

ALGEBRA II

Kevad 2019

Loengukonspekt

Lektor: Valdis Laan

20. juuni 2019. a.

Sisukord

1 Üldise algebra põhimõisted ja -konstruktsioonid	4
1.1 Ω -algebra	4
1.2 Homomorfismid	4
1.3 Alamalgebra	8
1.4 Faktoralgebra	10
1.5 Kõrvalklassid, Lagrange'i teoreem	12
1.6 Faktorruhm	13
1.7 Faktorring	16
1.8 Faktorruum	18
1.9 Ω -algebrate otsekorrutis	18
1.10 Moodulid üle ringi	19
1.11 R -moodulite väligne otsesumma	20
1.12 R -moodulite sisemine otsesumma	21
1.13 Vektorruumide otsesummad	23
2 Polünoomid, algebra põhiteoreem	27
2.1 Mitme muutuja polünoomide ringid	27
2.2 Sümmeetrilised polünoomid	29
2.3 Polünoomi lahutuskorpus	31
2.4 Algebra põhiteoreem	33
3 Lineaarteisenduse kanooniline baas	37
3.1 Probleemi püstitus ja põhitulemuse sõnastus	37
3.2 Invariantsed alamruumid	37
3.3 Nilpotentse lineaarteisenduse kanooniline baas	38
3.4 Nilpotentse maatriksi Jordani normaalkuju leidmine	43
3.5 Piisav tingimus kanoonilise baasi olemasoluks	43
3.6 Cayley-Hamiltoni teoreem	46
3.7 Kanoonilise baasi ja Jordani normaalkuju leidmine	50
4 Funktsionaalid ja vormid	51
4.1 Lineaarsed funktsionaalid ja lineaarvormid	51
4.2 Bilineaarsed funktsionaalid ja bilineaarvormid	54
4.3 Ruutfunktsionaalid ja ruutvormid	56
4.4 Ruutfunktsionaalid vektorruumidel üle \mathbb{C} ja \mathbb{R}	59
5 Abeli rühmad	64
5.1 Tsüklilised rühmad	64
5.2 Rühma elemendi järk	65
5.3 Perioodilised Abeli rühmad	67
5.4 Lõplikud Abeli p -rühmad	68

Sissejuhatus

Tegemist on 2019. aasta kevadel 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 eelmissse kursusse 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 parandamisele ja täiendamisele on kaasa aidanud mitmed üliõpilased: Jaagup Kirme, Indrek Pertman, Tähvend Uustalu. Tänud neile!

1 Üldise algebra põhimõisted ja -konstruktsioonid

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

1.1 Ω -algebra

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

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

nimetatakse **n -aarseks** ehk **n -kohaliseks tehteks** hulgat 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 mittelöikuvate 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 tehemärkide hulgast, kusjuures Ω_i all peame silmas kõigi i -kohaliste tehete märkide hulka.

Definitsioon 1.3 Olgu Ω tüüp. Mittetühja hulka A nimetatakse **Ω -algebraks**, kui iga $n \in \{0, 1, 2, \dots\}$ ja iga $\omega \in \Omega_n$ jaoks on hulgat 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 tehte märki, peab ka Ω -algebra A olema kindlasti mittetühi.

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 .

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 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 teht, mis fikseerib nullelemendi, ühekohaline skalariga korrutamise tehe iga $k \in K$ jaoks (neid on lõpmata palju, kui K on lõpmatu) ja kahekohalise liitmistehte. Vastandelemendi võtmise tehet ei ole vaja eraldi vaadelda, sest see teht on sama, mis skalariga -1 korrutamine.

1.2 Homomorfismid

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

Definitsioon 1.5 Olgu 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 tehte 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 tähistatse 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 nullkohalise tehte, mis fikseerib rühma ühikelemendi;
- iga $x \in A$ korral $\varphi(x^{-1}) = (\varphi(x))^{-1}$, s.t. φ säilitab ühekohalise pöördelemendi võtmise tehte;
- iga $x, y \in A$ korral $\varphi(xy) = \varphi(x)\varphi(y)$, s.t. φ säilitab kahekohalise korrutamistehte.

Märkus 1.7 Kui meil on kaks rühma A ja B , siis formaalselt võttes peaksime nullkohalise tehtemärgi 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.

Algebraate puhul võib olla nii, et mingite tehete säilitamisest järel dub mingite teiste tehete säilitamine. Nii näiteks rühmade korrutamise säilitamisest järel dub nii ühikelemendi säilitamine kui ka pöördelentide 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

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

TÖESTUS. Tarvilikkus on definitsiooni põhjal ilmne. Piisavuse töestamiseks peame näitama, et korrutamise säilitamisest järel dub ühikelemendi ja pöördelemendi võtmise säilitamine. Eeldame, et kujutus $\varphi : A \rightarrow B$ säilitab korrutamise. 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 elemendiga $\varphi(1)^{-1}$ ja kasutades rühma tehete omadusi saame võrduse $\varphi(1) = 1$. Seega φ säilitab ühikelemendi fikseerimise tehte. 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 $\varphi(x^{-1}) = (\varphi(x))^{-1}$. \square

Abeli rühmade korral räägitakse harilikult liitmistehest ja seega eelnev lause saab järgmisse kuju.

Lause 1.9 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 1.10 Olgu A ja B ringid. Arvestades lauset 1.9 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 1.11 Olgu A ja B vektorruumid üle korpuse K . Arvestades jällegi lauset 1.9 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 1.12 Vektorruumide homomorfismidest (lineaarkujutustest) oleme vaadelnud hulgaliselt näiteid kursuses “Algebra I”.

Vaatleme regulaarsete maatriksite rühma $GL_n(\mathbb{R})$ korrutamise suhtes ja nullist erinevate reaalarvude rühma \mathbb{R}^* korrutamise suhtes. Siis kujutus

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

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

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 $\psi\varphi : A \rightarrow C$ on defineeritud eeskirjaga

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

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

Lause 1.13 *Kui kahe Ω -algebra homomorfismi korrutis on defineeritud, siis see korrutis on ise ka Ω -algebra homomorfism.*

TÖESTUS. 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

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

Samuti iga $\omega \in \Omega_0$ korral

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

□

Definitsioon 1.14 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 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 1.15 Iga Ω -algebra A korral on hulk $\text{End}(A)$ monoid kujutuste korrutamise (s.t. järjest rakendamise) suhtes.

TÖESTUS. Selle lihtsa tõestuse jätame läbimõttlemiseks lugejale. \square

Definitsioon 1.16 Bijektiivset homomorfismi nimetatakse **isomorfismiks**.

Definitsioon 1.17 Ω -algebraid A ja B nimetatakse **isomorfseteks**, kui leidub isomorfism $\varphi : A \rightarrow B$.

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

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 1.18 Isomorfsusseos on ekvivalentsiseos kõigi Ω -algebrate klassil, s.t. ta on refleksiivne, sümmeetriline ja transitiivne.

TÖESTUS. On selge, et Ω -algebra A korral on samasusteisendus $1_A : A \rightarrow A$ isomorfism ja seega $A \simeq A$. Samuti on selge, et kahe isomorfismi korrutis on isomorfism ja seega on isomorfsusseos 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 $\varphi^{-1}(b) = a$ siis ja ainult siis, kui $\varphi(a) = b$. On selge, et kujutus φ^{-1} on bijektiivne. Olgu nüüd $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $b_1, \dots, b_n \in B$. Kuna φ on surjektiivne, siis leiduvad sellised elemendid $a_1, \dots, a_n \in A$, et $\varphi(a_i) = b_i$ iga $i \in \{1, \dots, n\}$ korral. Siis

$$\begin{aligned}\varphi^{-1}(\omega_B(b_1, \dots, b_n)) &= \varphi^{-1}(\omega_B(\varphi(a_1), \dots, \varphi(a_n))) \\ &= \varphi^{-1}(\varphi(\omega_A(a_1, \dots, a_n))) \\ &= (\varphi^{-1}\varphi)(\omega_A(a_1, \dots, a_n)) \\ &= 1_A(\omega_A(a_1, \dots, a_n)) \\ &= \omega_A(a_1, \dots, a_n) \\ &= \omega_A(\varphi^{-1}(b_1), \dots, \varphi^{-1}(b_n)).\end{aligned}$$

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 1.19 Bijektiivset endomorfismi nimetatakse **automorfismiks**.

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

Lause 1.20 Iga Ω -algebra A korral on hulk $\text{Aut}(A)$ rühm kujutuste korrutamise (s.t. järjest rakendamise) suhtes.

TÖESTUS. Ka selle tõestuse jätame lugejale läbimõttlemiseks. \square

1.3 Alamalgebra

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

Defintsioon 1.21 Ω -algebra A mittetühja alamhulka B nimetatakse algebra A **alamalgebraiks**, 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

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

Asjaolu, et B on Ω -algebra A alamalgebra, tähistame järgmiselt: $B \leq A$. On selge, et iga algebra on iseenda alamalgebra, s.t. $A \leq A$. Samuti on lihtne aru saada, et alamalgebraks olemise seos on transitiivne, s.t. et kui $A \leq B$ ja $B \leq C$, siis ka $A \leq C$. Kui $A \leq B$ ja $B \leq A$, siis $A = B$, mis tähendab, et seos \leq on antisümmeetriline. Seega on ta järjestusseos kõigi Ω -algebrate klassil.

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

Järgmiste lemma töestus peaks olema ilmne.

Lemma 1.22 *Kui B on Ω -algebra A 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

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

Näide 1.23 Defintsiooni järgi on mittetühi 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 1.24 *Rühma mittetühi alamhulk on selle rühma alamrühm parajasti siis, kui see alamhulk on kinnine pöördelemendi võtmise ja korrutamise suhtes.*

TÖESTUS. Tarvilikkus on ilmne. Piisavuse töestamiseks 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 $b \in B$. Siis eelduse põhjal ka $b^{-1} \in B$ ja $1 = bb^{-1} \in B$. \square

Näide 1.25 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 $A \leq B$, 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. Teatud mõttes on õige ka vastupidine, s.t. iga üksühese homomorfismiga seostub teatud alamalgebra.

Lause 1.26 *Kui A ja B on Ω -algebrad ning leidub üksühene homomorfism $\varphi : B \rightarrow A$, siis kujutis $\varphi(B) = \{\varphi(b) \mid b \in B\}$ on A alamalgebra, mis on isomorfne algebraga B .*

TÖESTUS. 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. On selge, et kujutus

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

on Ω -algebrate isomorfism.

□

Näide 1.27 Vaatleme 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 järgmised seosed.

Lause 1.28 *Olgu antud Ω -algebrate homomorfism $\varphi : A \rightarrow B$ ning olgu antud alamalgebrad $C \leq A$ ja $D \leq B$. Siis $\varphi(C) \leq B$ ja $\varphi^{-1}(D) \leq A$, kui $\varphi^{-1}(D) = \{a \in A \mid \varphi(a) \in D\} \neq \emptyset$.*

TÖESTUS. Töestame esimese väite. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $\varphi(c_1), \dots, \varphi(c_n) \in \varphi(C)$, kusjuures $c_1, \dots, c_n \in C$. Kuna φ on homomorfism ja C on A alamalgebra, siis

$$\omega_B(\varphi(c_1), \dots, \varphi(c_n)) = \varphi(\omega_A(c_1, \dots, c_n)) = \varphi(\omega_C(c_1, \dots, c_n)) \in \varphi(C).$$

Samuti

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

iga $\omega \in \Omega_0$ korral. Seega $\varphi(C)$ on algebra B alamalgebra.

Teise väite töestamiseks 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 $\varphi(0_A^\omega) = 0_B^\omega = 0_D^\omega$, siis

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

iga $\omega \in \Omega_0$ korral.

□

Lause 1.29 *Olgu antud Ω -algebra A alamalgebrate süsteem $B_i, i \in I$, kusjuures $B = \bigcap_{i \in I} B_i \neq \emptyset$. Siis $B \leq A$.*

TÖESTUS. Olgu $B = \bigcap_{i \in I} B_i \neq \emptyset$, 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 järeltub, et kui X on Ω -algebra A mittetihi alamhulk, siis leidub algebra A vähim alamalgebra, mis sisaldab hulka X . Töepooltest: vaatleme kõikvõimalikke alamalgebraid, 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 alamalgebraiks** 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 algebra A tehete abil (nende korduval rakendamisel). Näiteks kui A on vektorruum, siis $\langle X \rangle$ on alamhulga X lineaarne kate.

1.4 Faktoralgebra

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

Definitsioon 1.30 Ekvivalentsiseost ρ Ω -algebra 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 1.31 Poolrühma A kongruents on ekvivalentsiseos ρ , mis rahuldab tingimust

$$x_1\rho y_1 \wedge x_2\rho y_2 \Rightarrow (x_1x_2)\rho(y_1y_2)$$

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

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

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

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

ja nullkahalised tehted $\omega \in \Omega_0$ võrdusega

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

Tänu sellele, kuidas on defineeritud kongruentsid, on faktoralgebra tehted korrektelt 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 surjektiivne.

Lause 1.33 *Kui ρ on Ω -algebra A kongruents, siis loomulik kujutus $\pi : A \rightarrow A/\rho$ on surjektiivne Ω -algebraate homomorfism.*

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

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

Nullkohalise tehte ω korral

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

□

Defintsioon 1.34 Kujutuse $\varphi : A \rightarrow B$ **tuumaks** nimetatakse binaarset seost $\ker \varphi$ hulgat 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 hulgat A .

Lause 1.35 *Kui $\varphi : A \rightarrow B$ on Ω -algebrate homomorfism, siis $\ker \varphi$ on algebra A kongruents.*

TÖESTUS. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja elemendid $x_1, \dots, x_n, y_1, \dots, y_n \in A$ 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

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

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

Lause 1.36 *Kui ρ on Ω -algebra A kongruents ja $\pi : A \rightarrow A/\rho$ on loomulik homomorfism, siis $\ker \pi = \rho$.*

TÖESTUS. Kuna

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

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

Teoreem 1.37 (Homomorfismiteoreem) *Kui $\varphi : A \rightarrow B$ on Ω -algebrate sürjektiivne homomorfism, siis*

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

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

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

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

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

Tänu seosele (1) on kujutus ψ korrektelt defineeritud ja üksühene. Kuna φ on päalekujutus, siis ka ψ on päalekujutus. Kui $n \in \mathbb{N}$, $\omega \in \Omega_n$, $a_1, \dots, a_n \in A$, siis

$$\begin{aligned}\psi(\omega_{A/\ker\varphi}(\overline{a_1}, \dots, \overline{a_n})) &= \psi(\overline{\omega_A(a_1, \dots, a_n)}) = \varphi(\omega_A(a_1, \dots, a_n)) \\ &= \omega_B(\varphi(a_1), \dots, \varphi(a_n)) = \omega_B(\psi(\overline{a_1}), \dots, \psi(\overline{a_n})).\end{aligned}$$

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 algebraaliste struktuuride puhul.

1.5 Kõrvalklassid, Lagrange'i teoreem

Defintsioon 1.38 Olgu G (multiplikatiivne) rühm ja H tema alamrühm. Siis hulki

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

($Ha = \{ha \mid h \in H\}$) 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.

Lause 1.39 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 $ab^{-1} \in H$.

TÖESTUS. TARVILIKKUS. Kehtigu võrdus $aH = bH$. Kuna $b \in bH = aH$, siis leidub selline element $h \in H$, et $b = ah$. Järelikult $a^{-1}b = h \in H$.

PIISAVUS. Oletame, et $a^{-1}b \in H$ ja tähistame $h := a^{-1}b$. Siis $b = ah$, milles järeltäpsustatakse, et $bH \subseteq aH$. Samuti $a^{-1} = hb^{-1}$ ehk $a = (hb^{-1})^{-1} = (b^{-1})^{-1}h^{-1} = bh^{-1} \in bH$, milles järeltäpsustatakse, et $aH \subseteq bH$. Kokkuvõttes $aH = bH$. \square

Järeldus 1.40 Kui H on rühma G alamrühm ja $b \in G$, siis $H = bH$ parajasti siis, kui $b \in H$.

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

Lause 1.41 Olgu G rühm ja $H \leq G$. Siis iga $a \in A$ korral $|aH| = |H| = |Ha|$.

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

$$f(h) := ah,$$

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

Defintsioon 1.42 Lõpliku rühma **järguks** nimetatakse tema elementide arvu.

Järgmine teoreem on nime saanud prantsuse matemaatiku Joseph-Louis Lagrange'i (1736–1813) järgi.

Teoreem 1.43 (Lagrange'i teoreem) *Lõpliku rühma iga alamrühma järk jagab selle rühma järu.*

TÖESTUS. 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 hulgad aH on mittetühjad. Samuti on selge, et

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

Veendume, et kui hulgad 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 1.39 põhjal $aH = bH$. Sellega oleme näidanud, et tegemist on klassijaotusega. Lause 1.41 põhjal teame, et kõik vasakpoolsed kõrvalklassid on sama võimsusega (võimsusega $|H|$). Seega kui neid kõrvalklasse on m tükki, siis

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

ehk $|H|$ jagab naturaalarvu $|G|$. □

1.6 Faktorrühm

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

Definitsioon 1.44 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 1.45 Iga rühma G korral on alamrühmad G ja $\{1\}$ normaalsed.

Näide 1.46 Kommutatiivse rühma kõik alamrühmad on normaalsed.

Näide 1.47 Rühma $GL_n(\mathbb{R})$ alamrühm $SL_n(\mathbb{R})$ on normaalne.

Lause 1.48 *Rühma G alamrühm H on normaalne parajasti siis, kui iga $g \in G$ korral $gH = Hg$.*

TÖESTUS. 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 $gh' = hg$. Järelikult $g^{-1}hg = h' \in H$. □

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

Teoreem 1.49 *Iga rühma G korral leidub üksühene vastavus hulkade $\text{Con}(G)$ ja $\mathcal{N}(G)$ vahel.*

TÖESTUS. 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 selge, et ρ_H on ekvivalentsiseos. Näitame, et ρ_H on rühma G kongruents (vt. näidet 1.31). 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 pöördelemendi võtmise suhtes, siis saame, et $(x^{-1})^{-1}y^{-1} = xy^{-1} = (yx^{-1})^{-1} \in H$. 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

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

Sellega oleme tõestanud võrduse $\kappa\nu = 1_{\text{Con}(G)}$.

Tõestamaks võrdust $\nu\kappa = 1_{\mathcal{N}(G)}$ vaatleme suvalist normaalset alamrühma $H \in \mathcal{N}(G)$. Siis

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

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

Olgu H rühma G normaalne alamrühm. Teoreemi 1.49 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

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

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

$$a/\rho = aH.$$

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

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

võib esitada kujul

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

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

Definitsioon 1.50 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 pöördelement on $a^{-1}H$.

Olgu $\varphi : G \rightarrow G'$ rühmade homomorfism. Tänu lausele 1.35 on selle tuum rühma G kongruents. Rakendades kongruentsile ker $\varphi \in \text{Con}(G)$ teoreemi 1.49 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

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

kui rühmad. Seega võib rühmade homomorfismiteoreemi sõnastada järgmisel kujul.

Teoreem 1.51 Kui $\varphi : G \rightarrow G'$ on surjektiivne rühmade homomorfism, siis $G' \simeq G / \text{Ker } \varphi$.

Lause 1.52 Kui H on rühma G normaalne alamrühm, siis loomuliku homomorfismi

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

tuum on H .

TÖESTUS. Tänu järeldusele 1.40

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

□

Abeli rühma kõik alamriühmad on normaalsed. Kui A on aditiivne Abeli rühm (s.t. tema kahekohalist tehet tähistame sümboliga $+$) ja H tema alamriühm, 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 1.39 põhjal mistahes elementide $a, b \in A$ korral

$$a + H = b + H \iff -a + b \in H \iff a - b \in H. \tag{2}$$

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 1.53 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 $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$. Selle faktorrühma puhul on tegemist hästituntud jäägiklasside aditiivse rühmaga mooduli n järgi.

1.7 Faktorring

Käesolevas kursuses peame ringide all silmas ühikelemendiga assotsiatiivseid ringe. Meenutame definitsiooni.

Definitsioon 1.54 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. $(\forall a, b, c \in R) \quad a(b + c) = ab + ac \text{ ja } (a + b)c = ac + bc.$

Ekvivalentiseos 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 järeltub tingimusest 2 ja ringis alati kehtivast omadusest $(-1)x = -x$.

Sarnaselt rühmadega saab ka faktorringide moodustamiseks kongruentside asemel kasutada teatud alamhulki, mida kutsutakse ideaalideks.

Definitsioon 1.55 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 1.56 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 1.57 Iga ringi R korral leidub üksühene vastavus hulkade $\text{Con}(R)$ ja $\text{Id}(R)$ vahel.

TÖESTUS. Olgu $\rho \in \text{Con}(R)$. Näitame, et $0/\rho \in \text{Id}(R)$. Kuna ρ on muuhulgas rühma $(R; +)$ kongruents, siis teoreemi 1.49 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 1.49 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 $\kappa\nu = 1_{\text{Con}(R)}$ ja $\nu\kappa = 1_{\text{Id}(R)}$ järelduvad täpselt samamoodi nagu teoreemi 1.49 tõestuses.

□

Defintsioon 1.58 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 1.59 Kui $\varphi : R \rightarrow R'$ on surjektiivne ringide homomorfism, siis $R' \simeq R / \text{Ker } \varphi$.

Lause 1.60 Kui I on ringi R ideaal, siis loomuliku homomorfismi

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

tuum on I .

Näide 1.61 Lihtne on veenduda, et alamhulk $n\mathbb{Z}$ ($n \geq 2$) on ringi $(\mathbb{Z}; +, \cdot)$ ideaal. Faktorringiks $\mathbb{Z}/n\mathbb{Z}$ on jäädikklassiring \mathbb{Z}_n mooduli n järgi, milles liitmine ja korrutamine on defineeritud võrdustega

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

1.8 Faktorruum

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

Analoogiliselt rühmade ja ringide juhtumiga saab tõestada järgmiste teoreemite.

Teoreem 1.62 *Iga vektorruumi V korral leidub üksühene vastavus hulkade $\text{Con}(V)$ ja $\text{Sub}(V)$ vahel.*

Definitsioon 1.63 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

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

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

Meenutame, et vektorruumide homomorfisme nimetatakse lineaarkujutusteks.

Teoreem 1.64 *Kui $\varphi : V \rightarrow V'$ on surjektivne lineaarkujutus, siis $V' \simeq V/\text{Ker } \varphi$.*

Lause 1.65 *Kui W on vektorruumi V alamruum, siis loomuliku homomorfismi*

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

tuum on W .

1.9 Ω -algebrate otsekorrutis

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

Loenduva hulga mittetühjade hulkade A_1, A_2, \dots otsekorrutis on kõigi jadade (a_1, a_2, \dots) hulk, kus $a_i \in A_i$ iga $i \in \mathbb{N}$ 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 $A_i, i \in I$, otsekorrutis 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 $A = \prod_{i \in I} A_i$, 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 otsekorrutise A i -ndaks projektsiooniks. On selge, et mittetühjade hulkade otsekorrutise kõik projektsioonid on päalekujutused.

Definitsioon 1.66 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 1.67 Olgu A_1, \dots, A_m rühmad. Siis otsekorrutisel

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

defineeritakse kahekohaline korrutamistehe võrdusega

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

ühekohaline 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 ühik-element.

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 1.68 Kui A on Ω -algebra A_i , $i \in I$, otsekorrutis, siis kõik projektsioonid $\pi_i : A \rightarrow A_i$, $i \in I$, on Ω -algebraid homomorfismid.

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

$$\pi_i(\omega_A(a^1, \dots, a^n)) = \pi_i\left(\left(\omega_{A_j}(a_j^1, \dots, a_j^n)\right)_{j \in I}\right) = \omega_{A_i}(a_i^1, \dots, a_i^n) = \omega_{A_i}(\pi_i(a^1), \dots, \pi_i(a^n))$$

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

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

□

Kuna tehted defineeritakse otsekorrutisel komponenthaaval, siis kehtivad Ω -algebraid A_i , $i \in I$, otsekorrutisel kõik samasused, mis kehtivad kõigil neil algebraitel. Teisisõnu, kui mingi Ω -algebraid 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 korpusse K vaadeldavate vektorruumide otsekorrutis on vektorruum üle korpusse K . Küll aga kahe korpusse otsekorrutis ei ole korpus.

1.10 Moodulid üle ringi

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

Definitsioon 1.69 **Vasakpoolseks mooduliks üle ringi** R ehk **vasakpoolseks R -mooduliks** nimetatakse Abeli rühma $(A; +)$, kui iga elemendi $r \in R$ jaoks on defineeritud ühekohaline tehe

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

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 1.70** 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

$$na := a + \dots + a, \\ (-n)a := -(a + \dots + a)$$

(summades on n liidetavat) ja

$$0a = 0$$

(võrduse vasakul pool on täisarv 0 ja paremal pool 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.

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

Lause 1.71 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. $r(a - b) = ra - rb$;
5. $(r - s)a = ra - sa$.

Erinevalt vektoruumide 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 $a = \bar{2}$.

Kuna R -moodulid on Ω -algebrad teatava Ω jaoks, siis saab kasutada eespool esitatud definitsioone alamalgebra (alammooduli), 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.

1.11 R -moodulite väligne otsesumma

Definitsioon 1.72 Olgu R ring. R -moodulite $A_i, i \in I$, **väliseks otsesummaks** nimetatakse nende moodulite otsekorrutise $\prod_{i \in I} A_i$ alammoodulit $\bigoplus \sum_{i \in I} A_i$, mis koosneb kõigist neist üldistatud jadadest $(a_i)_{i \in I}$, millel on ainult lõplik arv nullist erinevaid komponente.

Seega

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

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

On selge, et lõpliku arvu R -moodulite väligne otsesumma on sama, mis nende otsekorrutis, s.t.

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

1.12 R -moodulite sisemine otsesumma

Definitsioon 1.73 R -mooduli A alammoodulite $A_i, i \in I$, **summaks** nimetatakse R -mooduli A kõigi nende elementide hulka, mis esituvad alammoodulitesse A_i kuuluvate elementide summana.

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

$$a_{i_1} + a_{i_2} + \dots + a_{i_n}, \quad (3)$$

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 (3) võrdub elemendiga a_{i_1} . See tähendab, et summa $\sum_{i \in I} A_i$ sisaldab kõiki alammooduleid $A_i, i \in I$.

Lause 1.74 R -mooduli A alammoodulite $A_i, i \in I$, summa on mooduli A vähim alammoodul, mis sisaldab kõiki alammooduleid $A_i, i \in I$.

TÖESTUS. Kui B on mooduli A alammoodul, mis sisaldab kõiki alammooduleid $A_i, i \in I$, siis peab B sisaldama kõiki summasid (3) (est B peab olema kinnine liitmise suhtes), seega $\sum_{i \in I} A_i \subseteq B$. \square

Definitsioon 1.75 R -mooduli A alammoodulite A_1, \dots, A_n summat nimetatakse (**sisemiseks**) **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 1.76 Olgu A_1, \dots, A_n R -mooduli A alammoodulid. Siis järgmised tingimused on saavatäärised:

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

$$A_i \cap (A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_n) = \{0\}; \quad (4)$$

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

TÖESTUS. 1. \Rightarrow 2. Eeldame, et $A_1 + \dots + A_n = A_1 + \dots + A_n$. Olgu

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

Siias 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 (4) 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 1.77 Vaatleme moodulit $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ üle ringi \mathbb{Z} koos komponenthaaval defineeritud teheteega. 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 alammoodulid ja et $A = A_1 + A_2 + A_3$. Samuti on selge, et

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

Kuna teoreemi 1.76 tingimus 2 on rahuldatud, siis võime öelda, et

$$A = A_1 + A_2 + A_3.$$

Alammoodulite sisemise otsesumma saab defineerida ka siis, kui neid alammooduleid on lõpmata palju.

Defintsioon 1.78 R -mooduli A alammoodulite $A_i, i \in I$, 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 alammoodulite A_{i_1}, \dots, A_{i_n} summa on otsesumma.

Teoreem 1.76 kandub samuti üle üldjuhule, s.t. juhule, kui alammooduleid ei pruugi olla lõplik arv.

Teoreem 1.79 *Olgu $A_i, i \in I$, R -mooduli A alammoodulid. Siis järgmised tingimused on samaväärsed:*

1. alammoodulite $A_i, i \in I$, 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 $a_1 = \dots = a_n = 0$.

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

Teoreem 1.80 *Kui $A = \sum_{i \in I} A_i$, kus $A_i, i \in I$, on mooduli A alammoodulid, 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 alammoodulid $A_i, i \in I$, nii et $A = \sum_{i \in I} A_i$ ja $A_i \simeq B_i$ iga $i \in I$ korral.*

TÖESTUS. 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

$$\begin{aligned} \varphi((a_i)_{i \in I} + (b_i)_{i \in I}) &= \varphi((a_i + b_i)_{i \in I}) = \sum_{i \in I} (a_i + b_i) = \sum_{i \in I} a_i + \sum_{i \in I} b_i \\ &= \varphi((a_i)_{i \in I}) + \varphi((b_i)_{i \in I}), \\ \varphi(r(a_i)_{i \in I}) &= \varphi((ra_i)_{i \in I}) = \sum_{i \in I} (ra_i) = r \sum_{i \in I} a_i = r\varphi((a_i)_{i \in I}). \end{aligned}$$

On selge, et φ on päälukujutus. Oletame, et $\varphi((a_i)_{i \in I}) = \varphi((b_i)_{i \in I})$. Siis $\sum_{i \in I} a_i = \sum_{i \in I} b_i$, kusjuures mõlemas summas on lõplik arv nullist erinevaid liidetavaid. Kuna A on alamruumide $A_i, i \in I$, otsesumma, siis peab $a_i = b_i$ iga $i \in I$ korral. Seega $(a_i)_{i \in I} = (b_i)_{i \in I}$ ja φ on üksühene. 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 on i -ndal kohal). On lihtne aru saada, et A_i on mooduli A alammoodul $A_i \simeq B_i$ 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 sümboleiga $\beta_{j_i}, i = 1, \dots, n$, 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. Selline esitus on ühene tänu sellele, et liitmine on moodulil A defineeritud komponenthaaval. Seega A on alammoodulite $A_i, i \in I$, sisemine otsesumma. \square

1.13 Vektorruumide otsesummad

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

Lause 1.81 *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.

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

$$k_1 e_1 + \dots + k_r e_r + l_{r+1} a_{r+1} + \dots + l_s a_s + j_{r+1} b_{r+1} + \dots + j_t b_t = 0. \quad (5)$$

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 (5) 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 (5) 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. Mõõtmete kohta saame eelmisest lausest järgmise tulemuse.

Lause 1.82 *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 1.83 *Olgu V_1 ja V_2 vektorruumi V lõplikumõõtmelised alamruumid. Siis*

$$V_1 + V_2 = V_1 \dotplus V_2 \iff \dim(V_1 + V_2) = \dim(V_1) + \dim(V_2).$$

Matemaatilise induktsiooni abil saab lause 1.82 üldistada suvalise lõpliku arvu alamruumide V_1, \dots, V_m juhule. Et alamruumi $V_1 \cap \dots \cap V_m$ mõõde on mittenegatiivne, siis kehtib järgmine tulemus.

Järeldus 1.84 *Kui V_1, \dots, V_m on vektorruumi V lõplikumõõtmelised alamruumid, siis*

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

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

Lause 1.85 *Olgu V_1, \dots, V_m ($m \geq 2$) vektorruumi V lõplikumõõtmelised alamruumid. Siis*

$$V_1 + \dots + V_m = V_1 \dotplus \dots \dotplus V_m$$

parajasti siis, kui

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

TÖESTUS. Töestame väite induktsiooniga m järgi. Juhul kui $m = 2$ kehtib vaadeldav väide tänu järeldusele 1.83. Oletame, et $m > 2$ ja väide kehtib, kui liidetavaid alamruume on vähem kui m . Töestame väite m alamruumi jaoks.

TARVILIKKUS. Olgu alamruumide V_1, V_2, \dots, V_m summa nende alamruumide otsesumma. Siis teoreemi 1.76 punkti 2 põhjal $V_1 \cap (V_2 + \dots + V_m) = \{0\}$. Teoreemi 1.76 punkti 3 abil on lihtne näha, et $V_2 + \dots + V_m = V_2 \dotplus \dots \dotplus V_m$. Induktsiooni eelduse põhjal peab kehtima võrdus $\dim(V_2 + \dots + V_m) = \dim(V_2) + \dots + \dim(V_m)$. Kasutades lauset 1.82 saame nüüd

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

PIISAVUS. Eeldame, et kehtib võrdus $\dim(V_1 + \dots + V_m) = \dim(V_1) + \dots + \dim(V_m)$. Siis lause 1.82 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 pooltest 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 järeldusele 1.84. Seega $\dim(V_2) + \dots + \dim(V_m) = \dim(V_2 + \dots + V_m)$. Induktsiooni eelduse põhjal

$$V_2 + \dots + V_m = V_2 \dotplus \dots \dotplus V_m. \tag{6}$$

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 järelduse 1.83 ja võrduse (6) põhjal

$$V_1 + V_2 + \dots + V_m = V_1 \dotplus (V_2 + \dots + V_m) = V_1 \dotplus V_2 \dotplus \dots \dotplus V_m.$$

□

Lause 1.86 Olgu B lõplikumõõtmelise vektorruumi V baas, olgu $\{B_1, \dots, B_m\}$ klassijaotus hulgat B ja olgu V_i , $i = 1, \dots, m$, hulga B_i poolt tekitatud alamruum (*s.t. lineaarne kate*). Siis

$$V = V_1 + \dots + V_m.$$

TÕESTUS. On selge, et $V = V_1 + \dots + V_m$. Väide järeltub eelmisest lausest, sest

$$\dim(V_1 + \dots + V_m) = \dim(V) = |B| = |\cup_{i=1}^m B_i| = |B_1| + \dots + |B_m| = \dim(V_1) + \dots + \dim(V_m).$$

□

Lause 1.87 Olgu V_1, \dots, V_m lõplikumõõtmelise vektorruumi V alamruumid,

$$V = V_1 + \dots + V_m$$

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 1.76 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 1.81 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. 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 elementid 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 liide-tavaiks 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

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

Defintsioon 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 $k_1, \dots, k_n \in \mathbb{N} \cup \{0\}$.

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

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

Üksliikmeid nimetatakse **sarnasteks**, kui nad on võrdsed või nende kordajad (ringi R elementid) 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 $4Y$.

Defintsioon 2.2 Üksliikme $aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ **astmeksi** nimetatakse mittenegatiivset täisarvu $k_1 + \dots + k_n$. Polünoomi **astmeksi** nimetatakse suurimat tema liikmete astmetest. Polünoomi f astet tähistatakse $\deg(f)$.

Defintsioon 2.3 Ringi $R[X_1, \dots, X_n]$ kuuluvate üksliikmete hulgal saab defineerida nn. leksi-kograafilise 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

$$m \leq_{\text{lex}} m' \iff m <_{\text{lex}} m' \text{ või } m = m'.$$

Ei ole keeruline näha, et seos \leq_{lex} on järjestusseos kõigi üksliikmete hulgal.

Lemma 2.4 Kui R on nullitegureita ring ja m_1, m_2, m on üksliikmed ringist $R[X_1, \dots, X_n]$ ja $m_1 \leq_{\text{lex}} m_2$, siis ka $m_1 m \leq_{\text{lex}} m_2 m$ ja $mm_1 \leq_{\text{lex}} mm_2$.

TÖESTUS. Töestame neist väidetest esimese (teine on analoogiline). Olgu

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

Siis

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

Kui $m_1 = m_2$, siis on väide ilmne. Kui $l_1 < k_1$, siis $l_1 + j_1 < k_1 + j_1$ ja seega $m_1 m \leq_{\text{lex}} m_2 m$. Kui $k_1 = l_1, \dots, k_i = l_i$, kuid $l_{i+1} < k_{i+1}$, siis $k_1 + j_1 = l_1 + j_1, \dots, k_i + j_i = l_i + j_i$, kuid $l_{i+1} + j_{i+1} < k_{i+1} + j_{i+1}$. Järelikult jälgigi $m_1 m \leq_{\text{lex}} m_2 m$. \square

Antud n muutuja polünoomi liikmete hulgas leidub alati kõrgeim liige (s.t. suurim element järjestuse \leq_{lex} suhtes).

Lause 2.5 *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.*

TÖESTUS. Olgu m_f polünoomi f kõrgeim liige ja m_g polünoomi g kõrgeim liige. Siis polünoomide korrutise fg suvaline liige esitub kujul mm' , kus m on polünoomi f liige, m' on polünoomi g liige, $m \leq_{\text{lex}} m_f$ ja $m' \leq_{\text{lex}} m_g$. Siis lemma 2.4 põhjal

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

Seega $m_f m_g$ on polünoomi fg kõrgeim liige. \square

Järeldus 2.6 *Kui ring R on nullitegureita, siis iga naturaalarvu n korral on ka polünoomide ring $R[X_1, \dots, X_n]$ nullitegureita.*

Lause 2.7 *Kui R on nullitegureita ring ning $f, g \in R[X_1, \dots, X_n] \setminus \{0\}$, siis*

$$\deg(fg) = \deg(f) + \deg(g).$$

TÖESTUS. See väide kehtib tänu sellele, et üksliikmete korrutise aste on võrdne tegurite astmete summaga. \square

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

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

Kahe homogeense polünoomi korrutis on homogenne. 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

Defintsioon 2.10 Mitme muutuja polünoomi nimetatakse **sümmeetriliseks**, kui ta ei muudu muutujate mistahes substitutsiooni 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 koos iga oma liikmega $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ sisaldab ta ka kõik üksliikmed

$$aX_{\sigma(1)}^{k_1}X_{\sigma(2)}^{k_2}\dots X_{\sigma(n)}^{k_n}, \quad \sigma \in S_n.$$

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.

TÖESTUS. Olgu $f, g \in S[X_1, \dots, X_n]$. Vaatleme summa $f + g$ liiget $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$. Kui see liige on ka f liige või g liige, siis on selge, et $aX_{\sigma(1)}^{k_1}X_{\sigma(2)}^{k_2}\dots X_{\sigma(n)}^{k_n}$ on $f + g$ liige iga $\sigma \in S_n$ korral. Kui aga $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ on f liikme $bX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ ja g liikme $cX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ summa, siis $a = b + c$ ning f sisaldab liiget $bX_{\sigma(1)}^{k_1}X_{\sigma(2)}^{k_2}\dots X_{\sigma(n)}^{k_n}$ ja g sisaldab liiget $cX_{\sigma(1)}^{k_1}X_{\sigma(2)}^{k_2}\dots X_{\sigma(n)}^{k_n}$. Seega $f + g$ sisaldab liiget

$$bX_{\sigma(1)}^{k_1}X_{\sigma(2)}^{k_2}\dots X_{\sigma(n)}^{k_n} + cX_{\sigma(1)}^{k_1}X_{\sigma(2)}^{k_2}\dots X_{\sigma(n)}^{k_n} = aX_{\sigma(1)}^{k_1}X_{\sigma(2)}^{k_2}\dots X_{\sigma(n)}^{k_n}.$$

Sellega oleme näidanud, et $f + g \in S[X_1, \dots, X_n]$. Analoogiliselt võib veenduda, et ka polünoomid $-f$ ja fg on sümmeetrilised. On selge, et konstantne polünoom 1 on sümmeetriline. \square

Defintsioon 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 kirjeldada seoseid unitaarse ühe muutuja polünoomi kordajate ja juurte vahel. Meenutame, et polünoomi unitaarsus tähendab seda, et tema päaliikme 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. Viete'i valemid:

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

TÖESTUS. Meenutame kursusest Algebra I, et kui n -nda astme 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 pool peavad olema võrdsed, siis neid omavahel võrreldes saamegi nõutud valemid. \square

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

TÖESTUS. Oletame vastuväiteliselt, et $f \in S[X_1, \dots, X_n]$ kõrgeima liikme $m = aX_1^{k_1} \dots X_n^{k_n}$ korral $k_1 \geq k_2 \geq \dots \geq k_{i-1} < k_i$. Vahetades ära muutujad X_{i-1} ja X_i saame polünoomi f liikme $aX_1^{k_1} \dots X_{i-1}^{k_{i-1}} X_i^{k_{i-1}} \dots X_n^{k_n}$, mis on kõrgem kui m , sest $k_i > k_{i-1}$. See on vastuolu. \square

Teoreem 2.16 *Iga n muutuja sümmeetriline polünoom üle ringi R on esitatav polünoomina n muutuja sümmeetrilistest põhipolünoomidest.*

TÖESTUS. 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. Siis tänu lemmale 2.15 on $k_1 \geq k_2 \geq \dots \geq k_n$. Moodustame 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. Kuna sümmeetriliste põhipolünoomide $\sigma_1, \sigma_2, \dots, \sigma_n$ kõrgeimad liikmed on vastavalt $X_1, X_1 X_2, \dots, X_1 X_2 \dots X_n$, siis lause 2.5 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.

Olgu nüüd

$$f_1 := f - g_1.$$

Tänu lausele 2.12 on see polünoom sümmeetriline 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

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

$r \in \mathbb{N}$. 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

2.3 Polünoomi lahutuskorpus

Selles paragrahvis vaatleme 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 lineaarpolünoomide 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 Korpusi K ja K' nimetatakse **isomorfseteks**, kui nad on isomorfsed ringidena.

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

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

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 faktorringi

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

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 .

TÖESTUS. 1. Teame, et $pK[X] = \{pg \mid g \in K[X]\}$ on polünoomide ringi $K[X]$ ideaal (vt. näidet 1.56). Kuna ring $K[X]$ on kommutatiivne, siis ka tema faktorring 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 faktorringis

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

Muuhulgas $\bar{f} = \bar{0}$ parajasti siis, kui $p \mid f$, ning 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 $fu + pv = 1$. Faktorringis 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. Lihtne on veenduda, et konstantsete polünoomide kõrvalklasside hulk

$$K' = \{\bar{k} \mid k \in K\} \subseteq K_p$$

on korpuse K_p alamkorpus. Näitame, et $K \simeq K'$. Selleks defineerime kujutuse $\varphi : K \rightarrow K'$ võrdusega

$$\varphi(k) := \bar{k}$$

mistahes $k \in K$ korral. On selge, et see kujutus on surjektiivne. Lihtne on näidata, et ta on ringide homomorfism. Injektiivsuse näitamiseks 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 ja kokkuvõttes isomorfism. Edaspidi samastame elemendid k ja \bar{k} .

3. Olgu

$$p = p(X) = a_0 X^m + \dots + a_{m-1} X + a_m,$$

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

$$\begin{aligned} p(\bar{X}) &= a_0 \bar{X}^m + \dots + a_{m-1} \bar{X} + a_m \\ &= \bar{a}_0 \bar{X}^m + \dots + \bar{a}_{m-1} \bar{X} + \bar{a}_m \\ &= \overline{a_0 X^m} + \dots + \overline{a_{m-1} X} + \bar{a}_m \\ &= \overline{a_0 X^m + \dots + a_{m-1} X + a_m} \\ &= \bar{p} = \bar{0}. \end{aligned}$$

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

Meil läheb veel vaja järgmist hästi tundud fakti (vt. [1], järelalus 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 kommutatiivne 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.

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

$$f = p_1 p_2 \dots p_s \tag{7}$$

(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 on olemas. Vastasel korral leidub nende polünoomide hulgas mõni, mille aste on vähemalt 2, olgu see näiteks p_1 (vajaduse korral võime tegureid esituses (7) 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 töestuses. 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 $\deg(p'_1) \geq 1$. Võib juhtuda, et ka polünoomidest

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 korrutisena üle korpusse K_{p_1} saame mängi lahutuse

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

kus lineaartegureid on vähemalt ühe vörra rohkem kui lahutuses (7). 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 korpusse

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

milles polünoomil q_1 leidub mängi juur c_2 . Siis q_1 jagub lineaarpolünoomiga $X - c_2$. Paneme tähele, et c_1 ja c_2 on ka polünoomi f juured. Seega analoogiliselt jätkates peame hiljemalt $n = \deg(f)$ sammuga jöudma olukorranzi, kus f on n lineaarteguri korrutis. \square

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

Kui $f(X) \in K[X]$ on n -nda astme polünoom ja \overline{K} tema lahutuskorpus, siis leiduvad sellised $a_1, \dots, a_n, b_1, \dots, b_n \in \overline{K}$, 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: $-a_i^{-1} b_i$, $i \in \{1, \dots, n\}$.

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

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

Kuna iga polünoomi üle \mathbb{R} saab jäätida jagada polünoomiga $X^2 + 1$ nii, et jääägi 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 faktorringis \mathbb{R}_p kehtib võrdus $\overline{X^2 + 1} = \overline{0}$ ehk $\overline{X^2} = \overline{-1}$. Lisaks sellele

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

Lihtrne 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 konstrueritakse harilikult teatud taandumatute polünoomide lahutuskorpusena (vt. [3]). Lõplikel korpustell on väga oluline roll krüptograafias ja kodeerimisteoorias.

2.4 Algebra põhiteoreem

Selle paragrahvi eesmärgiks on töestada teoreem, mida tuntakse algebra põhiteoreemi nime all. See käsitleb kompleksarvuliste kordajatega polünoomide juuri. Me alustame tulemusega, mille kehtivus peaks olema üsna ilmne.

Lemma 2.25 Olgu K korpus ja

$$f(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in K[X],$$

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

$$X^n + (a_1 a_0^{-1}) X^{n-1} + \dots + (a_{n-1} a_0^{-1}) X + a_n a_0^{-1}$$

on ühed ja samad juured.

Lause 2.26 Igal paarituarvulise astmega reaalarvuliste kordajatega polünoomil leidub reaalarvuline juur.

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

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

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. Et 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 funktsionid $f(r)$ ja r^n on ekvivalentsed protsessis $r \rightarrow -\infty$ ja protsessis $r \rightarrow \infty$ (nende jagatise piirväärustus on 1), siis

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

Järelikult leiduvad sellised reaalarvud a ja b , et $f(a) < 0$ ja $f(b) > 0$. Lõigus $[a, b]$ pideval funktsionil, mille vääritud 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

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

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

ja olgu $n = \deg(f(X)) = 2^k q$, kus q on paaritu arv. Viime tõestuse läbi induktsiooniga k järgi. Kui $k = 0$, siis leidub polünoomil $f(X)$ lause 2.26 põhjal isegi reaalarvuline juur. Eeldame nüüd, 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 $f(X)$ leidub kompleksarvuline juur.

Kuna $f(X) \in \mathbb{C}[X]$, siis teoreemi 2.23 põhjal leidub korpus F , mis sisaldab korpust \mathbb{C} alamkorpusena ja milles polünoomil $f(X)$ on n juurt c_1, \dots, c_n . Olgu r mingi reaalarv. Vaatleme korpuse F elemente

$$a_{ij} := c_i c_j + r(c_i + c_j), \quad i, j = 1, 2, \dots, n, i < j. \quad (8)$$

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 arvud a_{ij} , $i, j = 1, 2, \dots, n$, $i < j$, 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 valemite põhjal

$$b_k = (-1)^k \sigma_k(a_{12}, a_{13}, \dots, a_{n-1,n}), \quad k = 1, \dots, n_0. \quad (9)$$

Tänu võrdustele (8) võime öelda, et

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

kus $g_k(c_1, \dots, c_n)$ on reaalarvuliste kordajatega polünoom c_1, \dots, c_n suhtes. Veelgi enam, me võime öelda, et $g_k(c_1, \dots, c_n)$ on sümmeetrisiline 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 (tänu võrdusele (9)). Teoreemi 2.16 põhjal saab sümmeetrilise polünoomi $g_k(c_1, \dots, c_n)$ avaldada reaalarvuliste kordajatega polünoomina sümmeetrilistest põhipolünoomidest

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

See aga tähendab, et b_1, \dots, b_{n_0} on reaalarvud.

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} . Kuna polünoome $f_r(X)$ 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 ülemisest võrdusest alumise saame $m_1 - m_2 = (r_1 - r_2)(c_i + c_j)$, millest $r_1 \neq r_2$ tõttu

$$c_i + c_j = \frac{m_1 - m_2}{r_1 - r_2} \quad (10)$$

ja

$$c_i c_j = m_1 - r_1(c_i + c_j). \quad (11)$$

Võrdustest (10) ja (11) näeme, et $c_i + c_j$ ja $c_i c_j$ on kompleksarvud. Viete'i valemite põhjal on c_i ja c_j 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 pool 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 mittekonstantsel polünoomil leidub kompleksarvuline juur.*

TÖESTUS. 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

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

kus $\overline{a_i}$ 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

$$b_k = \sum_{i+j=k} a_i \overline{a_j}$$

iga $k = 1, 2, \dots, 2n$ korral. Kasutades kaaskompleksarvude omadusi saame, et

$$\bar{b}_k = \overline{\sum_{i+j=k} a_i \overline{a_j}} = \sum_{i+j=k} \overline{a_i} \overline{\overline{a_j}} = \sum_{i+j=k} \overline{a_i} \overline{a_j} = \sum_{i+j=k} \overline{a_i} a_j = \sum_{i+j=k} a_i \overline{a_j} = b_k,$$

mis 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

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

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

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

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

Algebra põhiteoreemi on aegade jooksul töestanud ja töestada üritanud paljud nimekad matemaatikud. Esimese täielikult korrektse töestuse andis Gauss¹ aastal 1816. Ülevaate algebra põhiteoreemi ajaloost võib leida raamatust [1], lk. 229–231.

¹Carl Friedrich Gauss (1777–1855) — saksa matemaatik

3 Lineaarteisenduse kanooniline baas

3.1 Probleemi püstitus ja põhitulemuse sõnastus

Olgu V lõplikumõõtmeline vektoruum üle korpuse K ja φ selle vektoruumi lineaarteisendus. Kui vektoruumis V on valitud mingi baas e , siis tekib selle teisenduse maatriks baasi e suhtes $A_\varphi^e \in \text{Mat}_n(K)$. See maatriks sõltub baasi valikust. Eesmärk on leida antud lineaarteisenduse jaoks selline baas, mille suhtes oleks teisenduse maatriks võimalikult lihtne. Käesolevas päätükis anname sellele probleemile ühe lahenduse juhul, kui K on algebraliselt kinnine korpus.

Selles päätükis eeldame vaikimisi, et *kõik vaadeldavad vektoruumid on lõplikumõõtmelised ja kõik korpused on kommutatiivsed*.

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

Seega

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

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

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

$$\text{diag}(J_{m_1}(\lambda_1), \dots, J_{m_s}(\lambda_s)).$$

Defintsioon 3.3 Vektoruumi V lineaarteisenduse **kanooniliseks baasiks** nimetatakse sellist V baasi, mille suhtes selle teisenduse maatriks on Jordani maatriks.

Teoreem 3.4 *Kui $V \neq \{0\}$ on vektoruum üle algebraliselt kinnise korpuse, siis selle vektorruumi iga lineaarteisenduse jaoks leidub kanooniline baas.*

Meenutame, et sama järu ruutmaatrikseid A ja B nimetatakse **sarnasteks**, kui leidub regulaarne maatriks C nii, et $B = C^{-1}AC$. Kui φ on vektoruumi 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' .

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

Teoreem 3.6 *Iga ruutmaatriks üle algebraliselt kinnise korpuse omab Jordani normaalkuju.*

3.2 Invariantsed alamruumid

Defintsioon 3.7 Olgu φ vektoruumi V lineaarteisendus. Vektoruumi 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 3.8 Alamruumid V , $\{0\}$, $\text{Ker}(\varphi)$ ja $\text{Im}(\varphi)$ on iga $\varphi \in \text{End}(V)$ korral φ -invariantsed alamruumid.

Lihtne on näha, et kehtib järgmine lause.

Lause 3.9 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.

Lause 3.10 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.

TÖESTUS. Oletame, et $a \in V \setminus \{0\}$ on lineaarteisenduse φ omavektor, mis vastab omaväärtusele $\lambda \in K$. Siis $\varphi(a) = \lambda a$ ja iga $k \in K$ korral $\varphi(ka) = k\lambda a \in \langle a \rangle$. Seega $\langle a \rangle$ on φ -invariantne alamruum.

Olgu nüüd U vektorruumi V ühemõõtmeline φ -invariantne alamruum, mille baasivektoriks on e . Siis alamruumi U nullist erinevad vektorid on kujul ke , kus $k \in K \setminus \{0\}$. Et U on φ -invariantne, siis leidub selline $l \in K$, et $\varphi(e) = le$. Siis 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 . \square

Lause 3.11 Olgu φ vektorruumi V lineaarteisendus ja olgu vektorruum V oma φ -invariantsete alamruumide otsesumma

$$V = U_1 + \dots + U_m.$$

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

$$A_\varphi^B = \text{diag} (A_{\varphi_1}^{B_1}, \dots, A_{\varphi_m}^{B_m}), \quad (12)$$

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

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

TÖESTUS. Hulk $B = B_1 \cup \dots \cup B_m$ on vektorruumi V baas tänu lausele 1.87. Tänu alamruumi U_i φ -invariantsusele on olemas lineaarteisendused $\varphi_i : U_i \rightarrow U_i$. Võrdus (12) tuleneb vahetult lineaarteisenduse maatriksi definitsioonist. \square

3.3 Nilpotentse lineaarteisenduse kanooniline baas

Definitsioon 3.12 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**.

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

Meenutame, et ringi $\text{End}(V)$ elementideks on vektorruumi V lineaarteisendused, liitmine on defineeritud punktivisiliselt, korrutamine on defineeritud järjestrakendamise abil, ühikelementiks on vektorruumi V samasusteisendus ja nullelementiks on nullteisendus. Rääkides lineaarteisenduse φ astmetest loeme, et $\varphi^0 = 1_V$.

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

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

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

2. Olgu n fikseeritud naturaalarv ja vaatleme vektorruumi

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

üle korpuuse \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.*

TÖESTUS. 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 $\lambda \neq 0$, siis ka $\lambda^r \neq 0$. Korrutades nüüd võrduse $0 = \lambda^r a$ mõlemaid pooli 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 $k \in \{0, 1, \dots, r\}$ korral tähistame*

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

Sis

$$\{0\} = H_0 \subset H_1 \subset H_2 \subset \dots \subset H_{r-1} \subset H_r = V. \quad (13)$$

TÖESTUS. Võrdused $\{0\} = H_0$ ja $H_r = V$ on ilmsed. Kui $\varphi^{k-1}(a) = 0$, siis ka $\varphi^k(a) = 0$ ja seega $H_{k-1} \subseteq H_k$ iga $k \in \{1, \dots, r\}$ korral. Kuna φ nilpotentsuse indeks on r , siis leidub vektor $b \in V$, et $\varphi^{r-1}(b) \neq 0$. Nüüd $\varphi^{r-k}(b) \in H_k \setminus H_{k-1}$, sest

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

ja

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

Seega kõik sisalduvused ahelas (13) on ranged. \square

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

$$H_{k+1} = H_k \dot{+} \langle b_1, \dots, b_l \rangle, \quad (14)$$

siis leiduvad vektorid $b_{l+1}, \dots, b_p \in H_k$ nii, et süsteem $\varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p$ on lineaarselt sõltumatu ja

$$H_k = H_{k-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle.$$

TÖESTUS. Tähistades

$$W_{k+1} := \langle b_1, \dots, b_l \rangle$$

võime kirjutada

$$H_{k+1} = H_k \dot{+} W_{k+1}. \quad (15)$$

Näitame, et lineaarkujutus $\varphi|_{W_{k+1}} : W_{k+1} \rightarrow V$ on üksühene. Lineaarkujutus on üksühene parajasti siis, kui tema tuum koosneb ainult nullvektorist ([1], lause 4.1.10). Niisiis piisab näidata, et $\text{Ker}(\varphi|_{W_{k+1}}) = \{0\}$. Olgu $a \in \text{Ker}(\varphi|_{W_{k+1}})$. Siis $a \in W_{k+1}$ ja $\varphi(a) = 0$. Järelikult $\varphi^k(a) = 0$ ja $a \in W_{k+1} \cap H_k = \{0\}$ (H_{k+1} on W_{k+1} ja H_k sisemine otsesumma), mis tähendab, et $a = 0$. Sellega oleme näidanud, et $\text{Ker}(\varphi|_{W_{k+1}}) = \{0\}$.

Kuna lineaarkujutus $\varphi|_{W_{k+1}} : W_{k+1} \rightarrow V$ on üksühene, siis

$$W_{k+1} \simeq \text{Im}(\varphi|_{W_{k+1}}) = \varphi(W_{k+1}).$$

Et vektorruumide isomorfism viib baasi baasiks, siis $\varphi(b_1), \dots, \varphi(b_l)$ on alamruumi $\varphi(W_{k+1})$ baas. Kuna $b_1, \dots, b_l \in H_{k+1}$, siis $\varphi(b_1), \dots, \varphi(b_l) \in H_k$. Seega

$$\varphi(W_{k+1}) = \langle \varphi(b_1), \dots, \varphi(b_l) \rangle \subseteq H_k.$$

Näitame, et vektorruumi H_k alamruumide summa

$$H_{k-1} + \varphi(W_{k+1})$$

on otsesumma. Selleks oletame, et $a \in H_{k-1} \cap \varphi(W_{k+1})$. Kuna $a \in \varphi(W_{k+1})$, siis leidub $x \in W_{k+1}$ nii, et $a = \varphi(x)$. Järelikult, kuna $a \in H_{k-1}$, siis

$$\varphi^k(x) = \varphi^{k-1}(\varphi(x)) = \varphi^{k-1}(a) = 0.$$

See tähendab, et $x \in H_k \cap W_{k+1} = \{0\}$ (vt. võrdust (15)) ehk $x = 0$. Järelikult ka $a = \varphi(x) = 0$. Sellega oleme näidanud, et $H_{k-1} \cap \varphi(W_{k+1}) = \{0\}$. Teoreemi 1.76 põhjal võime öelda, et

$$H_{k-1} + \varphi(W_{k+1}) = H_{k-1} \dot{+} \varphi(W_{k+1}) \subseteq H_k.$$

Olgu B alamruumi H_{k-1} suvaline baas. Siis $B \cup \{\varphi(b_1), \dots, \varphi(b_l)\}$ on lause 1.87 põhjal vektorruumi H_k alamruumi $H_{k-1} \dot{+} \varphi(W_{k+1})$ baas. Täiendame selle baasi alamruumi H_k baasiks mingite vektoritega $b_{l+1}, \dots, b_p \in H_k$. Siis on selge, et vektorid $\varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p$ on lineaarselt sõltumatud ning lause 1.86 põhjal

$$H_k = H_{k-1} \dot{+} \varphi(W_{k+1}) \dot{+} \langle b_{l+1}, \dots, b_p \rangle = H_{k-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle.$$

□

Anname sellele lemmale veel teise töestuse.

TÖESTUS. 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

$$k_1b_1 + \dots + k_lb_l \in \text{ker}(\varphi) = H_1 \subset H_2 \subset \dots \subset H_k,$$

millest tänu võrdusele (14) saame, 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

$$H_{k-1} \cap \langle \varphi(b_1), \dots, \varphi(b_l) \rangle = \{0\}.$$

Selleks oletame, et $a = k_1\varphi(b_1) + \dots + k_l\varphi(b_l) \in H_{k-1}$, kus $k_1, \dots, k_l \in K$. Siis

$$0 = \varphi^{k-1}(a) = \varphi^k(k_1b_1 + \dots + k_lb_l)$$

ehk

$$k_1b_1 + \dots + k_lb_l \in H_k \cap \langle b_1, \dots, b_l \rangle = \{0\}.$$

Kuna vektorid b_1, \dots, b_l on lineaarselt sõltumatud, siis võrdusest $k_1b_1 + \dots + k_lb_l = 0$ saame, et $k_1 = \dots = k_l = 0$. Järelikult ka $a = 0$.

Teoreemi 1.76 põhjal

$$H_{k-1} + \langle \varphi(b_1), \dots, \varphi(b_l) \rangle = H_{k-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l) \rangle \subseteq H_k.$$

Olgu B alamruumi H_{k-1} suvaline baas. Siis $B \cup \{\varphi(b_1), \dots, \varphi(b_l)\}$ on lause 1.87 põhjal vektorruumi H_k alamruumi $H_{k-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l) \rangle$ baas. Täiendame selle baasi alamruumi H_k baasiks mingite vektoritega $b_{l+1}, \dots, b_p \in H_k$. Siis on selge, et vektorid $\varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p$ on lineaarselt sõltumatud ning lause 1.86 põhjal

$$H_k = H_{k-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l) \rangle \dot{+} \langle b_{l+1}, \dots, b_p \rangle = H_{k-1} \dot{+} \langle \varphi(b_1), \dots, \varphi(b_l), b_{l+1}, \dots, b_p \rangle.$$

□

Teoreem 3.17 *Iga vektorruumi $V \neq \{0\}$ igal nilpotentsel lineaarteisendusel on olemas kanooniline baas.*

TÖESTUS. Olgu φ vektorruumi $V \neq \{0\}$ nilpotentne lineaarteisendus indeksiga r . Vaatleme V alamruumide jada (13). Olgu $a_1, \dots, a_{p_1} \in V$ vektorid, mis täiendavad alamruumi H_{r-1} mingi baasi $H_r = V$ baasiks. Siis a_1, \dots, a_{p_1} on lineaarselt sõltumatud ja lause 1.86 põhjal

$$V = H_r = H_{r-1} \dot{+} \langle a_1, \dots, a_{p_1} \rangle.$$

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

$$H_{r-1} = H_{r-2} \dot{+} \langle \varphi(a_1), \dots, \varphi(a_{p_1}), a_{p_1+1}, \dots, a_{p_2} \rangle.$$

Seega

$$\begin{aligned} V &= H_{r-2} \dot{+} \langle \varphi(a_1), \dots, \varphi(a_{p_1}), a_{p_1+1}, \dots, a_{p_2} \rangle \dot{+} \langle a_1, \dots, a_{p_1} \rangle \\ &= H_{r-2} \dot{+} \langle \varphi(a_1), \dots, \varphi(a_{p_1}), a_{p_1+1}, \dots, a_{p_2}, a_1, \dots, a_{p_1} \rangle \end{aligned}$$

ja süsteem $\varphi(a_1), \dots, \varphi(a_{p_1}), a_{p_1+1}, \dots, a_{p_2}, a_1, \dots, a_{p_1}$ on lineaarselt sõltumatu tänu lausele 1.87. Samamoodi jätkates jõuame lõpuks olukorrali, kus leiduvad vektorid $a_{p_{r-1}+1}, \dots, a_{p_r} \in H_1$ nii, et

$$H_1 = H_0 \dot{+} \langle \varphi^{r-1}(a_1), \dots, \varphi^{r-1}(a_{p_1}), \varphi^{r-2}(a_{p_1+1}), \dots, \varphi^{r-2}(a_{p_2}), \dots, a_{p_{r-1}+1}, \dots, a_{p_r} \rangle$$

ja selle võrduse paremas pool esinev vektorite süsteem on lineaarselt sõltumatu. Seega

$$\begin{aligned} V &= \\ &\langle \varphi^{r-1}(a_1), \dots, \varphi^{r-1}(a_{p_1}), \varphi^{r-2}(a_{p_1+1}), \dots, \varphi^{r-2}(a_{p_2}), \dots, \varphi(a_{p_{r-2}+1}), \dots, \varphi(a_{p_{r-1}}), a_{p_{r-1}+1}, \dots, a_{p_r}, \\ &\varphi^{r-2}(a_1), \dots, \varphi^{r-2}(a_{p_1}), \varphi^{r-3}(a_{p_1+1}), \dots, \varphi^{r-3}(a_{p_2}), \dots, a_{p_{r-2}+1}, \dots, a_{p_{r-1}}, \\ &\dots \quad \dots \\ &\varphi(a_1), \dots, \varphi(a_{p_1}), \quad a_{p_1+1}, \dots, a_{p_2}, \\ &a_1, \dots, a_{p_1} \rangle, \end{aligned}$$

kusjuures siin esinev vektorite süsteem B on lineaarselt sõltumatu. Seega on see süsteem vektorruumi V baas. Veendume, et B on vektorruumi V kanooniline baas.

Järjestame baasi B vektorid nii, et kõigepäält on esimese veeru vektorid ülevallt alla, siis teise veeru vektorid ülevallt 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). Tõepooolest, 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 3.11 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 päädiagonaalil 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.

□

Kuna iga ruutmaatriks üle korpuse on vaadeldav mingi vektoruumi mingi lineaarteisenduse maatriksina ja kaks maatriksit on sarnased parajasti siis, kui nad on sama teisenduse maatriksid kahe baasi suhtes, siis võime sõnastada järgneva tulemuse maatriksite kohta.

Teoreem 3.18 *Igal nilpotentsel ruutmaatriksil üle mistahes korpuse on olemas Jordani normaalkuju.*

Teoreemi 3.17 tõestus annab meile ka meetodi nilpotentse lineaarteisenduse kanoonilise baasi leidmiseks. Olgu φ vektoruumi V nilpotentne lineaarteisendus, mis on antud oma maatriksiga $A = A_\varphi^e$ mingi baasi $e = \{e_1, \dots, e_n\}$ suhtes.

- Kõigepäält leiame teisenduse φ nilpotentsuse indeksi r , mis on ühtlasi maatriksi 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 nullmaatriks.
- Iga $k \in \{1, \dots, r-1\}$ jaoks leiame V alamruumi $H_k := \text{Ker}(\varphi^k)$ baasi. Selleks leiame sellise homogeense lineaarvõrandisüsteemi lahendite alamruumi baasi (fundamentaalsüsteemi) B_k , mille maatriks on A^k .
- Vaatleme baasi B_{r-1} . Täiendame selle baasi mingite vektoritega vektoruumi 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 maatriksi Jordani normaalkuju leidmine

Lihtne on veenduda, et kehtivad järgmised kaks lauset.

Lause 3.19 *Mistahes ruutmaatriksite 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 maatriksite astakud on võrdsed.*

TÖESTUS. Olgu maatriksid A ja B sarnased. Siis leidub regulaarne maatriks C nii, et $B = C^{-1}AC$. On teada (vt. [1], lause 4.6.6), et maatriksite 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 maatriksi 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 maatriks ja olgu $J(A)$ maatriksi A Jordani normaalkuju. Olgu s_k , $k = 1, \dots, n$, Jordani kastide $J_k(0)$ arv maatriksis $J(A)$. Siis arvud s_k saab leida lineaarvõrrandisüsteemist*

$$\begin{aligned} s_1 + s_2 + s_3 + s_4 + \dots + s_n &= n - u_1 \\ s_2 + s_3 + s_4 + \dots + s_n &= u_1 - u_2 \\ s_3 + s_4 + \dots + s_n &= u_2 - u_3 \\ &\dots \\ s_n &= u_{n-1} - u_n, \end{aligned}$$

kus $u_i = \text{rank}(A^i)$ iga $i = 1, \dots, n$ korral.

TÖESTUS. Kuna maatriksid A ja $J(A)$ on sarnased, siis on ka A^i ja $J(A)^i$ sarnased iga $i = 1, \dots, n$ korral. Et sarnaste maatriksite 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 $s_1 + s_2 + \dots + s_n$. Maatriksi $J(A)$ astak on maatriksi $J(A)^2$ 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 olemasolukseks

Hakkame nüüd vaatlema suvalisi lineaarteisendusi (mis ei pruugi olla nilpotentsed). Meie eesmärgiks selles paragrahvis on anda piisav tingimus selleks, et lineaarteisendus omaks kanoonilist baasi.

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

$$g(\varphi) = k_01_V + k_1\varphi + k_2\varphi^2 + \dots + k_n\varphi^n.$$

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 lineaarteisendus, mis viib vektori $a \in V$ vektoriks

$$g(\varphi)(a) = (31_V - 2\varphi + 5\varphi^2)(a) = 3a - 2\varphi(a) + 5\varphi(\varphi(a)).$$

Definitsioon 3.25 Olgu V vektorruum üle korpuse K ja $\varphi \in \text{End}(V)$. Nullist erinevat polünoomi $g(X) \in K[X]$ nimetatakse lineaarteisenduse φ **annulleerivaks polünoomiks**, kui $g(\varphi)$ on nullteisendus. Analoogiliselt defineeritakse maatriksi $A \in \text{Mat}_n(K)$ annulleeriv polünoom.

Lause 3.26 Olgu V vektorruum üle korpuse K , $\varphi \in \text{End}(V)$ ning olgu A lineaarteisenduse φ maatriks mingu baasi suhtes. Polünoom $g(X) \in K[X]$ annulleerib lineaarteisenduse φ parajasti siis, kui ta annulleerib maatriksi A .

TÖESTUS. Olgu $g(X) = k_0 + k_1X + \dots + k_nX^n$ ja olgu e vektorruumi V baas. Meenutame, et kujutus

$$\psi : \text{End}(V) \rightarrow \text{Mat}_n(K), \quad \varphi \mapsto A_\varphi^e$$

on nii ringide kui vektoruumide isomorfism ([1], teoreemid 4.1.12 ja 4.2.12). Tänu sellele

$$\begin{aligned} \psi(g(\varphi)) &= \psi(k_01_V + k_1\varphi + \dots + k_n\varphi^n) \\ &= k_0\psi(1_V) + k_1\psi(\varphi) + \dots + k_n\psi(\varphi)^n \\ &= k_0E + k_1A + \dots + k_nA^n \\ &= g(A). \end{aligned}$$

Et ψ on muuhulgas injektiivne homomorfism, siis $g(\varphi) = 0$ parajasti siis, kui $g(A) = 0$. \square

Lause 3.27 Igal ruutmaatriksil üle korpuse on olemas annulleeriv polünoom. Iga vektorruumi igal lineaarteisendusel on olemas annulleeriv polünoom.

TÖESTUS. Tõestame selle väite maatriksite jaoks. Vastav tulemus lineaarteisenduste kohta järeltub siis lausest 3.26.

Olgu $A \in \text{Mat}_n(K)$. Teatavasti $\dim(\text{Mat}_n(K)) = n^2$. Järelkult 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 $k_0, k_1, \dots, k_{n^2} \in K$, 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. \square

Lause 3.28 Olgu V vektorruum üle korpuse K ning lahutugu lineaarteisenduse $\varphi \in \text{End}(V)$ annulleeriv polünoom $g(X) \in K[X]$ 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 -invariantsed alamruumid.

TÖESTUS. 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 $g(\varphi) = 0$. 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 $1_V = g_1(\varphi)u(\varphi) + g_2(\varphi)v(\varphi)$ ehk iga $a \in V$ korral

$$a = (g_1(\varphi)u(\varphi))(a) + (g_2(\varphi)v(\varphi))(a). \quad (16)$$

Kuna

$$g_2(\varphi)[(g_1(\varphi)u(\varphi))(a)] = [g_2(\varphi)g_1(\varphi)](u(\varphi)(a)) = [g(\varphi)](u(\varphi)(a)) = 0(u(\varphi)(a)) = 0,$$

siis $(g_1(\varphi)u(\varphi))(a) \in \text{Ker}(g_2(\varphi))$. Analoogiliselt $(g_2(\varphi)v(\varphi))(a) \in \text{Ker}(g_1(\varphi))$. Seega võrdust (16) arvestades saame,

$$V = \text{Ker}(g_1(\varphi)) + \text{Ker}(g_2(\varphi)).$$

Veendume, et see summa on otsesumma. Selleks oletame, et $b \in \text{Ker}(g_1(\varphi)) \cap \text{Ker}(g_2(\varphi))$. Siis

$$\begin{aligned} b &= (g_1(\varphi)u(\varphi))(b) + (g_2(\varphi)v(\varphi))(b) = (u(\varphi)g_1(\varphi))(b) + (v(\varphi)g_2(\varphi))(b) \\ &= u(\varphi)(g_1(\varphi)(b)) + v(\varphi)(g_2(\varphi)(b)) = u(\varphi)(0) + v(\varphi)(0) = 0 + 0 = 0. \end{aligned}$$

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

$$g_i(\varphi)(\varphi(a)) = (g_i(\varphi)\varphi)(a) = (\varphi g_i(\varphi))(a) = \varphi(g_i(\varphi)(a)) = \varphi(0) = 0.$$

Seega $\varphi(a) \in \text{Ker}(g_i(\varphi))$. □

Teoreem 3.29 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.

TÖESTUS. Olgu lineaarteisendusel φ annulleeriv polünoom

$$g(X) = (X - \lambda_1)^{r_1} \cdot \dots \cdot (X - \lambda_m)^{r_m},$$

kus $\lambda_1, \dots, \lambda_m \in K$ on paarikaupa erinevad. Siis on selge, et $\text{SÜT}(X - \lambda_i, X - \lambda_j) = 1$, kui $i \neq j$. Lause 3.28 põhjal

$$V = \text{Ker}(\varphi - \lambda_1 1_V)^{r_1} \dot{+} \dots \dot{+} \text{Ker}(\varphi - \lambda_m 1_V)^{r_m},$$

kusjuures otseliidetavad on φ -invariantsed alamruumid. Tähistame

$$U_i := \text{Ker}(\varphi - \lambda_i 1_V)^{r_i},$$

$i = 1, \dots, m$. 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

$$\begin{aligned}\varphi_{U_i} : a &\mapsto \varphi(a), \\ (\lambda_i 1_V)_{U_i} : a &\mapsto \lambda_i a, \\ (\varphi - \lambda_i 1_V)_{U_i} : a &\mapsto \varphi(a) - \lambda_i a.\end{aligned}$$

Kuna lineaarteisendus $(\varphi - \lambda_i 1_V)_{U_i} \in \text{End}(U_i)$ on nilpotentne (tema r_i -s aste on nullteisendus), siis leidub selle teisenduse jaoks kanooniline baas B_i ruumis U_i . Et $\varphi = (\varphi - \lambda_i 1_V) + \lambda_i 1_V$, siis ka $\varphi_{U_i} = (\varphi - \lambda_i 1_V)_{U_i} + (\lambda_i 1_V)_{U_i}$ ja

$$A_{\varphi_{U_i}}^{B_i} = A_{(\varphi - \lambda_i 1_V)_{U_i}}^{B_i} + A_{(\lambda_i 1_V)_{U_i}}^{B_i}.$$

Kuna $A_{(\varphi - \lambda_i 1_V)_{U_i}}^{B_i}$ on Jordani maatriks, mille päädiagonaalil on nullid ja $A_{(\lambda_i 1_V)_{U_i}}^{B_i}$ on diagonaalmaatriks, mille kõik päädiagonaalali elemendid on võrdsed elemendiga λ_i , siis $A_{\varphi_{U_i}}^{B_i}$ on Jordani maatriks, mille päädiagonaalil on kõikjal λ_i . Tähistades $B := B_1 \cup \dots \cup B_m$ võime lause 3.11 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 3.30 Olgu V vektorruum üle korpuse \mathbb{C} . Siis igal lineaarteisendusel $\varphi \in \text{End}(V)$ leidub kanooniline baas.

TÖESTUS. Tänu lausele 3.27 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 3.29 põhjal. \square

3.6 Cayley-Hamtoni teoreem

Selle paragrahvi eesmärgiks on tõestada tulemus, mida tänapäeval tuntakse Cayley-Hamiltoni teoreemina, ja mis ütleb, et lineaarteisenduse karakteristlik polünoom on tema annulleeriv polünoom. Cayley² ja Hamilton³ töestasid selle väite teatud erijuhtude jaoks, üldjuhul andis esimese töestuse Frobenius⁴ 1878. aastal.

Defintsioon 3.31 Lineaarteisenduse **minimaalseks polünoomiks** nimetatakse selle lineaarteisenduse minimaalse astmega unitaarset annulleerivat polünoomi. Analoogiliselt defineeritakse ruutmaatriksi minimaalne polünoom.

Tänu lausele 3.27 on igal lineaarteisendusel olemas nii annulleeriv kui minimaalne polünoom.

Lause 3.32 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 .

TÖESTUS. Tõestame väite lineaarteisenduste jaoks. Maatriksite korral on tõestus analoogiline. TARVILIKKUS. Olgu $g(X) \in K[X]$ teisenduse φ annulleeriv polünoom. Jagades polünoomi $g(X)$ jäädiga teisenduse φ minimaalse polünoomiga $m(X)$ saame leida polünoomid $q(X), r(X) \in K[X]$ nii, et

$$g(X) = m(X)q(X) + r(X) \quad \text{ja} \quad \deg(r(X)) < \deg(m(X)).$$

²Arthur Cayley (1821–1895) — inglise matemaatik

³William Rowan Hamilton (1805–1865) — iiri matemaatik

⁴Ferdinand Georg Frobenius (1849–1917) — saksa matemaatik

Järelikult $g(\varphi) = m(\varphi)q(\varphi) + r(\varphi)$ ja kuna $g(\varphi) = 0 = m(\varphi)$, siis ka $r(\varphi) = 0$. Et $m(X)$ on minimaalne polünoom, siis viimane võrdus saab kehtida vaid siis, kui $r(X) = 0$. See aga tähendab, et $g(X) = m(X)q(X)$ ehk polünoom $g(X)$ jagub polünoomiga $m(X)$.

PIISAVUS. Oletame, et teisenduse φ annulleeriv 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 $g(\varphi) = m(\varphi)q(\varphi) = 0$. \square

Järeldus 3.33 *Igal lineaarteisendusel ja igal ruutmaatriksil üle korpuse leidub üheselt määratud minimaalne polünoom.*

TÖESTUS. Olgu $m_1(X)$ ja $m_2(X)$ lineaarteisenduse $\varphi \in \text{End}(V)$ minimaalsed polünoomid. Siis neil on sama aste. Kuna $m_1(\varphi) = 0$ ja $m_2(X)$ on minimaalne polünoom, siis lause 3.32 põhjal $m_2(X) | m_1(X)$. Et nende polünoomide aste on sama, siis leidub $k \in K$ nii, et $km_2(X) = m_1(X)$. Kuna $m_1(X)$ ja $m_2(X)$ on unitaarsed polünoomid, siis $k = 1$. \square

Lause 3.34 *Olgu V vektorruum üle korpuse K , $\varphi \in \text{End}(V)$ ning oltu 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.*

TÖESTUS. Lause 3.26 põhjal on teisendusel φ ja maatriksil A samad annulleerivad polünoomid. Analoogiliselt järelduse 3.33 tõestusega saab näidata, et φ ja A minimaalsed polünoomid langevad kokku. \square

Järeldus 3.35 *Sarnastel maatriksitel on samad annulleerivad polünoomid ja võrdsed minimaalsed polünoomid.*

Lemma 3.36 *Olgu K korpus, $\lambda \in K$ ja $n \in \mathbb{N}$. Polünoomi $(X - \lambda)^n$ unitaarsed jagajad polünoomide ringis $K[X]$ on kujul $(X - \lambda)^k$, kus $k \leq n$.*

TÖESTUS. 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

$$k \in \mathbb{N} \cup \{0\} \text{ suurim selline arv, et } (X - \lambda)^k | f(X), \quad (17)$$

$$l \in \mathbb{N} \cup \{0\} \text{ suurim selline arv, et } (X - \lambda)^l | h(X). \quad (18)$$

Siis

$$k + l \leq \deg(f(X)) + \deg(h(X)) = n$$

ning $(X - \lambda)^k \cdot f_1(X) = f(X)$ ja $(X - \lambda)^l \cdot h_1(X) = h(X)$ mingite polünoomide $f_1(X), h_1(X) \in K[X]$ korral. 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, 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 $(X - \lambda) | f_1(X)$ ja $(X - \lambda)^{k+1} | f(X)$, mis on vastuolus eeldusega (17). 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 $k = \deg(f(X))$ ja $l = \deg(h(X))$. Tänu unitaarsusele $(X - \lambda)^k = f(X)$. \square

Lause 3.37 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.

TÖESTUS. Kuna

$$0 = J_n(0)^n = (J_n(\lambda) - \lambda E)^n,$$

siis $(X - \lambda)^n \in K[X]$ on maatriksi $J_n(\lambda)$ annulleeriv polünoom. Tänu lausele 3.32 jagub see polünoom maatriksi $J_n(\lambda)$ minimaalse polünoomiga. See aga tähendab, et maatriksi $J_n(\lambda)$ minimaalne polünoom on kujul $(X - \lambda)^k$, kus $k \leq n$. Kuna $J_n(0)^{n-1} \neq 0$, siis $k = n$, s.t. $J_n(\lambda)$ minimaalne polünoom on $(X - \lambda)^n$. Teisest küljest maatriksi $J_n(\lambda)$ karakteristlik polünoom on

$$\det(J_n(\lambda) - XE) = (\lambda - X)^n = (-1)^n(X - \lambda)^n.$$

□

Lause 3.38 Jordani maatriksi minimaalne polünoom on tema kastide minimaalsete polünoomide vähim ühiskordne.

TÖESTUS. 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 3.32 põhjal $m_i(X) | m(X)$ iga $i \in \{1, \dots, s\}$ korral, mis tähendab, et $m(X)$ on polünoomide $m_1(X), \dots, m_s(X)$ vähim ühine kordne.

Olgu nüüd $p(X) \in K[X]$ selline polünoom, et $m_i(X) | p(X)$ 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 $m(X) | p(X)$. Sellega oleme töestanud, et $m(X)$ on polünoomide $m_1(X), \dots, m_s(X)$ vähim ühiskordne. □

Teoreem 3.39 (Cayley-Hamtoni teoreem) Iga lineaarteisenduse karakteristlik polünoom on tema annulleeriv polünoom.

TÖESTUS. Lineaarteisenduse karakteristlik polünoom defineeritakse kui tema maatriksi karakteristlik polünoom. Seega tänu lausele 3.26 piisab, kui näitame, et iga maatriksi karakteristlik polünoom 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 3.27). Teoreemi 2.23 põhjal leidub selline korpus \bar{K} , et K on \bar{K} alamkorpus ja $g(X)$ lahutub lineaarpolünoomide korrutiseks ringis $\bar{K}[X]$. Olgu nüüd V n -mõõtmeline vektorruum üle korpuse \bar{K} ja $\varphi \in \text{End}(V)$ selline lineaarteisendus, mille maatriks mingi baasi suhtes on A . Siis $g(X) \in K[X] \subseteq \bar{K}[X]$ on ka lineaarteisenduse φ annulleeriv polünoom. Teoreemi 3.29 põhjal leidub lineaarteisendusel φ kanooniline baas. Teisenduse φ maatriks selle kanoonilise baasi suhtes on Jordani maatriks, olgu see J . Et nii A kui J on teisenduse φ maatriksid mingite baaside suhtes, siis on nad sarnased maatriksid. Seega on neil samad karakteristikud polünoomid ([1], lause 8.2.9) ja samad annulleerivad polünoomid (tänu lausele 3.26). Seega piisab näidata, et J karakteristlik polünoom annulleerib maatriksi J .

Olgu

$$J = \text{diag}(J_{n_1}(\lambda_1), \dots, J_{n_s}(\lambda_s)).$$

Siis Jordani kasti $J_{n_i}(\lambda_i)$ minimaalne polünoom on lause 3.37 põhjal

$$m_i(X) = (X - \lambda_i)^{n_i} = (-1)^{n_i} \det(J_{n_i}(\lambda_i) - XE).$$

Paneme tähele, et maatriksi J karakteristlik polünoom on

$$\begin{aligned} \det(J - XE) &= \det(J_{n_1}(\lambda_1) - XE) \cdot \dots \cdot \det(J_{n_s}(\lambda_s) - XE) \\ &= (-1)^{n_1} m_1(X) \cdot \dots \cdot (-1)^{n_s} m_s(X) = (-1)^{n_1 + \dots + n_s} \cdot m_1(X) \cdot \dots \cdot m_s(X). \end{aligned}$$

Seega $\det(J - XE)$ on polünoomide $m_1(X), \dots, m_s(X)$ ühine kordne. Maatriksi J minimaalne polünoom $m(X)$ on aga lause 3.38 tõttu polünoomide $m_1(X), \dots, m_s(X)$ vähim ühiskordne. Vähima ühiskordse definitsiooni põhjal peab $m(X)$ jagama polünoomi $\det(J - XE)$. Tänu lausele 3.32 saame, et $\det(J - XE)$ on maatriksi annulleeriv polünoom, mida oligi tarvis tõestada.

□

Anname sellele teoreemile veel teise tõestuse.

TÖESTUS. 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 3.27). Teoreemi 2.23 põhjal leidub selline korpus \bar{K} , et K on \bar{K} alamkorpus ja $g(X)$ lahutub lineaarpolünoomide korrutiseks ringis $\bar{K}[X]$. Teoreemi 3.29 analoog maatriksite jaoks ütleb, et leidub Jordani maatriks $J \in \text{Mat}_n(\bar{K})$ nii, et maatriksid A ja J on sarnased. Järelikult on neil samad karakteristikud polünoomid ([1], lause 8.2.9) ja samad annulleerivad polünoomid (tänu lausele 3.26). Seega tõestuse lõpetamiseks piisab näidata, et J karakteristlik polünoom annulleerib maatriksi J .

Olgu

$$J = \text{diag}(J_{n_1}(\lambda_1), \dots, J_{n_s}(\lambda_s)).$$

Siis maatriksi J karakteristlik polünoom on

$$\det(J - XE) = \det(J_{n_1}(\lambda_1) - XE) \cdot \dots \cdot \det(J_{n_s}(\lambda_s) - XE).$$

Lihitne on näha, et kui B on blokk-diagonaalne maatriks, $B = \text{diag}(B_1, \dots, B_s)$ ja $h(X)$ on polünoom üle selle korpuuse, kuhu kuuluvad B elemendid, siis

$$h(B) = \text{diag}(h(B_1), \dots, h(B_s)).$$

Vöttes $h(X) := \det(J - XE)$ näeme, et

$$h(J) = \text{diag}(h(J_{n_1}(\lambda_1)), \dots, h(J_{n_s}(\lambda_s))).$$

Lause 3.37 põhjal iga $i \in \{1, \dots, s\}$ korral Jordani kasti $J_{n_i}(\lambda_i)$ karakteristlik polünoom $h_i(X) = \det(J_{n_i}(\lambda_i) - XE)$ annulleerib selle Jordani kasti. Kuna $h(X) = h_1(X) \cdot \dots \cdot h_s(X)$, siis $h(J)$ on blokk-diagonaalne maatriks, mille kõik blokid on nullmaatriksid. Seega J karakteristlik polünoom annulleerib maatriksi J . □

Teoreem 3.40 Olgu V vektorruum üle korpuuse K ja $\varphi \in \text{End}(V)$. Lineaarteisendusel φ leidub kanooniline baas parajasti siis, kui tema karakteristlik polünoom lahutub lineaarpolünoomide korrutiseks üle korpuuse K .

TÖESTUS. 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-Hamtoni teoreemi tõttu on teisendusel φ olemas lineaartegureiks lahutuv annulleeriv polünoom. Seega teoreemi 3.29 tõttu on tal olemas kanooniline baas. \square

3.7 Kanoonilise baasi ja Jordani normaalkuju leidmine

Olgu φ vektoruumi V lineaarteisendus, mis on antud oma maatriksiga $A = A_\varphi^e$ mingi baasi $e = \{e_1, \dots, e_n\}$ suhtes.

- Kõigipäält 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. vektoruumi 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 vektoruumi U_i nilpotentne lineaarteisendus ja $V = U_1 + \dots + U_s$.
- Leiame iga teisenduse ψ_i , $i \in \{1, \dots, s\}$, jaoks kanoonilise baasi. Siis nende kanooniliste baaside ühend ongi φ kanooniline baas.

Kui on vaja leida ainult ruutmaatriksi A Jordani normaalkuju $J(A)$, siis tuleb iga i , $i \in \{1, \dots, s\}$, jaoks koostada ja lahendada lineaarvõrrandisüsteem, mis on sarnane sellele, mis on antud teoreemis 3.22. Olgu s_k Jordani kastide $J_k(\lambda_i)$ arv maatriksis $J(A)$. Siis arvud s_k saab leida lineaarvõrrandisüsteemist

$$\begin{aligned} s_1 + s_2 + s_3 + s_4 + \dots + s_{n_i} &= n - u_1 \\ s_2 + s_3 + s_4 + \dots + s_{n_i} &= u_1 - u_2 \\ s_3 + s_4 + \dots + s_{n_i} &= u_2 - u_3 \\ &\vdots \\ s_{n_i} &= u_{n_i-1} - u_{n_i}, \end{aligned}$$

kus $u_j = \text{rank } ((A - \lambda_i E)^j)$ iga $j = 1, \dots, n_i$ korral.

4 Funktsionaalid ja vormid

4.1 Lineaarsed funktsionaalid ja lineaarvormid

Meenutame, et iga korpust K võib loomulikul viisil vaadelda vektorruumina üle iseenda. Selles päätükis eeldame, et kõik vaadeldavad korpused on kommutatiivsed.

Definitsioon 4.1 Olgu V vektoruum üle korpuse K . Lineaarkujutust vektorruumist V korpuesse K nimetatakse **lineaarseks funktsionaaliks** vektorruumil V .

Kõigi lineaarsete funktsionaalide hulka vektorruumil V tähistame sümboliga $\text{Hom}(V, K)$ või lühidalt V^* . Sellel hulgal saab defineerida tehted niiöeldala punktiviisiliselt:

$$(\varphi + \psi)(a) := \varphi(a) + \psi(a), \\ (k\varphi)(a) := k\varphi(a)$$

mistahes $\varphi, \psi \in \text{Hom}(V, K)$ ja $a \in V$ korral. On teada, et nende tehete suhtes on $\text{Hom}(V, K)$ vektoruum ([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**.

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

$$\bar{x}_e := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \text{Mat}_{n,1}(K)$$

ja nimetame seda üheveerulist maatriksit vektori x **koordinaatide veeruks** baasi e suhtes. Olgu φ lineaarne funktsionaal sellel vektorruumil. Tähistades

$$\varphi(e_i) =: a_i \in K$$

võime kirjutada

$$\varphi(x) = \varphi \left(\sum_{i=1}^n x_i e_i \right) = \sum_{i=1}^n x_i \varphi(e_i) = \sum_{i=1}^n a_i x_i. \quad (19)$$

Definitsioon 4.5 Homogeenset polünoomi $\sum_{i=1}^n a_i X_i$ nimetatakse lineaarsele funktionsionaalile φ vastavaks **lineaarvormiks** baasi e suhtes.

Lause 4.6 Olgu V n -mõõtmeline vektorruum üle korpuse K . Vektorruumi V baasi fikseerimine tekitab üksühese vastavuse selle vektorruumi lineaarsele funktionsionaalide ja n muutuja lineaarvormide vahel, mille kordajad on korpusest K .

TÖESTUS. Kasutame eelneaid 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 funktionsionaalile φ vastavusse talle vastava lineaarvormi $\sum_{i=1}^n a_i X_i$, ja olgu

$$\beta : K_1[X_1, \dots, X_n] \rightarrow \text{Hom}(V, K)$$

kujutus, mis viib lineaarvormi $k_1 X_1 + \dots + k_n X_n$ lineaarseks funktionsionaaliks $\beta(k_1 X_1 + \dots + k_n X_n) : V \rightarrow K$, mis on defineeritud 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 $\alpha\beta$ ja $\beta\alpha$ 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 lineaarteisen-duse φ maatriks baaside e ja 1 suhtes. Harilikult nimetatakse seda üherealist maatriksit lihtsalt **lineaarse funktionsionaali φ maatriksiks** baasi e suhtes.

Arvestades võrdust (19) ja samastades ühe-elemendilise maatriksi tema ainsa elemendiga võime lineaarse funktionsionaali esitada maatriksite korrutamise abil:

$$\varphi(x) = \bar{a} \bar{x}_e. \quad (20)$$

Kuidas sõltub lineaarsele funktionsionaalile φ vastav lineaarvorm vektorruumi V baasi valikust?

Lause 4.7 Üleminekul ühelt baasilt teisele korrutub lineaarse funktionsionaali maatriks paremalt üleminekumaatriksiga.

TÖESTUS. Kasutame eelneaid tähistusi. Olgu vektorruumis V antud veel baas $e' = \{e'_1, \dots, e'_n\}$. Siis vektor x avaldub ka kujul $x = x'_1 e'_1 + \dots + x'_n e'_n$, 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 funktionsionaali 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 baasidevektori 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 (20) saame, et iga $i \in \{1, \dots, n\}$ korral

$$a'_i = \bar{a}'(\bar{e}'_i)_{e'} = \varphi(e'_i) = (\bar{a}T)(\bar{e}'_i)_{e'} = (b_1 \dots b_n)(\bar{e}'_i)_{e'} = b_i.$$

Seega kehtib maatriksite võrdus

$$\overline{a'} = \overline{a} T,$$

s.t. φ maatriks e' suhtes on tema maatriks e suhtes korda T . Seda oligi tarvis tõestada. \square

Lause 4.8 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

$$e^i \left(\sum_{j=1}^n x_j e_j \right) := x_i.$$

Sis $\{e^1, \dots, e^n\}$ on baas vektorruumis $\text{Hom}(V, K)$.

TÖESTUS. 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 korrutamisega. 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 on 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 4.9 Iga vektorruum on isomorfne oma kaasruumiga.

TÖESTUS. Kaks lõplikumõõtmelist vektorruumi üle sama korpuse on isomorfsed parajasti siis, kui nende mõõtmed on samad ([1], teoreem 3.4.5). Lause 4.8 põhjal on vektorruumi kaasruumi mõõde sama, mis selle vektorruumi mõõde. Seega $V \simeq V^*$. \square

Definitsioon 4.10 Lauses 4.8 defineeritud kaasruumi V^* baasi $\{e^1, \dots, e^n\}$ nimetatakse baasi e **kaasbaasiks** ja tähistatakse sümboliga e^* .

Definitsioon 4.11 Vektorruumi V **teiseks kaasruumiks** nimetatakse vektorruumi

$$V^{**} = (V^*)^* = \text{Hom}(\text{Hom}(V, K), K).$$

Järeldust 4.9 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 vektoruumide V ja V^{**} vahel leidub teatud loomulikul viisil defineeritud isomorfism.

Teoreem 4.12 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.

TÖESTUS. 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. Järelkult $\Phi(e_1), \dots, \Phi(e_n)$ on vektorruumi V^{**} baas. Kui $f \in V^{**}$ on suvaline, siis ta avaldub kujul

$$f = k_1\Phi(e_1) + \dots + k_n\Phi(e_n) = \Phi(k_1e_1 + \dots + k_ne_n),$$

kus $k_1, \dots, k_n \in K$. See näitab, et Φ on päalekujutus ja seega kokkuvõttes isomorfism. \square

4.2 Bilineaarsed funktsionaalid ja bilineaarvormid

Definitsioon 4.13 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 4.14 Skalaarkorrutamine mistahes eukleidilisel ruumil on bilineärne funktsionaal.

Definitsioon 4.15 Olgu V vektorruum üle korpuse K , olgu f bilineärne 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.

Näeme, et nii nagu lineaarsetegi funktsionaalide korral on maatriksi elementideks baasidevektorite kujutised.

Kui f on bilineaarne funktsionaal vektorruumil V ja A on f maatriks baasi e suhtes, siis iga $x, y \in V$ korral

$$\begin{aligned} f(x, y) &= f(x_1 e_1 + \dots + x_n e_n, y_1 e_1 + \dots + y_n e_n) = \sum_{i,j=1}^n f(x_i e_i, y_j e_j) \\ &= \sum_{i,j=1}^n x_i y_j f(e_i, e_j) = \sum_{i,j=1}^n f(e_i, e_j) x_i y_j \end{aligned}$$

kus x_1, \dots, x_n ja y_1, \dots, y_n on vastavalt vektorite x ja y koordinaadid baasi e suhtes. Seega

$$f(x, y) = \sum_{i,j=1}^n a_{ij} x_i y_j, \quad (21)$$

Defintsioon 4.16 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 bilineaarsel funktsionaalile f vastavaks **bilineaarvormiks** muutujate $X_1, \dots, X_n, Y_1, \dots, Y_n$ suhtes.

Analoogiliselt lausega 4.6 saab tõestada järgmise lause.

Lause 4.17 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 4.18 Üleminekul ühelt baasilt teisele korrutub bilineaarse funktsionaali maatriks paremalt üleminekumaatriksiga ja vasakult üleminekumaatriksi transponeeritud maatriksiga.

TÖESTUS. 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 (21) ja samastades jällegi ühe-elemendilise maatriksi tema ainsa elemendiga võime bilineaarse funktsionaali esitada maatrikskujul

$$f(x, y) = \bar{x}_e^t A_f^e \bar{y}_e, \quad (22)$$

kus \bar{x}_e ja \bar{y}_e on vektorite $x, y \in V$ koordinaatide veerud baasi e suhtes. Siis $\bar{x}_e = T \bar{x}_{e'}$, $\bar{y}_e = T \bar{y}_{e'}$ 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

$$(\bar{e}'_i)^t A_f^{e'} (\bar{e}'_j)_{e'} = (\bar{e}'_i)^t (T^t A_f^e T) (\bar{e}'_j)_{e'}.$$

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. \square

Defintsioon 4.19 Bilineaarset funktsionaali f vektorruumil V nimetatakse **sümmeetriliseks**, kui

$$f(x, y) = f(y, x)$$

iga $x, y \in V$ korral.

Sümmeetrilise bilineaarse funktsionaali maatriks mistahes baasi suhtes on sümmeetriline ja ka vastupidi: kui mingi bilineaarse funktsionaali maatriks mingi baasi suhtes on sümmeetriline, siis see funktsionaal on ka sümmeetriline.

4.3 Ruutfunktsionaalid ja ruutvormid

Selles paragraahvis uurime ruutfunktsionaale ja ruutvorme. Need leiavad kasutust arvuteoorias, rühmateoorias, matemaatilises statistikas ja mujal.

Defintsioon 4.20 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.

Defintsioon 4.21 Öeldakse, et korpuse K **karakteristika on 2**, kui selles korpuses $\mathbf{1} + \mathbf{1} = \mathbf{0}$ (ühiklemendi liitmisel iseendale saame nullelementi).

Sümboliga **2** tähistame korpuse elementi $\mathbf{1} + \mathbf{1}$. Paneme tähele, et iga $k \in K$ korral

$$k + k = \mathbf{1} \cdot k + \mathbf{1} \cdot k = (\mathbf{1} + \mathbf{1})k = \mathbf{2}k.$$

Kui korpuse karakteristika ei ole 2, siis tema element **2** on pööratav ja saame rääkida elemendiga **2** jagamisest. Nimelt loeme,

$$\frac{k}{\mathbf{2}} = k \cdot \mathbf{2}^{-1},$$

kus $k \in K$.

Lause 4.22 *Kui F on ruutfunktsionaal vektorruumil üle korpuse K , mille karakteristika ei ole 2, siis sümmeetriline bilineaarne funktsionaal f , mis määrab ära F , on üheselt määratud.*

TÖESTUS. Olgu $F(x) = f(x, x)$ iga $x \in V$ korral, kus f on sümmeetriline bilineaarne funktsionaal. Siis mistahes $x, y \in V$ korral

$$\begin{aligned} F(x + y) &= f(x + y, x + y) = f(x, x) + f(x, y) + f(y, x) + f(y, y) \\ &= f(x, x) + f(x, y) + f(x, y) + f(y, y) = F(x) + \mathbf{2}f(x, y) + F(y), \end{aligned}$$

millest

$$f(x, y) = \frac{F(x + y) - F(x) - F(y)}{\mathbf{2}}.$$

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 päätüki jooksul, et korpuse K karakteristika ei ole 2. Seda tingimust rahuldavad näiteks korpused $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ja \mathbb{Z}_p , kus $p \neq 2$.

Defintsioon 4.23 **Ruutfunktsionaali maatriksiks** mingi baasi suhtes nimetatakse teda määrama sümmeetrilise bilineaarse funktsionaali maatriksit selle baasi suhtes.

Lause 4.24 *Olgu F ruutfunktsionaal n -mõõtmelisel vektorruumil V , mille maatriks baasi e suhtes on $A = (a_{ij})$ ning olgu vektori $x \in V$ koordinaadid baasi e suhtes x_1, \dots, x_n . Siis*

$$F(x) = \sum_{i,j=1}^n a_{ij}x_i x_j.$$

TÖESTUS. Kui ruutfunktsionaal F on määratud sümmeetrilise bilineaarse funktsionaali f poolt, siis

$$F(x) = f(x, x) = f\left(\sum_{i,j=1}^n x_i e_i, \sum_{i,j=1}^n x_j e_j\right) = \sum_{i,j=1}^n x_i x_j f(e_i, e_j) = \sum_{i,j=1}^n a_{ij} x_i x_j.$$

□

Definitsioon 4.25 Olgu F sümmeetrilise bilineaarse funktsionaali f poolt määratud ruutfunktsionaal. Siis n muutuja polünoomi

$$\sum_{i,j=1}^n a_{ij} X_i X_j,$$

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 korpuuse 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 vordne $X_j X_i$ kordajaga iga $i, j, i \neq j$ korral.

Näide 4.26 Ruutvormide esitamisel 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 korpuuse \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 vordust (22) võime selle ruutfunktsionaali esitada maatrikskujul järgmiselt:

$$F(x) = \bar{x}_e^t A \bar{x}_e.$$

Lause 4.27 Olgu V n -mõõtmeline vektorruum üle korpuuse K . Vektorruumi V baasi fikseerimine tekib üksühes vastavused sellel vektorruumil defineeritud ruutfunktsionaalide, n muutuja ruutvormide (üle K) ja n -ndat järku sümmeetriliste ruutmaatriksite (üle K) vahel.

TÖESTUS. 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 ruutmaatriksite vahel. Tähistame sümboliga $RF(V)$ 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 vordusega

$$f_A(x, y) := \bar{x}_e^t A \bar{y}_e.$$

Kuna $\bar{y}_e^t A \bar{x}_e$ on (1×1) -maatriks, siis ta transponeerimisel ei muudu, 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

$$\begin{aligned} f_A(x+z, y) &= \overline{x+z}_e^t A \bar{y}_e = (\bar{x}_e^t + \bar{z}_e^t) A \bar{y}_e = \bar{x}_e^t A \bar{y}_e + \bar{z}_e^t A \bar{y}_e = f_A(x, y) + f_A(z, y), \\ f_A(kx, y) &= \overline{kx}_e^t A \bar{y}_e = k \bar{x}_e^t A \bar{y}_e = kf_A(x, y) \end{aligned}$$

mistahes $x, y, z \in V$ ja $k \in K$ korral. Järelkult f_A on sümmeetrisiline 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 $f_A(e_i, e_j) = (\bar{e}_i)_e^t A (\bar{e}_j)_e = a_{ij}$. \square

Tänu ruutfunktsionaali maatriksi definitsioonile ja lausele 4.18 võime öelda, et kehtib järgmine tulemus.

Lause 4.28 Üleminekul ühelt baasilt teisele korrutub ruutfunktsionaali maatriks paremalt üleminekumaatriksiga ja vasakult üleminekumaatriksi transponeeritud maatriksiga.

Kui ruutfunktsionaali maatriks baasi e suhtes on A ja baasi e' suhtes on A' ning T on üleminekumaatriks baasilt e baasile e' , siis

$$A' = T^t A T.$$

Definitsioon 4.29 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 4.30 Ruutvorm

$$3X_1^2 - 5X_2^2 + 2X_4^2$$

üle \mathbb{R} on kanoonilisel kujul.

Definitsioon 4.31 Baasi, mille suhtes ruutfunktsionaalile vastab kanoonilisel kujul olev ruutvorm, nimetatakse selle ruutfunktsionaali **kanooniliseks baasiks**.

Teoreem 4.32 Igal ruutfunktsionaalil on olemas kanooniline baas.

TÖESTUS. 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 4.28 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 teisen-dust maatriksi ridadega teeme samasuguse teisenduse veergudega. Näiteks pärast i -nda ja j -nda rea ärvahetamist vahetame kohe ära ka i -nda ja j -nda veeru. Teatavasti elementaarteisenduse ri-dadega võib sooritada vastava elementaarmaatriksiga antud maatriksit vasakult korrutades ([1],

lause 4.7.6). Et sooritada samasugune elementaarteisendus veergudega, tuleb maatriks korruada sellesama elementaarmaatriksi transponeeritud 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 töesti 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 $a_{11}^{-1} a_{11}$, 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 päädiagonaali 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 sümmeetiline ja korpuse karakteristika ei ole 2). Edasi saame toimida kasutades eelnevat mõttekäiku.

Kui esimeses reas ja veerus on kõik elemendid (välja arvatud esimene) nullid, siis kordame protseduuri alammaatriksis, mis koosneb ridadest ja veergudest numbritega $2, \dots, n$. \square

Meenutame, et **eukleidiliseks ruumiks** nimetatakse vektorruumi üle korpuse \mathbb{R} koos mingi skalaarkorрутamisega sellel vektorruumil ([1], def. 9.1.1).

Teoreem 4.33 *Igal eukleidilise ruumi ruutfunktsionaalil on olemas ortonormeeritud kanooniline baas.*

TÖESTUS. Olgu E eukleidiline ruum, olgu e suvaline ortonormeeritud baas ruumis E ja olgu F ruutfunktsionaal ruumil E . Siis maatriks $A := A_F^e$ on sümmeetiline. 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 sümmeetiline 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 üleminnekumaatriks baasilt e baasile e' . Siis T on ortogonaalmaatriks ([1], lause 9.2.4), s.t. $T^t = T^{-1}$, ja $A_\varphi^{e'} = T^{-1} A_F^e T$ ([1], lause 8.2.5). Seega

$$A_\varphi^{e'} = T^{-1} A_F^e T = T^{-1} A T = T^t A_F^e T = A_F^{e'},$$

kus viimane võrdus tuleb lausest 4.28. 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 .

Defintsioon 4.34 Kahte n muutuja ruutvormi nimetatakse **ekvivalentseteks**, kui nad vastavad samale ruutfunktsionaalile mingite baaside suhtes.

On selge, et ruutvormide ekvivalentsuse seos on tõepoolust refleksiivne, sümmeetrisiline ja transitiivne.

Teoreemi 4.32 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**.

Olgu ruutvorm üle \mathbb{C} viidud kanoonilisele kujule $a_{11}X_1^2 + \dots + a_{rr}X_r^2$, kus kõik kordajad on nullist erinevad. Olgu $\sqrt{a_{ii}}$ mingi ruutjuur kompleksarvust a_{ii} , $i = 1, \dots, r$. Korrutades kanoonilisele kujule vastava maatriksi i -ndat rida ja i -ndat veergu ($i = 1, \dots, r$) arvuga $\frac{1}{\sqrt{a_{ii}}}$ saame ruutvormi viia kanoonilisele kujule $X_1^2 + \dots + X_r^2$. Seda kuju nimetatakse üle korpuse \mathbb{C} vaadeldava ruutvormi **normaalkujuks**. Erinevalt kanoonilisest kujust on normaalkuju üheselt määratud.

Teoreem 4.35 *Kaks ruutvormi üle \mathbb{C} on ekvivalentsed parajasti siis, kui nende maatriksite astakud on võrdsed.*

TÖESTUS. Kuna korrutamisel regulaarse maatriksiga maatriksi astak ei muudu, siis tänu lausele 4.28 on ekvivalentsete ruutvormide maatriksite astakud võrdsed.

Kui aga kahe maatriksi (üle \mathbb{C}) astakud on võrdsed, siis neile vastavate ruutvormide normaalkujud on võrdsed. Kuna kumbki neist ruutvormidest on ekvivalentne selle normaalkujuga, siis on ka esialgsed ruutvormid ekvivalentsed. \square

Vaatleme nüüd reaalarvuliste kordajatega ruutvorme. Me saame sellise ruutvormi viia kanoonilisele kujule, mis tähendab, et tema maatriks on diagonaalmaatriks. Siis tehes ridade ja veergude vahetamise teisendusi saame maatriksit teisendada nii, et päädiagonaalil 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 töestas Sylvester⁵ aastal 1852.

Teoreem 4.36 (Ruutvormide inertsiseadus) *Reaalarvuliste kordajatega ruutvormi positiivsete (negatiivsete) kordajate arv tema kanoonilises kujus ei sõltu kanoonilisest baasist.*

TÖESTUS. 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

$$a_{11}X_1^2 + \dots + a_{nn}X_n^2 \text{ ja } b_{11}X_1^2 + \dots + b_{nn}X_n^2,$$

kus a_{11}, \dots, a_{rr} on esimese ruutvormi positiivsed kordajad ja b_{11}, \dots, b_{ss} on teise ruutvormi positiivsed kordajad. Oletame vastuväiteliselt, et $r > s$. (Kui $r < s$, siis on töestus 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 1.83 põhjal summa $V_1 + V_2$ ei ole otsesumma ja teoreemi 1.76 tõttu $V_1 \cap V_2 \neq \{0\}$. Seega leidub nullist erinev vektor $x \in V_1 \cap V_2$. Olgu

$$x = k_1e_1 + \dots + k_re_r = l_{s+1}e'_{s+1} + \dots + l_ne'_n,$$

kus $k_1, \dots, k_r, l_{s+1}, \dots, l_n \in \mathbb{R}$. Siis

$$F(x) = a_{11}k_1^2 + \dots + a_{rr}k_r^2 > 0,$$

⁵James Joseph Sylvester (1814–1897) — inglise matemaatik

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 4.37 *Kaks ruutvormi üle \mathbb{R} on ekvivalentsed parajasti siis, kui nende kanoonilises kujus on ühepalju positiivseid kordajaid ja ühepalju negatiivseid kordajaid.*

TÕESTUS. Tarvilikkus järeltub Teoreemist 4.36.

Piisavuse töestamiseks 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 ($i = 1, \dots, s$) arvuga $\frac{1}{\sqrt{a_{ii}}}$ saame ruutvormi viia kanoonilisele kujule

$$X_1^2 + \dots + X_r^2 - X_{r+1}^2 - \dots - X_s^2.$$

Seda kuju nimetatakse üle korpu \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 4.38 Ruutfunktionsionaali 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 ruutfunktionsional on positiivselt (negatiivselt) määratud.

Lihtne on aru saada, et kehtib järgmine tulemus.

Lause 4.39 *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.*

Järgnevalt tahame näidata, et positiivselt määratuse kontrollimiseks piisab n miinori arvutamisest.

Definitsioon 4.40 n -ndat järku ruutmaatriksi $A = (a_{ij})$ **päämiinoriteks** 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, päämiinorid asuvad maatriksi A ülemises vasakpoolses nurgas.

Teoreem 4.41 Ruutfunktsionaal vektorruumil üle \mathbb{R} on positiivselt määratud parajasti siis, kui tema maatriksi kõik päämiinorid on positiivsed.

TÖESTUS. TARVILIKKUS. Olgu F positiivselt määratud ruutfunktsionaal n -mõõtmelisel vektorruumil V üle \mathbb{R} , mille maatriks baasi $e = \{e_1, \dots, e_n\}$ suhtes on

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

Kuna F on positiivselt määratud, siis $a_{ii} = F(e_i) > 0$ iga $i \in \{1, \dots, n\}$ korral. Asume maatriksit A teisendama teoreemis 4.32 kirjeldatud meetodil. Kuna $a_{11} > 0$, siis saame esimese rea ja veeru ülejäänud elemendid muuta nullideks liites vastavale reale (veerule) sobiva elemendiga korrutatud esimese rea (veeru). Nii tehes 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 suhtes. Seega $b_{22} > 0$ 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 päämiinoreid. Seega

$$M_k = d_{11}d_{22} \dots d_{kk},$$

$k \in \{1, \dots, n\}$, mis kõik on positiivsed.

PIISAVUS. Olgu F positiivselt määratud ruutfunktsionaal n -mõõtmelisel vektorruumil V üle \mathbb{R} , mille maatriks baasi $e = \{e_1, \dots, e_n\}$ suhtes on

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

Eeldame, et maatriksi A kõik päämiinorid M_k , $k \in \{1, \dots, n\}$ on kõik positiivsed. Hakkame maatriksit A teisendama samamoodi nagu tarvilikkuse töestuses. Selle käigus jällegi päämiinorid ei muudu.

Kasutades seda, et $a_{11} = M_1 > 0$, saame esimese rea ja veeru ülejäänud elemendid muuta nullideks. Seega saame maatriksi

$$\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & b_{22} & b_{23} & \dots & b_{2n} \\ 0 & b_{32} & b_{33} & \dots & b_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & b_{n2} & b_{n3} & \dots & b_{nn} \end{pmatrix}.$$

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 maatriksi

$$\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & a_{22} & 0 & \dots & 0 \\ 0 & 0 & c_{33} & \dots & c_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & c_{n3} & \dots & c_{nn} \end{pmatrix}.$$

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 ruutfunktionsaali F maatriks mingi baasi suhtes. Siit on näha, et F on positiivselt määratud. \square

5 Abeli rühmad

Selles päätükis käitleme Abeli rühmi (kommutatiivseid rühmi). Need on oma nime saanud Niels Henrik Abeli⁶ järgi. Põhitähelepanu on perioodilistel ja lõplikel Abeli rühmadel. Üheks olulisemaks Abeli rühmade näiteks on tsüklilised rühmad, mille vaatlemisest alustamegi.

5.1 Tsüklilised rühmad

Olgu (G, \cdot) rühm, $k \in \mathbb{N}$ ja $g \in G$. Tähistame

$$g^k := \underbrace{g \cdot \dots \cdot g}_k \text{ tegurit}, \quad g^{-k} := (g^{-1})^k = \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_k \text{ tegurit}, \quad g^0 := 1.$$

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 poole **tekitatud** (või **moodustatud**) **alamrühmaks**.

Defintsioon 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 $0 \leq r < b$.

Lause 5.4 Mistahes $a, b \in \mathbb{Z}$ korral $SÜT(a, b) = 1$ 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 tsüklilise rühm on isomorfne rühmaga $(\mathbb{Z}, +)$ ja iga n -elemendiline tsüklilise rühm on isomorfne rühmaga $(\mathbb{Z}_n, +)$.

TÖESTUS. 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,

$$G = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}. \tag{23}$$

⁶Niels Henrik Abel (1802–1829) — norra matemaatik

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

$$G = \{1, g, g^2, \dots, g^{n-1}\}. \quad (24)$$

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 (24).

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 $|G| = n$.

Niisiis iga tsükliline rühm G on esitatav kas kujul (23) või kujul (24) mingi $n \in \mathbb{N}$ jaoks.

Näitame, et juhul (23) on $(G, \cdot) \simeq (\mathbb{Z}, +)$. Selleks defineerime kujutuse $\varphi : G \rightarrow \mathbb{Z}$ võrdusega

$$\varphi(g^k) := k.$$

Ei ole raske näha, et φ on isomorfism.

Juhul (24) on $(G, \cdot) \simeq (\mathbb{Z}_n, +)$, kusjuures isomorfismiks $\varphi : G \rightarrow \mathbb{Z}_n$ sobib kujutus

$$\varphi(g^k) := \bar{k}.$$

□

Järeldus 5.6 Iga tsükliline rühm on Abeli rühm.

5.2 Rühma elemendi jäärk

Definitsioon 5.7 Olgu g rühma (G, \cdot) element. Kui $|\langle g \rangle| = n \in \mathbb{N}$, siis öeldakse, et elemendi g **jäärk 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 jäärku element**.

Definitsioonist tuleb välja, et igas rühmas on täpselt üks esimest jäärku 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 $\text{ord}_G((0, 5)) = \infty$.

2. Substitutsionirühmas S_3 on tsükli $(1, 3, 2)$ järguks 3.

Lagrange'i teoreemist järeltub vahetult järgmine väide.

Lause 5.9 Lõpliku rühma iga elemendi jäärk jagab rühma jäärku.

Teoreemi 5.5 tõestuse põhjal võime öelda, et kehtib järgmine tulemus.

Lause 5.10 Kui rühma (G, \cdot) elemendi g jäärk 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 jäärk on lõplik ja jagab arvu k .

TÖESTUS. Kuna $g^k = 1$, siis g on kindlasti lõplikku järu element, olgu $\text{ord}(g) = n$. Jagades arvu k jäädiga 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 järu 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 moodustaja parajasti siis, kui $SÜT(k, n) = 1$.

TÖESTUS. 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 $ku - 1 = nq$ ehk $ku - nq = 1$ mingi $q \in \mathbb{Z}$ korral. Lause 5.4 põhjal $SÜT(k, n) = 1$.

PIISAVUS. Olgu $SÜT(k, n) = 1$. Siis lause 5.4 põhjal leiduvad sellised $u, v \in \mathbb{Z}$, et $ku + nv = 1$. Järelikult

$$g = g^{ku+nv} = g^{ku} \cdot g^{nv} = g^{ku} = (g^k)^u$$

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 $\text{ord}(g^m) = n$.

TÖESTUS. Töestamiseks 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

Töestatud 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 mittetrviaalne lõplik rühm. Rühmal G ei ole mittetrviaalseid pärisalamrühmi parajasti siis kui G on algarvulise järguga tsükliline rühm.

TÖESTUS. TARVILIKKUS. Eeldame, et rühmal $G \neq \{1\}$ ei ole mittetrviaalseid 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 mittetrviaalne pärisalamrühm rühmas G , vastuolu. Järelikult $|G|$ on 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 $SÜT(p, k) = 1$, siis lause 5.12 põhjal

$$G = \langle g^k \rangle \subseteq H \subseteq G,$$

kust $H = G$. Seega rühmal G puuduvad mittetrviaalsed pärisalamrühmad. \square

5.3 Perioodilised Abeli rühmad

Definitsioon 5.17 Rühma nimetatakse **perioodiliseks**, kui tema kõik elemendid on lõplikku järgu.

Iga lõplik rühm on perioodiline, kuid on 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 järgu.

Lemma 5.19 Olgu $(A, +)$ Abeli rühm ja p algarv. Siis hulk

$$A_p = \{a \in A \mid \text{ord}(a) = p^k, k \in \mathbb{N} \cup \{0\}\}$$

on rühma A alamrühm.

TÖESTUS. 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 Hulka A_p nimetatakse Abeli rühma $(A, +)$ **p -komponendiks**.

Näide 5.21 Abeli rühma $(\mathbb{Z}_{24}, +)$ 3-komponent on alamrühm $\{\bar{8}, \bar{16}, \bar{0}\}$.

Tähistame sümboliga \mathbb{P} kõigi algarvude hulka.

Teoreem 5.22 Perioodiline Abeli rühm on oma p -komponentide otsesumma.

TÖESTUS. Näitame, et

$$A = \sum_{p \in \mathbb{P}} A_p.$$

Selleks töestame, 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 $p_i^{k_i}(u_i n_i a) = (p_i^{k_i} u_i n_i) a = (u_i n) a = u_i (n a) = 0$, siis 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 1.79 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 $\text{ord}(a_{p_i}) = p_i^{k_i}$. Olgu $n = p_1^{k_1} \dots p_s^{k_s}$. Siis $na = n a_{p_1} + \dots + n a_{p_s} = 0$, millest järeltub, et $q^k = \text{ord}(a) \mid n$. Aritmeetika põhiteoreemi tõttu on see võimalik vaid siis, kui $k = 0$. Järelikult $\text{ord}(a) = q^0 = 1$ ehk $a = 0$. Sellega oleme näidanud, et $A_q \cap \sum_{p \in \mathbb{P} \setminus \{q\}} A_p = \{0\}$. Järelikult 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.

Lõpliku Abeli rühma p -komponendid on 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 paragraahi põhieesmärk.

Alustuseks tõestame ühe kasuliku teoreemi.

Teoreem 5.24 (Cauchy) *Olgu $(A, +)$ lõplik Abeli rühm ja olgu $p \mid |A|$ algarv. Siis rühmas A leidub element, mille järk on p .*

TÖESTUS. Tõestame väite induktsiooniga rühma A järgu 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 järu 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. Oletame, et rühmal A ei ole mittetrviaalseid pärisalamrühmi. Siis lause 5.16 põhjal on A tsükliline rühm järguga p , seega sisaldab p -ndat järu elementi.

Vaatleme nüüd juhtumit, kus A sisaldab mittetrviaalset pärisalamrühma B . Lagrange'i teoreemi (teoreem 1.43) põhjal

$$|A| = |A/B| \cdot |B|,$$

kusjuures $|B| < |A|$ ja $|A/B| < |A|$. 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 järu elementi ning selle elemendi järk on p ka rühmas A .

2) $p \mid |A/B|$. Sel juhul faktorrühm A/B rahuldab ka induktsiooni eeldust ja peab sisaldama mingit p -ndat järu 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 $p \mid n$, s.t. $pk = n$ mingi $k \in \mathbb{N}$ korral. Kuna $\text{ord}(a) = pk$, siis järeldusest 5.15 saame, et $\text{ord}_A(ka) = p$. \square

Järeldus 5.25 *Lõplik Abeli rühm on p -rühm parajasti siis, kui tema järk on p aste.*

TÖESTUS. TARVILIKKUS. Olgu A lõplik Abeli p -rühm. Oletame vastuväiteliselt, et $|A|$ ei ole p aste, siis ta jagub mingi teise algarvuga q . Teoreemi 5.24 põhjal leidub rühmas A q -ndat järu 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 5.26 *Lõplik Abeli p -rühm on oma mingite tsükliliste alamrühmade otsesumma.*

TÖESTUS. Järelduse 5.25 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 5.24 põhjal sisaldab ta p -ndat järu elementi, seega on ta tsükliline rühm ja meil on triviale 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 jäirk 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

$$pA = \langle pa_1 \rangle + \dots + \langle pa_r \rangle. \quad (25)$$

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 1.76 tingimust 3. Oletame, et

$$k_1a_1 + \dots + k_ra_r = 0, \quad (26)$$

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. $k_i = pm_i$, $m_i \in \mathbb{Z}$. Siis

$$m_1(pa_1) + \dots + m_r(pa_r) = 0,$$

kust võrduse (25) 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 (26) saame, et

$$k_1(pa_1) + \dots + k_r(pa_r) = 0,$$

kust võrduse (25) tõttu järeltäpsustatakse, et $pk_j a_i = 0$ 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 $e \leq 1$. Järeltäpsustatakse $pa_j = 0$, vastuolu.

Kuna võrdusest (26) järeltäpsustatakse, 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 järuku 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

$$pa = k_1(pa_1) + \dots + k_r(pa_r).$$

Järeltäpsustatakse $p(a - k_1a_1 - \dots - k_ra_r) = 0$ 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 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

$$B_1 = B + \langle c_1 \rangle$$

ja $B < B_1 \leq A$. Kui nüüd $B_1 = A$, siis on vajalik esitus A jaoks olemas. Vastasel korral kordame mõttækäiku valides mingi $c_2 \in C \setminus B_1$. Sarnaselt eelnevaga saame otsesumma

$$B_2 = B_1 + \langle c_2 \rangle = B + \langle c_1 \rangle + \langle c_2 \rangle.$$

Kuna A on lõplik, siis pärast lõplikku arvu samme jõuame lahutuseni

$$A = B_s = B + \langle c_1 \rangle + \dots + \langle c_s \rangle = \langle a_1 \rangle + \dots + \langle a_r \rangle + \langle c_1 \rangle + \dots + \langle c_s \rangle.$$

□

Teoreemidest 5.22 ja 5.26 saame nüüd järgmise tulemuse.

Teoreem 5.27 *Lõplik Abeli rühm on oma mingite tsükliliste alamrühmade otsesumma.*

Lõplike Abeli rühmade kirjelduse andis 1870. aastal Kronecker⁷.

Näide 5.28 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 $A = A_2 + A_3$. Teoreemi 1.80 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 otsekorrutisega, siis võime öelda, et

$$A \simeq A_2 \times A_3 \simeq \mathbb{Z}_4 \times \mathbb{Z}_3.$$

⁷Leopold Kronecker (1823–1891) — preisi matemaatik

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/Arvuteoria_k2019/kon_2019.pdf .