 1$ parajasti siis, kui leiduvad $u, v \in \mathbb{Z}$ nii, et $au + bv = 1$.

Teoreem 5.5 Sama järku tsüklilised rühmad on isomorfsed, kusjuures iga lõpmatu tsükliline rühm on isomorfne rühmaga $(\mathbb{Z}, +)$ ja iga n -elemendiline tsükliline rühm on isomorfne rühmaga $(\mathbb{Z}_n, +)$.

TÕESTUS. Olgu $(G, \cdot)$ rühm ja $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Siis on kaks võimalust.

1) g astmete hulgas pole võrdseid. Siis G on lõpmatu,

$$G = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}. \quad (24)$$

Ei ole raske näha, et kujutus $\varphi : G \rightarrow \mathbb{Z}$, mis on defineeritud võrdusega

$$\varphi(g^k) := k.$$

on isomorfism. Seega $(G, \cdot) \simeq (\mathbb{Z}, +)$,

2) g astmete hulgas on võrdseid. See tähendab, et leiduvad $k, l \in \mathbb{Z}$, $k \neq l$, nii et $g^k = g^l$. Olgu $k > l$. Siis korrutades võrduse $g^k = g^l$ pooli elemendiga g^{-l} saame $g^{k-l} = g^0 = 1$. Et $k > l$, siis $k - l \in \mathbb{N}$. Olgu n vähim naturaalarv, mille korral $g^n = 1$. Näitame, et

$$G = \{1, g, g^2, \dots, g^{n-1}\}. \quad (25)$$

Selleks tuleb veenduda, et $G \subseteq \{1, g, g^2, \dots, g^{n-1}\}$. Vaatleme rühma G suvalist elementi $g^k \in G$, kus $k \in \mathbb{Z}$. Lause 5.3 põhjal leiduvad sellised $q, r \in \mathbb{Z}$, et $k = nq + r$ ja $0 \leq r < n$. Järelikult

$$g^k = g^{nq+r} = (g^n)^q g^r = 1^q g^r = g^r \in \{1, g, g^2, \dots, g^{n-1}\}$$

ja kehtib võrdus (25).

Veendume veel, et elemendid $1, g, g^2, \dots, g^{n-1}$ on paarikaupa erinevad. Selleks oletame vastuväiteliselt, et $g^k = g^l$, kus $0 \leq l < k \leq n-1$. Siis $g^{k-l} = g^{l-l} = 1$, kus $k-l < n$. See on vastuolus n minimaalsusega. Seega elemendid $1, g, g^2, \dots, g^{n-1}$ on paarikaupa erinevad ja $|G| = n$.

Tõestame, et $(G, \cdot) \simeq (\mathbb{Z}_n, +)$. Isomorfismiks $\varphi : G \rightarrow \mathbb{Z}_n$ sobib kujutus

$$\varphi(g^k) := \bar{k},$$

$k \in \{0, 1, \dots, n-1\}$. Eespool nägime, et

$$(\forall k, l \in \{0, 1, \dots, n-1\})(g^k = g^l \iff k = l).$$

Seega φ on korrektselt defineeritud ja injektiivne. On selge, et φ on surjektiivne. Näitame, et φ on homomorfism. Mistahes $k, l \in \{0, 1, \dots, n-1\}$ korral olgu $k + l = nq + r$, kus $0 \leq r < n$. Siis

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = \varphi(g^r) = \bar{r} = \overline{k+l} = \bar{k} + \bar{l} = \varphi(g^k) + \varphi(g^l).$$

□

Järeldus 5.6 Iga tsükliline rühm on Abeli rühm.

5.2 Rühma elemendi järk

Definitsioon 5.7 Olgu g rühma $(G, \cdot)$ element. Kui $|\langle g \rangle| = n \in \mathbb{N}$, siis öeldakse, et elemendi g **järk on** n ja kirjutatakse $\text{ord}_G(g) = n$ või lihtsalt $\text{ord}(g) = n$. Kui $\langle g \rangle$ on lõpmatu rühm, siis öeldakse, et g on **lõpmatut järku element**.

Definitsioonist tuleb välja, et igas rühmas on täpselt üks esimest järku element — see on ühikelement.

Näide 5.8 1. Vaatleme rühmade $(\mathbb{Z}_3, +)$ ja $(\mathbb{Z}, +)$ otsekorrutist $G = \mathbb{Z}_3 \times \mathbb{Z}$. Siis $\text{ord}_G((\bar{2}, 0)) = 3$ ja $\text{ord}_G((\bar{0}, 5)) = \infty$.

2. Substitutsioonirühmas S_3 on tsükli $(1, 3, 2)$ järguks 3.

Lagrange'i teoreemist järeldeb vahetult järgmine väide.

Lause 5.9 Lõpliku rühma iga elemendi järk jagab rühma järku.

Teoreemi 5.5 tõestuse põhjal võime öelda, et kehtib järgmine tulemus.

Lause 5.10 Kui rühma $(G, \cdot)$ elemendi g järk on lõplik, siis on see vähim selline naturaalarv n , mille korral $g^n = 1$.

Lause 5.11 Kui g on rühma $(G, \cdot)$ element ja $g^k = 1$ mingi naturaalarvu k korral, siis g järk on lõplik ja jagab arvu k .

TÕESTUS. Kuna $g^k = 1$, siis g on kindlasti lõplikku järku element, olgu $\text{ord}(g) = n$. Jagades arvu k jäägiga arvuga n saame leida $q, r \in \mathbb{Z}$ nii, et $k = nq + r$ ja $0 \leq r < n$. Järelikult

$$1 = g^k = g^{nq+r} = g^{nq} \cdot g^r = (g^n)^q \cdot g^r = 1 \cdot g^r = g^r.$$

Kuna n on vähim naturaalarv, mille korral $g^n = 1$, siis $r = 0$, s.t. $k = nq$. Seega n jagab arvu k . $\square$

Lause 5.12 Olgu G n -ndat järku tsükliline rühm, $G = \langle g \rangle = \{1, g, \dots, g^{n-1}\}$ ja olgu $k \in \{1, \dots, n-1\}$. Element g^k on rühma G tekitaaja paraajasti siis, kui $\text{SÜT}(k, n) = 1$.

TÕESTUS. TARVILIKKUS. Olgu $G = \langle g^k \rangle$. Siis leidub selline $u \in \mathbb{Z}$, et $(g^k)^u = g$. Järelikult $g^{ku} = g$ ja $g^{ku-1} = 1$. Lause 5.11 põhjal $n \mid ku - 1$. Seega leidub $q \in \mathbb{Z}$ nii, et $ku - 1 = nq$ ehk $ku - nq = 1$. Lause 5.4 põhjal $\text{SÜT}(k, n) = 1$.

PIISAVUS. Olgu $\text{SÜT}(k, n) = 1$. Siis lause 5.4 põhjal leiduvad sellised $u, v \in \mathbb{Z}$, et $ku + nv = 1$. Järelikult

$$g = g^{ku+nv} = g^{ku} \cdot g^{nv} = (g^k)^u \cdot (g^n)^v = (g^k)^u \cdot 1^v = (g^k)^u$$

ja $g^l = (g^k)^{ul}$ iga $l \in \{1, \dots, n\}$ korral. Viimane tähendab, et $G = \langle g^k \rangle$. $\square$

Lihtne on veenduda, et kehtib järgmine omadus.

Lemma 5.13 Kui $(G, \cdot)$ on rühm ja $g \in G$, siis $\text{ord}(g) = \text{ord}(g^{-1})$.

Lemma 5.14 Olgu $(G, \cdot)$ rühm, $g \in G$, $m, n \in \mathbb{N}$. Kui $\text{ord}(g) = mn$, siis $\text{ord}(g^m) = n$.

TÕESTUS. Tõestamiseks kasutame lauset 5.10. Olgu $\text{ord}(g) = mn$. Siis $(g^m)^n = g^{mn} = 1$. Kui oletada, et leidub $n' < n$, mille korral $(g^m)^{n'} = 1$, siis ka $g^{mn'} = 1$ ja $mn' < mn$, mis on vastuolus eeldusega. Seega n on vähim astendaja, mille korral $(g^m)^n = 1$; teiste sõnadega: $\text{ord}(g^m) = n$. $\square$

Tõestatud lemmat kasutame alljärgnevas aditiivsete rühmade korral.

Järeldus 5.15 Olgu $(A, +)$ rühm, $a \in A$, $m, n \in \mathbb{N}$. Kui $\text{ord}(a) = mn$, siis $\text{ord}(ma) = n$.

Meenutame, et **triviaalseks rühmaks** loetakse üheelemendilist rühma.

Lause 5.16 Olgu G mittetriviaalne lõplik rühm. Rühmal G ei ole mittetriviaalseid pärisalamrühmi parajasti siis kui G on algarvulise järguga tsükliline rühm.

TÕESTUS. TARVILIKKUS. Eeldame, et rühmal $G \neq \{1\}$ ei ole mittetriviaalseid pärisalamrühmi. Võtame mingi elemendi $g \in G \setminus \{1\}$. Siis $\langle g \rangle = G$ (seega G on tsükliline) ja $\text{ord}(g) = |G|$. Oletame vastuväiteliselt, et $|G|$ ei ole algarv. Siis $|G| = mn$, kus $m, n \in \mathbb{N}$, $m, n \neq 1$. Lemma 5.14 põhjal

$$n = \text{ord}(g^m) = |\langle g^m \rangle|.$$

Kuna $n < |G|$, siis $\langle g^m \rangle$ on mittetriviaalne pärisalamrühm rühmas G , vastuolu. Järelikult $|G|$ peab olema algarv.

PIISAVUS. Olgu $G = \{1, g, g^2, \dots, g^{p-1}\}$ tsükliline rühm algarvulise järguga p ja $\{1\} \neq H \leq G$. Siis leidub $k \in \{1, \dots, p-1\}$ nii, et $g^k \in H$. Kuna $\text{SÜT}(k, p) = 1$, siis lause 5.12 põhjal

$$G = \langle g^k \rangle \subseteq H \subseteq G,$$

kust $H = G$. Seega rühmal G puuduvad mittetriviaalsed pärisalamrühmad. $\square$

5.3 Perioodilised Abeli rühmad

Definitsioon 5.17 Rühma nimetatakse **perioodiliseks**, kui kõik tema elemendid on lõplikku järku.

Iga lõplik rühm on perioodiline, kuid leidub ka lõpmatuid perioodilisi rühmi.

Näide 5.18 Jäägiklassirühma $(\mathbb{Z}_2, +)$ loenduv otseaste

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots$$

on lõpmatu, kuid samas perioodiline, sest kõik tema nullist erinevad elemendid on teist järku.

Lemma 5.19 Olgu $(A, +)$ Abeli rühm ja p algarv. Siis hulk

$$A_p = \{a \in A \mid (\exists k \in \mathbb{N} \cup \{0\}) \text{ord}(a) = p^k\}$$

on rühma A alamrühm.

TÕESTUS. Kuna $\text{ord}(0) = 1 = p^0$, siis $0 \in A_p$ ja $A_p \neq \emptyset$.

Olgu $a, b \in A_p$, s.t. $\text{ord}(a) = p^k$ ja $\text{ord}(b) = p^l$, kus $k, l \in \mathbb{N} \cup \{0\}$. Siis $p^{\max(k,l)}(a+b) = 0$ ning järelikult $a+b$ järk peab jagama arvu $p^{\max(k,l)}$. Seega on see järk p aste ja $a+b \in A_p$.

Kui $a \in A_p$ ja $\text{ord}(a) = p^k$, siis lemma 5.13 põhjal $\text{ord}(-a) = \text{ord}(a) = p^k$ ja seega $-a \in A_p$. $\square$

Definitsioon 5.20 Alamrühma A_p nimetatakse Abeli rühma $(A, +)$ **p -komponendiks**.

Näide 5.21 Abeli rühma $(\mathbb{Z}_{24}, +)$ 3-komponent on alamrühm $\{\overline{8}, \overline{16}, \overline{0}\}$.

Tähistame sümboliga $\mathbb{P}$ kõigi algarvude hulka.

Teoreem 5.22 *Perioodiline Abeli rühm on oma p -komponentide otsesumma.*

TÕESTUS. Olgu A perioodiline Abeli rühm. Näitame, et A on oma p -komponentide summa:

$$A = \sum_{p \in \mathbb{P}} A_p.$$

Selleks tõestame, et $A \subseteq \sum_{p \in \mathbb{P}} A_p$ (vastupidine sisalduvus on ilmne). Olgu $a \in A$ suvaline element ja olgu tema järk n . Kui $n = 1$, siis $a = 0$ ja $a \in \sum_{p \in \mathbb{P}} A_p$. Kui $n \neq 1$, siis aritmeetika põhiteoreemi põhjal $n = p_1^{k_1} \dots p_s^{k_s}$, kus $p_1, \dots, p_s$ on paarikaupa erinevad algarvud ja $k_1, \dots, k_s$ on naturaalarvud. Tähistame

$$n_i := \frac{n}{p_i^{k_i}}.$$

Siis $\text{SÜT}(n_1, \dots, n_s) = 1$ ja lause 5.4 üldistuse tõttu leiduvad $u_1, \dots, u_n \in \mathbb{Z}$ nii, et $u_1 n_1 + \dots + u_s n_s = 1$. Järelikult

$$a = 1 \cdot a = (u_1 n_1 + \dots + u_s n_s) a = u_1 n_1 a + \dots + u_s n_s a.$$

Kuna iga $i \in \{1, \dots, s\}$ korral

$$p_i^{k_i}(u_i n_i a) = (p_i^{k_i} u_i n_i) a = (u_i p_i^{k_i} n_i) a = (u_i n) a = u_i(na) = u_i 0 = 0,$$

siis lause 5.11 põhjal elemendi $u_i n_i a$ järk on $p_i^{k_i}$ jagaja, seega p_i aste. Järelikult iga i korral $u_i n_i a \in A_{p_i}$ ja $a \in \sum_{p \in \mathbb{P}} A_p$.

Veel tuleb näidata, et rühma A alamrühmade A_p , $p \in \mathbb{P}$, summa on otsesumma. Kasutame selleks teoreemi 1.88 tingimust 2. Olgu q mingi algarv ja oletame, et $a \in A_q \cap \sum_{p \in \mathbb{P} \setminus \{q\}} A_p$. Et $a \in A_q$, siis $\text{ord}(a) = q^k$ mingi $k \in \mathbb{N} \cup \{0\}$ korral. Teisest küljest $a \in \sum_{p \in \mathbb{P} \setminus \{q\}} A_p$ ja seega leiduvad $p_1, \dots, p_s \in \mathbb{P} \setminus \{q\}$, elemendid $a_{p_1}, \dots, a_{p_s} \in A$ ja arvud $k_1, \dots, k_s \in \mathbb{N} \cup \{0\}$ nii, et

$$a = a_{p_1} + \dots + a_{p_s}$$

ja iga $i \in \{1, \dots, s\}$ korral $\text{ord}(a_{p_i}) = p_i^{k_i}$. Olgu $n = p_1^{k_1} \dots p_s^{k_s}$. Siis $na = na_{p_1} + \dots + na_{p_s} = 0$, millest järeldub, et $q^k = \text{ord}(a) \mid n$. Kui $k \geq 1$, siis arvul n oleks algtegur $q \notin \{p_1, \dots, p_s\}$, mis aritmeetika põhiteoreemi tõttu on välistatud. Järelikult $k = 0$ ja $\text{ord}(a) = q^0 = 1$ ehk $a = 0$. Sellega oleme näidanud, et

$$A_q \cap \sum_{p \in \mathbb{P} \setminus \{q\}} A_p = \{0\}.$$

See tähendab, et A on alamrühmade A_p , $p \in \mathbb{P}$, otsesumma. $\square$

5.4 Lõplikud Abeli p -rühmad

Definitsioon 5.23 Olgu p algarv. Rühma nimetatakse **p -rühmaks**, kui tema iga elemendi järk on p aste.

Näide 5.24 Rühm $(\mathbb{Z}_{81}, +)$ on 3-rühm, sest tema iga elemendi järk peab olema $3^4 = 81$ jagaja, seega 3 aste.

Lõpliku Abeli rühma p -komponendid on definitsiooni järgi p -rühmad ja me teame, et lõplik Abeli rühm esitub oma p -komponentide otsesummana. Seega lõplike Abeli rühmade kirjeldamiseks piisab, kui me oskame kirjeldada lõplikke Abeli p -rühmi. See ongi selle paragrahvi põhieesmärk.

Alustuseks tõestame ühe kasuliku teoreemi.

Teoreem 5.25 (Cauchy) *Olgu p algarv. Kui $(A, +)$ on lõplik Abeli rühm ja $p \mid |A|$, siis rühmas A leidub element, mille järk on p .*

TÕESTUS. Tõestame väite induktsiooniga rühma A järgu $|A|$ järgi.

Alus. Kui $|A| = p$, siis selles rühmas peab leiduma element $a \neq 0$. Kuna $\text{ord}(a) \neq 1$ ja $\text{ord}(a)$ jagab rühma järku p , siis $\text{ord}(a) = p$. See tähendab, et A on tsükliline rühm tekitajaga a .

Samm. Eeldame, et $|A| > p$ ja et väide kehtib väiksema elementide arvuga rühmade korral. Siis A järk ei saa olla algarv. Seega lause 5.16 põhjal A sisaldab mittetriviaalset pärisalamrühma B . Lagrange'i teoreemi (teoreem 1.47) põhjal

$$|A| = |A/B| \cdot |B|,$$

kusjuures $|B| < |A|$. Et B on mittetriviaalne, siis $|B| > 1$ ja seega $|A/B| < |A|$. Kuna $p \mid |A|$ ja p on algarv, siis on 2 võimalust.

1) $p \mid |B|$. Siis induktsiooni eelduse põhjal rühm B sisaldab p -ndat järku elementi ning selle elemendi järk on p ka rühmas A .

2) $p \nmid |A/B|$. Sel juhul faktorrühm A/B rahuldab ka induktsiooni eeldust ja peab sisaldama mingit p -ndat järku elementi $a + B$. Olgu $n := \text{ord}_A(a)$. Kuna $na = 0$, siis ka

$$n(a + B) = (na) + B = 0 + B = B$$

faktorrühmas A/B . Lause 5.11 tõttu $p \mid n$, järelikult $pk = n$ mingi $k \in \mathbb{N}$ korral. Kuna $\text{ord}_A(a) = pk$, siis järeldusest 5.15 saame, et $\text{ord}_A(ka) = p$. $\square$

Järeldus 5.26 *Lõplik Abeli rühm on p -rühm parajasti siis, kui tema järk on p aste.*

TÕESTUS. TARVILIKKUS. Olgu A lõplik Abeli p -rühm. Oletame vastuväiteliselt, et $|A|$ ei ole p aste, siis ta jagub mingi teise algarvuga q . Teoreemi 5.25 põhjal leidub rühmas A q -ndat järku element, mis on vastuolus sellega, et A on p -rühm.

PIISAVUS. Olgu $|A| = p^n$. Siis lause 5.9 põhjal iga A elemendi järk on p^n jagaja, seega p aste. $\square$

Järgnev teoreem annab lõplike Abeli p -rühmade kirjelduse.

Teoreem 5.27 *Lõplik Abeli p -rühm on oma mingite tsükliliste alamrühmade otsesumma.*

TÕESTUS. Järelduse 5.26 põhjal on lõpliku Abeli p -rühma järk algarvu p aste. Tõestame teoreemi induktsiooniga rühma järgu järgi.

Alus. Kui Abeli p -rühma järk on p , siis teoreemi 5.25 põhjal sisaldab ta p -ndat järku elementi, seega on ta tsükliline rühm ja meil on triviaalne otsesumma ühe otseliidetavaga.

Samm. Olgu A Abeli p -rühm ja $|A| = p^n$, kus $n \geq 2$. Lihtne on näha, et hulk

$$pA = \{pa \mid a \in A\} \subseteq A$$

on rühma A alamrühm. Kui $\text{ord}(a) = p^k$, siis järelduse 5.15 põhjal $\text{ord}(pa) = p^{k-1}$, seega pA on samuti p -rühm. Kui oletada, et $pA = A$, siis

$$A = pA = p^2A = \dots = p^nA = \{0\},$$

sest lause 5.9 põhjal on iga A elemendi järk p^n jagaja. Vastuoluline võrdus $A = \{0\}$ näitab, et $pA \subset A$ ja seega saame rühmale pA rakendada induktsiooni eeldust. Selle põhjal leiduvad nullist erinevad elemendid $pa_1, \dots, pa_r$ rühmas pA nii, et

$$pA = \langle pa_1 \rangle + \dots + \langle pa_r \rangle. \quad (26)$$

Tähistame

$$B := \langle a_1 \rangle + \dots + \langle a_r \rangle \leq A$$

ja näitame, et see tsükliliste alamrühmade summa on otsesumma. Selleks kontrollime teoreemi 1.83 tingimust 3. Oletame, et

$$k_1a_1 + \dots + k_ra_r = 0, \quad (27)$$

kus $k_1, \dots, k_r \in \mathbb{Z}$. On 2 võimalust.

1) Iga $i \in \{1, \dots, r\}$ korral $p \mid k_i$, s.t. $k_i = pm_i$ mingi $m_i \in \mathbb{Z}$ korral. Siis

$$m_1(pa_1) + \dots + m_r(pa_r) = 0,$$

kust võrduse (26) tõttu $0 = m_i pa_i = k_i a_i$ iga $i \in \{1, \dots, r\}$ korral.

2) Leidub $j \in \{1, \dots, r\}$ nii, et $p \nmid k_j$. Võrdusest (27) saame, et

$$k_1(pa_1) + \dots + k_r(pa_r) = 0,$$

kust võrduse (26) tõttu järeldub, et $pk_i a_i = 0$ iga $i \in \{1, \dots, r\}$ korral, muuhulgas $pk_j a_j = 0$. Olgu $\text{ord}(a_j) = p^e$, $e \in \mathbb{N} \cup \{0\}$. Lause 5.11 põhjal $p^e \mid pk_j$. Kuna $p \nmid k_j$, siis $p^e \mid p$ ehk $e \leq 1$. Järelikult $pa_j = 0$, mis on vastuolus sellega, et pa_j pidi olema nullist erinev.

Kuna võrdusest (27) järeldus, et $k_1a_1 = \dots = k_ra_r = 0$, siis oleme tõestanud, et

$$B = \langle a_1 \rangle + \dots + \langle a_r \rangle \leq A.$$

Tähistame

$$C := \{a \in A \mid pa = 0\} \leq A$$

(s.t. C koosneb rühma A p -ndat järku elementidest ja 0-st) ning näitame, et

$$A = B + C.$$

Selleks võtame suvalise $a \in A$. Siis $pa \in pA$ ja seega leiduvad $k_1, \dots, k_r \in \mathbb{Z}$ nii, et

$$pa = k_1(pa_1) + \dots + k_r(pa_r).$$

Järelikult $p(a - k_1a_1 - \dots - k_ra_r) = 0$ ehk

$$c := a - k_1a_1 - \dots - k_ra_r \in C.$$

See tähendab, et

$$a = (k_1a_1 + \dots + k_ra_r) + c \in B + C.$$

Kui nüüd $B = A$, siis on tõestus lõppenud. Kui $B \neq A$, siis $C \not\subseteq B$ ja leidub mingi element $c_1 \in C \setminus B$. Siis $c_1 \neq 0$ ja summa

$$B_1 := B + \langle c_1 \rangle$$

on otsesumma, sest $\langle c_1 \rangle$ on tsükliline rühm algarvulise järguga p , seega lause 5.16 põhjal tema alamrühm $B \cap \langle c_1 \rangle$ peab olema triviaalne, $B \cap \langle c_1 \rangle = \{0\}$. Niisiis

$$B_1 = B \dot{+} \langle c_1 \rangle$$

ja $B < B_1 \leq A$. Kui nüüd $B_1 = A$, siis on vajalik esitus A jaoks olemas. Vastasel korral kordame mõttekäiku valides mingi $c_2 \in C \setminus B_1$. Sarnaselt eelnevaga saame otsesumma

$$B_2 = B_1 \dot{+} \langle c_2 \rangle = B \dot{+} \langle c_1 \rangle \dot{+} \langle c_2 \rangle.$$

Kuna A on lõplik, siis pärast lõplikku arvu samme jõuame lahutuseni

$$A = B_s = B \dot{+} \langle c_1 \rangle \dot{+} \dots \dot{+} \langle c_s \rangle = \langle a_1 \rangle \dot{+} \dots \dot{+} \langle a_r \rangle \dot{+} \langle c_1 \rangle \dot{+} \dots \dot{+} \langle c_s \rangle.$$

□

Teoreemidest 5.22 ja 5.27 saame nüüd järgmise tulemuse.

Teoreem 5.28 *Lõplik Abeli rühm on oma mingite tsükliliste alamrühmade otsesumma.*

Järeldus 5.29 *Rühm A on lõplik Abeli rühm parajasti siis kui leiduvad $n_1, \dots, n_s \in \mathbb{N}$ nii, et $A \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$.*

Lõplike Abeli rühmade kirjelduse andis 1870. aastal saksa matemaatik Leopold Kronecker (1823–1891). On võimalik täpsustada, millisel kujul peavad arvud $n_1, \dots, n_s$ olema.



Leopold Kronecker

Näide 5.30 Vaatleme lõplikku Abeli rühma $A = (\mathbb{Z}_{12}, +)$. Selle rühma p -komponendid on

$$\begin{aligned} A_2 &= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \simeq \mathbb{Z}_4, \\ A_3 &= \{\bar{0}, \bar{4}, \bar{8}\} \simeq \mathbb{Z}_3, \\ A_p &= \{\bar{0}\}, \text{ kui } p \in \mathbb{P} \setminus \{2, 3\}. \end{aligned}$$

Seega $A = A_2 \dot{+} A_3$. Teoreemi 1.89 põhjal on A isomorfne oma alamrühmade A_2 ja A_3 välise otsesummaga, $A \simeq A_2 \oplus A_3$. Et lõpliku arvu rühmade väline otsesumma on isomorfne nende otsekorutisega, siis võime öelda, et

$$A \simeq A_2 \times A_3 \simeq \mathbb{Z}_4 \times \mathbb{Z}_3.$$

5.5 Vabad Abeli rühmad

Sarnaselt vektorruumidega saab Abeli rühmades rääkida lineaarkombinatsioonidest. Ainus vahe on selles, et korpuse elementide asemel on täisarvud.

Definitsioon 5.31 Olgu $a_1, \dots, a_n$ Abeli rühma A elemendid ja olgu $k_1, \dots, k_n$ täisarvud. Avaldist

$$k_1 a_1 + \dots + k_n a_n, \quad (28)$$

aga ka selle avaldise poolt määratud rühma A elementi, nimetatakse elementide $a_1, \dots, a_n$ **lineaarkombinatsiooniks**. Arve $k_1, \dots, k_n$ nimetatakse selle lineaarkombinatsiooni **kordajateks**. Lineaarkombinatsiooni nimetatakse **triviaalseks**, kui tema kõik kordajad on nullid.

Definitsioon 5.32 Abeli rühma A elementide süsteemi $a_1, \dots, a_n$ nimetatakse

- **lineaarselt sõltumatuks**, kui

$$(\forall k_1, \dots, k_n \in \mathbb{Z})(k_1 a_1 + \dots + k_n a_n = 0 \implies k_1 = \dots = k_n = 0),$$

- **lineaarselt sõltuvaks**, kui ta ei ole lineaarselt sõltumatu.

Lõpmatut elementide süsteemi nimetatakse **lineaarselt sõltumatuks**, kui tema iga lõplik alamsüsteem on lineaarselt sõltumatu.

Vektorruumis on vähemalt kahest vektorist koosnev lõplik vektorite süsteem lineaarselt sõltuv parajasti siis, kui selle süsteemi mingi vektor avaldub ülejäänud vektorite lineaarkombinatsioonina. Abeli rühmade puhul see nii ei ole.

Näide 5.33 Vaatleme Abeli rühmas $\mathbb{Z}$ elementide 2 ja 3 lineaarkombinatsiooni

$$3 \cdot 2 + (-2) \cdot 3 = 0.$$

Kuna kordaja $3 \neq 0$, siis see süsteem on lineaarselt sõltuv. Samas kumbki arvudest 2 ja 3 ei avaldu teise lineaarkombinatsioonina.

Definitsioon 5.34 Abeli rühma **baasiks** nimetatakse tema lineaarselt sõltumatut moodustajate süsteemi. Abeli rühma nimetatakse **vabaks**, kui temas leidub baas.

On võimalik tõestada, et vaba Abeli rühma mistahes kaks baasi on sama võimsusega. Selles kursuses me seda tõestust ei anna. Vaba Abeli rühma baasi võimsust nimetatakse selle rühma **astakuks**.

Näide 5.35 1. Abeli rühm $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}$ komponenthaaval defineeritud liitmise suhtes on vaba, kusjuures baasiks võib võtta $e_1 = (1, 0)$, $e_2 = (0, 1)$ (aga ka näiteks $(1, 0)$, $(0, -1)$). See süsteem on moodustajate süsteem, sest

$$(\forall (k, l) \in \mathbb{Z} \times \mathbb{Z})(k, l) = k e_1 + l e_2$$

ja ta on lineaarselt sõltumatu, sest

$$(\forall k, l \in \mathbb{Z})(k e_1 + l e_2 = (0, 0) \implies (k, l) = (0, 0) \implies k = 0 \text{ ja } l = 0).$$

2. Rühm $(\mathbb{Z}_2, +)$ ei ole vaba. Selles rühmas $\bar{1}$ on küll moodustajate süsteem, aga ta on lineaarselt sõltuv, sest $2 \cdot \bar{1} = \bar{0}$, kuid $0 \neq 2 \in \mathbb{Z}$.

Järgnev tulemus näitab, et kõik vabad Abeli rühmad on teatud mõttes sarnased näites 5.35 vaadeldud Abeli rühmaga.

Teoreem 5.36 *Abeli rühm on vaba parajasti siis, kui ta on isomorfne lõpmatute tsükliliste rühmade välise otsesummaga.*

TÕESTUS. PIISAVUS. Teoreemi 5.5 põhjal on kõik lõpmatud tsüklilised rühmad isomorfseid rühmaga $(\mathbb{Z}, +)$. Vaatleme välist otsesummat $\oplus \sum_{i \in I} A_i$, kus $A_i = (\mathbb{Z}, +)$ iga $i \in I$ korral. Tähistame iga $i \in I$ korral $e_i = (x_j)_{j \in I}$, kus

$$x_j = \begin{cases} 1, & \text{kui } j = i, \\ 0, & \text{kui } j \neq i. \end{cases}$$

Lihtne on aru saada, et $\{e_i \mid i \in I\}$ on Abeli rühma $\oplus \sum_{i \in I} A_i$ baas ning seega see rühm on vaba.

TARVILIKKUS. Olgu F vaba Abeli rühm baasiga $e = \{e_i \mid i \in I\}$. On lihtne veenduda, et hulgad $\mathbb{Z}e_i = \{ke_i \mid k \in \mathbb{Z}\} \subseteq F$ on rühma F alamrühmad. Kuna e on moodustajate süsteem, siis iga $a \in F$ jaoks leiduvad $i_1, \dots, i_n \in I$ ja $k_1, \dots, k_n \in \mathbb{Z}$ nii, et

$$a = k_1 e_{i_1} + \dots + k_n e_{i_n} \in \sum_{i \in I} \mathbb{Z}e_i.$$

Seega

$$F = \sum_{i \in I} \mathbb{Z}e_i.$$

Näitame, et see summa on otsesumma. Selleks vaatleme Abeli rühma F moodulina üle ringi $\mathbb{Z}$ ja kontrollime teoreemi 1.88 tingimust 3. Olgu $i_1, \dots, i_n \in I$ paarikaupa erinevad indeksid, $k_1 e_{i_1} \in \mathbb{Z}e_{i_1}, \dots, k_n e_{i_n} \in \mathbb{Z}e_{i_n}$, ning oletame, et

$$k_1 e_{i_1} + \dots + k_n e_{i_n} = 0.$$

Kuna e on linearselt sõltumatu, siis $k_1 = \dots = k_n = 0$ ja seega $k_1 e_{i_1} = \dots = k_n e_{i_n} = 0$. Sellega oleme tõestanud, et

$$F = \sum_{i \in I} \mathbb{Z}e_i.$$

Teoreemi 1.89 põhjal

$$F \simeq \oplus \sum_{i \in I} \mathbb{Z}e_i.$$

Tõestuse lõpetamiseks veendume, et $\mathbb{Z}e_i \simeq \mathbb{Z}$ iga $i \in I$ korral. Selleks vaatleme kujutust

$$f : \mathbb{Z} \rightarrow \mathbb{Z}e_i, \quad k \mapsto ke_i.$$

Kuna mistahes $k, l \in \mathbb{Z}$ korral

$$f(k + l) = (k + l)e_i = ke_i + le_i = f(k) + f(l),$$

siis f on rühmade homomorfism. On selge, et f on sürjektiivne. Kui $ke_i = f(k) = 0$, siis linearselt sõltumatuse tõttu $k = 0$. Seega $\text{Ker}(f) = \{0\}$ ja f on ka injektiivne. Kokkuvõttes f on isomorfism ja rühmad $\mathbb{Z}e_i$, $i \in I$, on lõpmatud tsüklilised rühmad. $\square$

Lause 5.37 Iga Abeli rühm on isomorfnene mingi vaba Abeli rühma faktorrühmaga.

TÕESTUS. Olgu A suvaline Abeli rühm. Vaatleme hulka A indekseid hulga A moodustavate välise otsesumma

$$F = \bigoplus_{a \in A} A_a,$$

kus $A_a = (\mathbb{Z}, +)$ on tsüklilised rühmad. Teoreemi 5.36 tõttu on F vaba Abeli rühm. Vaatleme kujutust

$$f : F \rightarrow A, \quad (k_a)_{a \in A} \mapsto \sum_{a \in A} k_a a.$$

Kuna üldistatud jadas $(k_a)_{a \in A}$ esineb lõplik arv nullist erinevaid täisarve, siis summa $\sum_{a \in A} k_a a$ on samuti lõplik. Lihtne on veenduda, et f on rühmade homomorfism. Ta on ka surjektiivne, sest elemendi $a \in A$ originaaliks sobib jada, mille a -komponent on täisarv 1 ja ülejäänud komponendid on nullid. Rühmade homomorfismiteoreem (teoreem 1.55) ütleb, et

$$A \simeq F / \text{Ker}(f).$$

□

Lõpetuseks soovime uurida vabade Abeli rühmade alamrühmi. Selleks läheb meil vaja kahte lauset.

Lause 5.38 Rühma $(\mathbb{Z}, +)$ alamrühmad on parajasti kujul $m\mathbb{Z}$, kus $m \in \mathbb{N} \cup \{0\}$.

TÕESTUS. On selge, et alamhulga $m\mathbb{Z} \subseteq \mathbb{Z}$ on alamrühmad. Näitame, et teisi alamrühmi ei ole. Olgu $H \neq \{0\}$ rühma $\mathbb{Z}$ alamrühm. Siis peab leiduma vähim naturaalarv m , mis kuulub hulka H . Kuna H on alamrühm, siis $m\mathbb{Z} \subseteq H$. Vastupidise sisalduvuse tõestamiseks võtame suvalise $a \in H$ ja jagame selle jäägiga arvuga m :

$$a = mq + r, \quad 0 \leq r < m.$$

Et $a, mq \in H$, siis ka $r = a - mq \in H$. Kui $r \neq 0$, siis oleme saanud vastuolu m valikuga. Seega $r = 0$ ja $a = mq \in m\mathbb{Z}$. Niisiis $H \subseteq m\mathbb{Z}$ ja kokkuvõttes $H = m\mathbb{Z}$. □

Lause 5.39 Kui A on Abeli rühm, F on vaba Abeli rühm ja $f : A \rightarrow F$ on surjektiivne homomorfism, siis

$$A \simeq \text{Ker}(f) \oplus F.$$

TÕESTUS. Olgu $\{e_i \mid i \in I\}$ vaba Abeli rühma F baas. Iga $i \in I$ jaoks valime elemendi $a_i \in A$ nii, et

$$f(a_i) = e_i.$$

Defineerime kujutuse $g : F \rightarrow A$ võrdusega

$$g(k_1 e_{i_1} + \dots + k_n e_{i_n}) := k_1 a_{i_1} + \dots + k_n a_{i_n}.$$

See kujutus on korrektselt defineeritud, sest rühma F iga element avaldub üheselt summana $k_1 e_{i_1} + \dots + k_n e_{i_n}$, kus $i_1, \dots, i_n \in I$ on paarikaupa erinevad ja $k_1, \dots, k_n \in \mathbb{Z}$. Lihtne on näha, et g on rühmade homomorfism. Kuna

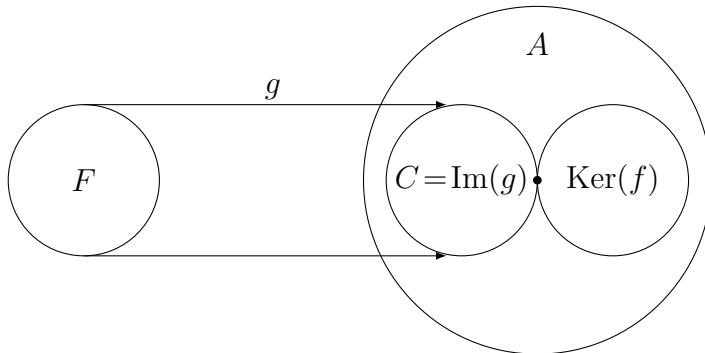
$$\begin{aligned} (f \circ g)(k_1 e_{i_1} + \dots + k_n e_{i_n}) &= f(k_1 a_{i_1} + \dots + k_n a_{i_n}) = k_1 f(a_{i_1}) + \dots + k_n f(a_{i_n}) \\ &= k_1 e_{i_1} + \dots + k_n e_{i_n}, \end{aligned}$$

siis $f \circ g = \text{id}_F$. Sellest järeldub, et kujutus g on üksühene. Seega

$$C := \text{Im}(g) \simeq F,$$

kus C on rühma A alamrühm. Tõestame, et

$$A = \text{Ker}(f) \dot{+} C.$$



Kui $a \in A$, siis

$$f(a - (g \circ f)(a)) = f(a) - (f \circ g \circ f)(a) = f(a) - f(a) = 0.$$

Seega $b := a - (g \circ f)(a) \in \text{Ker}(f)$ ja $a = b + g(f(a)) \in \text{Ker}(f) + C$. Niisiis $A = \text{Ker}(f) + C$. Kui $a \in \text{Ker}(f) \cap C$, siis leidub $x \in F$ nii, et $a = g(x)$. Järelikult

$$x = (f \circ g)(x) = f(a) = 0,$$

kust $a = g(x) = g(0) = 0$. Seega $\text{Ker}(f) \cap C = \{0\}$ ja $A = \text{Ker}(f) \dot{+} C$ tänu teoreemile 1.83. Teoreemi 1.89 põhjal

$$A \simeq \text{Ker}(f) \oplus C \simeq \text{Ker}(f) \oplus F.$$

□

Teoreem 5.40 *Lõpliku baasiga vaba Abeli rühma iga nullist erinev alamrühm on vaba.*

TÕESTUS. Tõestame induktsiooniga n järgi, et kui F on vaba Abeli rühm, milles leidub n elemendist koosnev baas, siis igas tema nullist erinevas alamrühmas leidub ülimalt n elemendist koosnev baas.

Alus. Kui baasis on 1 element, siis on meie Abeli rühm isomorfne rühmaga $(\mathbb{Z}, +)$. Selle nullist erinevad alamrühmad on lause 5.38 põhjal kujul $m\mathbb{Z}$, $m \in \mathbb{N}$, ja need on samuti vabad Abeli rühmad 1 baasielemendiga m .

Samm. Olgu $n > 1$ ja eeldame, et väide kehtib Abeli rühmade jaoks, kus on baas, mille elementide arv on $< n$. Vaatleme vaba Abeli rühma, kus on olemas n elemendist koosnev baas. Teoreemi 5.36 tõestuse põhjal on see rühm isomorfne rühmaga

$$F = Z_1 \oplus \dots \oplus Z_n = Z_1 \times \dots \times Z_n,$$

kus $Z_i = (\mathbb{Z}, +)$ iga $i \in \{1, \dots, n\}$ korral. Piisab, kui tõestada väide rühma F jaoks.

Olgu $B \neq \{(0, \dots, 0)\}$ rühma F alamrühm ja näitame, et B on vaba. Vaatleme kujutust

$$f : F \rightarrow Z_1, \quad (k_1, k_2, \dots, k_n) \mapsto k_1$$

(s.t. f on otsekorrutise projektsioon esimesele tegurile Z_1). See on kahtlemata sürjektiivne rühmade homomorfism. Vaatleme kujutust

$$f' : B \rightarrow f(B), \quad b \mapsto f(b).$$

Ka see on sürjektiivne rühmade homomorfism. Tähistame

$$B' := \text{Ker}(f') = \{b \in B \mid f(b) = 0\} = \text{Ker}(f) \cap B.$$

Siis

$$B' \subseteq \text{Ker}(f) = \{(0, k_2, \dots, k_n) \mid k_2, \dots, k_n \in \mathbb{Z}\} \simeq Z_2 \times \dots \times Z_n.$$

Vabas Abeli rühmas $Z_2 \times \dots \times Z_n$ leidub $n - 1$ elemendist koosnev baas (järjendid, mille üks komponent on 1 ja ülejäänud 0-d) ja B' on isomorfne selle alamrühmaga. Induktsiooni eelduse põhjal kas B' on nullalamrühm või ta on vaba Abeli rühm, milles leidub ülimalt $n - 1$ elemendist koosnev baas.

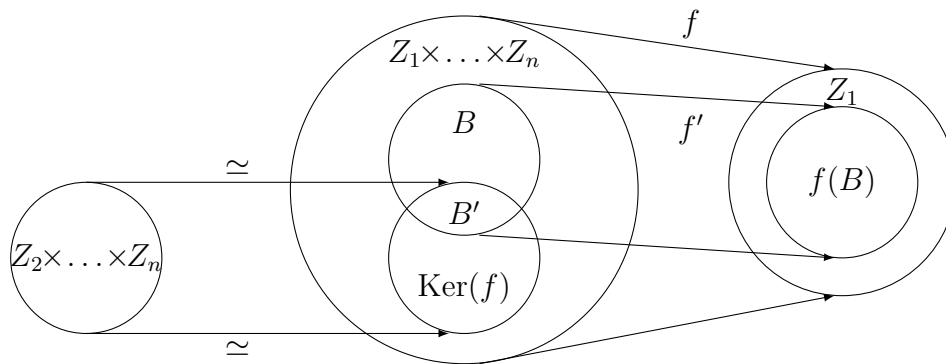
On kaks võimalust.

1) $f(B) = \{0\}$. Siis iga $(l_1, l_2, \dots, l_n) \in B$ korral $l_1 = 0$, seega $B \subseteq \text{Ker}(f)$. Nii nagu eespool B' jaoks, saame induktsiooni eelduse abil järeldada, et B on vaba Abeli rühm, milles leidub ülimalt $n - 1$ elemendist koosnev baas.

2) $f(B) \neq \{0\}$. Siis $f(B) \leq Z_1$ on ühe baasielemendiga vaba Abeli rühm, nagu nägime induktsiooni aluse tõestuses. Lause 5.39 põhjal

$$B \simeq \text{Ker}(f') \oplus f(B) = B' \oplus f(B).$$

Seega B on vaba Abeli rühm, milles leidub ülimalt $(n - 1) + 1 = n$ elemendist koosnev baas.



□

Kasutatud kirjandus

1. M. Kilp, Algebra I, Eesti Matemaatika Selts, Tartu, 2005.
2. K. Kaarli, Algebra II loengute slaidid,
http://math.ut.ee/pmi/kursused/algebraII/algebra2_slides.pdf .
3. L. Tart, Arvuteooria loengukonspekt,
http://kodu.ut.ee/~ltart/Arvuteooria_k2019/kon_2019.pdf .