Sissejuhatus algebra struktuuridesse

Sügis 2021

Lektor: Valdis Laan
Konspekt: Valdis Laan, Lauri Tart

6. jaanuar 2022. a.

Sisukord

Eessõna

Ülikoolis õpetatava algebra võib suures plaanis jagada kaheks: lineaaralgebra ja abstraktne algebra. Esimene neist on väga paljude teiste ainete "alustalaks": funktsionaalanalüüs, algebraline arvuteooria, diferentsiaal- ja integraalvõrrandite lahendamine, matemaatiline statistika, arvutigraafika jpt. Käesolevas kursuses käsitletakse abstraktset ehk üldalgebrat, mis uurib niinimetatud algebralisi struktuure. Erinevate konkreetsete struktuuride uurimine hõlmab endas tervet rida omaette matemaatilisi uurimisvaldkondi (rühmateooria, ringiteooria, poolrühmateooria, universaalalgebra jt.) ja on samas aluseks teistele nii teoreetilistele kui praktilistele uurimisvaldkondadele. Kursuse peamine eesmärk on tutvustada erinevaid algebra osasid sedavõrd, et edaspidi vastavat teooriat või selle rakendusi kohates oleks võimalik neis vähemalt minimaalselt orienteeruda. Lisaks sellele soovime igas peatükis anda ka vähemalt ühe mittetriviaalse (ja enamasti klassikalise) teoreemi tõestuse.

Kursuse jooksul eeldame, et üliõpilane on tuttav põhiliste mõistete ja tulemustega hulgateooriast (tehted hulkadega, kujutused, ekvivalentsiseosed), lineaaralgebrast (maatriksid, vektorruumid ja lineaarteisendused) ja abstraktsest algebrast (rühmad, ringid, polünoomid).

Loengukonspekt tugineb peamiselt raamatutele [2] ja [1]. Lause 4.16 tõestus on pärit Hendrik Vijalt. Soovin tänada ka Simmo Saani, kes leidis konspektist mitmeid vigu.

Peatükk 1

Vektorruum

Algebraline struktuur on hulk, millel on defineeritud mingid tehted, mis rahuldavad teatud tingimusi. Algebraliste struktuuridega käivad kaasas sellised mõisted nagu alamstruktuur, homomorfism, isomorfism, faktorstruktuur. Selles päätükis vaatleme esialgu kõiki neid mõisteid üldisest vaatepunktist ja siis uurime, mida need tähendavad konkreetsel juhul vektoruumide jaoks. Loodetavasti on lugeja vektorruumi mõistega kokku puutunud mõnes varasemas kursuses.

1.1 Algebraline tehe

Definitsioon 1.1 Olgu n mittenegatiivne täisarv. **n-kohaline** (ehk **n-aarne**) **algebraline tehe** hulgal A on kujutus hulgast A^n hulka A.

Märkus 1.2 Sõna "algebraline" selles definitsioonis rõhutab seda, et tehte tulemus kuulub ka hulka A. Põhimõtteliselt võib vaadelda ka tehteid $A^n \to B$, kus $B \neq A$. Näiteks kolmemõõtmelise ruumi vabavektorite liitmine on kahekohaline algebraline tehe $\mathbb{E}_3 \times \mathbb{E}_3 \to \mathbb{E}_3$, aga skalaarkorrutamine on tehe $\mathbb{E}_3 \times \mathbb{E}_3 \to \mathbb{R}$, mis ei ole algebraline.

Niisiis n-kohaline tehe hulgal A seab A elementide järjestatud jadale $(a_1, \ldots, a_n)$ vastavusse hulga A elemendi.

Kõige levinumad on kahekohalised algebralised tehted. Kahekohalisest tehtest rääkides kirjutatakse tehtemärk harilikult hulga elementide vahele. Seega kahekohalise tehte $* : A \times A \to A$ korral kirjutatakse $*((a, b))$ asemel harilikult $a * b$ ja võib öelda, et tehe $*$ seab paarile (a, b) vastavusse hulga A elemendi $a * b$. Ühekohalised algebralised tehted on kujutused $A \to A$. Nullkohalised algebralised tehted on kujutused $A^0 \to A$. Kuna A^0 on hulk, milles on üks element, siis kujutuse $A^0 \to A$ defineerimine tähendab sisuliselt ühe konkreetse elemendi väljavalimist (fikseerimist) hulgast A. Kui $\omega : A^0 \to A$ on nullkohaline tehe, siis selle tehte poolt väljavalitud hulga A elementi tähistame sümboliga 0_ω või 0_ω^A (kui tahame rõhutada, et see element kuulub hulka A).

Selleks, et rääkida algebralistest struktuuridest üldiselt, on kasulik teha vahet tehetel kui konkreetsetel kujutustel $A^n \to A$ ja tehtemärkidel kui sümbolitel. Selleks kasutatakse tüübi mõistet. Tüüpi mõistame kui tehtemärkide hulka.

Definitsioon 1.3 Hulka Ω koos tükeldusega

$$\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$$

alamhulkade Ω_n (mis võivad olla ka tühjad) lõikumatuks ühendiks nimetame **tüübiks** ehk **signatuuriks**. Iga $\omega \in \Omega_n$ korral loeme, et tehtemärgi ω aarsus on n.

Definitsioon 1.4 Olgu Ω tüüp ja A hulk. Kui iga arvu $n \in \mathbb{N} \cup \{0\}$ korral vastab igale tehtemärgile $\omega \in \Omega_n$ üks konkreetne n-kohaline algebraline tehe $\omega^A : A^n \to A$, siis ütleme, et paar $(A, \{\omega^A \mid \omega \in \Omega\})$ on **Ω-algebra**.

Näide 1.5 Olgu meil fikseeritud signatuur $\Omega = \Omega_2 = \{+, \cdot\}$ koos kahe kahekohalise tehtemärgiga (siin $\Omega_n = \emptyset$ iga $n \in \mathbb{N} \cup \{0\}$, $n \neq 2$ korral). Siis võime hulka $\mathbb{Z}$ vaadelda Ω-algebrana täisarvude hariliku liitmise ja korrutamise suhtes. Aga võime ka näiteks hulka $\mathbb{N}$ vaadelda Ω-algebrana, kus tehtemärgile $+$ vastab maksimumi võtmise tehe max ja tehtemärgile $\cdot$ vastab miinimumi võtmise tehe min.

Algebras huvitavad meid harilikult mitte suvalised theted vaid sellised, millel on mingeid häid omadusi (assotsiatiivsus, kommutatiivsus, distributiivsus jne.). **Algebralise struktuuri** all peetakse harilikult silmas Ω-algebrat, mille tehted rahuldavad teatud tingimusi (mõnikord kutsutakse neid aksioomideks).

Üheks oluliseks algebraliseks struktuuriks, millega lugeja on kindlasti juba kokku puutunud, on vektorruumid. Tuletame meelde, kuidas harilikult defineeritakse vektorruum üle korpuse K. (Selles kursuses eeldame, et korpuse korrutamine on kommutatiivne.)

Definitsioon 1.6 Hulka V nimetatakse **vektorruumiks** ehk **lineaarseks ruumiks** üle korpuse K, kui on defineeritud kujutused

$$V \times V \to V, \quad (a, b) \mapsto a + b,$$
$$K \times V \to V, \quad (k, a) \mapsto ka$$

nii, et

VR1. $(a + b) + c = a + (b + c)$ iga $a, b, c \in V$ korral;

VR2. leidub element $0 \in V$ nii, et iga $a \in V$ korral $a + 0 = a = 0 + a$;

VR3. iga elemendi $a \in V$ korral leidub element $-a \in V$ nii, et $a + (-a) = 0 = (-a) + a$;

VR4. $a + b = b + a$ iga $a, b \in V$ korral;

VR5. $k(a + b) = ka + kb$ iga $a, b \in V$ ja $k \in K$ korral;

VR6. $(k + l)a = ka + la$ iga $a \in V$ ja $k, l \in K$ korral;

VR7. $(kl)a = k(la)$ iga $a \in V$ ja $k, l \in K$ korral;

VR8. $1a = a$ iga $a \in V$ korral.

Vektorruumi V elemente on tavaks nimetada **vektoriteks** ja korpuse K elemente **skalaarideks**. Elementi $a+b \in V$ nimetatakse vektorite a ja b **summaks** ning elementi $ka \in V$ skalaari k ja vektori a **korrutiseks**. Elementi $0 \in V$ tingimuses VR2 nimetatakse **nullvektoriks** ja elementi $-a \in V$ tingimuses VR3 nimetatakse vektori a **vastandvektoriks**.

On selge, et vektorruumis on olemas üks kahekohaline algebraline tehe — liitmine. Aga varjatumalt on selles struktuuris veel rida teisi tehteid. Niisiis vektorruumi tehted on järgmised:

- kahekohaline tehe liitmine, $(a,b) \mapsto a+b$,
- nullkohaline tehe, mis fikseerib vektorruumi nullelemendi,
- ühekohaline tehe vastandelemendi võtmine, $a \mapsto -a$,
- iga skalaari $k \in K$ jaoks on olemas ühekohaline tehe $a \mapsto ka$ (selle skalaariga korrutamine).

Seega võime vektorruumi vaadelda Ω-algebrana, kus

$$\begin{aligned}
&\Omega_0 = \{0\},\\
&\Omega_1 = \{-()\} \cup \{k\cdot \mid k \in K\},\\
&\Omega_2 = \{+\},\\
&\Omega_n = \emptyset \quad \text{iga } n \geqslant 3 \text{ korral.}
\end{aligned}$$

Nagu näha, mingil algebralisel struktuuril võib põhimõtteliselt olla lõpmata palju tehteid. Nii on see näiteks vektorruumi korral üle lõpmatu korpuse.

Lisaks definitsioonis sisalduvatele tehetele (neid kutsutakse algebralise struktuuri põhiteheteks) võib algebralisel struktuuril defineerida veel uusi tehteid (nn. tuletatud tehteid). Näiteks vektorruumi puhul on kasulik lisaks põhitehetele vaadelda veel kahekohalist lahutamistehet, mis defineeritakse põhitehete abil järgmiselt:

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

Definitsiooni kasutades on lihtne näidata, et vektorruumis kehtib veel terve rida omadusi, mis aitavad arvutusi hõlbustada. Selles kursuses loeme, et $\mathbb{N} = \{1,2,3,\ldots\}$.

Lause 1.7 *Olgu V vektorruum üle korpuse K.*

1. $k(a_1 + \ldots + a_n) = ka_1 + \ldots + ka_n$ *iga* $n \in \mathbb{N}$, $k \in K$ *ja* $a_1, \ldots, a_n \in V$ *korral.*
2. $(k_1 + \ldots + k_n)a = k_1a + \ldots + k_na$ *iga* $n \in \mathbb{N}$, $k_1, \ldots, k_n \in K$ *ja* $a \in V$ *korral.*
3. *Iga* $a, b, c \in V$ *korral, kui* $a + b = c$, *siis* $a = c - b$.
4. $0a = 0$ *iga* $a \in V$ *korral. (Selle võrduse vasakul poolel olev* 0 *tähistab korpuse* K *nullelementi ja paremal poolel olev* 0 *vektorruumi* V *nullelementi.)*
5. $k0 = 0$ *iga* $k \in K$ *korral. (Selles võrduses on mõlemad* 0*-d* V *elemendid.)*

6. $(-1)a = -a$ *iga* $a \in V$ *korral. (Siin* -1 *on korpuse* K *ühikelemendi vastandelement.)*

7. $(-k)a = k(-a) = -(ka)$ *iga* $k \in K$ *ja* $a \in V$ *korral.*

8. $k(a-b) = ka - kb$ *iga* $k \in K$ *ja* $a, b \in V$ *korral.*

9. $(k-l)a = ka - la$ *iga* $k, l \in K$ *ja* $a \in V$ *korral.*

Märkus 1.8 Kuigi enamasti uuritakse algebras struktuure, mille aarsus on 0, 1 või 2, on olemas siiski ka loomulikke näiteid struktuuridest, millel leidub suurema aarsusega tehteid.

Vaatleme vektorruumil $\mathrm{Mat}_{m,n}(\mathbb{R})$ (üle korpuse $\mathbb{R}$) kolmekohalist algebralist tehet

$$\mathrm{Mat}_{m,n}(\mathbb{R}) \times \mathrm{Mat}_{m,n}(\mathbb{R}) \times \mathrm{Mat}_{m,n}(\mathbb{R}) \longrightarrow \mathrm{Mat}_{m,n}(\mathbb{R}), \quad (A, B, C) \mapsto AB^TC\,.$$

Selline algebraline struktuur on erijuhuks struktuuridest, mida kutsutakse *Hestenesi algebrateks*. Kolmekohalist algebralist tehet omavad ka Lie kolmiksüsteemid (*Lie triple system*), mida kasutatakse diferentsiaalgeomeetrias.

Hulgateooriast teame, et on võimalik vaadelda alamhulki, faktorhulki ja kujutusi hulkade vahel. Põhimõtteliselt võib hulgast mõelda kui algebralisest struktuurist, kus on defineeritud null algebralist tehet. Üldisemalt võib mistahes algebraliste struktuuride puhul rääkida alamstruktuuridest, faktorstruktuuridest ja homomorfismidest. Järgnevates paragrahvides uurimegi neid mõisteid.

1.2 Alamstruktuurid

Definitsioon 1.9 Ω-algebra A alamhulka A' nimetatakse **alamalgebraks**, kui A' on kinnine kõigi tehete $\omega^A, \omega \in \Omega$ suhtes. See tähendab, et

1. $\omega^A(a_1, a_2, \ldots, a_n) \in A'$ iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, a_2, \ldots, a_n \in A'$ korral,

2. $0^A_\omega \in A'$ iga $\omega \in \Omega_0$ korral.

Vektorruumide alamalgebraid kutsutakse **alamruumideks**.

Lause 1.10 *Vektorruumi* V *mittetühi alamhulk* V' *on alamruum parajasti siis, kui*

AR1 *iga* $a, b \in V'$ *korral* $a + b \in V'$ *(s.t.* V' *on kinnine liitmise suhtes);*

AR2 *iga* $a \in V'$ *ja* $k \in K$ *korral* $ka \in V'$ *(s.t.* V' *on kinnine skalaariga korrutamiste suhtes).*

Tõestus. Tarvilikkus. See on ilmne.
Piisavus. Eeldame, et kehtivad AR1 ja AR2. Vastavalt definitsioonile 1.9 peame veel näitama, et V' sisaldab vektorruumi V nullelementi ja on kinnine vastandelemendi võtmise suhtes.

Kuna V' on mittetühi, siis leidub mingi $a \in V'$. Tingimuse AR2 ja lause 1.7(4) tõttu $0 = 0a \in V'$. Kui $a \in V'$, siis lause 1.7 põhjal võib öelda, et $(-1)a = -a$. Kuna AR2 tõttu $(-1)a \in V'$, siis ka $-a \in V'$. Seega on V' kõigi tehete suhtes kinnine. □

Lause 1.11 *Vektorruumi V iga alamruum on ise ka vektorruum tehete suhtes, mis on defineeritud samamoodi nagu vektorruumi V tehted.*

TÕESTUS. Olgu V' vektorruumi V alamruum. Alamruumi definitsioon ütleb seda, et defineerides tehted hulgal V' samamoodi nagu nad on defineeritud hulgal V saame algebralised tehted hulgal V'. Kuna tingimused VR1–VR8 on täidetud kõigi V elementide jaoks, siis on nad rahuldatud ka V' elementide jaoks. Seega on V' vektorruum. □

1.3 Homomorfismid

Definitsioon 1.12 Olgu A ja B Ω-algebrad. Kujutust $f : A \to B$ nimetatakse **homomorfismiks**, kui f säilitab kõik nendel struktuuridel defineeritud tehted. See tähendab, et

1. $f(\omega^A(a_1, a_2, \ldots, a_n)) = \omega^B(f(a_1), f(a_2), \ldots, f(a_n))$ iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, a_2, \ldots, a_n \in A$ korral,
2. $f(0_\omega^A) = 0_\omega^B$ iga $\omega \in \Omega_0$ korral.

Kahekohalise tehte $*$ korral võtab tingimus 1 eelmises definitsioonis kuju

$$f(a_1 * a_2) = f(a_1) * f(a_2).$$

Ühekohalise tehte ω säilitamine tähendab seda, et

$$f(\omega^A(a)) = \omega^B(f(a))$$

iga $a \in A$ korral.

Definitsioon 1.13 Homomorfismi Ω-algebrast struktuurist A iseendasse nimetatakse Ω-algebra A **endomorfismiks**.

Kõigi homomorfismide hulka Ω-algebrast A Ω-algebrasse B tähistatakse sümboliga $\mathrm{Hom}(A, B)$. Ω-algebra A kõigi endomorfismide hulka tähistatakse sümboliga $\mathrm{End}(A)$.

Lause 1.14 *Olgu V ja U vektorruumid üle korpuse K. Kujutus $f : V \to U$ on vektorruumide homomorfism parajasti siis, kui*

LK1. *$f(a + b) = f(a) + f(b)$ iga $a, b \in V$ korral (s.t. f säilitab liitmist);*

LK2. *$f(ka) = kf(a)$ iga $a \in V$ ja $k \in K$ korral (s.t. f säilitab skalaaridega korrutamisi).*

TÕESTUS. TARVILIKKUS. See on ilmne.
PIISAVUS. Kehtigu LK1 ja LK2. Peame näitama, et f säilitab nullelemendi ja vastandelemendi võtmise.

Tingimuse LK1 põhjal $f(0) = f(0 + 0) = f(0) + f(0)$. Liites selle võrduse mõlemale poolele $-f(0)$ saame võrduse $0 = f(0)$.

Tingimuse LK2 tõttu $f(-a) = f((-1)a) = (-1)f(a) = -f(a)$ iga $a \in V$ korral. □

Definitsioon 1.15 Vektorruumide homomorfisme nimetatakse **lineaarkujutusteks** ja vektoruumide endomorfisme nimetatakse **lineaarteisendusteks**.

Meenutame nüüd hulgateooriast kujutise mõistet.

Definitsioon 1.16 Kui $f : A \to B$ on kujutus hulgast A hulka B, siis f **kujutiseks** nimetatakse hulka

$$\operatorname{Im} f = \{b \in B \mid (\exists a \in A)\ f(a) = b\} = \{f(a) \mid a \in A\} \subseteq B.$$

Lause 1.17 *Kui $f : A \to B$ on Ω-algebrate homomorfism, siis* $\operatorname{Im} f$ *on Ω-algebra B alamalgebra.*

TÕESTUS. Kontrollime alamstruktuuri definitsiooni tingimusi.
1. Olgu $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $b_1, \ldots, b_n \in \operatorname{Im} f$. Siis leiduvad elemendid $a_1, \ldots, a_n$ nii, et $f(a_i) = b_i$ iga $i \in \{1, \ldots, n\}$ korral. Kuna f on homomorfism, siis

$$\omega^B(b_1, \ldots, b_n) = \omega^B(f(a_1), \ldots, f(a_n)) = f(\omega^A(a_1, \ldots, a_n)),$$

kust näeme, et $\omega^B(b_1, \ldots, b_n) \in \operatorname{Im} f$.
2. Kui $\omega \in \Omega_0$, siis $0_\omega^B = f\left(0_\omega^A\right)$ ja seega $0_\omega^B \in \operatorname{Im} f$. □

Kui $f : A \to B$ ja $g : B \to C$ on kujutused, siis on võimalik vaadelda nende kujutuste korrutist $gf : A \to C$ (mõnikord kirjutatakse $g \circ f : A \to C$), mis defineeritakse nende kujutuste järjestrakendamise abil: kui $a \in A$, siis

$$(gf)(a) := g(f(a)).$$

Lause 1.18 *Ω-algebrate homomorfismide korrutis on Ω-algebrate homomorfism.*

TÕESTUS. Olgu A, B ja C Ω-algebrad ning olgu $f : A \to B$ ja $g : B \to C$ homomorfismid. Näitame, et $gf : A \to C$ on homomorfism.
1. Olgu $\omega \in \Omega_n$ $(n \in \mathbb{N})$ ja $a_1, \ldots, a_n \in A$. Siis

$$\begin{aligned}(gf)(\omega^A(a_1, \ldots, a_n)) &= g(f(\omega^A(a_1, \ldots, a_n))) = g(\omega^B(f(a_1), \ldots, f(a_n))) \\ &= \omega^C(g(f(a_1)), \ldots, g(f(a_n))) = \omega^C((gf)(a_1), \ldots, (gf)(a_n))\,.\end{aligned}$$

2. Kui $\omega \in \Omega_0$, siis

$$(gf)(0_\omega^A) = g(f(0_\omega^A)) = g(0_\omega^B) = 0_\omega^C\,.$$

□

Lause 1.19 *Ω-algebra A endomorfismide hulk* $\operatorname{End}(A)$ *on monoid kujutuste korrutamise suhtes.*

TÕESTUS. Lause 1.18 tõttu on kujutuste korrutamine algebraline tehe hulgal $\operatorname{End}(A)$. Hulgateooriast on teada, et see tehe on alati assotsiatiivne, ja samasusteisendus 1_A on ilmselt homomorfism, kusjuures $1_A f = f = f 1_A$ iga $f \in \operatorname{End}(A)$ korral. □

1.4 Isomorfismid

Definitsioon 1.20 Bijektiivseid Ω-algebrate homomorfisme nimetatakse **isomorfismideks**. Ω-algebraid A ja B nimetatakse **isomorfseteks**, kui leidub isomorfism $f : A \to B$. Sellisel juhul kirjutatakse $A \cong B$.

Definitsioon 1.21 Isomorfismi Ω-algebrast iseendasse nimetatakse **automorfismiks**. Ω-algebra A kõigi automorfismide hulka tähistatakse sümboliga $\mathrm{Aut}(A)$.

Näide 1.22 Vektorruumid $\mathrm{Mat}_2(\mathbb{R})$ ja $\mathbb{R}^4$ (üle korpuse $\mathbb{R}$) on isomorfsed. Isomorfismiks sobib näiteks kujutus $f : \mathrm{Mat}_2(\mathbb{R}) \to \mathbb{R}^4$, mis on defineeritud võrdusega

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := (a, b, c, d).$$

Isomorfsetel Ω-algebratel on samasugused algebralised omadused. Näiteks kui A ja B on isomorfsed Ω-algebrad, millel on üks kahekohaline tehe ja algebral A on see tehe kommutatiivne, siis ka algebral B on see tehe kommutatiivne. Või kui A ja B on isomorfsed Ω-algebrad ja algebral A on kolmteist alamalgebrat, siis ka algebral B on kolmteist alamalgebrat.

Kuna algebralises mõttes ei ole isomorfsetel Ω-algebratel olulist vahet (vahe seisneb ainult selles, kuidas me elemente ja tehteid tähistame, aga mitte selles, kuidas me tehteid teeme), siis algebras tihti isomorfsed Ω-algebrad samastatakse.

Tõestame mõned lihtsamad isomorfismide omadused.

Lause 1.23 *Isomorfismide korrutis on isomorfism.*

Tõestus. Hulgateooriast teame, et bijektiivsete kujutuste korrutis on bijektiivne. Lause 1.18 põhjal on ka homomorfismide korrutis homomorfism. □

Hulgateooriast teame, et iga bijektiivse kujutuse $f : A \to B$ jaoks leidub pöördkujutus $f^{-1} : B \to A$ nii, et

$$ff^{-1} = 1_B \quad \text{ja} \quad f^{-1}f = 1_A.$$

Lause 1.24 *Isomorfismi pöördkujutus on isomorfism.*

Tõestus. Olgu $f : A \to B$ Ω-algebrate isomorfism. Kuna f on bijektiivne, siis tal leidub pöördkujutus $f^{-1} : B \to A$, kusjuures see pöördkujutus defineeritakse iga $b \in B$ korral võrdusega

$$f^{-1}(b) := a,$$

kus $a \in A$ on selline element, et $f(a) = b$ (see a leidub tänu kujutuse f sürjektiivsusele). Hulgateooriast teame, et kujutus f^{-1} on bijektiivne. Seega jääb veel näidata, et f^{-1} on kooskõlas tehetega (s.t. homomorfism).

1. Olgu $\omega \in \Omega_n$ ($n \in \mathbb{N}$) ja $b_1, \ldots, b_n \in B$. Tänu f sürjektiivsusele leiduvad elemendid $a_1, \ldots, a_n \in A$ nii, et $f(a_i) = b_i$ iga $i \in \{1, \ldots, n\}$ korral. Siis

$$\begin{aligned} f^{-1}(\omega^B(b_1, \ldots, b_n)) &= f^{-1}(\omega^B(f(a_1), \ldots, f(a_n))) = f^{-1}(f(\omega^A(a_1, \ldots, a_n))) \\ &= (f^{-1}f)(\omega^A(a_1, \ldots, a_n)) = 1_A(\omega^A(a_1, \ldots, a_n)) \\ &= \omega^A(a_1, \ldots, a_n) = \omega^A(f^{-1}(b_1), \ldots, f^{-1}(b_n)) \,. \end{aligned}$$

2. Kui $\omega \in \Omega_0$, siis

$$f^{-1}(0_\omega^B) = f^{-1}(f(0_\omega^A)) = (f^{-1}f)(0_\omega^A) = 1_A(0_\omega^A) = 0_\omega^A.$$

□

Osutub, et isomorfismiseos on refleksiivne, sümmeetriline ja transitiivne.

Lause 1.25 *Olgu A, B ja C Ω-algebrad. Siis*

1. *$A \cong A$;*
2. *kui $A \cong B$, siis $B \cong A$;*
3. *kui $A \cong B$ ja $B \cong C$, siis $A \cong C$.*

TÕESTUS. 1. Kuna samasusteisendus $1_A : A \to A$ on isomorfism, siis $A \cong A$.

2. Kui $A \cong B$, siis leidub isomorfism $f : A \to B$. Tänu lausele 1.24 on ka kujutus $f^{-1} : B \to A$ isomorfism ja seega $B \cong A$.

3. Olgu $A \cong B$ ja $B \cong C$. Siis leiduvad isomorfismid $f : A \to B$ ja $g : B \to C$. Lause 1.23 põhjal on ka $gf : A \to C$ isomorfism, mis tähendab, et $A \cong C$. □

Algebraliste struktuuride uurimisel on üheks põhiliseks küsimuseks: kirjeldada kõik teatud omadustega struktuurid. Sellise kirjeldamise all mõeldakse enamasti just kirjeldamist isomorfismi täpsuseni. See tähendab, et üritatakse välja selgitada, millised on ekvivalentsiklassid isomorfsusseose järgi ja võimaluse korral leida igast klassist üks võimalikult lihtne esindaja. Näiteks võib küsida: kui palju on (isomorfismi täpsuseni) neljaelemendilisi rühmi?

Mõnedest sellist tüüpi kirjeldustest on lugeja tõenäoliselt juba kuulnud. Näiteks on teada, et iga n-mõõtmeline vektorruum üle korpuse K on isomorfne vektorruumiga K^n ja iga lõplik Abeli rühm on isomorfne jäägiklassirühmade otsesummaga. Selle kursuse jooksul anname veel mitmete algebraliste struktuuride klasside kirjeldused isomorfismi täpsuseni.

1.5 Faktorstruktuurid

Kui hulkade faktorhulkade konstrueerimiseks on vaja ekvivalentsiseoseid, siis faktoralgebraid moodustatakse kongruentside järgi.

Definitsioon 1.26 Ω-algebra A **kongruents** on selline ekvivalentsiseos ρ hulgal A, mis on kooskõlas tehetega. See tähendab, et

$$a_1 \,\rho\, b_1 \ \wedge a_2 \,\rho\, b_2 \ \wedge \ldots \wedge a_n \,\rho\, b_n \implies \omega^A(a_1, a_2, \ldots, a_n) \,\rho\, \omega^A(b_1, b_2, \ldots, b_n)$$

iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in A$ korral.

Kooskõla kahekohalise tehtega $*$ tähendab seda, et

$$a_1 \,\rho\, b_1 \ \wedge a_2 \,\rho\, b_2 \implies (a_1 * a_2) \,\rho\, (b_1 * b_2)\,.$$

Näide 1.27 Vaatleme poolrühma $(\mathbb{N}, \cdot)$ (siin $\Omega = \Omega_2 = \{\cdot\}$). Lihtne on veenduda, et seos ρ, mis on defineeritud eeskirjaga

$$a \,\rho\, b \iff a \text{ ja } b \text{ on paarisarvud},$$

on kongruents poolrühmal $(\mathbb{N}, \cdot)$.

Kuna kongruents on ekvivalentsiseos, siis võib vaadelda ekvivalentsiklasse selle seose järgi. Tähistame elemendi a ekvivalentsiklassi kongruentsi ρ järgi kas $\overline{a}_\rho$ või lühemalt $\overline{a}$, kui segaduse tekkimise ohtu ei ole. Teised levinud tähistused on $[a]_\rho$ ja a/ρ. Niisiis

$$\overline{a} = \{b \in A \mid a \,\rho\, b\}\,.$$

Kõigi ekvivalentsiklasside hulka nimetatakse **faktorhulgaks** seose ρ järgi ja tähistatakse

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

Tuleb välja, et vektorruumi kongruentse saab kirjeldada alamruumide abil.

Lause 1.28 *Olgu V vektorruum üle korpuse K. Binaarne seos $\rho \subseteq V \times V$ on vektorruumi V kongruents parajasti siis, kui leidub vektorruumi V alamruum V' nii, et mistahes $a, b \in V$ korral*

$$a \,\rho\, b \iff a - b \in V'. \tag{1.1}$$

Tõestus. Tarvilikkus. Olgu ρ vektorruumi V kongruents. Tähistame nullelemendi ekvivalentsiklassi sümboliga V', s.t.

$$V' := \overline{0} = \{a \in V \mid a \,\rho\, 0\} \subseteq V.$$

Näitame, et V' on vektorruumi V alamruum.

Kuna refleksiivsuse tõttu $0 \,\rho\, 0$, siis $0 \in V'$ ja V' on mittetühi. Olgu nüüd $a, b \in V'$. Siis $a \,\rho\, 0$ ja $b \,\rho\, 0$. Kuna ρ on kongruents, siis $a + b \,\rho\, 0 + 0 = 0$. Seega $a + b \in V'$. Kui veel $k \in K$, siis $ka \,\rho\, k0 = 0$, mis tähendab, et $ka \in V'$. Kuna V' rahuldab tingimusi AR1 ja AR2, siis lause 1.10 põhjal on V' alamruum.

Oletame, et $a \,\rho\, b$. Kuna ka $-b \,\rho\, -b$, siis kasutades ρ kooskõla liitmisega saame, et $a - b \,\rho\, b - b = 0$. Järelikult $a - b \in V'$. Vastupidi, kui $a - b \in V'$, siis $a - b \,\rho\, 0$. Kuna $b \,\rho\, b$, siis saame, et $a - b + b \,\rho\, 0 + b$, kust $a \,\rho\, b$.

Piisavus. Oletame, et leidub V mingi alamruum V' nii, et kehtib (1.1). Näitame, et ρ on kongruents. Kõigepäält veendume, et ρ on ekvivalentsiseos.

Kuna $a - a = 0 \in V'$ iga $a \in V$ korral, siis seos ρ on refleksiivne. Olgu $a \,\rho\, b$. Siis $a - b \in V'$, aga kuna V' on kinnine vastandelemendi võtmise suhtes, siis ka $b - a = -(a - b) \in V'$. Seega $b \,\rho\, a$ ning ρ on sümmeetriline. Transitiivsuse näitamiseks eeldame, et $a \,\rho\, b$ ja $b \,\rho\, c$ ehk $a - b, b - c \in V'$. Siis ka $a - c = (a - b) + (b - c) \in V'$ ehk $a \,\rho\, c$. Järelikult ρ on transitiivne ning me oleme näidanud, et ta on ekvivalentsiseos.

Veendume nüüd, et ρ on kooskõlas tehetega. Kui $a_1 \,\rho\, b_1$ ja $a_2 \,\rho\, b_2$, siis $a_1 - b_1, a_2 - b_2 \in V'$. Kuna V' on kinnine liitmise suhtes, siis

$$(a_1 + a_2) - (b_1 + b_2) = a_1 + a_2 - b_1 - b_2 = (a_1 - b_1) + (a_2 - b_2) \in V'.$$

Järelikult $(a_1 + a_2)\,\rho\,(b_1 + b_2)$. Sellega on näidatud, et ρ on kooskõlas liitmisega.

Olgu nüüd $a\,\rho\,b$ ja $k \in K$. Siis $a - b \in V'$ ning samuti $ka - kb = k(a - b) \in V'$. Tänu seosele (1.1) võime öelda, et $ka\,\rho\,kb$. Võttes $k = -1$ saame, et $(-a)\,\rho\,(-b)$. Seega on ρ kooskõlas ka kõigi ühekohaliste tehetega. □

Olgu ρ mingi kongruents Ω-algebral A. Vaatleme faktorhulka

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

Iga $\omega \in \Omega_n$ jaoks defineerime ka hulgal A/ρ n-kohalise tehte $\omega^{A/\rho}$ võrdusega

$$\omega^{A/\rho}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) := \overline{\omega^A(a_1, a_2, \ldots, a_n)}.$$

Kongruentsi kooskõla tehtega ω^A ütleb täpselt seda, et see definitsioon on korrektne (s.t. ei sõltu ekvivalentsiklasside esindajate valikust). Iga nullkohalise tehte ω korral defineerime

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

Nii saame faktoralgebra A/ρ, mis on esialgse algebraga A sama tüüpi.

Vaatleme vektorruumi V (üle korpuse K) kongruentsi ρ, mille korral $\overline{0} = V'$. Siis

$$\overline{a} = \{b \in V \mid b\,\rho\,a\} = \{b \in V \mid b - a \in V'\}.$$

Näitame, et

$$\overline{a} = a + V',$$

kus $a + V' := \{a + v \mid v \in V'\}$. Tõepoolest, kui $b \in \overline{a}$, siis $b = a + (b - a) \in a + V'$ ja seega $\overline{a} \subseteq a + V'$. Vastupidi, kui $v \in V'$, siis $(a + v) - a = v \in V'$, järelikult $a + v \in \overline{a}$ ning seega $a + V' \subseteq \overline{a}$.

Lause 1.28 ütleb muuhulgas, et iga alamruum V' tekitab ühe kongruentsi vektorruumil V, kusjuures ekvivalentsiklassid selle kongruentsi järgi on hulgad $a + V'$, $a \in V$. Hulka $a + V'$ nimetatakse **kõrvalklassiks alamruumi V' järgi esindajaga a**. On selge, et

$$a + V' = b + V' \iff \overline{a} = \overline{b} \iff a\,\rho\,b \iff a - b \in V'.$$

Faktorhulka sellise kongruentsi järgi tähistatakse

$$V/V' = \{a + V' \mid a \in V\} = \{\overline{a} \mid a \in V\}.$$

Vastavalt eespoolöeldule defineeritakse faktorhulgal V/V' tehted järgmiselt:

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a + b}, \\ k\overline{a} &:= \overline{ka}, \\ -\overline{a} &:= \overline{-a}, \\ 0^{V/V'} &:= \overline{0} = V'. \end{aligned}$$

Lause 1.29 *Kui V' on vektorruumi V (üle korpuse K) alamruum, siis faktorhulk V/V' on ka vektorruum üle korpuse K eelpool defineeritud tehete suhtes.*

TÕESTUS. Nagu juba nägime, tehete definitsioonid on korrektsed.
VR1. Olgu $a, b, c \in V$. Siis

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c}).$$

VR2. Mistahes $a \in V$ korral

$$\overline{a} + \overline{0} = \overline{a+0} = \overline{a} = \overline{0+a} = \overline{0} + \overline{a}.$$

Ülejäänud tingimuste kontroll on analoogiline. □

Lause 1.30 *Olgu V' vektorruumi V (üle korpuse K) alamruum. Kujutus*

$$\pi : V \to V/V', \quad a \mapsto \overline{a}$$

on sürjektiivne lineaarkujutus.

TÕESTUS. Kujutuse π sürjektiivsus on ilmne. Ta on lineaarkujutus, sest mistahes $a, b \in V$ ja $k \in K$ korral

$$\pi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi(a) + \pi(b),$$
$$\pi(ka) = \overline{ka} = k\overline{a} = k\pi(a).$$

□

Lauses 1.30 defineeritud kujutust π nimetatakse vektoruumi V **loomulikuks projektsiooniks** faktorruumile V/V'.

Näide 1.31 Vaatleme vektorruumi $V := \mathbb{R}^2$ üle $\mathbb{R}$ ja selle alamruumi $V' := \{(z, 0) \mid z \in \mathbb{R}\}$. Siis kõrvalklassid V' järgi on kujul

$$(a, b) + V' = \{(a + c, b) \mid c \in \mathbb{R}\} = \{(c', b) \mid c' \in \mathbb{R}\}$$

(sõltumata a valikust kehtib võrdus $\{a + c \mid c \in \mathbb{R}\} = \mathbb{R}$). Üheks selle kõrvalklassi esindajaks on reaalarvupaar $(0, b)$. Kuna kõrvalklassid on kongruentsiklassid, siis kõrvalklassi esindajaks võib võtta suvalise selle kõrvalklassi esindaja. Seega

$$(a, b) + V' = (0, b) + V' =: \overline{(0, b)}\,.$$

Fikseerides tasandil ristkoordinaadistiku ja samastades reaalarvupaari (a, b) punktiga, mille koordinaatideks on (a, b), võime öelda, et

- V' on x-telg,
- kõrvalklassid on x-teljega paralleelsed sirged,
- faktorruum V/V' koosneb kõigist x-teljega paralleelsetest sirgetest.

Tehted faktorruumil on defineeritud kõrvalklasside esindajate abil:

$$\overline{(0, b)} + \overline{(0, b')} = \overline{(0, b + b')},$$
$$k\overline{(0, b)} = \overline{(0, kb)},$$
$$-\overline{(0, b)} = \overline{(0, -b)},$$
$$0^{V/V'} = \overline{(0, 0)} = V'\,.$$

1.6 Homomorfismiteoreem

Selles paragrahvis tõestame homomorfismiteoreemi vektorruumide jaoks. See ütleb, et iga lineaarkujutuse saab esitada injektiivse lineaarkujutuse ja sürjektiivse lineaarkujutuse korrutisena.

Definitsioon 1.32 Olgu V ja U vektorruumid üle korpuse K. Lineaarkujutuse $f : V \to U$ **tuum** $\operatorname{Ker} f$ defineeritakse järgmiselt:

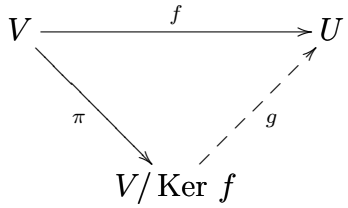
$$\operatorname{Ker} f = \{a \in V \mid f(a) = 0\}.$$

Lihtne on veenduda, et kehtivad järgmised tulemused tuumade kohta.

Lause 1.33 ([1], lemma 4.1.8) *Kui $f : V \to U$ on lineaarkujutus, siis* $\operatorname{Ker} f$ *on vektorruumi V alamruum.*

Lause 1.34 ([1], lause 4.1.10) *Lineaarkujutus $f : V \to U$ on üksühene parajasti siis, kui* $\operatorname{Ker} f = \{0\}$.

Teoreem 1.35 (Homomorfismiteoreem) *Olgu $f : V \to U$ lineaarkujutus. Siis leidub üksühene lineaarkujutus $g : V/\operatorname{Ker} f \to U$ nii, et $f = g\pi$, kus $\pi : V \to V/\operatorname{Ker} f$ on loomulik projektsioon.*



Tõestus. Defineerime kujutuse $g : V/\operatorname{Ker} f \to U$ võrdusega

$$g(\overline{a}) := f(a),$$

$a \in V$. Esimese asjana peame näitama, et selline definitsioon on korrektne, s.t. et ta ei sõltu kõrvalklassi esindaja valikust. Paneme tähele, et mistahes $a, b \in V$ korral

$$\overline{a} = \overline{b} \iff a - b \in \operatorname{Ker} f \iff f(a-b) = 0 \iff f(a) - f(b) = 0 \iff f(a) = f(b).$$

Sellega on tõestatud nii definitsiooni korrektsus kui g üksühesus. Kuna f on lineaarkujutus, siis

$$g(\overline{a} + \overline{b}) = g(\overline{a+b}) = f(a+b) = f(a) + f(b) = g(\overline{a}) + g(\overline{b}),$$
$$g(k\overline{a}) = g(\overline{ka}) = f(ka) = kf(a) = kg(\overline{a})$$

iga $a, b \in V$ ja $k \in K$ korral, s.t. et g on lineaarkujutus. Lõpuks märgime, et

$$(g\pi)(a) = g(\pi(a)) = g(\overline{a}) = f(a)$$

iga $a \in V$ korral ja seega $g\pi = f$. □

Järeldus 1.36 *Kui lineaarkujutus $f : V \to U$ on sürjektiivne, siis $V/\operatorname{Ker} f \cong U$.*

TÕESTUS. Näitame, et lineaarkujutus $g : V/\operatorname{Ker} f \to U$ on sürjektiivne (siis ta ongi isomorfism). Kui $u \in U$, siis f sürjektiivsuse tõttu leidub selline $a \in V$, et $f(a) = u$. Järelikult ka $g(\overline{a}) = u$. □

1.7 Baasi olemasolu

Vektorruumi nimetatakse **mittetriviaalseks**, kui temas on rohkem kui üks element. Kursuses "Algebra I" tõestatakse harilikult järgmine teoreem.

Teoreem 1.37 ([1], teoreem 3.2.3) *Kui mittetriviaalses vektoruumis on olemas lõplik moodustajate süsteem, siis selles vektorruumis leidub baas.*

Käesolevas paragrahvis on meie eesmärgiks näidata, et baas on olemas tegelikult suvalises mittetriviaalses vektorruumis. Selleks tuleb meil appi võtta Zorni lemma. Sellega seoses meenutame mõningaid järjestatud hulkadega seotud mõisteid.

Definitsioon 1.38 Osaliselt järjestatud hulk on hulk, millel on antud osalise järjestuse seos, s.t. binaarne seos, mis on refleksiivne, antisümmeetriline ja transitiivne.

Kui $(P, \leqslant)$ on osaliselt järjestatud hulk, siis hulgal P võib vaadelda nn. range järjestuse seost $<$, mis defineeritakse järgmiselt:

$$a < b \iff a \leqslant b \text{ ja } a \neq b\,.$$

Definitsioon 1.39 Ahel ehk **lineaarselt järjestatud hulk** on selline osaliselt järjestatud hulk $(P, \leqslant)$, kus iga $a, b \in P$ korral $a \leqslant b$ või $b \leqslant a$ (s.t. mistahes kaks elementi on võrreldavad).

Lõpliku ahela korral saab selle elemendid üles kirjutada kujul $p_1 < p_2 < \ldots < p_n$. Lõpmatu ahela korral seda nii teha ei saa.

Näide 1.40 Hulk $\mathbb{Q}$ on ahel osaliselt järjestatud hulgas $(\mathbb{R}, \leqslant)$. Samuti hulk, mis koosneb elementidest $-5 \leqslant -1 \leqslant 2 \leqslant 13$.

Definitsioon 1.41 Olgu A osaliselt järjestatud järjestatud hulga $(P, \leqslant)$ alamhulk. Elementi $u \in P$ nimetatakse hulga A **ülemiseks tõkkeks**, kui $a \leqslant u$ iga $a \in A$ korral.

Definitsioon 1.42 Öeldakse, et element $m \in P$ on osaliselt järjestatud järjestatud hulga $(P, \leqslant)$ **maksimaalne element**, kui ei leidu sellist elementi $p \in P$, et $m < p$.

Lemma 1.43 (Zorni lemma) *Kui mittetühja osaliselt järjestatud hulga igal ahelal leidub ülemine tõke, siis selles hulgas leidub maksimaalne element.*

Meenutame nüüd mõningaid baasidega seotud mõisteid.

Definitsioon 1.44 Olgu V vektorruum üle korpuse K ja $a_1, \ldots, a_s \in V$, kus $s \in \mathbb{N}$. Mistahes avaldist

$$k_1a_1 + k_2a_2 + \ldots + k_sa_s, \tag{1.2}$$

kus $k_1, \ldots, k_s \in K$, aga ka selle avaldise poolt määratud V elementi, nimetatakse vektorite $a_1, \ldots, a_s$ **lineaarkombinatsiooniks.** Skalaare $k_1, \ldots, k_s$ nimetatakse selle lineaarkombinatsiooni **kordajateks**.

Kuna käesolevas paragrahvis ei ole meil vaja vaadelda vektorite süsteeme, kus vektorid korduvad ja kus vektorite järjekord on fikseeritud, siis siin me räägime vektorite hulkadest (vektorite süsteemide asemel) ja kasutame vastavat sümboolikat.

Definitsioon 1.45 Vektorruumi V (mis on antud üle korpuse K) lõplikku vektorite hulka $\{a_1, a_2, \ldots, a_s\}$, $s \in \mathbb{N}$, nimetatakse **lineaarselt sõltumatuks**, kui mistahes skalaaride $k_1, k_2, \ldots, k_s \in K$ korral võrdusest

$$k_1a_1 + k_2a_2 + \ldots + k_sa_s = 0$$

järeldub, et

$$k_1 = k_2 = \ldots = k_s = 0.$$

Lisaks sellele loeme ka tühja vektorite hulga lineaarselt sõltumatuks. Lõpmatut vektorite hulka nimetatakse **lineaarselt sõltumatuks**, kui tema iga lõplik alamhulk on lineaarselt sõltumatu.

Definitsioon 1.46 Vektorite hulka nimetatakse **lineaarselt sõltuvaks**, kui ta ei ole lineaarselt sõltumatu

Järgmised kolm lauset on tuttavad kursusest Algebra I.

Lause 1.47 ([1], lause 3.1.3) *Ühestainsast vektorist a koosnev hulk on lineaarselt sõltumatu parajasti siis, kui $a \neq 0$.*

Lause 1.48 ([1], lause 3.1.4) *Lineaarselt sõltumatu vektorite hulga iga alamhulk on ka lineaarselt sõltumatu.*

Lause 1.49 ([1], lause 3.1.6) *Nullist erinevate vektorite lõplik hulk, mis sisaldab vähemalt kahte vektorit, on lineaarselt sõltuv parajasti siis, kui selle hulga vektorite mistahes järjestuse korral leidub vektor, mis avaldub eelnevate vektorite lineaarkombinatsioonina.*

Definitsioon 1.50 Vektorruumi V vektorite hulka B nimetatakse **baasiks**, kui

1. hulk B on lineaarselt sõltumatu,

2. vektoruumi V iga nullist erinev vektor avaldub hulka B kuuluvate vektorite lineaarkombinatsioonina.

Näide 1.51 Vaatleme reaalarvuliste kordajatega polünoomide vektorruumi $\mathbb{R}[X]$. Selles vektorruumis on üheks baasiks hulk

$$\{1, X, X^2, X^3, \ldots\}.$$

Selles vektorruumis ei leidu lõplikku baasi.

Tõestame nüüd selle paragrahvi põhitulemuse.

Teoreem 1.52 *Igas mittetriviaalses vektorruumis leidub baas.*

TÕESTUS. Olgu $V \neq \{0\}$ vektorruum üle korpuse K. Tõestuse idee on näidata, et V sisaldab maksimaalset lineaarselt sõltumatut alamhulka, mis osutubki baasiks.

Olgu P hulga V kõigi lineaarselt sõltumatute alamhulkade hulk, s.t.

$$P = \{A \subseteq V \mid A \text{ on lineaarselt sõltumatu}\}.$$

Vaatleme hulka P osaliselt järjestatud hulgana sisalduvusseose $\subseteq$ suhtes ja näitame, et ta rahuldab Zorni lemma eeldusi. Olgu $a \in V \setminus \{0\}$. Siis lause 1.47 tõttu on hulk $\{a\}$ lineaarselt sõltumatu. Seega $\{a\} \in P$ ja $P \neq \emptyset$.

Olgu nüüd $\{A_\alpha \mid \alpha \in I\}$ mingi ahel osaliselt järjestatud hulgas $(P, \subseteq)$. Vaatleme hulka

$$A := \bigcup_{\alpha \in I} A_\alpha \subseteq V$$

ja näitame, et see hulk on lineaarselt sõltumatu. Olgu $\{a_1, \ldots, a_s\}$ hulga A suvaline lõplik alamhulk. Siis leiduvad indeksid $\alpha_1, \ldots, \alpha_s \in I$ nii, et $a_i \in A_{\alpha_i}$ iga $i \in \{1, \ldots, s\}$ korral. Kuna hulgad A_{α_i} moodustavad lõpliku ahela, siis sisaldab üks neist hulkadest, olgu see näiteks A_{α_k}, kõiki ülejäänud hulki ning seega $a_1, \ldots, a_s \in A_{\alpha_k}$. Kuna $A_{\alpha_k} \in P$, siis on ta lineaarselt sõltumatu ja seega ka tema alamhulk $\{a_1, \ldots, a_s\}$ on lineaarselt sõltumatu tänu lausele 1.48. Sellega on näidatud, et A on lineaarselt sõltumatu, millest järeldub, et $A \in P$. Et $A_\alpha \subseteq A$ iga $\alpha \in I$ korral, siis A on ahela $\{A_\alpha \mid \alpha \in I\}$ ülemine tõke osaliselt järjestatud hulgas P. Sellega oleme näidanud, et Zorni lemma eeldused on täidetud. Lemmat rakendades saame järeldada, et hulgas P leidub maksimaalne element.

Olgu üheks hulga P maksimaalseks elemendiks B. Näitame, et B on vektorruumi V baas. Kuna $B \in P$, siis B on lineaarselt sõltumatu. Näitame, et V iga nullist erinev vektor avaldub B elementide lineaarkombinatsioonina. Olgu $a \in V \setminus \{0\}$. Kui $a \in B$, siis a avaldub B elementide lineaarkombinatsioonina: $a = 1a$. Eeldame edasises, et $a \notin B$. Kuna $B \subset B \cup \{a\}$ ja B on maksimaalne lineaarselt sõltumatu vektorite hulk, siis hulk $B \cup \{a\}$ peab olema lineaarselt sõltuv. Seega hulgal $B \cup \{a\}$ peab leiduma lõplik lineaarselt sõltuv alamhulk S. Kuna B on lineaarselt sõltumatu, siis ei ole võimalik, et $S \subseteq B$. Seega S peab sisaldama vektorit a. Järjestame hulga S vektorid nii, et a on viimane. Siis lause 1.49 põhjal avaldub mingi hulga S vektor eelnevate lineaarkombinatsioonina. Kuna B on lineaarselt sõltumatu, siis saab see olla vaid vektor a. Seega vektor a avaldub hulka B kuuluvate vektorite lineaarkombinatsioonina, mida oligi tarvis tõestada. □

Märkus 1.53 Kuna me lugesime tühja vektorite hulga lineaarselt sõltumatuks, siis vastavalt definitsioonile 1.50 on $\emptyset$ triviaalse vektorruumi $V = \{0\}$ baas.

1.8 Otsekorrutised ja otsesummad

Tuletame meelde hulkade otsekorrutisega seotud mõisted.

Olgu I mingi indeksite hulk (see võib olla ka lõpmatu) ja vaatame hulki X_i, $i \in I$ (s.t. iga indeksi $i \in I$ jaoks on fikseeritud üks hulk X_i, kusjuures need hulgad ei pruugi olla erinevad). Hulkade X_i, $i \in I$ **otsekorrutis** on hulk

$$\prod_{i\in I} X_i = \left\{ x : I \to \bigcup_{i\in I} X_i \;\middle|\; (\forall i \in I)\; x(i) \in X_i \right\}.$$

Tähistame kujutuse $x : I \to \bigcup_{i\in I} X_i$ korral $x_i := x(i)$. Sellist kujutust kirjutame üles kujul $x = (x_i)_{i\in I}$ ja kutsume **pereks, mis on indekseeritud hulga I järgi**. Elementi x_i kutsume pere $(x_i)_{i\in I}$ **i-ndaks komponendiks**. Niisiis otsekorrutis koosneb kõigist peredest $(x_i)_{i\in I}$, kus $x_i \in X_i$ iga $i \in I$ korral. Peresid $(x_i)_{i\in I}$ ja $(y_i)_{i\in I}$ loeme **võrdseteks**, kui nende vastavad komponendid on võrdsed, s.t.

$$(x_i)_{i\in I} = (y_i)_{i\in I} \iff (\forall i \in I)\; x_i = y_i.$$

Juhul kui indeksite hulk $I = \mathbb{N}$, siis ütleme pere $(x_i)_{i\in\mathbb{N}}$ kohta **jada** ja kasutame ka kirjaviisi $(x_1, x_2, x_3, \ldots)$. Otsekorrutist tähistatakse sel juhul ka $\prod_{i=1}^{\infty} X_i$.

Kui I on lõplik, siis harilikult loetakse, et $I = \{1, 2, \ldots, n\}$ ja $(x_i)_{i\in\{1,2,\ldots,n\}}$ asemel kirjutatakse $(x_1, x_2, \ldots, x_n)$. Selliseid peresid kutsutakse **järjenditeks** ehk **korteežideks** ehk **lõplikeks jadadeks**. Lõplikku otsekorrutist tähistatakse enamasti $X_1 \times X_2 \times \ldots \times X_n$. Kui $X_1 = X_2 = \ldots = X_n = X$, siis vastavat otsekorrutist nimetatakse hulga X **n-ndaks otseastmeks** ja tähistatakse X^n.

Vaatleme nüüd Ω-algebraid X_i, $i \in I$. Defineerime hulkade otsekorrutisel $X := \prod_{i\in I} X_i$ tehted n.ö. komponenthaaval:

$$\omega^X\left((x_i^1)_{i\in I}, (x_i^2)_{i\in I}, \ldots, (x_i^n)_{i\in I}\right) := \left(\omega^{X_i}(x_i^1, x_i^2, \ldots, x_i^n)\right)_{i\in I},$$

kui $\omega \in \Omega_n$ ($n \in \mathbb{N}$) ja

$$0_\omega^X := \left(0_\omega^{X_i}\right)_{i\in I},$$

kui $\omega \in \Omega_0$. Nii tehes saame Ω-algebra, mida nimetatakse esialgsete algebrate **otsekorrutiseks**.

Lause 1.54 *Üle korpuse K vaadeldavate vektorruumide otsekorrutis on vektorruum üle K.*

TÕESTUS. Olgu V_i, $i \in I$ vektorruumid üle sama korpuse K. Vaatleme hulka $V := \prod_{i\in I} V_i$ ja sellel hulgal komponenthaaval defineeritud tehteid. Näitame näiteks, et liitmine on kommutatiivne. Tõepoolest, kui $(x_i^1)_{i\in I}, (x_i^2)_{i\in I} \in \prod_{i\in I} V_i$, siis

$$(x_i^1)_{i\in I} + (x_i^2)_{i\in I} = (x_i^1 + x_i^2)_{i\in I} = (x_i^2 + x_i^1)_{i\in I} = (x_i^2)_{i\in I} + (x_i^1)_{i\in I}.$$

Ülejäänud tingimuste kontroll on analoogiline. □

Vaatleme nüüd vektorruumide V_i, $i \in I$ korral otsekorrutise alamhulka

$$\oplus\sum_{i\in I} V_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} V_i \;\middle|\; \text{peres } (x_i)_{i\in I} \text{ on lõplik arv nullist erinevaid komponente} \right\}.$$

Lihtne on veenduda, et see hulk on otsekorrutise $\prod_{i\in I} V_i$ alamruum. Seega lause 1.11 põhjal on $\oplus\sum_{i\in I} V_i$ ise ka vektorruum komponenthaaval defineeritud tehete suhtes. Seda vektorruumi nimetatakse **vektorruumide** $V_i, i \in I$ **väliseks otsesummaks**.

Kui $I = \{1, 2, \ldots, n\}$, siis vektorruumide $V_1, V_2, \ldots, V_n$ välist otsesummat tähistatakse harilikult $V_1 \oplus V_2 \oplus \ldots \oplus V_n$. On selge, et

$$V_1 \oplus V_2 \oplus \ldots \oplus V_n = V_1 \times V_2 \times \ldots \times V_n. \tag{1.3}$$

Meenutame, et korpust K saab loomulikul viisil vaadelda vektorruumina üle iseenda, kui liitmiseks võtta selle korpuse liitmine ja skalaariga k korrutamine defineerida korpuse korrutamistehte abil. Järgmine teoreem kirjeldab isomorfismi täpsuseni ära kõik vektorruumid üle korpuse K.

Teoreem 1.55 *Iga mittetriviaalse vektorruumi V korral (üle korpuse K) leidub selline hulk I, et*

$$V \cong \oplus\sum_{i\in I} V_i,$$

kus $V_i = K$.

Tõestus. Teoreemi 1.52 põhjal leidub vektoruumis V baas. Indekseerime selle baasi vektorid ära mingi hulga I elementidega, s.t. olgu see baas $\{e_i \mid i \in I\}$. Võtame iga $i \in I$ korral $V_i := K$. Defineerime kujutuse $f : \oplus\sum_{i\in I} V_i \to V$ võrdusega

$$f\left((k_i)_{i\in I}\right) := \sum_{i\in I} k_i e_i.$$

Kuna $(k_i)_{i\in I} \in \oplus\sum_{i\in I} V_i$, siis selles peres on lõplik arv nullist erinevaid elemente. Seega ka vektorite $k_i e_i, i \in I$ hulgas on lõplik arv nullist erinevaid. Nende nullist erinevate vektorite summat tähistamegi tähisega $\sum_{i\in I} k_i e_i$. Kui $k_i = 0$ iga $i \in I$ korral, siis mõistame summa $\sum_{i\in I} k_i e_i$ all nullvektorit. Tõestame, et f on bijektiivne homomorfism (s.t. isomorfism).

Veendume, et f on lineaarkujutus. Tõepoolest, mistahes $(k_i)_{i\in I}, (l_i)_{i\in I} \in \oplus\sum_{i\in I} V_i$ ja $k \in K$ korral

$$\begin{aligned} f\left((k_i)_{i\in I} + (l_i)_{i\in I}\right) &= f\left((k_i + l_i)_{i\in I}\right) = \sum_{i\in I}(k_i + l_i)e_i = \sum_{i\in I}(k_i e_i + l_i e_i) \\ &= \sum_{i\in I} k_i e_i + \sum_{i\in I} l_i e_i = f\left((k_i)_{i\in I}\right) + f\left((l_i)_{i\in I}\right), \\ f\left(k(k_i)_{i\in I}\right) &= f\left((kk_i)_{i\in I}\right) = \sum_{i\in I}(kk_i)e_i = \sum_{i\in I} k(k_i e_i) = k\sum_{i\in I} k_i e_i = kf\left((k_i)_{i\in I}\right). \end{aligned}$$

Näitame nüüd, et f on pealekujutus. Olgu $a \in V$. Kuna $\{e_i \mid i \in I\}$ on baas, siis leidub naturaalarv n, indeksid $i_1, \ldots, i_n \in I$ ja skalaarid $k_{i_1}, \ldots, k_{i_n} \in K$ nii, et

$$a = k_{i_1} e_{i_1} + \ldots + k_{i_n} e_{i_n}.$$

Võttes $k_i := 0$ iga $i \in I \setminus \{i_1, \ldots, i_n\}$ korral saame pere $(k_i)_{i\in I} \in \oplus\sum_{i\in I} V_i$, mille korral $f\left((k_i)_{i\in I}\right) = a$.

Kujutuse f üksühesuse kontrollimiseks kasutame lauset 1.34. Oletame, et

$$0 = f\left((k_i)_{i\in I}\right) = \sum_{i\in I} k_i e_i.$$

Kuna hulk $\{e_i \mid i \in I\}$ on lineaarselt sõltumatu, siis $k_i = 0$ iga $i \in I$ korral. Sellega on näidatud, et Ker $f = \{0\}$ ning järelikult f on üksühene. □

Järeldus 1.56 *Kui n on naturaalarv ja V on n-mõõtmeline vektorruum üle korpuse K, siis $V \cong K^n$.*

Tõestus. See järeldub teoreemist 1.55 ja võrdusest (1.3). □

Peatükk 2

Rühm

2.1 Rühm, alamrühm

Traditsiooniliselt antakse rühma definitsioon järgmisel kujul.

Definitsioon 2.1 **Rühm** on hulk G koos kahekohalise algebralise tehtega $*$, mis rahuldab järgmisi tingimusi:

G1. $(a * b) * c = a * (b * c)$ iga $a, b, c \in G$ korral;

G2. leidub element $e \in G$ nii, et $a * e = a = e * a$ iga $a \in G$ korral;

G3. iga $a \in G$ korral leidub element $b \in G$ nii, et $a * b = e = b * a$.

Elementi e tingimuses G2 nimetatakse selle rühma **ühikelemendiks**. Elementi b tingimuses G3 nimetatakse elemendi a **pöördelemendiks** ja tähistatakse sümboliga a^{-1}.

Rühma ühikelementi tähistatakse tihti ka sümboliga 1. Nii ühikelement kui iga elemendi pöördelement rühmas on üheselt määratud. Rühma tehet $*$ kutsutakse harilikult korrutamiseks ja $a * b$ asemel kirjutatakse ab. Seda teeme edasises ka meie. Meenutame veel, et rühma G mistahes elementide a, b korral

$$\left(a^{-1}\right)^{-1} = a \quad \text{ja} \quad (ab)^{-1} = b^{-1}a^{-1}.$$

Niisiis rühm on algebraline struktuur, millel on kolm algebralist tehet:

- kahekohaline tehe $(a, b) \mapsto ab$ (korrutamine),
- ühekohaline tehe $a \mapsto a^{-1}$ (pöördelemendi võtmine),
- nullkohaline tehe (ühikelemendi fikseerimine).

Näide 2.2 1. Iga $n \geq 2$ korral on $\mathbb{Z}_n$ rühm liitmise suhtes.

2. Iga hulga M korral on $\mathcal{S}(M) = \{f : M \longrightarrow M \mid f \text{ on bijektiivne}\}$ rühm teisenduste järjestrakendamise suhtes.

3. Iga $n \in \mathbb{N}$ korral on

$$GL_n(\mathbb{R}) = \{A \in Mat_n(\mathbb{R}) \mid \det(A) \neq 0\} \quad \text{ja} \quad SL_n(\mathbb{R}) = \{A \in Mat_n(\mathbb{R}) \mid \det(A) = 1\}$$

rühmad maatriksite korrutamise suhtes.

Lihtne on veenduda, et kehtib järgmine tulemus.

Lause 2.3 *Rühma G mittetühi alamhulk H on alamrühm parajasti siis, kui H on kinnine korrutamise ja pöördelemendi võtmise suhtes.*

Kui H on rühma G alamrühm, siis kirjutatakse $H \leq G$.

Definitsioon 2.4 Olgu H rühma G alamrühm ja $a \in G$. Hulka

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

($Ha = \{ha \mid h \in H\}$) nimetatakse rühma G **vasakpoolseks (parempoolseks) kõrvalklassiks alamrühma H järgi esindajaga** a.

Lause 2.5 *Olgu G rühm, $H \leq G$ ja $a, b \in G$. Siis järgmised väited on samaväärsed.*

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

TÕESTUS. 1 $\Rightarrow$ 2. Olgu $aH = bH$. Kuna $b \in bH = aH$, siis leidub selline $h \in H$, et $b = ah$. Järelikult $a^{-1}b = h \in H$.

2 $\Rightarrow$ 1. Oletame, et $a^{-1}b =: h \in H$. Siis $b = ah$, millest järeldub, et $bH \subseteq aH$. Kuna $b = ah$, siis $a = bh^{-1} \in bH$, millest järeldub sisalduvus $aH \subseteq bH$. Kokkuvõttes oleme tõestanud võrduse $aH = bH$.

Väidete 1 ja 3 samaväärsuse saab tõestada analoogiliselt. □

Järeldus 2.6 *Kui H on rühma G alamrühm ja $b \in G$, siis $H = bH$ parajasti siis, kui $b \in H$.*

Lause 2.7 *Olgu H rühma G alamrühm. Siis vasakpoolsed kõrvalklassid aH, $a \in G$ tekitavad hulga G tükelduse.*

TÕESTUS. Kuna $a \in aH$ 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 sama hulk. Selleks oletame, et leidub element $g = ah_1 = bh_2 \in aH \cap bH$. Siis $h_1 = a^{-1}bh_2$ ja $a^{-1}b = h_1h_2^{-1} \in H$. Lause 2.5 põhjal $aH = bH$. Sellega oleme näidanud, et tegemist on tükeldusega. □

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

Lause 2.8 *Olgu G rühm ja $H \leq G$. Siis iga $a \in G$ korral $|aH| = |H|$.*

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

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

$h \in H$. On selge, et f on sürjektiivne. Kui $ah = ah'$, $h, h' \in H$, siis korrutades selle võrduse mõlemaid pooli vasakult elemendiga a^{-1} saame $h = h'$. See tähendab, et f on injektiivne. Järelikult f on bijektiivne ja $|H| = |aH|$. □

Definitsioon 2.9 Lõpliku rühma **järguks** nimetatakse tema elementide arvu.

Teoreem 2.10 (Lagrange'i teoreem) *Lõpliku rühma iga alamrühma järk jagab rühma järku.*

TÕESTUS. Lause 2.8 põhjal teame, et kõik vasakpoolsed kõrvalklassid on sama võimsusega (võimsusega $|H|$). Samuti teame, et kõrvalklassid tekitavad hulga G tükelduse. Seega kui neid kõrvalklasse on m tükki, siis $|G| = m \cdot |H|$ ehk $|H|$ jagab arvu $|G|$. □

2.2 Normaaljagaja, faktorrühm

Definitsioon 2.11 Rühma G alamrühma H nimetatakse **normaalseks alamrühmaks** ehk **normaaljagajaks**, kui iga $g \in G$ korral $gH = Hg$.

Kui H on rühma G normaaljagaja, siis kirjutatakse $H \trianglelefteq G$.

Lause 2.12 *Rühma G alamrühm H on normaaljagaja parajasti siis, kui iga $g \in G$ ja $h \in H$ korral $g^{-1}hg \in H$.*

TÕESTUS. TARVILIKKUS. 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 $g^{-1}hg = h' \in H$.
PIISAVUS. Eeldame, et iga $g \in G$ ja $h \in H$ korral $g^{-1}hg \in H$. 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. □

Näide 2.13 Iga rühma G korral on alamrühmad G ja $\{1\}$ normaalsed. Neid normaaljagajaid nimetatakse **triviaalseteks**.

Näide 2.14 Kommutatiivse rühma kõik alamrühmad on normaaljagajad.

Näide 2.15 Rühma $GL_n(\mathbb{R})$ alamrühm $SL_n(\mathbb{R})$ on normaaljagaja.

Märkus 2.16 Üldiselt ei pruugi gH ja Hg võrdsed olla. Selle kohta võib näite leida raamatust [1] (näide 6.1.8).

Analoogiliselt lausega 1.14 saab tõestada järgmise tulemuse.

Lause 2.17 *Olgu G ja G' rühmad. Kujutus $f : G \to G'$ on rühmade homomorfism parajasti siis, kui*

$$f(ab) = f(a)f(b)$$

iga $a, b \in G$ korral.

Definitsioon 2.18 Olgu $f : G \to G'$ rühmade homomorfism. Hulka

$$\operatorname{Ker} f := \{a \in G \mid f(a) = 1\}$$

nimetatakse homomorfismi f **tuumaks**.

Lause 2.19 *Rühmade homomorfismi tuum on normaaljagaja.*

Tõestus. Olgu $f : G \to G'$ rühmade homomorfism, $a \in \operatorname{Ker} f$ ja $g \in G$. Siis

$$f(g^{-1}ag) = f(g^{-1})f(a)f(g) = f(g^{-1}) \cdot 1 \cdot f(g) = f(g^{-1}g) = f(1) = 1,$$

s.t. $g^{-1}ag \in \operatorname{Ker} f$. Järelikult $\operatorname{Ker} f \trianglelefteq G$ lause 2.12 põhjal. □

Saab näidata, et analoogiliselt vektorruumidega on rühma kongruentsid üksüheses vastavuses normaaljagajatega, kusjuures konguentsiklassideks on kõrvalklassid selle normaaljagaja järgi. Tänu normaaljagaja definitsioonile ei ole siin vahet, kas vaatleme vasakpoolseid või parempoolseid kõrvalklasse.

Olgu H rühma G normaaljagaja. Defineerime kõrvalklasside hulgal

$$G/H = \{aH \mid a \in G\}$$

korrutamise võrdusega

$$(aH)(bH) := (ab)H.$$

Osutub, et nii saame rühma, mille ühikelement on $1H = H$ ja kus elemendi aH pöördelemendiks on kõrvalklass $a^{-1}H$. Seda rühma nimetatakse rühma G **faktorrühmaks** normaaljagaja H järgi.

Saab näidata, et kujutus $\pi : G \to G/H, a \mapsto aH$ on rühmade homomorfism. Seda kujutust nimetatakse **loomulikuks projektsiooniks** faktorrühmale G/H.

Analoogiliselt teoreemiga 1.35 saab näidata, et kehtib järgmine teoereem.

Teoreem 2.20 (Homomorfismiteoreem) *Olgu $f : G \to G'$ rühmade homomorfism. Siis leidub üksühene homomorfism $g : G/\operatorname{Ker} f \to G'$ nii, et $f = g\pi$, kus $\pi : G \to G/\operatorname{Ker} f$ on loomulik projektsioon.*

Järeldus 2.21 *Kui $f : G \to G'$ on sürjektiivne rühmade homomorfism, siis $G' \cong G/\operatorname{Ker} f$.*

Näide 2.22 Kujutus

$$\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R} \setminus \{0\}, \quad A \mapsto \det(A)$$

on multiplikatiivsete rühmade homomorfism (Miks?), kusjuures $\operatorname{Ker}(\det) = \mathrm{SL}_n(\mathbb{R})$. See homomorfism on sürjektiivne, sest iga reaalarvu $r \in \mathbb{R} \setminus \{0\}$ jaoks leidub n-ndat järku ruutmaatriks (Milline?), mille determinant on r. Järelduse 2.21 põhjal võime öelda, et

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R} \setminus \{0\}.$$

2.3 Isomorfismiteoreemid

Selles paragrahvis tõestame kolm klassikalist teoreemi, mis käivad isomorfismide kohta teatud faktorrühmade vahel.

Kui H ja K on rühma G mingid alamhulgad siis tähistatakse

$$HK := \{hk \mid h \in H, k \in K\} \subseteq G\,.$$

Kui H ja K on G alamrühmad, siis HK ei pruugi veel olla G alamrühm. Küll aga saame alamrühma siis, kui vähemalt üks alamrühmadest H ja K on normaalne.

Lemma 2.23 *Kui G on rühm, $H \leq G$ ja $K \trianglelefteq G$, siis $HK \leq G$.*

Tõestus. Kontrollime lause 2.3 tingimusi. Kuna $1 = 11 \in HK$, siis $HK \neq \emptyset$.

Olgu $h_1k_1, h_2k_2 \in HK$, kus $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Kuna $k_1h_2 \in Kh_2 = h_2K$, siis leidub selline $k \in K$, et $k_1h_2 = h_2k$. Järelikult

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k)k_2 = (h_1h_2)(kk_2) \in HK.$$

Kui $hk \in HK$, siis

$$(hk)^{-1} = k^{-1}h^{-1} = (h^{-1}h)k^{-1}h^{-1} = h^{-1}((h^{-1})^{-1}k^{-1}h^{-1}) \in HK,$$

sest $h^{-1} \in H$ ja $(h^{-1})^{-1}k^{-1}h^{-1} \in K$. □

Lemma 2.24 *Kui G on rühm, $K \trianglelefteq G$ ja $K \subseteq H \leq G$, siis $K \trianglelefteq H$.*

Tõestus. On selge, et K on alamrühm rühmas H. Kuna $gK = Kg$ iga $g \in G$ korral, siis ka $hK = Kh$ iga $h \in H$ korral. See tähendab, et $K \trianglelefteq H$. □

Teoreem 2.25 (Esimene isomorfismiteoreem) *Olgu G rühm, $H \leq G$ ja $K \trianglelefteq G$. Siis*

$$H/(H \cap K) \cong HK/K.$$

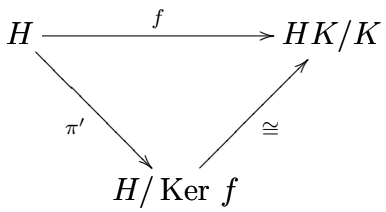
Tõestus. Lemma 2.23 põhjal $HK \leq G$. Kuna $K \trianglelefteq G$ ja $K \subseteq HK$, siis lemma 2.24 tõttu $K \trianglelefteq HK$ ja faktorrühm HK/K on olemas.

Defineerime kujutuse $f : H \to HK/K$ võrdusega

$$f(x) := xK$$

iga $x \in H$ korral. Kuna $f = \pi|_H$, kus $\pi : HK \to HK/K$ on loomulik projektsioon, siis f on homomorfism. Kui $(hk)K \in HK/K$, siis $f(h) = hK = h(kK) = (hk)K$, mis tähendab, et f on pealekujutus. Kasutades järeldust 2.21 võime öelda, et

$$H/\operatorname{Ker} f \cong HK/K.$$

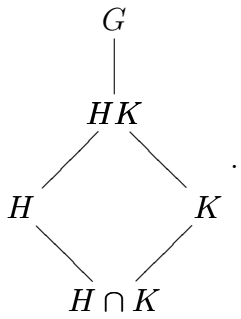


Kuna

$$x \in \operatorname{Ker} f \iff x \in H \wedge f(x) = K \iff x \in H \wedge xK = K$$
$$\iff x \in H \wedge x \in K \iff x \in H \cap K,$$

siis $\operatorname{Ker} f = H \cap K$. □

Märkus 2.26 Eelmises teoreemis esinevate alamrühmade vahelisi sisalduvusseoseid illustreerib järgmine diagramm (suuremad alamrühmad on ülevalpool):



Teoreem 2.27 (Teine isomorfismiteoreem) *Olgu G rühm, $H \trianglelefteq G$, $K \trianglelefteq G$ ja $K \subseteq H$. Siis*

$$(G/K)/(H/K) \cong G/H.$$

Tõestus. Kuna $K \trianglelefteq G$, siis ka $K \trianglelefteq H$. Seega on faktorrühmad G/K, H/K ja G/H olemas. Veendume, et $H/K \trianglelefteq G/K$. On selge, et $H/K \subseteq G/K$. Olgu $hK, h'K \in H/K$. Kuna $h, h' \in H$ ja $h^{-1} \in H$, siis ka $hh'K, h^{-1}K \in H/K$ ja seega on H/K alamrühm. Kui $g \in G$, siis $g^{-1}hg \in H$, sest $H \trianglelefteq G$. Järelikult

$$(g^{-1}K)(hK)(gK) = (g^{-1}hg)K \in H/K$$

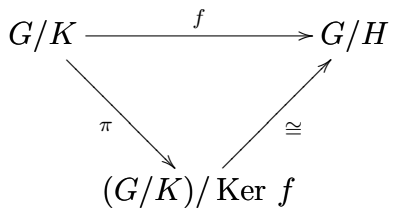
ja me oleme näidanud, et H/K on normaaljagaja rühmas G/K.

Defineerime nüüd kujutuse $f : G/K \to G/H$ võrdusega

$$f(gK) := gH,$$

$g \in G$. Oletame, et $g_1K = g_2K$. Siis $g_2^{-1}g_1 \in K \subseteq H$. Lause 2.5 põhjal $g_1H = g_2H$, mis näitab, et f on korrektselt defineeritud. Lihtne on näha, et f on sürjektiivne homomorfism. Järelduse 2.21 põhjal

$$(G/K)/\operatorname{Ker} f \cong G/H\,.$$



Kuna mistahes kõrvalklassi $gK \in G/K$ korral

$$gK \in \operatorname{Ker} f \iff f(gK) = H \iff gH = H \iff g \in H \iff gK \in H/K,$$

siis $\operatorname{Ker} f = H/K$ (need hulgad koosnevad samadest elementidest). Sellega on nõutud isomorfism tõestatud. □

Teoreem 2.28 (Kolmas isomorfismiteoreem) *Olgu G rühm, $H \trianglelefteq G$, $\pi : G \to G/H$ loomulik projektsioon, $N \trianglelefteq G/H$ ja $M = \pi^{-1}(N)$. Siis $M \trianglelefteq G$ ja*

$$G/M \cong (G/H)/N\,.$$

Tõestus. Kuna M on hulga N originaal kujutuse π suhtes, siis

$$M = \pi^{-1}(N) = \{x \in G \mid \pi(x) \in N\} = \{x \in G \mid xH \in N\}.$$

Et N on normaaljagaja faktorrühmas G/H, siis ta peab sisaldama faktorrühma ühikelementi H, s.t. $H \in N$. Kuna $hH = H \in N$ iga $h \in H$ korral, siis $H \subseteq M \subseteq G$.

Näitame, et $M \leq G$. Olgu $x, y \in M$, s.t. $xH, yH \in N$. Kuna N on G/H alamrühm, siis $(xy)H = (xH)(yH) \in N$ ja $x^{-1}H = (xH)^{-1} \in N$. Järelikult $xy, x^{-1} \in M$ ja M on alamrühm.

Veendume, et $M \trianglelefteq G$. Olgu $g \in G$ ja $x \in M$. Siis $xH \in N$ ja

$$(g^{-1}xg)H = (gH)^{-1}(xH)(gH) \in N,$$

sest N on normaaljagaja. Järelikult $g^{-1}xg \in M$ ja $M \trianglelefteq G$.

Kuna $H \trianglelefteq G$ ja $H \subseteq M$, siis $H \trianglelefteq M$. Veelgi enam,

$$M/H = \{xH \mid x \in M\} = \{xH \mid x \in G, xH \in N\} = N.$$

Teise isomorfismiteoreemi põhjal

$$(G/H)/N = (G/H)/(M/H) \cong G/M.$$

□

Märkus 2.29 Seoseid eelmises teoreemis esinevate alamrühmade vahel illustreerib järgnev diagramm:

$$\begin{array}{ccccc} H & \trianglelefteq & M & \trianglelefteq & G \\ & & \downarrow & & \downarrow \pi \\ \pi(M) = & & N & \trianglelefteq & G/H \end{array}\,.$$

Teoreem väljendab seda, et faktorrühma faktorrühmad on isomorfsed esialgse rühma faktorrühmadega.

2.4 Lihtsad rühmad

Definitsioon 2.30 Rühma nimetatakse **lihtsaks**, kui tal ei ole mittetriviaalseid normaaljagajaid.

Ülesanne 2.31 Näidake, et kui p on algarv, siis rühm $(\mathbb{Z}_p, +)$ on lihtne.

Selles paragrahvis on meie eesmärgiks näidata, et teatud substitutsioonide rühmad on lihtsad.

Meenutame, et **substitutsioon** n elemendist on hulga $\{1, 2, \ldots, n\}$ bijektiivne teisendus. Substitutsioone võib kirja panna kaherealiste tabelitena:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix},$$

kusjuures järjend $\langle \sigma(1), \sigma(2), \ldots, \sigma(n) \rangle$ peab olema **permutatsioon** arvudest $1, 2, \ldots, n$, s.t. nende arvude mingi ümberjärjestus. Sellist tabelit kutsume substitutsiooni σ **normaalkujuks**. Substitutsiooni

$$\varepsilon = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

nimetatakse **ühiksubstitutsiooniks**.

Substitutsiooni σ nimetatakse **paarissubstitutsiooniks**, kui inversioonide arv permutatsioonis $\langle \sigma(1), \sigma(2), \ldots, \sigma(n) \rangle$ on paarisarv. Vastasel korral on tegemist **paaritu substitutsiooniga**. Kõigi substitutsioonide hulka n elemendist tähistame sümboliga S_n ja kõigi paarissubstitutsioonide hulka sümboliga A_n. Algebra põhikursusest on teada, et S_n on rühm substitutsioonide korrutamise suhtes.

Definitsioon 2.32 Substitutsiooni nimetatakse **tsükliks**, kui ta paigutab mingeid elemente tsükliliselt ümber ning jätab ülejäänud elemendid paigale. Tsüklit σ, mis paigutab ümber elemente $i_1, i_2, \ldots, i_k$ nii, et

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \ldots,\ \sigma(i_{k-1}) = i_k,\ \sigma(i_k) = i_1,$$

tähistame lühidalt

$$(i_1, i_2, \ldots, i_k).$$

Arvu k nimetame tsükli $(i_1, i_2, \ldots, i_k)$ **pikkuseks**.

Definitsioon 2.33 Tsükleid $(i_1, i_2, \ldots, i_k)$ ja $(j_1, j_2, \ldots, j_l)$ nimetatakse **sõltumatuteks**, kui $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_l\} = \emptyset$.

Substitutsioonide korrutamisel on üldiselt tähtis, millises järjekorras me neid korrutame. Kui aga on tegemist kahe sõltumatu tsükliga, siis nende korrutamisel ei ole tegurite järjekord oluline, s.t. sõltumatud tsüklid kommuteeruvad.

Lihtne on aru saada, et kehtib järgmine lause.

Lause 2.34 *Iga substitutsiooni saab esitada sõltumatute tsüklite korrutisena.*

Näide 2.35 Rühmas S_9 saame esitada

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 9 & 7 & 4 & 2 & 1 & 8 & 3 \end{pmatrix} = (1,5,4,7)(2,6)(3,9)\,.$$

Definitsioon 2.36 Transpositsioon on tsükkel pikkusega 2.

Algebra põhikursuses tõestatakse harilikult järgmine tulemus.

Lause 2.37 ([1], lause 4.3.15) *Transpositsioon on paaritu substitutsioon.*

Lause 2.38 *Olgu $n \geq 2$. Iga paarissubstitutsioon n elemendist on esitatav paarisarvu transpositsioonide korrutisena. Iga paaritu substitutsioon n elemendist on esitatav paaritu arvu transpositsioonide korrutisena.*

Tõestus. Paneme tähele, et

$$\begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \sigma(1) & \dots & \sigma(i) & \dots & \sigma(j) & \dots & \sigma(n) \end{pmatrix}(i,j) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \sigma(1) & \dots & \sigma(j) & \dots & \sigma(i) & \dots & \sigma(n) \end{pmatrix}.$$

Seega normaalkujul oleva substitutsiooni σ korrutamisel transpositsiooniga (i,j) saame substitutsiooni σ', mille normaalkuju erineb σ normaalkujust selle poolest, et alumises permutatsioonis on i-s ja j-s element ära vahetatud. Algebra põhikursusest teame, et kahe elemendi äravahetamine permutatsioonis muudab permutatsiooni paarsust (vt. [1], lause 4.3.7). Järelikult σ ja σ' on erineva paarsusega.

Kõik permutatsioonid n elemendist on võimalik järjestada nii, et esimene on loomulik permutatsioon ja iga järgmine on saadud eelmisest kahe elemendi vahetamisel (vt. [1], lause 4.3.2). Moodustame nende permutatsioonide abil normaalkujul olevad substitutsioonid. Saame substitutsioonide järjestuse

$$\varepsilon = \sigma_0, \sigma_1, \sigma_2, \dots, \sigma_{n!-1},$$

kusjuures iga $k \in \{1,2,\dots,n!-1\}$ korral σ_k on ühiksubstitutsiooni ε ja k transpositsiooni korrutis. Kuna ε-ga korrutamine midagi ei muuda, siis iga σ_k on k transpositsiooni korrutis. Et σ_0 on paarissubstitutsioon, siis σ_1 on paaritu, σ_2 paaris jne. See tähendab, et kui σ_k on paarissubstitutsioon siis, ta on paarisarvu transpositsioonide korrutis ja kui σ_k on paaritu substitutsioon siis, ta on paaritu arvu transpositsioonide korrutis. □

Kuna $n!$ on paarisarv, kui $n \geq 2$, siis eelmise lause tõestusest järeldub järgmine fakt.

Järeldus 2.39 *Olgu $n \geq 2$. Siis on paaris- ja paarituid substitutsioone n elemendist ühepalju.*

Lause 2.40 *Olgu substitutsioon σ esitatav k transpositsiooni korrutisena. Siis σ on paarissubstitutsioon parajasti siis, kui k on paarisarv.*

TÕESTUS. Tõestame lause induktsiooniga transpositsioonide arvu k järgi.

Kui $k = 1$, siis σ on transpositsioon ja seega lause 2.37 põhjal paaritu substitutsioon.

Oletame, et $k > 1$ ja väide kehtib $k-1$ korral. Olgu $\sigma = \tau_1\tau_2 \dots \tau_{k-1} \cdot \tau_k$, kus τ_i-d on transpositsioonid. Induktsiooni eelduse põhjal on $\tau_1\tau_2 \dots \tau_{k-1}$ paarsus sama, mis $k-1$ paarsus. Transpositsiooniga τ_k korrutamine vahetab substitutsiooni $\tau_1\tau_2 \dots \tau_{k-1}$ normaalkuju alumises reas kaks elementi ära. Seega $\tau_1\tau_2 \dots \tau_{k-1}$ ja $\tau_1\tau_2 \dots \tau_{k-1}\tau_k$ on erineva paarsusega, nagu ka $k-1$ ja k. Järelikult $\tau_1\tau_2 \dots \tau_{k-1}\tau_k$ paarsus on sama, mis k paarsus. □

Järeldus 2.41 *Substitutsioonid σ ja σ^{-1} on sama paarsusega.*

TÕESTUS. Lause 2.38 tõestuses nägime, et iga substitutsiooni saab esitada transpositsioonide korrutisena. Olgu σ esitatud k transpositsiooni korrutisena ja σ^{-1} l transpositsiooni korrutisena. Kuna $\varepsilon = \sigma\sigma^{-1}$ on paarissubstitutsioon, siis lause 2.40 põhjal on $k+l$ paarisarv. Järelikult on k ja l sama paarsusega, millest järeldub, et σ ja σ^{-1} on sama paarsusega. □

Lause 2.42 *Tsükli $(i_1, i_2, \dots, i_k)$ paarsus on võrdne arvu $k-1$ paarsusega.*

TÕESTUS. Paneme tähele, et selle tsükli saab esitada $k-1$ transpositsiooni korrutisena:

$$(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_3)(i_1, i_2).$$

Lause 2.40 põhjal on tsükkel $(i_1, i_2, \dots, i_k)$ ja arv $k-1$ sama paarsusega. □

Lause 2.43 *Paarissubstitutsioonide hulk A_n on rühma S_n normaaljagaja.*

TÕESTUS. Näitame, et $A_n \leq S_n$. Kuna $\varepsilon \in A_n$, siis $A_n \neq \emptyset$.

Olgu $\sigma, \tau \in A_n$. Lause 2.38 põhjal saab σ ja τ esitada paarisarvu transpositsioonide korrutisena. Siis ka $\sigma\tau$ on paarisarvu transpositsioonide korrutis. Tänu lausele 2.40 on $\sigma\tau$ paarissubstitutsioon. Kuna pöördsubstitutsiooni paarsus on sama, mis esialgse oma, siis on A_n kinnine ka pöördelemendi võtmise suhtes.

Olgu nüüd $\sigma \in S_n$ ja $\tau \in A_n$, kusjuures σ on k transpositsiooni korrutis ja τ on $2l$ transpositsiooni korrutis. Kui σ^{-1} on m transpositsiooni korrutis, siis k ja m on sama paarsusega. Substitutsioon $\sigma^{-1}\tau\sigma$ on $m + 2l + k = 2l + m + k$ transpositsiooni korrutis, kus $m + k$ on paarisarv. Seega $\sigma^{-1}\tau\sigma$ on paarissubstitutsioon ehk $\sigma^{-1}\tau\sigma \in A_n$. □

Järeldus 2.44 *Kui $n \geq 3$, siis S_n ei ole lihtne.*

TÕESTUS. Kui $n \geq 3$, siis S_n sisaldab mittetriviaalset normaaljagajat A_n. □

Ülesanne 2.45 Millise hästituntud rühmaga on isomorfne faktorrühm S_n/A_n?

Teoreem 2.46 *Kui $n \geq 5$, siis A_n on lihtne rühm.*

TÕESTUS. Olgu N rühma A_n normaaljagaja, kusjuures $n \geq 5$ ja N sisaldab rohkem kui ühte elementi. Näitame, et sellisel juhul $N = A_n$. Kuna sisalduvus $N \subseteq A_n$ on ilmne, siis peame veenduma, et $A_n \subseteq N$. Tõestus jaguneb kolme ossa.

Esiteks näitame, et normaaljagaja N sisaldab vähemalt ühte 3-elemendilist tsüklit. Selleks võtame ühe substitutsiooni $\varphi \in N \setminus \{\varepsilon\}$. Siis ka $\varphi^{-1} \in N$ ning iga $\psi \in A_n$ korral

$$\psi\varphi^{-1}\psi^{-1}\varphi = \left((\psi^{-1})^{-1}\varphi^{-1}\psi^{-1}\right)\varphi \in N.$$

Olgu φ esitatud sõltumatute tsüklite korrutisena. Selle tsükliteks lahutuse puhul on järgmised võimalused.

1) Lahutuses leidub tsükkel, mille pikkus on vähemalt 4:

$$\varphi = (i_1, i_2, \ldots, i_s) \cdot \ldots,$$

kus $s \geq 4$. Võtame $\psi := (i_1, i_2, i_3) \in S_n$. Tänu lausele 2.42 on 3-elemendilised tsüklid paarissubstitutsioonid, seega $\psi \in A_n$. Järelikult $\psi\varphi^{-1}\psi^{-1}\varphi \in N$. Arvutame välja korrutise $\psi\varphi^{-1}\psi^{-1}\varphi$. Selleks peame arvudele $1, 2, \ldots, n$ rakendama järjest teisendusi $\varphi, \psi^{-1}, \varphi^{-1}$ ja ψ (just selles järjekorras). Paneme tähele, et kõik need teisendused jätavad arvud $j \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_s\}$ paigale, s.t. $(\psi\varphi^{-1}\psi^{-1}\varphi)(j) = j$. Vaatame, kuidas need teisendused teisendavad arve $i_1, i_2, \ldots, i_s$. Selleks koostame tabeli, kus iga rida näitab, kuidas vastav teisendus teisendab eelmises reas olevaid elemente:

$$\begin{array}{c|ccccccc} & i_1 & i_2 & i_3 & i_4 & \ldots & i_{s-1} & i_s \\ \varphi & i_2 & i_3 & i_4 & i_5 & \ldots & i_s & i_1 \\ \psi^{-1} & i_1 & i_2 & i_4 & i_5 & \ldots & i_s & i_3 \\ \varphi^{-1} & i_s & i_1 & i_3 & i_4 & \ldots & i_{s-1} & i_2 \\ \psi & i_s & i_2 & i_1 & i_4 & \ldots & i_{s-1} & i_3 \end{array}.$$

Võrreldes tabeli esimest ja viimast rida näme, et $\psi\varphi^{-1}\psi^{-1}\varphi = (i_1, i_s, i_3)$. Antud tabel vastab olukorrale, kus $s > 4$. Samamoodi saab näidata, et ka juhul $s = 4$ on $\psi\varphi^{-1}\psi^{-1}\varphi = (i_1, i_s, i_3)$. Järelikult N sisaldab tsüklit (i_1, i_s, i_3) pikkusega 3.

2) Lahutuses leidub vähemalt kaks 3-elemendilist tsüklit:

$$\varphi = (i_1, i_2, i_3)(j_1, j_2, j_3) \cdot \ldots.$$

Olgu $\psi := (i_3, j_1, j_2) \in A_n$. Analoogiliselt eelmise juhtumiga saame arvutada, et

$$\psi\varphi^{-1}\psi^{-1}\varphi = (i_2, j_2, i_3, j_1, j_3) \cdot \ldots \in N.$$

Sellega oleme vaadeldava olukorra taandanud juhule 1).

3) Lahutuses on üks 3-elemendiline tsükkel ja ülejäänud tsüklid on 2-elemendilised:

$$\varphi = (i_1, i_2, i_3)(j_1, j_2) \cdot \ldots.$$

Kuna iga transpositsiooni ruut on ε, siis $\varphi^2 = (i_1, i_3, i_2) \in N$.

4) Lahutuses on kõik tsüklid 2-elemendilised, kusjuures neid on vähemalt neli tükki:

$$\varphi = (i, j)(k, l)(a, b)(c, d) \cdot \ldots.$$

Olgu $\psi := (l,a)(b,c) \in A_n$. Sellisel juhul $\varphi^2 = \varepsilon$, $\psi^2 = \varepsilon$ ja

$$\psi\varphi^{-1}\psi^{-1}\varphi = \psi\varphi\psi\varphi = (k,c,b)(l,a,d)\cdot\ldots \in N.$$

Sellega on olukord taandatud juhule 2).

5) $\varphi = (i,j)(k,l)$. Kuna $n \geq 5$, siis leidub elementidest i,j,k,l erinev element m. Olgu $\psi := (i,j,m) \in A_n$. Siis

$$\psi\varphi^{-1}\psi^{-1}\varphi = (i,m,j) \in N.$$

Sellega oleme näidanud, et N peab sisaldama mingit 3-elemendilist tsüklit (i,j,k).

Teiseks näitame, et N sisaldab *kõiki* 3-elemendilisi tsükleid. Olgugi (i',j',k') suvaline kolmest elemendist koosnev tsükkel. Kuna $n \geq 5$, siis saab vaadelda paarissubstitutsiooni

$$\sigma = \begin{pmatrix} i' & j' & k' & l' & m' & \ldots \\ i & j & k & l & m & \ldots \end{pmatrix} \in A_n$$

(see, et $n \geq 5$, lubab vajaduse korral l ja m ära vahetada, et saada õige paarsus). Kuna N on normaaljagaja ja $(i,j,k) \in N$, siis $\sigma^{-1}\cdot(i,j,k)\cdot\sigma \in N$ ehk

$$(i',j',k') = \begin{pmatrix} i & j & k & l & m & \ldots \\ i' & j' & k' & l' & m' & \ldots \end{pmatrix}(i,j,k)\begin{pmatrix} i' & j' & k' & l' & m' & \ldots \\ i & j & k & l & m & \ldots \end{pmatrix} \in N.$$

Seega N sisaldab kõiki 3-elemendilisi tsükleid.

Tõestuse lõpetamiseks näitame, et $A_n \subseteq N$. Olgu $\psi \in A_n$ suvaline paarissubstitutsioon. Lause 2.38 põhjal on ψ esitatav paarisarvu transpositsioonide korrutisena:

$$\psi = \tau_1\tau_2\tau_3\tau_4\ldots\tau_{2s-1}\tau_{2s},$$

kus kõik tegurid on transpositsioonid. Jagame need transpositsioonid järjest paarideks. Kui paaris on transpositsioonid kujul (i,j) ja (i,k), siis $(i,j)(i,k) = (i,k,j)$. Kui paaris on sõltumatud transpositsioonid (i,j) ja (k,l), siis $(i,j)(k,l) = (i,k,j)(k,l,i)$. Seega saame ψ esitada 3-elemendiliste tsüklite korrutisena. Kuna kõik need tsüklid kuuluvad N-i, siis ka $\psi \in N$. □

Märkus 2.47 Saab näidata, et A_2 ja A_3 on lihtsad rühmad, aga A_4 ei ole.

Peatükk 3

Abeli rühm

3.1 Põhimõisted

Lühidalt öeldes on Abeli rühm selline rühm, mille tehe on kommutatiivne. Kuna Abeli rühmade puhul kasutatakse enamasti aditiivset sümboolikat ja terminoloogiat (räägitakse summast, nullelemendist, vastandelemendist), siis toome siin definitsiooni ära ka täispikkuses.

Definitsioon 3.1 Abeli rühm on hulk A koos kahekohalise algebralise tehtega $+$, mis rahuldab järgmisi tingimusi:

AG1. $(a+b)+c = a+(b+c)$ iga $a, b, c \in A$ korral;

AG2. leidub element $0 \in A$ nii, et $a+0 = a = 0+a$ iga $a \in A$ korral;

AG3. iga $a \in A$ korral leidub element $-a \in A$ nii, et $a+(-a) = 0 = (-a)+a$;

AG4. $a+b = b+a$ iga $a, b \in A$ korral.

Näide 3.2 1. Iga vektorruum on muuhulgas Abeli rühm.
2. Iga $n \geq 2$ korral on $(\mathbb{Z}_n, +)$ Abeli rühm.
3. Iga $n \geq 3$ korral S_n on rühm, mis ei ole Abeli rühm.

Abeli rühma korral räägitakse ka elementide a ja b **vahest**, mis defineeritakse võrdusega

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

Tingimuse AG3 põhjal on selge, et iga a korral

$$a - a = 0.$$

Kui $(A, +)$ on Abeli rühm, siis võib defineerida naturaalarvu n ja elemendi a korrutise:

$$na := a + a + \ldots + a,$$

kus liidetavaid on n tükki. Lisaks sellele loetakse, et

$$(-n)a = (-a) + (-a) + \ldots + (-a),$$

kus samuti on n liidetavat, ja et $0a = 0$. Sellega on defineeritud korrutis za iga $z \in \mathbb{Z}$ jaoks. Selliste korrutiste jaoks kehivad muuhulgas järgmised omadused: iga $z, w \in \mathbb{Z}$ ja $a, b \in A$ korral

$$(zw)a = z(wa),$$
$$(z + w)a = za + wa,$$
$$z(a + b) = za + zb,$$

Abeli rühma iga alamrühm on normaaljagaja, seega faktorrühmi saab moodustada kõigi alamrühmade järgi.

Abeli rühmade otsekorrutised ja välised otsesummad defineeritakse nii nagu vektorruumide otsekorrutised ja välised otsesummad.

3.2 Jaguvate Abeli rühmade lihtsamad omadused

Hakkame uurima Abeli rühmade klassi ühte olulist alamklassi — jaguvaid Abeli rühmi.

Definitsioon 3.3 Abeli rühma A nimetatakse **jaguvaks**, kui iga elemendi $a \in A$ ja iga naturaalarvu n korral leidub selline $b \in A$, et $nb = a$. Elementi b nimetatakse elemenedi a ja naturaalarvu n **jagatiseks**.

Näide 3.4 1. Rühma $(\mathbb{Z}, +)$ ei ole jaguv.

2. Rühm $(\mathbb{Q}, +)$ on jaguv.

Lemma 3.5 *Abeli rühm A on jaguv parajasti siis, kui iga elemendi $a \in A$ ja iga algarvu p korral leidub selline $b \in A$, et $pb = a$.*

Tõestus. Tarvilikkus. See on ilmne.
Piisavus. Olgu $a \in A$ ja $n > 1$ naturaalarv. Aritmeetika põhiteoreemi abil saab arvu n esitada kujul $n = p_1 p_2 \dots p_s$, kus $p_1, p_2, \dots, p_s$ on algarvud. Eelduse põhjal leiduvad elemendid $b_1, \dots, b_s \in A$ nii, et

$$a = p_1 b_1,\ b_1 = p_2 b_2,\ \dots,\ b_{s-1} = p_s b_s\,,$$

kust $a = p_1 \dots p_s b_s = nb_s$. □

Me ütleme, et Abeli rühm B on Abeli rühma A **epimorfne kujutis**, kui leidub sürjektiivne homomorfism $f : A \to B$.

Lemma 3.6 *Jaguva Abeli rühma epimorfne kujutis on jaguv.*

Tõestus. Vt. [2, lemma 2.3]. □

Lemma 3.7 *Jaguvate Abeli rühmade otsekorrutis ja väline otsesumma on jaguvad.*

Tõestus. Vt. [2, lemma 2.4]. □

Defineerime nüüd Abeli rühma alamrühmade summa ja sisemise otsesumma.

Definitsioon 3.8 Olgu A Abeli rühm ja $A_i, i \in I$ tema alamrühmad. Nende alamrühmade **summaks** nimetatakse alamrühma $\sum_{i\in I} A_i$, mis koosneb kõigist lõplikest summadest, kus liidetavateks on paarikaupa erinevate indeksitega alamrühmade elemendid, s.t.

$$\sum_{i\in I} A_i = \{a \in A \mid a = a_{i_1} + \ldots + a_{i_k}, k \in \mathbb{N}, i_1, \ldots, i_k \in I \text{ on paarikaupa erinevad},$$
$$a_{i_1} \in A_{i_1}, \ldots, a_{i_k} \in A_{i_k}\}.$$

Lõpliku indeksite hulga $I = \{i_1, \ldots, i_n\}$ korral kirjutatakse $\sum_{i\in I} A_i$ asemel $A_{i_1} + \ldots + A_{i_n}$ ja kehtib võrdus

$$A_{i_1} + \ldots + A_{i_n} = \{a_1 + \ldots + a_n \mid a_1 \in A_{i_1}, \ldots, a_n \in A_{i_n}\}.$$

Definitsioon 3.9 Abeli rühma A alamrühmade $A_i, i \in I$ summat $\sum_{i\in I} A_i$ nimetatakse **sisemiseks otsesummaks**, kui iga lõpliku alamhulga $\{i_0, i_1, \ldots, i_n\} \subseteq I$ korral

$$A_{i_0} \cap (A_{i_1} + \ldots + A_{i_n}) = \{0\}.$$

Kui alamrühmade $A_i, i \in I$ summa on sisemine otsesumma, siis kirjutatakse

$$\sum_{i\in I} A_i = \dot{\sum_{i\in I}} A_i.$$

Märgime, et siin antud definitsioon erineb raamatus [1] antud definitsioonist 3.5.9, kuid on tollega samaväärne.

Näide 3.10 Abeli rühm $(\mathbb{C}, +)$ on oma alamrühmade $\mathbb{R}$ ja $\mathbb{R}i = \{bi \mid b \in \mathbb{R}\}$ otsesumma, $\mathbb{C} = \mathbb{R} \dot{+} \mathbb{R}i$, sest $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ ja $\mathbb{R} \cap \mathbb{R}i = \{0\}$.

Teoreem 3.11 ([1], teoreem 2.7.13) *Olgu A Abeli rühm ja $A_i, i \in I$ tema alamrühmad. Kui nende alamrühmade sisemine otsesumma on olemas, siis on sisemine ja väline otsesumma isomorfsed.*

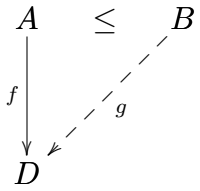
Kui tegemist on kahe alamrühmaga B ja C, siis kasutatakse summa ja sisemise otsesumma jaoks tähistusi $B + C$ ja $B \dot{+} C$.

Lause 3.12 *Abeli rühma A alamrühmade B ja C summa $B + C$ on sisemine otsesumma parajasti siis, kui iga $b, b' \in B$ ja $c, c' \in C$ korral*

$$b + c = b' + c' \implies b = b' \text{ ja } c = c'$$

Tõestus. Tarvilikkus. Olgu $B + C = B \dot{+} C$ ja oletame, et $b + c = b' + c'$, kus $b, b' \in B$ ja $c, c' \in C$. Siis $b - b' = c' - c \in B \cap C = \{0\}$. Järelikult $b' - b = 0 = c' - c$ ehk $b = b'$ ja $c = c'$.
Piisavus. Oletame, et $a \in B \cap C$. Siis võrdusest $a + 0 = 0 + a$ järeldub eelduse tõttu, et $a = 0$. Seega $B \cap C = \{0\}$ ja $B + C = B \dot{+} C$. □

Lause 3.13 *Olgu B Abeli rühm, $A \leq B$ ja olgu $f : A \to D$ mingi homomorfism, kusjuures D on jaguv Abeli rühm. Siis leidub homomorfism $g : B \to D$ nii, et $g|_A = f$.*



Tõestus. Kasutame tõestuseks Zorni lemmat. Vaatleme paaride hulka

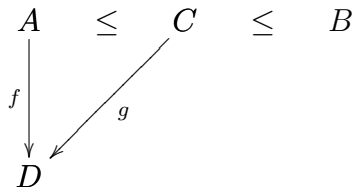
$$P = \{(X, h) \mid A \leq X \leq B, h \in \hom(X, D), h|_A = f\}.$$

Kuna $(A, f) \in P$, siis P ei ole tühi. Defineerime seose $\leq$ hulgal P järgmiselt:

$$(X_1, h_1) \leq (X_2, h_2) \iff X_1 \subseteq X_2 \text{ ja } h_2|_{X_1} = h_1.$$

Lihtne on kontrollida, et see seos on järjestusseos.

Saab näidata, et järjestatud hulk $(P, \leq)$ rahuldab Zorni lemma eeldusi. Zorni lemma põhjal leidub hulgas P maksimaalne element. Olgu selleks paar (C, g).



On kaks võimalust.

a) $C = B$. Sellisel juhul on meil teoreem tõestatud.

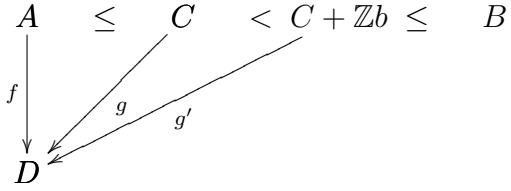
b) $A \leq C < B$. Näitame, et sellisel juhul tekib vastuolu.

Kuna $C \subset B$, siis leidub $b \in B \setminus C$. Vaatleme alamrühma $\mathbb{Z}b = \{zb \mid z \in \mathbb{Z}\} \leq B$. Siis $C < C + \mathbb{Z}b \leq B$. Vastuolu (C, g) maksimaalsusega saame, kui õnnestub defineerida homomorfism $g' : C + \mathbb{Z}b \to D$ nii, et $g'|_C = g$, sest siis ka $g'|_A = f$. Tuleb vaadelda kahte juhtumit.

1) Kui $C + \mathbb{Z}b = C \dot{+} \mathbb{Z}b$, siis võib defineerida

$$g'(c + zb) := g(c),$$

$c \in C$, $z \in \mathbb{Z}$. Lause 3.12 tõttu on see definitsioon korrektne. Lihtne on näha, et g' on homomorfism ja $g'|_C = g$.



2) Oletame, et $C + \mathbb{Z}b$ ei ole alamrühmade C ja $\mathbb{Z}b$ otsesumma. Siis $C \cap \mathbb{Z}b \neq \{0\}$. Olgu n vähim naturaalarv, mille korral $nb \in C$ (selline peab kindlasti leiduma). Kuna $g(nb) \in D$ ja D on jaguv, siis leidub $d \in D$ nii, et $nd = g(nb)$. Kasutades seda elementi d defineerime kujutuse $g' : C + \mathbb{Z}b \to D$ võrdusega

$$g'(c + zb) := g(c) + zd$$

iga $c \in C$ ja $z \in \mathbb{Z}$ korral. Veendume, et g' on korrektselt defineeritud. Selleks oletame, et $c_1 + z_1 b = c_2 + z_2 b$. Siis

$$(z_1 - z_2)b = c_2 - c_1 \in C.$$

Jagame täisarvu $z_1 - z_2$ jäägiga naturaalarvuga n:

$$z_1 - z_2 = qn + r, \quad 0 \leq r < n\,, \quad q, r \in \mathbb{Z}\,.$$

Siis $(z_1 - z_2)b = qnb + rb$. Et $nb \in C$, siis ka $qnb \in C$. Kuna $(z_1 - z_2)b, qnb \in C$ ja C on alamrühm, siis ka $rb = (z_1 - z_2)b - qnb \in C$, kust n valiku tõttu saame, et $r = 0$ ehk $z_1 - z_2 = qn$. Järelikult $(z_1 - z_2)b = qnb$ ja

$$\begin{aligned} g(c_2) - g(c_1) = g(c_2 - c_1) &= g((z_1 - z_2)b) = g(qnb) \\ &= q \cdot g(nb) = qnd = (z_1 - z_2)d = z_1 d - z_2 d, \end{aligned}$$

kust

$$g(c_1) + z_1 d = g(c_2) + z_2 d.$$

Sellega oleme tõestanud, et g' definitsioon on korrektne.

Näitame, et g' on homomorfism. Kui $c_1 + z_1 b, c_2 + z_2 b \in C + \mathbb{Z}b$, siis

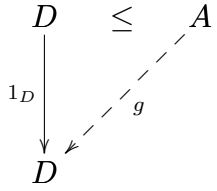
$$\begin{aligned} g'((c_1 + z_1 b) + (c_2 + z_2 b)) &= g'((c_1 + c_2) + (z_1 + z_2)b) = g(c_1 + c_2) + (z_1 + z_2)d \\ &= g(c_1) + g(c_2) + z_1 d + z_2 d = g(c_1) + z_1 d + g(c_2) + z_2 d \\ &= g'(c_1 + z_1 b) + g'(c_2 + z_2 b). \end{aligned}$$

On selge, et $g'|_C = g$. Kokkuvõttes olemegi saanud vastuolu sellega, et paar (C, g) on maksimaalne element hulgas P. □

Osutub, et jaguvad alamrühmad Abeli rühmades on otseliidetavad.

Lause 3.14 *Kui jaguv Abeli rühm D on Abeli rühma A alamrühm, siis leidub rühma A alamrühm B nii, et $A = D \dotplus B$.*

TÕESTUS. Lause 3.13 põhjal leidub homomorfism $g : A \to D$ nii, et $g|_D = 1_D$.



Siis $\mathrm{Ker}\,(g)$ on rühma A alamrühm. Näitame, et

$$A = D \dotplus \mathrm{Ker}\,(g).$$

Mistahes elemendi $a \in A$ võib esitada summana

$$a = g(a) + (a - g(a)),$$

kus $g(a) \in D$ ja $a - g(a) \in \mathrm{Ker}\,(g)$, sest

$$g(a - g(a)) = g(a) - g(g(a)) = g(a) - 1_D(g(a)) = g(a) - g(a) = 0.$$

Seega $A = D + \mathrm{Ker}\,(g)$. Oletame, et $d \in D \cap \mathrm{Ker}\,(g)$. Kuna $d \in D$, siis $g(d) = d$. Et aga $d \in \mathrm{Ker}\,(g)$, siis $g(d) = 0$. Järelikult $d = 0$ ja me oleme tõestanud, et $D \cap \mathrm{Ker}\,(g) = \{0\}$. Seega A on alamrühmade D ja $\mathrm{Ker}\,(g)$ otsesumma. □

3.3 Elementide järkudest

Meenutame Abeli rühma elemendi järgu mõistet.

Definitsioon 3.15 Olgu a Abeli rühma A element ja $n \in \mathbb{N}$. Öeldakse, et elemendi a **järk** on n, kui $na = 0$ ja n on vähim naturaalarv, mille korral selline võrdus kehtib. Kui $na \neq 0$ ühegi naturaalarvu n korral, siis öeldakse, et element a on **lõpmatut järku**. Elemendi a järku tähistatakse sümboliga $\mathrm{ord}(a)$.

On selge, et

$$\mathrm{ord}(a) = 1 \Longleftrightarrow a = 0.$$

Lemma 3.16 *Kui A on Abeli rühm, $a \in A$ ja $m \in \mathbb{N}$, siis*

$$ma = 0 \Longleftrightarrow \mathrm{ord}(a) \mid m.$$

Tõestus. Tarvilikkus. Olgu $ma = 0$ ja $n = \mathrm{ord}(a)$. Jagame jäägiga:

$$m = nq + r, \;\; 0 \leq r < n, \;\; q, r \in \mathbb{Z}\,.$$

Siis

$$0 = ma = (nq + r)a = nqa + ra = qna + ra = q0 + ra = ra.$$

Kui $r \neq 0$, siis saaksime vastuolu sellega, et $n = \mathrm{ord}(a)$. Järelikult $r = 0$ ehk $nq = m$ ehk $n \mid m$.
Piisavus. Oletame, et $n = \mathrm{ord}(a) \mid m$. Siis leidub selline $q \in \mathbb{N}$, et $nq = m$. Järelikult $ma = nqa = qna = q0 = 0$. □

Definitsioon 3.17 Abeli rühma **perioodiline osa** on tema alamhulk, mis koosneb tema kõigist lõplikku järku elementidest. Abeli rühma nimetatakse **perioodiliseks**, kui kõik tema elemendid on lõplikku järku.

Definitsioon 3.18 Kui A on Abeli rühm ja p on algarv, siis hulka

$$A_p = \{a \in A \mid \text{ord}(a) \text{ on } p \text{ aste}\} \subseteq A$$

nimetatakse rühma A **p-komponendiks**. Saab näidata, et A_p on A alamrühm (vt. [1], lemma 11.2.3). Kui $A = A_p$, siis öeldakse, et A on **p-rühm**.

Lemma 3.19 *Iga mittetriviaalne Abeli p-rühm sisaldab elementi, mille järk on p.*

TÕESTUS. Olgu A mittetriviaalne Abeli p-rühm. Siis leidub nullist erinev element $a \in A$. Olgu $\text{ord}(a) = p^k$, kus $k \in \mathbb{N}$. Siis $p(p^{k-1}a) = 0$. Olgu $n = \text{ord}(p^{k-1}a)$. Siis lemma 3.16 põhjal $n \mid p$. Kuna p on algarv, siis on kaks võimalust. Kui oletaksime, et $n = 1$, siis $p^{k-1}a = 0$, mis on vastuaolus sellega, et $\text{ord}(a) = p^k$. Järelikult $n = p$, mis tähendab, et otsitavaks p-ndat järku elemendiks sobib $p^{k-1}a$. □

Tähistame sümboliga $\mathbb{P}$ kõigi algarvude hulka.

Teoreem 3.20 *Perioodiline Abeli rühm on oma p-komponentide sisemine otsesumma.*

TÕESTUS. Näitame, et

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

Selleks tõestame, et $A \subseteq \sum_{p\in\mathbb{P}} A_p$ (vastupidine sisalduvus on ilmne). Olgu $a \in A$ suvaline element ja olgu tema järk n. Kui $n = 1$, siis $a = 0$ ja $a \in \sum_{p\in\mathbb{P}} A_p$. Kui $n \neq 1$, siis aritmeetika põhiteoreemi põhjal $n = p_1^{k_1} \dots p_s^{k_s}$, kus $p_1, \dots, p_s$ on paarikaupa erinevad algarvud ja $k_1, \dots, k_s$ on naturaalarvud. Tähistame $n_i := \frac{n}{p_i^{k_i}}$. Siis $\text{SÜT}(n_1, \dots, n_s) = 1$. Arvuteooriast on teada, et sellises olukorras 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 $p_i^{k_i}(u_i n_i a) = (p_i^{k_i} u_i n_i)a = (u_i n)a = u_i(na) = 0$, 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. Olgu $q, p_1, \dots, p_s$ erinevad algarvud ja oletame, et $a \in A_q \cap (A_{p_1} + \dots + A_{p_s})$. Et $a \in A_q$, siis $\text{ord}(a) = q^k$ mingi $k \in \mathbb{N} \cup \{0\}$ korral. Teisest küljest $a \in A_{p_1} + \dots + A_{p_s}$ ja seega leiduvad 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 $na = na_{p_1} + \dots + na_{p_s} = 0$. Lemmast 3.16 järeldub, 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 $A_q \cap (A_{p_1} + \dots + A_{p_s}) = \{0\}$. Definitsiooni 3.9 põhjal on A oma alamrühmade A_p, $p \in \mathbb{P}$, sisemine otsesumma. □

Näide 3.21 Vaatleme jäägiklassirühma $A = (\mathbb{Z}_{12}, +)$. Kuna $12 = 2^2 \cdot 3$ ja selle rühma elementide järgud peavad jagama arvu 12, siis on selles rühmas olemas ainult mittetriviaalne 2-komponent ja 3-komponent. Seega $A = A_2 \dot{+} A_3$, kus

$$A_2 = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \quad \text{ja} \quad A_3 = \{\overline{0}, \overline{4}, \overline{8}\}.$$

3.4 Väändeta jaguvad rühmad

Selles paragrahvis anname väändeta jaguvate Abeli rühmade kirjelduse (vt. teoreemi 3.27).

Definitsioon 3.22 Öeldakse, et Abeli rühm on **väändeta**, kui kõik tema nullist erinevad elemendid on lõpmatut järku.

Näide 3.23 Rühmad $(\mathbb{Z},+)$ ja $(\mathbb{Q},+)$ on väändeta.

Lemma 3.24 *Olgu B väändeta Abeli rühm. Siis*

1. $(\forall b,c\in B)(\forall x\in\mathbb{Z}\setminus\{0\})(xb=xc\Longrightarrow b=c)$,
2. $(\forall b\in B\setminus\{0\})(\forall x\in\mathbb{Z})(xb=0\Longrightarrow x=0)$,
3. $(\forall b\in B\setminus\{0\})(\forall x,y\in\mathbb{Z})(xb=yb\Longrightarrow x=y)$.

TÕESTUS. 1. Olgu $xb=xc$. Siis $x(b-c)=0$. Seega element $b-c$ on lõplikku järku. Et B on väändeta, siis $b-c=0$ ehk $b=c$.

2. Kui $x>0$, siis võrdus $xb=0$ tähendaks vastuolu sellega, et $\mathrm{ord}(b)=\infty$. Kui $x<0$ ja $xb=0$, siis ka $0=-(xb)=(-x)b$, kus $-x>0$, ning jällegi oleks tegemist vastuoluga. Seega peab kehtima võrdus $x=0$.

3. Kui $xb=yb$, siis $(x-y)b=xb-yb=0$. Eelmise osa tõttu $x-y=0$ ehk $x=y$. □

Olgu B jaguv väändeta Abeli rühm. Siis on iga $c\in B$ ja $n\in\mathbb{N}$ korral elemendi c ja arvu n jagatis üheselt määratud. Tõepoolest, kui $nd_1=c=nd_2$, kus $d_1,d_2\in B$, siis lemma 3.24 esimese osa põhjal $d_1=d_2$. Me tähistame seda üheselt määratud jagatist sümboliga c/n. Niisiis

$$(\forall c,d\in B)(\forall n\in\mathbb{N})(c/n=d\Longleftrightarrow nd=c).$$

Lemma 3.25 *Olgu B väändeta jaguv Abeli rühm. Siis iga $c,d\in B$, $x\in\mathbb{Z}$ ja $m,n\in\mathbb{N}$ korral*

1. $x(c/n)=(xc)/n$;
2. $c/n+d/n=(c+d)/n$;
3. $(mc)/mn=c/n$.

TÕESTUS. 1. Tähistame $d:=c/n$ ja $e:=(xc)/n$. Siis $nd=c$ ja $ne=xc$. Järelikult $ne=xc=xnd=nxd$, kust lemma 3.24(1) abil saame, et $e=xd$, mida oligi vaja näidata.

2. Tähistame $c_1:=c/n$, $d_1:=d/n$ ja $e:=(c+d)/n$. Siis $nc_1=c$, $nd_1=d$ ja $ne=c+d=nc_1+nd_1=n(c_1+d_1)$. Järelikult $e=c_1+d_1$.

3. Olgu $d:=(mc)/mn$. Siis $mnd=mc$, kust $nd=c$. Järelikult $d=c/n$. □

Lause 3.26 *Mittetriviaalne väändeta jaguv rühm sisaldab rühmaga $\mathbb{Q}$ isomorfset alamrühma.*

TÕESTUS. Olgu $B \neq \{0\}$ väändeta jaguv rühm. Siis leidub mingi nullist erinev element $b \in B$. Vaatleme hulka

$$Q(b) = \{(xb)/n \mid x \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq B.$$

Defineerime kujutuse $f : \mathbb{Q} \to B$ võrdusega

$$f\left(\frac{x}{n}\right) := (xb)/n,$$

$x \in \mathbb{Z}$, $n \in \mathbb{N}$. Kuna mistahes $x, y \in \mathbb{Z}$, $n, m \in \mathbb{N}$ korral

$$\begin{aligned}
\frac{x}{n} = \frac{y}{m} &\iff mx = ny && \text{(hulgas } \mathbb{Z}) \\
&\iff (mx)b = (ny)b && \text{(rühmas } B) \\
&\iff m(xb) = nyb && \text{(rühmas } B) \\
&\iff (nyb)/m = xb && \text{(rühmas } B) \\
&\iff n \cdot (yb)/m = xb && \text{(rühmas } B) \\
&\iff (xb)/n = (yb)/m, && \text{(rühmas } B)
\end{aligned}$$

siis näeme, et f on korrektselt defineeritud ja injektiivne.

Et mistahes $x, y \in \mathbb{Z}$ ja $m, n \in \mathbb{N}$ korral

$$\begin{aligned}
f\left(\frac{x}{n} + \frac{y}{m}\right) = f\left(\frac{mx+ny}{nm}\right) &= (mx+ny)b/nm = (mxb+nyb)/nm \\
&= (mxb)/nm + (nyb)/nm = (xb)/n + (yb)/m = f\left(\frac{x}{n}\right) + f\left(\frac{y}{m}\right),
\end{aligned}$$

siis f on rühmade homomorfism. Lause 1.17 põhjal on $\operatorname{Im} f = Q(b)$ rühma B alamrühm. Kuna kujutus $\mathbb{Q} \longrightarrow Q(b)$, $\frac{x}{n} \mapsto (xb)/n$ on isomorfism, siis $Q(b) \cong \mathbb{Q}$ ja B sisaldab rühmaga $\mathbb{Q}$ isomorfset alamrühma. □

Teoreem 3.27 *Mittetriviaalne väändeta jaguv rühm on rühmaga $\mathbb{Q}$ isomorfsete alamrühmade otsesumma.*

TÕESTUS. Olgu B mittetriviaalne väändeta jaguv rühm. Võtame hulga P, mille elementideks on sellised rühma B alamrühmade hulgad, millesse kuuluvad alamrühmad on isomorfsed rühmaga $\mathbb{Q}$ ja millesse kuuluvate alamrühmade summa on otsesumma. Vaatleme hulka P osaliselt järjestatud hulgana sisalduvusseose suhtes ja näitame, et ta rahuldab Zorni lemma eeldusi.

Tänu lausele 3.26 sisaldab hulk P üheelemendilist hulka $\{Q(b)\}$ ja on seega mittetühi. Vaatleme P elementide ahelat $\{X_i \mid i \in I\}$. Olgu $X := \cup_{i \in I} X_i$. Siis X on rühmaga $\mathbb{Q}$ isomorfsete B alamrühmade mingi hulk. Kasutades definitsiooni 3.9 näitame, et hulka X kuuluvate alamrühmade summa on otsesumma (siis X on vaadeldava ahela ülemine tõke hulgas P).

Peame näitama, et suvaliste $Q, Q_1, \ldots, Q_n \in X$ korral $Q \cap (Q_1 + \ldots + Q_n) = \{0\}$. Teame, et $Q, Q_1, \ldots, Q_n$ on B alamrühmad, mis on isomorfsed rühmaga $\mathbb{Q}$. Lisaks sellele leiduvad indeksid $i_0, i_1, \ldots, i_n \in I$ nii, et $Q \in X_{i_0}$, $Q_1 \in X_{i_1}, \ldots, Q_n \in X_{i_n}$. Kuna

$\{X_i \mid i \in I\}$ on ahel, siis leidub indeks $r \in \{i_0, i_1, \ldots, i_n\}$ nii, et $X_{i_0}, X_{i_1}, \ldots, X_{i_n} \subseteq X_r$. Seega $Q, Q_1, \ldots, Q_n \in X_r$. Et hulka X_r kuuluvate B alamrühmade summa on sisemine otsesumma, siis

$$Q \cap (Q_1 + \ldots + Q_n) = \{0\}.$$

Zorni lemma põhjal leidub hulgas P maksimaalne element. Seega rühmas B leidub alamrühm D, mis on rühmaga $\mathbb{Q}$ isomorfsete alamrühmade otsesumma ning ühegi alamrühma $\mathbb{Q} \cong Q \leq B$, $Q \not\subseteq D$ korral summa $D + Q$ ei ole otsesumma. Kuna $\mathbb{Q}$ on jaguv ja jaguvate rühmade otsesumma on ka jaguv, siis lause 3.7 põhjal D on jaguv. Vastavalt lausele 3.14 leidub alamrühm $C \leq B$ nii, et

$$B = D \dot{+} C.$$

Kuna C on jaguva rühma B epimorfne kujutis (võib vaadelda sürjektiivset homomorfismi $B \to C,\ d+c \mapsto c$), siis C on jaguv tänu lemmale 3.6. Olles väändeta rühma B alamrühm on ka C väändeta. Kui $C \neq \{0\}$, siis ta peaks lause 3.26 tõttu sisaldama mingit alamrühma Q, mis on isomorfne rühmaga $\mathbb{Q}$. Siis aga $D + Q$ oleks otsesumma, mis annab vastuolu. Järelikult $C = \{0\}$ ning $B = D$ on rühmaga $\mathbb{Q}$ isomorfsete alamrühmade otsesumma. □

Näide 3.28 Rühm $\mathbb{Q} \times \mathbb{Q}$ (komponenthaaval defineeritud liitmise suhtes) on väändeta jaguv rühm, sest ta on rühmaga $\mathbb{Q}$ isomorfsete alamrühmade

$$Q_1 = \{(a, 0) \mid a \in \mathbb{Q}\} \quad \text{ja} \quad Q_2 = \{(0, b) \mid b \in \mathbb{Q}\}$$

sisemine otsesumma, $\mathbb{Q} \times \mathbb{Q} = Q_1 \dot{+} Q_2$.

Peatükk 4

Ringid

4.1 Põhimõisted

Definitsioon 4.1 Hulka R koos kahe kahekohalise algebralise tehtega $+$ ja $\cdot$ nimetatakse (ühikelemendiga assotsiatiivseks) **ringiks**, kui

R1. $(a+b)+c = a+(b+c)$ iga $a, b, c \in R$ korral;

R2. leidub element $0 \in R$ nii, et $a+0 = a = 0+a$ iga $a \in R$ korral;

R3. iga $a \in R$ korral leidub element $-a \in R$ nii, et $a+(-a) = 0 = (-a)+a$;

R4. $a+b = b+a$ iga $a, b \in R$ korral;

R5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ iga $a, b, c \in R$ korral;

R6. leidub element $1 \in R$ nii, et $a \cdot 1 = a = 1 \cdot a$ iga $a \in R$ korral;

R7. $a \cdot (b+c) = a \cdot b + a \cdot c$ iga $a, b, c \in R$ korral;

R8. $(a+b) \cdot c = a \cdot c + b \cdot c$ iga $a, b, c \in R$ korral.

Niisiis ringidel on kaks kahekohalist tehet, üks ühkeohaline tehe ja kaks nullkohalist tehet (mis fikseerivad elemendid 0 ja 1).

Harilikult kirjutatakse ringi puhul $a \cdot b$ asemel lühemalt ab. Definitsiooni tingimustest R1–R4 näeme, et $(R, +)$ on Abeli rühm ja $(R, \cdot)$ on monoid. Tingimusi R7 ja R8 kutsutakse **distributiivsuse seadusteks**.

Definitsioon 4.2 Ringi $(R, +, \cdot)$ nimetatakse

- **jagamisega ringiks**, kui $(R \setminus \{0\}, \cdot)$ on rühm;
- **korpuseks**, kui $(R \setminus \{0\}, \cdot)$ on Abeli rühm.

Lihtne on kontrollida, et kehtib järgmine lause.

Lause 4.3 *Mistahes ringis R kehtivad järgmised arvutusreeglid:*

1. *iga* $a, b, c \in R$ *korral kui* $a + b = c$, *siis* $a = c - b$;
2. $0a = 0 = a0$ *iga* $a \in R$ *korral;*
3. $(-a)b = a(-b) = -(ab)$ *iga* $a, b \in R$ *korral;*
4. $a(b - c) = ab - ac$ *iga* $a, b, c \in R$ *korral;*
5. $(a - b)c = ac - bc$ *iga* $a, b, c \in R$ *korral.*

Märkus 4.4 Ringi puhul on võimalik, et $1 = 0$. Sellisel juhul see ring koosnebki ainult ühest elemendist, sest mistahes elemendi a korral $a = a1 = a0 = 0$. Järelikult, kui ringis on vähemalt kaks elementi, siis selles ringis $1 \neq 0$. Muuhulgas korpuses on alati $1 \neq 0$.

Lause 4.5 *Olgu* R_1 *ja* R_2 *ringid. Kujutus* $f : R_1 \to R_2$ *on ringide homomorfism parajasti siis, kui*

1. $f(a + b) = f(a) + f(b)$ *iga* $a, b \in R_1$ *korral;*
2. $f(ab) = f(a)f(b)$ *iga* $a, b \in R_1$ *korral;*
3. $f(1) = 1$.

Tõestus. Nii nagu lause 1.14 tõestuses saab ka siin näidata, et liitmise säilitamisest järeldub nullelemendi ja vastandelemendi säilitamine. □

Definitsioon 4.6 Ringide homomorfismi $f : R_1 \to R_2$ **tuumaks** nimetatakse hulka

$$\mathrm{Ker}\,(f) = \{a \in R_1 \mid f(a) = 0\}.$$

Nii nagu vektorruumidegi korral saab näidata, et kehtib järgmine tulemus.

Lause 4.7 *Ringide homomorfism* $f : R_1 \to R_2$ *on üksühene parajasti siis, kui* $\mathrm{Ker}\,(f) = \{0\}$.

Definitsioon 4.8 Ringi R mittetühja alamhulka I nimetatakse **parempoolseks (vasakpoolseks) ideaaliks**, kui

1. $a + b \in I$ iga $a, b \in I$ korral;
2. $ar \in I$ $(ra \in I)$ iga $a \in I$ ja $r \in R$ korral.

Parempoolset ideaali, mis on samaaegselt ka vasakpoolne ideaal, nimetatakse **ideaaliks**.

Mistahes ringi R korral on R ise ja $\{0\}$ ideaalid. Neid ideaale nimetatakse **triviaalseteks**.

Näide 4.9 Vaatame ringis $R = \mathrm{Mat}_n(S)$, kus S on mingi ring, alamhulka I, mis koosneb sellistest ruutmaatriksitest, kus nullist erinevad elemendid võivad esineda ainult esimeses reas. Seega

$$I = \left\{ \begin{pmatrix} a_{11} & \dots & a_{1n} \\ 0 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 0 \end{pmatrix} \mid a_{11}, \dots, a_{1n} \in S \right\}.$$

Lihtne on veenduda, et I on ringi R parempoolne ideaal.

Lause 4.10 *Ringide homomorfismi tuum on ideaal.*

Tõestus. Selle jätame läbimõtlemiseks lugejale. □

Lemma 4.11 *Olgu R ring ja $a \in R$. Siis*

1. *hulk*
$$aR = \{ar \mid r \in R\}$$
on ringi R parempoolne ideaal,

2. *hulk*
$$Ra = \{ra \mid r \in R\}$$
on ringi R vasakpoolne ideaal,

3. *hulk*
$$RaR = \left\{ \sum_{i=1}^{n} x_i a y_i \mid n \in \mathbb{N}, x_i, y_i \in R \right\}$$
on ringi R ideaal.

Tõestus. Tõestame neist väidetest ainult kolmanda (teiste tõestus on sarnane). On selge, et hulk RaR on kinnine liitmise suhtes. Kui $n \in \mathbb{N}$, $x_1, \dots, x_n, y_1, \dots, y_n, r \in R$, siis distributiivsuse ja assotsiatiivsuse tõttu ka

$$r \left(\sum_{i=1}^{n} x_i a y_i \right) = \sum_{i=1}^{n} (r x_i) a y_i \in RaR \quad \text{ja} \quad \left(\sum_{i=1}^{n} x_i a y_i \right) r = \sum_{i=1}^{n} x_i a (y_i r) \in RaR\,.$$

Seega rahuldab RaR ka definitsiooni 4.8 teist tingimust ja on ideaal. □

Definitsioon 4.12 Ideaale aR, Ra ja RaR nimetatakse vastavalt ringi R elemendi a poolt tekitatud **parempoolseks peaideaaliks**, **vasakpoolseks peaideaaliks** ja **(kahepoolseks) peaideaaliks**.

Lihtne on veenduda, et kehtib järgmine tulemus.

Lemma 4.13 *Ringi parempoolsete ideaalide (vasakpoolsete ideaalide, ideaalide) ühisosa on samuti parempoolne ideaal (vasakpoolne ideaal, ideaal).*

Lause 4.14 *Ringis, mis sisaldab vähemalt kahte elementi, ei ole mittetriviaalseid parempoolseid ideaale parajasti siis, kui see ring on jagamisega ring.*

TÕESTUS. TARVILIKKUS. Eeldame, et ringi R ainsad parempoolsed ideaalid on $\{0\}$ ja R. Kui $a \in R \setminus \{0\}$, siis hulk $aR = \{ar \mid r \in R\}$ on parempoolne ideaal ja $aR \neq \{0\}$. Järelikult $aR = R$. Muuhulgas leidub element $b \in R$ nii, et $ab = 1$. Me näitasime, et ringi R kõik nullist erinevad elemendid on paremalt pööratavad.

Olgu nüüd $x \in R \setminus \{0\}$ suvaline. Siis leidub $y \in R$ nii, et $xy = 1$. Kuna $0 \neq 1$, siis $y \neq 0$. Järelikult leidub $z \in R$ nii, et $yz = 1$. Seega

$$x = x1 = x(yz) = (xy)z = 1z = z$$

ehk x on elemendi y pöördelement. Järelikult ka y on x pöördelement ehk x on pööratav. Seega R on jagamisega ring.

PIISAVUS. Oletame, et $\{0\} \neq I$ on ringi R parempoolne ideaal. Näitame, et $I = R$. Selleks peame veenduma, et $R \subseteq I$.

Olgu $a \in I \setminus \{0\}$. Kuna ring on jagamisega, siis leidub $a^{-1} \in R$. Et I on parempoolne ideaal, siis $1 = aa^{-1} \in I$ ja seega ka $r = 1r \in I$ iga $r \in R$ korral. Olemegi näidanud, et $R \subseteq I$. □

Definitsioon 4.15 Ringi nimetatakse **lihtsaks**, kui temas ei ole mittetriviaalseid ideaale.

On selge, et kui ringis ei ole mittetriviaalseid parempoolseid ideaale, siis ei ole temas ka mittetriviaalseid ideaale, s.t. ta on lihtne. Vastupidine ei pruugi kehtida: lihtsas ringis võib leiduda mittetriviaalseid parempoolseid ideaale.

Lause 4.16 *Olgu D jagamisega ring ja $n \in \mathbb{N}$. Siis ring $\mathrm{Mat}_n(D)$ on lihtne.*

TÕESTUS. Olgu I ringi $\mathrm{Mat}_n(D)$ nullist erinev ideaal. Peame näitama, et $I = \mathrm{Mat}_n(D)$. Selleks võtame suvalise maatriksi $B = (b_{ij}) \in \mathrm{Mat}_n(D)$ ja näitame, et $B \in I$.

Kuna $I \neq \{0\}$, siis leidub maatriks $A = (a_{ij}) \in I$, mis ei ole nullmaatriks. Järelikult leiduvad sellised indeksid k ja l, et $a_{kl} \neq 0$. Tähistame sümboliga E_{ij} n-ndat järku ruutmaatriksi, kus kohla (i, j) on ringi D ühikelement 1 ja ülejäänud elemendid on nullid. Siis $E_{ik}A \in I$, kus nullist erinevad elemendid on vaid i-ndas reas, ja

$$M_i := (E_{ik}A)(a_{kl}^{-1}E_{li}) \in I,$$

kusjuures M_i on maatriks, milles kohal (i, i) on 1 ja kõik ülejäänud elemendid on nullid. Järelikult ka

$$E = M_1 + M_2 + \ldots + M_n \in I \quad \text{ja} \quad B = BE \in I.$$

□

4.2 Lihtsad minimaalse parempoolse ideaaliga ringid

Definitsioon 4.17 Ringi R parempoolset ideaali I nimetatakse **minimaalseks parempoolseks ideaaliks**, kui I on minimaalne element ringi R nullist erinevate parempoolsete ideaalide hulgas.

Seega parempoolne ideaal I on minimaalne, kui mistahes parempoolse ideaali J korral

$$J \neq \{0\} \text{ ja } J \subseteq I \Longrightarrow J = I.$$

Lause 4.18 *Olgu D jagamisega ring ja $n \in \mathbb{N}$. Siis ring $\mathrm{Mat}_n(D)$ sisaldab minimaalset parempoolset ideaali.*

Tõestus. Olgu I selliste maatriksite hulk, milles nullist erinevad elemendid esinevad ainult esimeses reas. Nagu mainisime näites 4.9 on I ringi $\mathrm{Mat}_n(D)$ parempoolne ideaal.

Näitame, et I on minimaalne. Selleks vaatleme parempoolset ideaali $\{0\} \neq J \subseteq I$. Tähistame sümboliga $E_{ij}(c)$ maatriksit ringist $\mathrm{Mat}_n(D)$, kus kohal (i, j) on element c ja kõik ülejäänud elemendid on nullid. Kuna $J \neq \{0\}$, siis leidub selline maatriks $A = (a_{ij}) \in J$, mis ei ole nullmaatriks. Seega peab tema esimeses reas leiduma mingi nullist erinev element, olgu see a_{1j}. Siis

$$AE_{ji}(a_{1j}^{-1}) = E_{1i}(1) \in J$$

iga $i \in \{1, \ldots, n\}$ korral. Võttes suvalise maatriksi $B = (b_{ij}) \in I$ näeme, et

$$B = E_{11}(1) \cdot b_{11}E + E_{12}(1) \cdot b_{12}E + \ldots + E_{1n}(1) \cdot b_{1n}E \in J,$$

sest J on parempoolne ideaal. Seega $I \subseteq J$, kust $I = J$. □

Ülesanne 4.19 Kas ringis $\mathrm{Mat}_n(D)$ võib olla mitu erinevat minimaalset parempoolset ideaali? Kui jah, siis tooge näide mõnest sellisest minimaalsest parempoolsest ideaalist, mis erineb lause 4.18 tõestuses antust.

Tuleb välja, et maatriksringid üle jagamisega ringide ongi ainsad lihtsad ringid, mis sisaldavad vähemalt ühte minimaalset parempoolset ideaali.

Teoreem 4.20 *Ring R on lihtne minimaalset parempoolset ideaali sisaldav ring parajasti siis, kui leidub jagamisega ring D ja naturaalarv n nii, et*

$$R \cong \mathrm{Mat}_n(D).$$

Tõestus. Piisavus. See järeldub lausest 4.16 ja lausest 4.18.
Tarvilikkus. Olgu R lihtne ring, mis sisaldab minimaalset parempoolset ideaali M. Siis $M \neq \{0\}$ ja seega leidub mingi element $x \in M \setminus \{0\}$. Et $0 \neq 1x1 \in RxR$ ja RxR on ideaal, siis lihtsuse tõttu $RxR = R$. Muuhulgas $1 \in RxR$ ja seega

$$1 = \sum_{i=1}^{t} x_i x y_i \tag{4.1}$$

mingite $t \in \mathbb{N}$, $x_i, y_i \in R$ korral. Et

$$0 \neq x = \sum_{i=1}^{t} x x_i x y_i,$$

siis leidub mingi $k \in \{1, \ldots, t\}$ nii, et liidetav $x x_k x y_k \neq 0$. Tähistades $a = x x_k \in M$ ja $b = x y_k \in M$ oleme saanud sellised elemendid $a, b \in M$, et $ab \neq 0$. Järelikult

$$aM = \{am \mid m \in M\} \neq \{0\}.$$

Hulk $aM \subseteq R$ on ilmselt kinnine liitmise suhtes. Kui $am \in aM$ ja $r \in R$, siis $mr \in M$ (sest M on parempoolne ideaal) ja seega $(am)r = a(mr) \in aM$. Järelikult aM on ringi R parempoolne ideaal. Kuna $a \in M$ ja M on parempoolne ideaal, siis ka $am \in M$ iga $m \in M$ korral, s.t. $aM \subseteq M$. Et M on minimaalne parempoolne ideaal, siis

$$M = aM.$$

Vaatleme hulka

$$I = \{r \in R \mid ar = 0\} \subseteq R.$$

Kui $r_1, r_2 \in I$, siis $a(r_1 + r_2) = ar_1 + ar_2 = 0 + 0 = 0$. Järelikult $r_1 + r_2 \in I$. Kui $r \in I$, siis iga $s \in R$ korral $a(rs) = (ar)s = 0s = 0$ ja seega $rs \in I$. Järelikult I on ringi R parempoolne ideaal.

Näitame, et

$$M \cap I = \{0\}.$$

Oletame vastuväiteliselt, et $M \cap I \neq \{0\}$. Tänu lemmale 4.13 on $M \cap I$ ringi R parempoolne ideaal. Kuna $\{0\} \subset M \cap I \subseteq M$ ja M on minimaalne, siis $M \cap I = M$ ehk $M \subseteq I$. Siis aga $am = 0$ iga $m \in M$ korral, mis on vasuolus sellega, et $ab \neq 0$, kus $b \in M$. Seega $M \cap I = \{0\}$.

Kuna $M = aM$, siis elemendi $a \in M$ jaoks leidub selline $e \in M$, et $a = ae$. Siis aga

$$a(e^2 - e) = ae^2 - ae = (ae)e - ae = ae - ae = 0,$$

kust näeme, et $e^2 - e \in I$. Järelikult $e^2 - e \in M \cap I = \{0\}$ ehk $e^2 = e$. (Sellist elementi, mille ruut võrdub selle elemendi endaga, nimetatakse idempotendiks.) Seega e on idempotent.

Kuna $a \neq 0$ ja $a = ae$, siis ka $e \neq 0$. Seega $\{0\} \subset eR \subseteq M$, kust M minimaalsuse tõttu järeldub, et

$$M = eR.$$

Kui $m \in M$, siis leidub selline $r \in R$, et $m = er$. Siis aga $em = e(er) = er = m$. See tähendab, et

$$(\forall m \in M)(em = m)\,.$$

Olgu

$$D := eRe = \{exe \mid x \in R\} \subseteq R\,.$$

Veendume, et D on ring tehete suhtes, mis on defineeritud samamoodi nagu ringi R tehted. Kui $x_1, x_2 \in R$, siis

$$\begin{aligned} &ex_1e + ex_2e = e(x_1e + x_2e) = e(x_1 + x_2)e \in D,\\ &(ex_1e)(ex_2e) = e(x_1ex_2)e \in D,\\ &-ex_1e = e(-x_1)e \in D,\\ &0 = e0e \in D,\\ &e = eee \in D. \end{aligned}$$

Seega liitmine ja korrutamine on algebralised tehted hulgal D, 0 on liitmise suhtes nullelement ja igal elemendil hulgast D leidub hulgas D vastandelement liitmise suhtes. On selge, et liitmine on assotsiatiivne ja kommutatiivne hulgal D, korrutamine on assotsiatiivne ja kehtivad distributiivsuse seadused. Kuna $e(exe) = exe = (exe)e$ iga $x \in R$ korral, siis e on ühikelement korrutamise suhtes. Niisiis D on tõepoolest ring. Veendume, et ta on jagamisega ring.

Olgu $0 \neq exe \in D$. Kuna $M = eR$, siis $exe \in M$ ja $\{0\} \subset (exe)R \subseteq M$, kust M minimaalsuse tõttu saame, et $M = (exe)R$. Järelikult leidub selline $y \in R$, et $e = (exe)y$. Siis aga

$$e = e^2 = exeye = ex(ee)ye = (exe)(eye).$$

Paneme tähele, et $eye \neq 0$, sest muidu oleks $e = 0$. Analoogilise mõttekäiguga saame eye jaoks leida sellise $eze \in D$, et $(eye)(eze) = e$. Siis aga

$$exe = exee = (exe)((eye)(eze)) = ((exe)(eye))(eze) = eeze = eze.$$

Kuna $(exe)(eye) = e$ ja $(eye)(exe) = e$, siis eye on elemendi exe pöördelement ringis D. Seega D on jagamisega ring.

Osutub, et me võime hulka $M = eR$ vaadelda vektorruumina üle jagamisega ringi $D = eRe$. Liitmistehtena vaatleme ringis R defineeritud liitmist ning skalaari exe ja vektori er korrutise defineerime võrdusega

$$(exe)(er) := exer \in M.$$

Lihtne on aru saada, et kõik vektorruumi tingimused on täidetud.

Uurime nüüd vektorruumi M kõigi lineaarteisenduste ringi $\mathrm{End}_D(M)$. Lineaarteisenduse $\varphi : M \to M$ rakendamise tulemust vektorile $m \in M$ tähistame sümboliga $m\varphi$. Antud tähistustega tähendab lineaarteisenduseks olemine seda, et

$$\begin{aligned} (m + m')\varphi &= m\varphi + m'\varphi,\\ (dm)\varphi &= d(m\varphi) \end{aligned}$$

iga $m, m' \in M$ ja $d \in D$ korral. Hulgal $\mathrm{End}_D(M)$ defineerime liitmise ja korrutamistehte $\bullet$ järgmiselt:

$$\begin{aligned} m(\varphi + \psi) &:= m\varphi + m\psi,\\ m(\varphi \bullet \psi) &:= (m\varphi)\psi \end{aligned}$$

mistahes $\varphi, \psi \in \mathrm{End}_D(M)$ ja $m \in M$ korral. Juhime tähelepanu, et teisenduste liitmine siin käib nii nagu harilikult, aga teisenduste korrutamine erineb harilikust korrutamisest, mis on defineeritud võrdusega

$$(\psi \circ \varphi)(m) := \psi(\varphi(m)).$$

Täpsemalt öeldes, $m(\varphi \bullet \psi) = (\psi \circ \varphi)(m)$ iga $m \in M$ korral ehk

$$\varphi \bullet \psi = \psi \circ \varphi.$$

Saab näidata, et $(\mathrm{End}_D(M), +, \bullet)$ on ring, kusjuures tema ühikelemendiks on samasusteisendus 1_M.

Meie eesmärk on näidata, et ring R on isomorfne ringiga $(\mathrm{End}_D(M), +, \bullet)$. Selleks defineerime kujutuse

$$g : R \to \mathrm{End}_D(M)$$

võrdusega

$$g(r) := \rho_r,$$

kus

$$\rho_r : M \to M, \quad m \mapsto mr.$$

Kuna M on parempoolne ideaal, siis $mr \in M$ iga $m \in M$ ja $r \in R$ korral. Lihnte on veenduda, et ρ_r on vektorruumi M lineaarteisendus. Näitame, et g on ringide isomorfism.

1) Olgu $r_1, r_2 \in R$. Siis iga $m \in M$ korral

$$\begin{aligned} mg(r_1 + r_2) &= m\rho_{r_1+r_2} = m(r_1 + r_2) = mr_1 + mr_2 = m\rho_{r_1} + m\rho_{r_2} \\ &= mg(r_1) + mg(r_2) = m(g(r_1) + g(r_2)), \end{aligned}$$

kust $g(r_1 + r_2) = g(r_1) + g(r_2)$.

2) Olgu $r_1, r_2 \in R$. Siis iga $m \in M$ korral

$$\begin{aligned} mg(r_1 r_2) &= m\rho_{r_1 r_2} = m(r_1 r_2) = (mr_1)r_2 = (mr_1)\rho_{r_2} \\ &= (m\rho_{r_1})\rho_{r_2} = m(\rho_{r_1} \bullet \rho_{r_2}) = m(g(r_1) \bullet g(r_2)), \end{aligned}$$

kust $g(r_1 r_2) = g(r_1) \bullet g(r_2)$.

3) Kuna

$$mg(1) = m\rho_1 = m1 = m = m1_M$$

iga $m \in M$ korral, siis $g(1) = 1_M$. Sellega on näidatud, et g on ringide homomorfism.

4) Näitame, et g on üksühene. Selleks oletame vastuväiteliselt, et $\mathrm{Ker}\,(g) \neq \{0\}$. Kuna $\mathrm{Ker}\,(g)$ on ringi R ideaal ja R on lihtne, siis peab $\mathrm{Ker}\,(g) = R$. Sel juhul $g(r) = 0$ ($g(r)$ on vektorruumi M nullteisendus) iga $r \in R$ korral. Muuhulgas $e = e\rho_1 = eg(1) = e0 = 0$, mis on vastuolu.

5) Veendume, et g on pealekujutus. Võtame suvalise $\varphi \in \mathrm{End}_D(M)$. Võrduses (4.1) võime elemendi x asendada korrutisega ex, sest $x \in M$. Seega

$$1 = \sum_{i=1}^{t} x_i e x y_i. \tag{4.2}$$

Olgu

$$r := \sum_{i=1}^{t} (x_i e)((exy_i)\varphi) \in R.$$

Eespool nägime, et $m = em$ iga $m \in M$ korral. Saame arvutada:

$$\begin{aligned}
m\rho_r &= mr && (\rho_r \text{ def.})\\
&= m\left(\sum_{i=1}^{t} (x_i e)((exy_i)\varphi)\right) && (r \text{ def.})\\
&= \sum_{i=1}^{t} (mx_i e)((exy_i)\varphi) && (R \text{ distributiivsus ja assotsiatiivsus})\\
&= \sum_{i=1}^{t} (emx_i e)((exy_i)\varphi) && (m = em)\\
&= \sum_{i=1}^{t} ((emx_i e)(exy_i))\varphi && (\varphi \text{ on lineaarteisendus, LK2})\\
&= \left(\sum_{i=1}^{t} (emx_i e)(exy_i)\right)\varphi && (\varphi \text{ on lineaarteisendus, LK1})\\
&= \left(\sum_{i=1}^{t} mx_i exy_i\right)\varphi && (m = em, e^2 = e, R \text{ assotsiatiivsus})\\
&= \left(m\left(\sum_{i=1}^{t} x_i exy_i\right)\right)\varphi && (R \text{ distributiivsus})\\
&= (m1)\varphi && (\text{võrdus } (4.2))\\
&= m\varphi\,. && (1 \text{ on ühikelement})
\end{aligned}$$

Seega $\varphi = \rho_r = g(r)$ ja g on pealekujutus. Oleme tõestanud, et g on ringide isomorfism.

Nüüd on kaks võimalust.

a) M on lõpmatumõõtmeline vektorruum üle D. Kuna R on lihtne, siis on ka $\mathrm{End}_D(M)$ lihnte ring. Vaatleme hulka

$$I = \{\varphi \in \mathrm{End}_D(M) \mid \dim(\mathrm{Im}\,(\varphi)) < \infty\}.$$

On selge, et $\{0\} \subseteq I \subseteq \mathrm{End}_D(M)$. Konstrueerime vastuolu lihtsusega näidates, et I on mittetriviaalne ideaal ringis $\mathrm{End}_D(M)$.

Kuna $\mathrm{Im}\,(1_M) = M$ on lõpmatumõõtmeline, siis $1_M \notin I$ ja seega $I \neq \mathrm{End}_D(M)$. Olgu $\{e_k \mid k \in K\}$, kus K on mingi indeksite hulk, vektorruumi M baas. Eelduse tõttu peab see baas olema lõpmatu. Fikseerime selles ühe vektori e_l, $l \in K$. Iga vektor $m \in M$ peab üheselt avalduma kujul

$$m = d_1 e_{k_1} + \ldots + d_n e_{k_v},$$

kus $v \in \mathbb{N}$, $d_1, \ldots, d_v \in D$ ja $e_{k_1}, \ldots, e_{k_v}$ on paarikaupa erinevad baasivektorid. Defineerime teisenduse $\varphi : M \to M$ võrdusega

$$\varphi(m) := \begin{cases} d_j e_{k_j}, & \text{kui leidub } j \in \{1, \ldots, v\} \text{ nii, et } k_j = l, \\ 0, & \text{vastasel juhul.} \end{cases}$$

Saab näidata, et φ on lineaarteisendus, kusjuures $\mathrm{Im}\,(\varphi) = De_l = \{de_l \mid d \in D\}$ ja seega $\dim(\mathrm{Im}\,(\varphi)) = 1$. Järelikult $\varphi \in I$. Kuna φ ei ole nullkujutus, siis $I \neq \{0\}$.

Näitame, et I on ringi $\mathrm{End}_D(M)$ ideaal. Veendume, et I on kinnine liitmise suhtes. Olgu $\varphi, \psi \in I$, s.t. $\mathrm{Im}\,(\varphi)$ ja $\mathrm{Im}\,(\psi)$ on lõplikumõõtmelised. Siis on ka nende alamruumide summa $\mathrm{Im}\,(\varphi) + \mathrm{Im}\,(\psi)$ lõplikumõõtmeline. Samas

$$\mathrm{Im}\,(\varphi + \psi) \subseteq \mathrm{Im}\,(\varphi) + \mathrm{Im}\,(\psi),$$

sest iga $m \in M$ korral $m(\varphi+\psi) = m\varphi+m\psi$. Järelikult ka $\mathrm{Im}\,(\varphi+\psi)$ on lõplikumõõtmeline ehk $\varphi + \psi \in I$.

Olgu nüüd $\varphi \in I$ ja $\psi \in \mathrm{End}_D(M)$. Siis alamruumis $\mathrm{Im}\,(\varphi)$ leidub mingi lõplik baas $\{e'_1, \ldots, e'_u\}$. Olgu $m \in \mathrm{Im}\,(\varphi \bullet \psi)$. Siis leidub $m' \in M$ nii, et $m = (m'\varphi)\psi$. Kuna $m'\varphi \in \mathrm{Im}\,(\varphi)$, siis leiduvad $d_1 \ldots, d_u \in D$ nii, et $m'\varphi = d_1e'_1 + \ldots + d_ue'_u$. Järelikult

$$m = (d_1e'_1 + \ldots + d_ue'_u)\psi = d_1(e'_1\psi) + \ldots + d_u(e'_u\psi).$$

Siit näeme, et alamruumil $\mathrm{Im}\,(\varphi \bullet \psi)$ leidub lõplik moodustajate süsteem $e'_1\psi, \ldots, e'_u\psi$, seega leidub tal ka lõplik baas (lõplikust moodusatajate süsteemist saab alati lõpliku baasi välja eraldada). Järelikult $\varphi\bullet\psi \in I$. Kuna $\mathrm{Im}\,(\psi\bullet\varphi) \subseteq \mathrm{Im}\,(\varphi)$, siis ka alamruum $\mathrm{Im}\,(\psi\bullet\varphi)$ on lõplikumõõtmeline. Järelikult $\psi\varphi \in I$. Sellega on tõestatud, et I on ringi R ideaal ja kuna ta on mittetriviaalne, siis oleme saanud vastuolu.

b) M on lõplikumõõtmeline vektorruum üle D. Siis on temas olemas mingi lõplik baas $B = \{e_1, \ldots, e_n\}$. Iga lineaarteisenduse $\varphi \in \mathrm{End}_D(M)$ korral võib vaadelda selle teisenduse maatriksit A^B_φ baasi B suhtes. See on n-ndat järku ruutmaatriks üle D, mille i-ndas veerus on vektori $\varphi(e_i)$ koordinaadid baasi B suhtes. Defineerime kujutuse

$$f : \mathrm{End}_D(M) \to \mathrm{Mat}_n(D)$$

võrdusega

$$f(\varphi) := \left(A^B_\varphi\right)^T.$$

Lineaaralgebrast teame, et

$$A^B_\varphi + A^B_\psi = A^B_{\varphi+\psi}, \quad A^B_{\varphi\circ\psi} = A^B_\varphi A^B_\psi, \quad A^B_{1_M} = E,$$

kui $\varphi, \psi \in \mathrm{End}_D(M)$. Järelikult

$$\begin{aligned} f(\varphi + \psi) &= \left(A^B_{\varphi+\psi}\right)^T = \left(A^B_\varphi + A^B_\psi\right)^T = \left(A^B_\varphi\right)^T + \left(A^B_\psi\right)^T = f(\varphi) + f(\psi), \\ f(\varphi \bullet \psi) &= \left(A^B_{\varphi\bullet\psi}\right)^T = \left(A^B_{\psi\circ\varphi}\right)^T = \left(A^B_\psi A^B_\varphi\right)^T = \left(A^B_\varphi\right)^T \left(A^B_\psi\right)^T = f(\varphi)f(\psi), \\ f(1_M) &= \left(A^B_{1_M}\right)^T = E^T = E, \end{aligned}$$

s.t. f on ringide homomorfism.

Kui $\varphi \in \mathrm{Ker}\,(f)$, siis $\left(A_\varphi^B\right)^T$ on nullmaatriks, kust järeldub, et ka A_φ^B on nullmaatriks, ning seega φ on nullteisendus. Järelikult $\mathrm{Ker}\,(f) = \{0\}$ ja f on üksühene.

Näitame lõpuks, et f on pealekujutus. Olgu $X \in \mathrm{Mat}_n(D)$. Siis ka $X^T \in \mathrm{Mat}_n(D)$. Lineaaralgebrast on teada, et leidub lineaarkujutus $\varphi \in \mathrm{End}_D(M)$ nii, et $X^T = A_\varphi^B$. Siis aga

$$f(\varphi) = \left(A_\varphi^B\right)^T = \left(X^T\right)^T = X.$$

Sellega oleme tõestanud, et f on isomorfism ja

$$R \cong \mathrm{End}_D(M) \cong \mathrm{Mat}_n(D).$$

□

Peatükk 5

Moodulid

5.1 Mooduli definitsioon

Mooduli definitsioon näeb välja täpselt samasugune nagu vektorruumi definitsioon, ainult et korpuse asemel on ring R.

Definitsioon 5.1 Hulka A nimetatakse **mooduliks** üle ringi R, kui on defineeritud kujutused

$$A \times A \to A, \quad (a,b) \mapsto a+b,$$
$$R \times A \to A, \quad (k,a) \mapsto ka$$

nii, et

M1. $(a+b)+c = a+(b+c)$ iga $a,b,c \in A$ korral;

M2. leidub element $0 \in A$ nii, et iga $a \in A$ korral $a+0 = a = 0+a$;

M3. iga elemendi $a \in A$ korral leidub element $-a \in A$ nii, et $a+(-a) = 0 = (-a)+a$;

M4. $a+b = b+a$ iga $a,b \in A$ korral;

M5. $k(a+b) = ka+kb$ iga $a,b \in A$ ja $k \in R$ korral;

M6. $(k+l)a = ka+la$ iga $a \in A$ ja $k,l \in R$ korral;

M7. $(kl)a = k(la)$ iga $a \in A$ ja $k,l \in R$ korral;

M8. $1a = a$ iga $a \in A$ korral.

Selliseid mooduleid, nagu me siin defineerisime, nimetatakse harilikult vasakpoolseteks mooduliteks üle ringi R (sest R elementidega korrutamine toimub vasakult) ehk vasakpoolseteks R-mooduliteks ja tähistatakse ${}_RA$. Analoogiliselt saab defineerida parempoolsed moodulid. Selles kursuses vaatleme ainult vasakpoolseid mooduleid ja jätame sõna "vasakpoolne" harilikult ära.

Alammoodul, moodulite homomorfism, moodulite väline otsesumma jm. mõisted defineeritakse sarnaselt vastavate mõistetega vektorruumide korral. Mooduli A alammoodulite B_i, $i \in I$, summa ja sisemine otsesumma langevad kokku Abeli rühma A alamrühmade B_i, $i \in I$, summa ja sisemise otsesummaga.

Näide 5.2 1. Iga vektorruum üle korpuse on moodul üle selle korpuse.

2. Otsekorrutis $\mathbb{Z}^n$ on vasakpoolne $\mathbb{Z}$-moodul, kui tehted defineerida komponenthaaval. Kuna $\mathbb{Z}$ ei ole korpus, siis see moodul ei ole vektorruum.

3. Iga Abeli rühma A saab loomulikul viisil vaadelda moodulina üle ringi $\mathbb{Z}$, kui korrutised za, kus $z \in \mathbb{Z}$ ja $a \in A$, defineerida nii nagu paragrahvis 3.1.

4. Ringi R iga vasakpoolne ideaal I on moodul üle ringi R. Muuhulgas ka R on vasakpoolne moodul üle R.

5. Olgu $R = \mathrm{Mat}_m(D)$, kus D on jagamisega ring. Siis hulk $A = \mathrm{Mat}_{m,n}(D)$ on vasakpoolne moodul moodul üle R, kui liitmiseks on maatriksite liitmine ja kujutus $R \times A \to A$ on defineeritud maatriksite korrutamise abil.

5.2 Täpsed jadad

Selles paragrahvis on kõik vaadeldavad moodulid vasakpoolsed moodulid üle fikseeritud ringi R.

Olgu meil antud alljärgnev jada moodulitest A_α ning nendevahelistest homomorfismidest f_α:

$$\ldots \xrightarrow{f_{\alpha-1}} A_\alpha \xrightarrow{f_\alpha} A_{\alpha+1} \xrightarrow{f_{\alpha+1}} \ldots . \tag{5.1}$$

See jada võib olla lõplik, aga ka ühes või isegi mõlemas suunas lõpmatu.

Sarnaselt vektorruumide juhuga võib veenduda, et moodulite homomorfismi tuum ja kujutis on alammoodulid.

Definitsioon 5.3 Moodulite jada kujul (5.1) nimetatakse **täpseks kohal** α, kui

$$\mathrm{Ker}\,(f_\alpha) = \mathrm{Im}\,(f_{\alpha-1})\,.$$

Sellist jada, mis on täpne igal kohal, nimetatakse **täpseks**.

Jada täpsusest kohal α järeldub otseselt, et $f_\alpha f_{\alpha-1} = 0$, ehk täpsel kohal kahe homomorfismi järjestikune rakendamine annab tulemuseks nullhomomorfismi.

Näide 5.4 Vaatleme Abeli rühmi $\mathbb{Z}$ ja $\mathbb{Z}_2$ moodulitena üle ringi $\mathbb{Z}$. Siis leidub täpne jada

$$\mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}_2,$$

kus homomorfismid f ja g on defineeritud võrdustega

$$f(a) := 2a,$$
$$g(a) := \overline{a}.$$

Täpsed jadad on üks oluline tööriist moodulite teoorias, sest nende abil saab kirjeldada homomorfismide ja moodulite mitmeid omadusi. Järgnevas tekstis tähistame sümboliga 0 nii mooduli nullelementi, üheelemendilist moodulit kui ka nullhomomorfismi. Loodetavasti on kontekstist selge, mida parasjagu silmas peetakse.

Lemma 5.5 *Moodulite jada*

1. $0 \longrightarrow A \xrightarrow{f} B$ *on täpne parajasti siis kui* f *on injektiivne;*
2. $A \xrightarrow{f} B \longrightarrow 0$ *on täpne parajasti siis kui* f *on sürjektiivne;*
3. $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ *on täpne parajasti siis kui* f *on bijektiivne.*

TÕESTUS. 1. Paneme tähele, et on olemas täpselt üks homomorfism $0 \longrightarrow A$, see peab viima nullelemendi nullelemendiks. Harilikult selle homomorfismi tähist joonisele ei kanta. Selle homomorfismi kujutis on $\{0\}$. Nüüd

$$0 \longrightarrow A \xrightarrow{f} B \text{ on täpne} \iff \ker(f) = \{0\} \iff f \text{ on injektiivne.}$$

2. Ainuke homomorfism $B \longrightarrow 0$ on nullhomomorfism, mille tuum on B. Seega

$$A \xrightarrow{f} B \longrightarrow 0 \text{ on täpne} \iff \operatorname{Im}(f) = B \iff f \text{ on sürjektiivne.}$$

3. See järeldub vahetult osadest 1 ja 2. □

Definitsioon 5.6 Täpset jada kujul

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

nimetatakse **lühikeseks täpseks jadaks**.

Suvalise lühikese täpse jada kohta saab teha järgmised tähelepanekud:

1. f on injektiivne;
2. g on sürjektiivne;
3. $C \cong B/\operatorname{Ker}(g) = B/\operatorname{Im}(f)$ tänu järelduse 1.36 analoogile moodulite jaoks;
4. kui samastada A ja sellega isomorfne B alammoodul $\operatorname{Im}(f)$, siis võiks tinglikult kirjutada $C \cong B/A$.

Järgmine teoreem käsitleb selliseid lühikesi täpseid jadasid, kus üks keskel asuvatest homomorfismidest on ühelt poolt pööratav.

Teoreem 5.7 *Olgu*

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

lühike täpne jada. Siis järgmised väited on samaväärsed.

(i) *Leidub homomorfism* $\varphi : B \to A$ *nii, et* $\varphi\iota = 1_A$.

(ii) *Leidub endomorfism* $f : B \to B$ *nii, et* $f^2 = f$ *ja* $\mathrm{Im}\,(f) = \mathrm{Im}\,(\iota)$.

(iii) *Leidub mooduli* B *alammoodul* H *nii, et* $B = \mathrm{Im}\ \iota \dotplus H$.

(iv) *Leidub homomorfism* $\psi : C \to B$ *nii, et* $\pi\psi = 1_C$.

TÕESTUS. (ii) $\Rightarrow$ (iii) Veendume, et väide kehtib, kui võtta $H = \mathrm{Ker}\,(f)$, s.t. $B = \mathrm{Im}\,(\iota) \dotplus \mathrm{Ker}\,(f)$. Näitame esmalt, et $B = \mathrm{Im}\,(\iota) + \mathrm{Ker}\,(f)$. Selleks paneme tähele, et iga $b \in B$ korral $b - f(b) \in B$ ning

$$f(b - f(b)) = f(b) - f^2(b) = f(b) - f(b) = 0\,,$$

s.t. $b - f(b) \in \mathrm{Ker}\,(f)$ ja seega

$$b = f(b) + (b - f(b)) \in \mathrm{Im}\,(f) + \mathrm{Ker}\,(f) = \mathrm{Im}\,(\iota) + \mathrm{Ker}\,(f)\,.$$

Olgu nüüd $b \in \mathrm{Im}\,(f) \cap \mathrm{Ker}\,(f)$, s.t. $f(b) = 0$ ja $b = f(b')$ mingi $b' \in B$ korral. Siis $b = f(b') = f^2(b') = f(f(b')) = f(b) = 0$. Järelikult kehtibki $B = \mathrm{Im}\,(\iota) \dotplus \mathrm{Ker}\,(f)$, s.t. moodul B on oma alammoodulite $\mathrm{Im}\,(\iota)$ ja $\ker(f)$ otsesumma.

(iii) $\Rightarrow$ (i) Olgu $B = \mathrm{Im}\ \iota \dotplus H$, kus H on mooduli B mingi alammoodul. Siis iga $b \in B$ esitub üheselt kujul $b = \iota(x) + y$, kus $x \in A$, $y \in H$. Tänu ι injektiivsusele on ühene mitte ainult $\iota(x)$, vaid isegi x. Seega saame defineerida kujutuse $\varphi : B \to A$ võrdusega

$$\varphi(b) = \varphi(\iota(x) + y) = x\,.$$

Ei ole raske kontrollida, et φ on moodulite homomorfism. Lisaks sellele, iga $a \in A$ korral

$$(\varphi\iota)(a) = \varphi(\iota(a) + 0) = a = 1_A(a).$$

Sellega olemegi näidanud, et $\varphi\iota = 1_A$.

(i) $\Rightarrow$ (iv) Kujutuse $\psi : C \to B$ defineerime võrdusega

$$\psi(c) = b - (\iota\varphi)(b)\,,$$

kus $b \in B$ on üks neist elementidest, mille korral $\pi(b) = c$ (meenutame, et π on sürjektiivne). Kontrollime, et eelnev definitsioon ei sõltu elemendi b valikust. Olgu ka $b' \in B$ selline, et $\pi(b') = c$. Siis $\pi(b - b') = 0$ ja $b - b' \in \mathrm{Ker}\,(\pi) = \mathrm{Im}\,(\iota)$. Järelikult leidub $a \in A$ nii, et $b - b' = \iota(a)$. Nüüd

$$\begin{aligned}(\iota\varphi)(b) - (\iota\varphi)(b') &= (\iota\varphi)(b - b') = (\iota\varphi)(\iota(a)) \\ &= (\iota(\varphi\iota))(a) = (\iota 1_A)(a) = \iota(a) = b - b',\end{aligned}$$

mistõttu

$$\psi(c) = b - (\iota\varphi)(b) = b' - (\iota\varphi)(b')\,.$$

Sellega on kujutuse ψ korrektsus tõestatud. Ei ole jälle raske veenduda, et ψ on homomorfism.

Viimaks näeme, et iga $c \in C$ korral

$$(\pi\psi)(c) = \pi(b - (\iota\varphi)(b)) = \pi(b) - (\pi\iota)(\varphi(b)) = \pi(b) - 0 = c = 1_C(c)\,.$$

Seega tõesti $\pi\psi = 1_C$.

(iv) $\Rightarrow$ (ii) Defineerime kujutuse $f : B \to B$ võrdusega

$$f = 1_B - \psi\pi\,.$$

Kuna f on mooduli B endomorfismide 1_B ja $\psi\pi$ vahe, siis on ta B endohomomorfism. Lisaks sellele

$$f^2 = (1_B - \psi\pi)(1_B - \psi\pi) = 1_B - \psi\pi - \psi\pi + \psi(\pi\psi)\pi = 1_B - \psi\pi - \psi\pi + \psi(1_C)\pi = 1_B - \psi\pi = f\,.$$

Jääb veel veenduda, et $\mathrm{Im}\,(\iota) = \mathrm{Im}\,(f)$. Iga $a \in A$ korral

$$f(\iota(a)) = (1_B - \psi\pi)(\iota(a)) = 1_B(\iota(a)) - (\psi\pi)(\iota(a)) = \iota(a) - \psi((\pi\iota)(a)) = \iota(a) - \psi(0) = \iota(a)\,,$$

kust on näha, et $\mathrm{Im}\,(\iota) \subseteq \mathrm{Im}\,(f)$. Teisipidi, kui $b \in B$, siis

$$\pi(f(b)) = \pi(b - (\psi\pi)(b)) = \pi(b) - (\pi\psi\pi)(b) = \pi(b) - (1_C\pi)(b) = 0\,,$$

mistõttu $f(b) \in \mathrm{Ker}\,(\pi) = \mathrm{Im}\,(\iota)$, kust $\mathrm{Im}\,(f) \subseteq \mathrm{Im}\,(\iota)$ ja kokkuvõttes $\mathrm{Im}\,(f) = \mathrm{Im}\,(\iota)$. □

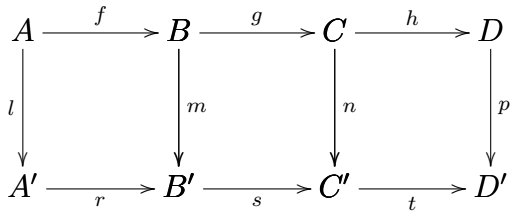
Näide 5.8 Vaatleme vasakpoolsete $\mathbb{Z}$-moodulite homomorfisme $\iota : \mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$, $a \mapsto (a, 0)$, ja $\pi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(a, b) \mapsto b$. Siis

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\ \iota\ } \mathbb{Z} \times \mathbb{Z} \xrightarrow{\ \pi\ } \mathbb{Z} \longrightarrow 0$$

on lühike täpne jada, sest ι on injektiive, π on sürjektiivne ja lisaks sellele $\mathrm{Im}\,(\iota) = \{(a, 0) \mid a \in \mathbb{Z}\} = \ker(\pi)$. See jada rahuldab ka teoreemi 5.7 tingimusi, sest võime võtta $\varphi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(a, b) \mapsto a$.

Algebras vaadeldakse tihti diagramme, mille tippudeks on algebralised struktuurid ja noolteks tippude vahel on homomorfismid. Sellisteks diagrammideks on näiteks homomorfismiteoreemi kolmnurk või täpne jada. Me võime sellist diagrammi vaadelda suunatud graafina. Diagrammi nimetatakse **kommutatiivseks**, kui selles suunatud graafis mistahes kahe tipu vahel mistahes kahe suunatud ahela servadeks olevaid homomorfisme järjest rakendades saame sama tulemuse. Üks natuke suuremat sorti kommutatiivne diagramm esineb meil järgmises teoreemis.

Teoreem 5.9 (4-lemma) *Kui kommutatiivse diagrammi*



read on täpsed jadad, m ja p on injektiivsed ja l on sürjektiivne, siis n on injektiivne.

TÕESTUS. Kujutuse n injektiivsuse näitamiseks piisab, kui tõestame, et $\mathrm{Ker}\,(n) = \{0\}$.

- Olgu $c \in \mathrm{Ker}\,(n)$, s.t. $n(c) = 0$.
- Siis $t(n(c)) = 0$.
- Kommutatiivsuse tõttu $p(h(c)) = 0$ ehk $h(c) \in \mathrm{Ker}\,(p)$.
- Kuna p on injektiivne, siis $h(c) = 0$ ehk $c \in \mathrm{Ker}\,(h) = \mathrm{Im}\,(g)$.
- Kuna $c \in \mathrm{Im}\,(g)$, siis leidub $b \in B$ nii, et $g(b) = c$.
- Kasutades kommutatiivsust saame, et $s(m(b)) = n(g(b)) = n(c) = 0$ ehk $m(b) \in \mathrm{Ker}\,(s) = \mathrm{Im}\,(r)$.
- Kuna $m(b) \in \mathrm{Im}\,(r)$, siis leidub $a' \in A'$ nii, et $r(a') = m(b)$.
- Et l on sürjektiivne, siis leidub $a \in A$ nii, et $l(a) = a'$.
- Kommutatiivsuse põhjal $m(f(a)) = r(l(a)) = r(a') = m(b)$.
- Kuna m on injektiivne, siis $f(a) = b$.
- Seega $c = g(f(a))$.
- Kuna $gf = 0$, siis $c = 0$.
- Järelikult $\mathrm{Ker}\,(n) = \{0\}$ ja n on injektiivne.

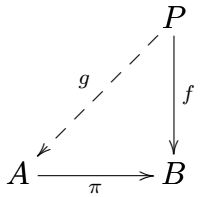
□

Märkus 5.10 Tõestatud teoreemi tuntakse inglise keeles nime all “four lemma”. Tegelikult on 4-lemmasid kaks tükki, siin tõestasime neist ühe.

Sedalaadi diagramme kasutatakse palju selles algebra osas, mida kutsutakse homoloogiliseks algebraks. Tõestustehnika, mida antud teoreemi tõestamiseks kasutasime, kannab inglise keeles nime “diagram chasing”. Eestikeelseks vasteks on prof. Mati Kilp pakkunud “diagrammis tuhnimine”.

5.3 Projektiivsed moodulid

Definitsioon 5.11 Moodulit ${}_RP$ nimetatakse **projektiivseks**, kui iga sürjektiivse moodulite homomorfismi $\pi : {}_RA \to {}_RB$ ja iga moodulite homorfismi $f : {}_RP \to {}_RB$ korral leidub moodulite homomorfism $g : {}_RP \to {}_RA$ nii, et $f = \pi g$.



Definitsioon 5.12 Moodulit nimetatakse **vabaks** kui temas leidub baas, s.t. lineaarselt sõltumatu moodustajate süsteem.

Lineaarselt sõltumatud süsteemid ja moodustajate süsteemid defineeritakse moodulite korral samamoodi nagu vektorruumide korral.

Lause 5.13 *Vasakpoolne R-moodul F on vaba parajasti siis, kui ta on isomorfne välise otsesummaga sellistest moodulitest A_i, kus $A_i \cong {}_RR$ iga $i \in I$ korral:*

$$F \cong \oplus \sum_{i \in I} A_i.$$

TÕESTUS. Selle lause tõestust me käesolevas kursuses ei anna. □

Näide 5.14 Näiteks $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ on vaba $\mathbb{Z}$-moodul, kusjuures üheks tema baasiks on $\{(1,0,0),(0,1,0),(0,0,1)\}$.

Lause 5.15 *Iga vaba moodul F on projektiivne.*

TÕESTUS. Olgu F vaba vasakpoolne R-moodul baasiga $\{e_i \mid i \in I\}$. Näitame, et F on projektiivne. Olgu A, B moodulid, $f : F \longrightarrow B$ homomorfism ja $\pi : A \longrightarrow B$ sürjektiivne homomorfism. Tähistame $b_i := f(e_i)$ iga $i \in I$ korral. Et π on sürjektiivne, siis iga $i \in I$ jaoks saame valida mingi elemendi $a_i \in A$ nii, et $\pi(a_i) = b_i$.

Defineerime nüüd kujutuse $g : F \longrightarrow A$. Iga nullist erineva element $x \in F$ esitub üheselt lineaarkombinatsioonina

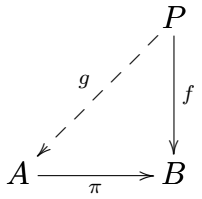
$$x = r_{i_1} e_{i_1} + \ldots + r_{i_n} e_{i_n} = \sum_{k=1}^{n} r_{i_k} e_{i_k},$$

kus $n \in \mathbb{N}$ ja $r_{i_1}, \ldots, r_{i_n} \in R$. Me defineerime

$$g(x) := \sum_{k=1}^{n} r_{i_k} a_{i_k}$$

ja $g(a) := 0$. Tänu esituse ühesusele on g korrektselt defineeritud. Lihtne on veenduda, et g on moodulite homomorfism.

Tõestuse lõpetamiseks veendume, et kolmnurk



on kommutatiivne. On selge, et $(\pi g)(0) = 0 = f(0)$. Kui $x \in F \setminus \{0\}$ on selline nagu eespool, siis

$$\begin{aligned}
(\pi g)(x) &= \pi\left(\sum_{k=1}^{n} r_{i_k} a_{i_k}\right) && (g \text{ definitsioon}) \\
&= \sum_{k=1}^{n} r_{i_k} \pi(a_{i_k}) && (\pi \text{ on homomorfism}) \\
&= \sum_{k=1}^{n} r_{i_k} b_{i_k} && (\pi(a_{i_k}) = b_{i_k}) \\
&= \sum_{k=1}^{n} r_{i_k} f(e_{i_k}) && (f(e_{i_k}) = b_{i_k}) \\
&= f\left(\sum_{k=1}^{n} r_{i_k} e_{i_k}\right) && (f \text{ on homomorfism}) \\
&= f(x)\,.
\end{aligned}$$

Seega $\pi g = f$. □

Me ütleme, et moodul A on mooduli B epimorfne kujutis, kui leidub sürjektiivne homomorfism $B \longrightarrow\!\!\!\!\!\rightarrow A$. Sellisel juhul on B tänu homomorfismiteoreemile isomorfne mooduli B faktormooduliga.

Lause 5.16 *Iga moodul on vaba mooduli epimorfne kujutis (faktormoodul).*

TÕESTUS. Olgu A vasakpoolne R-moodul. Vaatleme hulka A indeksite hulgana, defineerime $M_a := {}_R R$ ja vaatleme moodulite M_a, $a \in A$, välist otsesummat $F := \oplus \sum_{a \in A} M_a$. Lause 5.13 põhjal on F vaba moodul. Elemendi $x = (x_a)_{a \in A} \in F$ korral defineerime

$$f(x) := \sum_{a \in A} x_a a\,.$$

Paneme tähele, et see summa on lõplik, sest peres $(x_a)_{a \in A}$ on lõplik arv nullist erinevaid elemente. Seega meil tekib kujutus $f : F \longrightarrow\!\!\!\!\!\rightarrow A$. Lihtne on veenduda, et see on moodulite homomorfism.

Olgu nüüd $e_a \in F$ selline pere, mille a-komponent on ringi R ühikeleent ja kõik ülejäänud komponendid on nullid. Siis $f(e_a) = 1 \cdot a = a$, mis tähendab, et f on sürjektiivne. □

Järeldus 5.17 *Iga moodul on projektiivse mooduli epimorfne kujutis (faktormoodul).*

Lause 5.18 *Kui P ja Q on R-moodulid ja moodul $P \oplus Q$ on projektiivne, siis ka P ja Q on projektiivsed.*

TÕESTUS. Tõestame, et P on projektiivne (Q jaoks on tõestus analoogiline). Vaatleme diagrammi

$$\begin{array}{ccc} & & P \\ & & \downarrow f \\ A & \xrightarrow[\pi]{} & B \end{array},$$

kus f ja π on homomorfismid ja π on sürjektiivne. Meenutame, et $P \oplus Q = P \times Q$, sest tegemist on lõpliku arvu moodulite välise otsesummaga. Lihtne on näha, et ka kujutus

$$f' : P \times Q \longrightarrow B, \quad (p, q) \mapsto f(p)$$

on homomorfism. Eelduse tõttu leidub homomorfism $g' : P \times Q \longrightarrow A$ nii, et $\pi g' = f'$.

$$\begin{array}{ccc} & & P \times Q \\ & \overset{g'}{\swarrow} & \downarrow f' \\ A & \xrightarrow[\pi]{} & B \end{array}.$$

Vaatleme veel moodulite homomorfismi

$$\iota_P : P \longrightarrow P \times Q, \quad p \mapsto (p, 0)$$

ja defineerime homomorfismi $g : P \longrightarrow A$ korrutisena $g := g'\iota_P$. Siis

$$(\pi g)(p) = (\pi g'\iota_P)(p) = (f'\iota_P)(p) = f'(p, 0) = f(p)$$

iga $p \in P$ korral. Järelikult $\pi g = f$. □

Teoreem 5.19 *Järgmised väited R-mooduli P kohta on samaväärsed.*

(i) *Moodul P on projektiivne.*

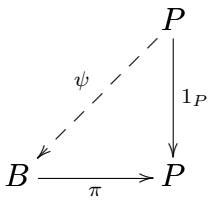
(ii) *Iga lühikese täpse jada*

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} P \longrightarrow 0$$

korral leidub homomorfism $\psi : P \to B$ nii, et $\pi\psi = 1_P$.

(iii) *Leidub vaba moodul F nii, et $F = A \dot{+} B$, kusjuures üks otseliidetavatest on isomorfne mooduliga P.*

TÕESTUS. (i) $\Rightarrow$ (ii) Rakendame P projektiivsust homomorfismidele $\pi : B \to P$ ja $1_P : P \to P$. Siis leidub selline homomorfism $\psi : P \to B$, et $\pi\psi = 1_P$, mida oligi tarvis tõestada.



(ii) $\Rightarrow$ (iii) Lause 5.16 tõttu leidub meil lühike täpne jada

$$0 \longrightarrow \mathrm{Ker}\,(\pi) \xrightarrow{\iota} F \xrightarrow{\pi} P \longrightarrow 0\,,$$

kus F on vaba moodul ja ι on sisestus. Eelduse (ii) kohaselt leidub homomorfism $\psi : P \to F$ nii, et $\pi\psi = 1_P$, mis teoreemist 5.7 tulenevalt annab meile, et $F = \mathrm{Im}\,(\iota) \dotplus B$ mingi F alammooduli B korral. Kujutus

$$f : F \longrightarrow B, \;\; \iota(a) + b \mapsto b$$

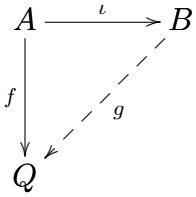
on sürjektiivne homomorfism, mille tuum on $\mathrm{Im}\,(\iota)$. Homomorfismiteoreemi tõttu $B \cong F/\,\mathrm{Im}\,(\iota)$. Homomorfismiteoreemi ja jada täpsuse tõttu kehtib

$$P \cong F/\,\mathrm{Ker}\,(\pi) = F/\,\mathrm{Im}\,(\iota) \cong B.$$

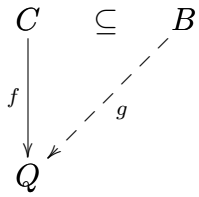
(iii) $\Rightarrow$ (i) Vaba moodul $F = A \dotplus P \cong A \oplus P = A \times P$ on projektiivne lause 5.15 tõttu. Lause 5.18 annabki nüüd, et nii A kui P on projektiivsed. □

5.4 Injektiivsed moodulid

Definitsioon 5.20 Moodulit ${}_RQ$ nimetatakse **injektiivseks**, kui iga injektiivse homomorfismi $\iota : {}_RA \to {}_RB$ ja iga homomorfismi $f : {}_RA \to {}_RQ$ korral leidub homomorfism $g : {}_RB \to {}_RQ$ nii, et $f = g\iota$.



Lause 5.21 *Moodul ${}_RQ$ on injektiivne parajasti siis, kui iga mooduli ${}_RB$, selle mistahes alammooduli ${}_RC$ ja iga homomorfismi $f : {}_RC \to {}_RQ$ korral leidub homomorfism $g : {}_RB \to {}_RQ$ nii, et $g|_C = f$.*



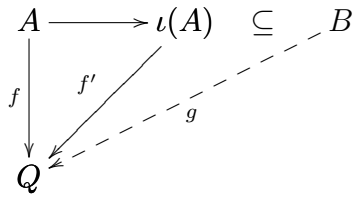
TÕESTUS. TARVILIKKUS. Sisestuskujutus $\iota : C \longrightarrow B$ on moodulite injektiivne homomorfism. Seega leidub homomorfism $g : B \longrightarrow Q$ nii, et $g\iota = f$. Järelikult iga $c \in C$ korral $g(c) = g(\iota(c)) = f(c)$ ehk $g|_C = f$.
PIISAVUS. Vaatleme homomorfismi $f : A \longrightarrow Q$ ja injektiivset homomorfismi $\iota : A \longrightarrow B$. Siis $\iota(A)$ on mooduli B alammoodul ja

$$f' : \iota(A) \longrightarrow Q,\ \iota(a) \mapsto f(a)$$

on moodulite homomorfism. Eelduse põhjal leidub homomorfism $g : B \longrightarrow Q$ nii, et $g|_{\iota(A)} = f'$. Järelikult

$$(g\iota)(a) = g(\iota(a)) = f'(\iota(a)) = f(a)$$

iga $a \in A$ korral, s.t. $g\iota = f$.



□

Mooduli ${}_RR$ alammoodulid on parajasti ringi R vasakpoolsed ideaalid. Zorni lemma abil saab tõestada (kuigi selles kursuses me seda tõestust ei anna), et kehtib järgmine teoreem.

Teoreem 5.22 *Moodul ${}_RQ$ on injektiivne parajasti siis, kui ringi R iga vasakpoolse ideaali I ja iga homomorfismi $f : {}_RI \to {}_RQ$ korral leidub homomorfism $g : {}_RR \to {}_RQ$ nii, et $g|_I = f$.*

Lause 5.23 *Abeli rühm vaadelduna vasakpoolse $\mathbb{Z}$-moodulina on injektiivne parajasti siis kui see Abeli rühm on jaguv.*

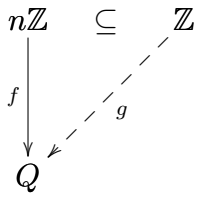
TÕESTUS. TARVILIKKUS. Olgu Q Abeli rühm, mis on $\mathbb{Z}$-moodulina injektiivne. Tõestame, et ta on jaguv. Olgu $q \in Q$ ja $n \in \mathbb{N}$ suvalised. Siis $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ on ringi $\mathbb{Z}$ kahepoolne ideaal. Defineerime kujutuse $f : n\mathbb{Z} \longrightarrow Q$ võrdusega

$$f(na) := aq.$$

Kuna

$$na = nb \implies a = b \implies aq = bq,$$

siis f on korrektselt defineeritud. Lihtne on näha, et f on $\mathbb{Z}$-moodulite homomorfism.



Eelduse tõttu leidub $\mathbb{Z}$-moodulite homomorfism $g : \mathbb{Z} \longrightarrow Q$ nii, et $g|_{n\mathbb{Z}} = f$. Nüüd

$$q = 1q = f(n \cdot 1) = g(n) = g(1 + \ldots + 1) = g(1) + \ldots + g(1)) = ng(1),$$

kus $g(1) \in Q$. Seega tõesti Q on jaguv.
Piisavus. See on tõestatud lauses 3.13. □

Niisiis näiteks moodul ${}_{\mathbb{Z}}\mathbb{Q}$ on injektiivne $\mathbb{Z}$-moodul.

Peatükk 6

Poolrühmad

6.1 Põhidefinitsioonid

Definitsioon 6.1 Poolrühmaks nimetatakse hulka S koos sellel defineeritud kahekohalise algebralise tehtega $\cdot$, mis on assotsiatiivne, see tähendab, et mistahes $a, b, c \in S$ korral $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Harilikult kirjutatakse $a \cdot b$ asemel lihtsalt ab.

Definitsioon 6.2 Poolrühma S nimetatakse **monoidiks**, kui temas leidub ühikelement, s.t. selline element e, et iga $a \in S$ korral $ea = a = ae$.

Poolrühma ühikelement (kui ta leidub) on üheselt määratud ja harilikult tähistatakse teda sümboliga 1.

Näide 6.3 1. $(\mathbb{N}, +)$ on poolrühm, mis ei ole monoid.

2. $(\mathbb{N}, \cdot)$ on monoid ühikelemendiga 1.

3. Kordarvude hulk on poolrühm korrutamise suhtes.

4. Mittetühja hulga X kõigi teisenduste hulk $\mathcal{T}(X)$ on monoid teisenduste järjestrakendamise suhtes. Selle monoidi ühikelement on hulga X samasusteisendus 1_X.

5. Olgu X suvaline mittetühi hulk. Defineerides

$$xy := x$$

iga $x, y \in X$ korral saame poolrühma, mida nimetatakse vasakpoolsete nullide poolrühmaks.

Definitsioon 6.4 Olgu S ja T poolrühmad. Kujutust $f\colon S \longrightarrow T$ nimetatakse **poolrühmade homomorfismiks**, kui

$$f(xy) = f(x)f(y)$$

iga $x, y \in S$ korral.

Definitsioon 6.5 Poolrühmade **isomorfismiks** nimetatakse homomorfismi, mis on bijektiivne.

Definitsioon 6.6 Poolrühma S alamhulka U nimetatakse **alampoolrühmaks**, kui ta on kinnine korrutamise suhtes.

Definitsioon 6.7 Monoidi S alamhulka U nimetatakse **alammonoidiks**, kui ta on kinnine korrutamise suhtes ja sisaldab monoidi S ühikelementi.

Näide 6.8 Paarisarvude hulk $2\mathbb{N}$ on poolrühma $(\mathbb{N}, \cdot)$ alampoolrühm, aga ta ei ole monoidi $(\mathbb{N}, \cdot)$ alammonoid, sest ei sisalda selle ühikelementi 1.

Nii nagu ringiteooriaski, on ka poolrühmateoorias oluline roll ideaalidel.

Definitsioon 6.9 Alamhulka I poolrühmas S nimetatakse poolrühma S **parempoolseks (vasakpoolseks) ideaaliks**, kui

$$as \in I \ (sa \in I)$$

mistahes $a \in I$, $s \in S$ korral. Poolrühma S **ideaaliks** nimetatakse parempoolset ideaali I, mis on samal ajal ka vasakpoolne ideaal.

Definitsiooni järgi loeme ka poolrühma tühja alamhulga ideaaliks.
On selge, et poolrühma ideaal on alampoolrühm. Vastupidine üldjuhul ei kehti.

Näide 6.10 Vaatleme poolrühma $S = (\mathbb{N}, \cdot)$. Siis paaritute naturaalarvude hulk U on selle poolrühma alampoolrühm, kuid ei ole ideaal, sest näiteks $3 \in U$, $2 \in S$ ja $3 \cdot 2 \notin U$.

Poolrühma S kõigi ideaalide hulka $\mathsf{Id}(S)$ võib vaadelda järjestatud hulgana sisalduvusseose suhtes. Selle järjestatud hulga vähim element on $\emptyset$ ja suurim element on S.

Definitsioon 6.11 Poolrühma S ideaali I nimetatakse **minimaalseks ideaaliks**, kui

1. $I \neq \emptyset$
2. iga ideaali J korral
$$J \neq \emptyset \ \text{ ja } \ J \subseteq I \Rightarrow J = I\,.$$

Analoogiliselt saab defineerida minimaalsed vasak- ja parempoolsed ideaalid.

Definitsioon 6.12 Olgu S poolrühm, olgu 1 mingi element, mis ei kuulu hulka S ja

$$S^1 = S \cup \{1\}.$$

Defineerime hulgal S^1 korrutamise nii, et poolrühma S elementide omavahelisi korrutisi ei muudeta, $1 \cdot 1 = 1$ ja

$$1s = s1 = s$$

iga $s \in S$ korral. Ilmselt on S^1 monoid ühikelemendiga 1. Öeldakse, et monoid S^1 on saadud poolrühmast S **ühikelemendi välisel lisamisel**.

Näide 6.13 Lõpliku poolrühma korrutustehe antakse sageli tabeli abil, mida kutsutakse Cayley tabeliks. Sellises tabelis on elemendiga a märgistatud rea ja elemendiga b märgistatud veeru lõikekohas korrutis ab. Näiteks võib vaadelda poolrühma

$$S = \{e, a, f, b\},$$

mille Cayley tabel on

	e	a	f	b
e	e	e	e	b
a	e	e	a	b
f	e	e	f	b
b	b	b	b	e

.

Välise ühikelemendi lisamisel saame poolrühma $S^1 = \{e, a, f, b, 1\}$, mille Cayley tabel on

	e	a	f	b	1
e	e	e	e	b	e
a	e	e	a	b	a
f	e	e	f	b	f
b	b	b	b	e	b
1	e	a	f	b	1

.

Mistahes poolrühma S ja elemendi $a \in S$ korral tähistame

$$\begin{aligned} Sa &= \{sa \mid s \in S\}, \\ aS &= \{as \mid s \in S\}, \\ SaS &= \{sat \mid s, t \in S\}. \end{aligned}$$

Siis

$$\begin{aligned} S^1a &= Sa \cup \{a\}, \\ aS^1 &= aS \cup \{a\}, \\ S^1aS^1 &= SaS \cup Sa \cup aS \cup \{a\}. \end{aligned}$$

Lihtne on veenduda, et kehtib järgmine lemma.

Lemma 6.14 *Olgu S poolrühm ja $a \in S$. Siis*

1. *S^1a on vähim vasakpoolne ideaal, mis sisaldab elementi a,*
2. *aS^1 on vähim parempoolne ideaal, mis sisaldab elementi a,*
3. *S^1aS^1 on vähim ideaal, mis sisaldab elementi a.*

Definitsioon 6.15 Öeldakse, et S^1a (aS^1, S^1aS^1) on poolrühma S elemendi a poolt tekitatud **vasakpoolne peaideaal** (vastavalt **parempoolne peaideaal, peaideaal**).

6.2 Lihtsad poolrühmad

Definitsioon 6.16 Poolrühma S ideaali I nimetatakse **pärisideaaliks**, kui $I \neq S$.

Definitsioon 6.17 Poolrühma S nimetatakse **lihtsaks,** kui ta ei sisalda mittetühje pärisideaale.

Seega poolrühm on lihtne parajasti siis, kui tema ainsad ideaalid on $\emptyset$ ja S.

Lause 6.18 *Poolrühm S on lihtne parajasti siis, kui $SaS = S$ iga $a \in S$ korral.*

TÕESTUS. TARVILIKKUS. Oletame, et S on lihtne poolrühm ja olgu $a \in S$ suvaline. Kui $sat \in SaS$ ja $u \in S$ siis

$$u(sat) = (us)at \in SaS, \quad (sat)u = sa(tu) \in SaS.$$

Seega SaS on ideaal. See ideaal on mittetühi, sest $aaa \in SaS$. Kuna S on lihtne, siis $SaS = S$.
PIISAVUS. Oletame, et $SaS = S$ iga $a \in S$ korral ja olgu I poolrühma S mittetühi ideaal. On vaja näidata, et $S \subseteq I$. Võtame $s \in S$. Kuna $I \neq \emptyset$ siis leidub mingi element $a \in I$. Eelduse põhjal $SaS = S$. Järelikult leiduvad $x, y \in S$ nii, et $s = xay$. Kuna I on vasakpoolne ideaal poolrühmas S, siis $xa \in I$. Et ta on ka parempoolne ideaal, siis $s = xay \in I$. Seega $I = S$ ning S on lihtne poolrühm. □

Ülesanne 6.19 Näidake, et iga rühm on lihtne poolrühm.

Kui A ja B on poolrühma S alamhulgad, siis kasutatakse tähistust

$$AB = \{ab \mid a \in A, b \in B\}.$$

Muuhulgas $A = B = S$ korral kirjutatakse $SS = S^2$.

Definitsioon 6.20 Poolrühma S nimetatakse **faktoriseeruvaks**, kui $S^2 = S$.

Teiste sõnadega: poolrühm on faktoriseeruv, kui selle iga element on esitatav kahe elemendi korrutisena. On selge, et iga monoid S on faktoriseeruv, sest $s = s1$ iga $s \in S$ korral. Poolrühm $(\{2, 3, 4, 5, \ldots\}, \cdot)$ aga ei ole faktoriseeruv, sest näiteks elementi 2 ei saa esitada kahe elemendi korrutisena.

Lause 6.21 *Lihtne poolrühm on faktoriseeruv.*

TÕESTUS. Tühja poolrühma korral võrdus $S^2 = S$ ilmselt kehtib. Olgu S lihtne mittetühi poolrühm. Kerge on näha, et S^2 on poolrühma S mittetühi ideaal. Järelikult $S^2 = S$. □

Lause 6.22 *Kui M on minimaalne ideaal poolrühmas S, siis M on ise lihtne poolrühm.*

TÕESTUS. Olgu M minimaalne ideaal poolrühmas S. Siis ka hulk $M^2 = \{mn \mid m, n \in M\}$ on ideaal poolrühmas S ja $M^2 \subseteq M$. Tänu M minimaalsusele peab kehtima võrdus $M^2 = M$. Kuid siis ka $M = M^3$.

Näitame, et M on lihtne poolrühm. Kui $a \in M$, siis S^1aS^1 on poolrühma S ideaal ja $S^1aS^1 \subseteq M$. Tänu M minimaalsusele kehtib võrdus $M = S^1aS^1$. Järelikult

$$MaM \subseteq S^1aS^1 = M = M^3 = M(S^1aS^1)M = (MS^1)a(S^1M) \subseteq MaM,$$

kust järeldub, et $MaM = M$. Lause 6.18 põhjal on M lihtne poolrühm. □

6.3 Greeni seosed

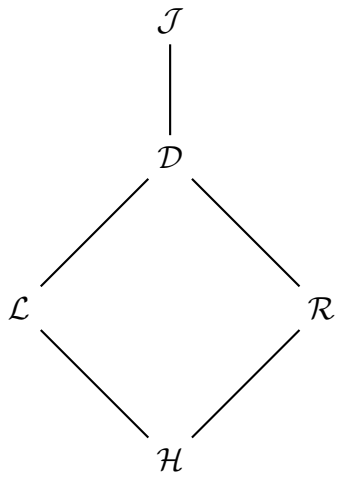
Poolrühmade struktuuri uurimisel on suureks abiks teatud ideaalide abil defineeritud seosed, mida kutsutakse nende defineerija järgi Greeni[1] seosteks.

Definitsioon 6.23 Olgu $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ ja $\mathcal{D}$ seosed poolrühmal S, mis on defineeritud järgmiselt:

$$a\mathcal{J}b \iff S^1aS^1 = S^1bS^1$$
$$a\mathcal{R}b \iff aS^1 = bS^1$$
$$a\mathcal{L}b \iff S^1a = S^1b$$
$$\mathcal{H} = \mathcal{L} \cap \mathcal{R}$$
$$\mathcal{D} = \mathcal{L} \circ \mathcal{R}$$

mistahes $a, b \in S$ korral. Seoseid $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ ja $\mathcal{D}$ nimetatakse **Greeni seosteks** poolrühmal S.

Märkus 6.24 Lihtne on aru saada, et $\mathcal{R}$, $\mathcal{L}$ ja $\mathcal{J}$ on ekvivalentsiseosed hulgal S. Saab näidata, et $\mathcal{H} = \mathcal{L} \wedge \mathcal{R}$ ja $\mathcal{D} = \mathcal{L} \vee \mathcal{R}$, kus alumine ja ülemine raja $\mathcal{R}$ ja $\mathcal{L}$ vahel leitakse hulga S kõigi ekvivalentsiseoste hulgas, mis on järjestatud hulk sisalduvusseose suhtes. Sümbol $\circ$ tähistab binaarsete seoste korrutamist. Saab näidata, et $\mathcal{D} \subseteq \mathcal{J}$. On selge, et $\mathcal{H} \subseteq \mathcal{L} \subseteq \mathcal{D}$ ja $\mathcal{H} \subseteq \mathcal{R} \subseteq \mathcal{D}$. Seega Greeni seoste vahelisi sisalduvusi võib kirjeldada järgmise diagrammi abil:



.

Elemendi $a \in S$ $\mathcal{L}$-klassi ($\mathcal{R}$-klassi, $\mathcal{H}$-klassi, $\mathcal{D}$-klassi ja $\mathcal{J}$-klassi) tähistatakse L_a (vastavalt R_a, H_a, D_a ja J_a). Lihtne on veenduda, et kehtib järgmine lause.

Lause 6.25 *Mistahes poolrühma S ja elementide $a, b \in S$ korral*

$$a\mathcal{R}b \iff (\exists u, v \in S^1)(a = bu \wedge b = av);$$
$$a\mathcal{L}b \iff (\exists u, v \in S^1)(a = ub \wedge b = va);$$
$$a\mathcal{J}b \iff (\exists u, v, s, t \in S^1)(a = ubv \wedge b = sat).$$

[1] James Alexander Green (1926–2014) — briti matemaatik

Näide 6.26 Mistahes hulkade A ja X korral on hulk $S = A \times X$ poolrühm korrutamise

$$(a, x)(a', x') := (a, x')$$

suhtes. Vaatleme olukorda, kus $A = \{a, b\}$ ja $X = \{x, y, z\}$. Otsekorrutise $A \times X$ elemendid võib kirjutada üles tabelina

(a, x)	(a, y)	(a, z)
(b, x)	(b, y)	(b, z)

.

On võimalik näidata, et selle tabeli read on poolrühma $A \times X$ $\mathcal{R}$-klassid ja veerud on $\mathcal{L}$-klassid. Seega $\mathcal{H}$-klassid on üheelemendilised ja poolrühmal on üksainus $\mathcal{D}$-klass, mis koosneb kõigist tema elementidest.

Lisaks kongruentsidele räägitakse poolrühmade puhul ka ühepoolsetest kongruentsidest.

Lause 6.27 *Seos $\mathcal{R}$ on vasakpoolne kongruents poolrühmal S ja seos $\mathcal{L}$ on parempoolne kongruents poolrühmal S, see tähendab, et iga $a, b, c \in S$ korral*

$$a\mathcal{R}b \Longrightarrow ca\mathcal{R}cb,$$
$$a\mathcal{L}b \Longrightarrow ac\mathcal{L}bc.$$

TÕESTUS. Olgu $a, b, c \in S$ ja olgu $a\mathcal{R}b$. Siis $aS^1 = bS^1$. Tänu lausele 6.25 leiduvad elemendid $u, v \in S^1$ nii, et $a = bu$ ja $b = av$. Kuid siis kehtivad ka võrdused $ca = cbu$ ja $cb = cav$. Jällegi Lause 6.25 põhjal võime öleda, et $ca\mathcal{R}cb$.

Analoogiliselt saab näidata, et $\mathcal{L}$ on parempoolne kongruents. □

Definitsioon 6.28 Poolrühma S elementi e nimetatakse **idempotendiks,** kui $e^2 = e$. Poolrühma S kõigi idempotentide hulka tähistatakse $E(S)$.

Lihtne on veenduda, et kehtib järgmine väide.

Lemma 6.29 *Kui S on rühm, siis temas on täpselt üks idempotent.*

Näide 6.30 Poolrühmas $(\mathbb{Z}, \cdot)$ on kaks idempotenti: 0 ja 1. Vasakpoolsete nullide poolrühmas (vt. näidet 6.3) on kõik elemendid idempotendid.

6.4 Täiesti lihtsad poolrühmad

Ei ole võimalik kirjeldada ära kõiki lihtsaid poolrühmi. Küll aga on võimalik ära kirjeldada lihtsate poolrühmade klassi üks alamklass — täiesti lihtsate poolrühmade klass.

Definitsioon 6.31 Poolrühma S idempotenti e nimetatakse **primitiivseks,** kui iga $f \in E(S)$ korral:

$$ef = fe = f \quad \Rightarrow \quad e = f.$$

Definitsioon 6.32 Lihtsat poolrühma S, mis sisaldab primitiivset idempotenti, nimetatakse **täiesti lihtsaks.**

Üks võimalik lähenemisviis täiesti lihtsatele poolrühmadele on kasutada minimaalseid ühepoolseid ideaale. Need defineeritakse sarnaselt minimaalsete ideaalidega (vt. definitsiooni 6.11).

Lemma 6.33 *Poolrühma iga minimaalne vasakpoolne (parempoolne) ideaal on selle poolrühma $\mathcal{L}$-klass ($\mathcal{R}$-klass).*

TÕESTUS. Teeme läbi tõestuse minimaalse vasakpoolse ideaali korral. Olgu L poolrühma S minimaalne vasakpoolne ideaal ja $x \in L$ suvaline element. Siis $S^1x \subseteq L$ ja tänu L minimaalsusele $S^1x = L$. Fikseerides mingi elemendi $a \in L$ näeme, et iga $x \in L$ korral $S^1x = L = S^1a$. Järelikult $x\mathcal{L}a$ ehk $x \in L_a$. Seega $L \subseteq L_a$.

Kui aga $c \in L_a$, siis $c \in S^1c = S^1a = L$. See tähendab, et $L_a \subseteq L$. Kokkuvõttes oleme näidanud, et $L = L_a$, s.t. L on elemendi a $\mathcal{L}$-klass. □

Lause 6.34 *Olgu S poolrühm.*

1. *Kui L on poolrühma S minimaalne vasakpoolne ideaal, siis $L = Sa$ iga $a \in L$ korral.*
2. *Kui R on poolrühma S minimaalne parempoolne ideaal, siis $R = aS$ iga $a \in R$ korral.*

TÕESTUS. Hulk Sa on vasakpoolne ideaal poolrühma S jaoks ning $Sa \subseteq L$. Kuna L on minimaalne vasakpoolne ideaal, siis $Sa = L$.

Lause teise poole tõestus on analoogiline. □

Järgmiseks tõestame ühe piisava tingimuse selleks, et poolrühm oleks oma minimaalsete vasakpoolsete (parempoolsete) ideaalide ühend.

Lause 6.35 *Kui S on lihtne poolrühm ja sisaldab minimaalset vasakpoolset ideaali L (minimaalset parempoolset ideaali R), siis S on oma minimaalsete vasakpoolsete (parempoolsete) ideaalide ühend.*

TÕESTUS. Olgu S lihtne poolrühm ja olgu L minimaalne vasakpoolne ideaal. Olgu $s \in S$, tähistame $Ls = \{as \mid a \in L\}$. Siis hulk Ls on vasakpoolne ideaal poolrühmas S. Näitame, et Ls on minimaalne vasakpoolne ideaal. Oletame, et $B \neq \emptyset$ on vasakpoolne ideaal poolrühmas S ja $B \subseteq Ls$. Siis hulk

$$A = \{a \in L \mid as \in B\} \subseteq L$$

on vasakpoolne ideaal poolrühmas S. Tänu L minimaalsusele kehtib võrdus $A = L$. Teiste sõnadega: iga $a \in L$ korral $as \in B$ ehk $Ls \subseteq B$. Seega $B = Ls$. Nüüd olgu

$$M = \bigcup_{s \in S} Ls.$$

Siis kindlasti M on vasakpoolne ideaal. See on tegelikult ideaal, sest kui $m \in Ls \subseteq M$, siis $mt \in L(st) \subseteq M$ iga $t \in S$ korral. Siit järeldub S lihtsuse tõttu, et $M = S$, ning oleme näidanud, et S on minimaalsete vasakpoolsete ideaalide Ls ühend.

Lause teise poole tõestus on analoogiline. □

Järgmine tulemus on erijuhuks niinimetatud Greeni lemmast. Greeni lemma sõnastuse ja tõestuse üldjuhul võib leida raamatust [2] (lemma 6.8.2).

Lemma 6.36 *Olgu S poolrühm, $a, b \in S$ ja $b \mathcal{H} ab$. Tähistame $H := H_b = H_{ab}$. Siis kujutus*

$$\lambda_a : H \to H, \quad x \mapsto ax$$

on bijektiivne.

TÕESTUS. Väite tõestamiseks näitame, et a) eeskiri $x \mapsto ax$ on kujutus $H \longrightarrow H$ ja et b) sellel kujutusel leidub pöördkujutus.

Kuna $ab \mathcal{H} b$, siis $ab \mathcal{L} b$. Lause 6.25 põhjal leidub selline element $v \in S^1$, et $vab = b$.

Olgu $x \in H = H_b = H_{ab}$. Siis $x \mathcal{R} b$ ja seega $x = bs$ mingi elemendi $s \in S^1$ korral. Järelikult

$$vax = vabs = bs = x. \tag{6.1}$$

Kuna $\mathcal{R}$ on vasakpoolne kongruents, siis $ax \mathcal{R} ab$. Et $vax = x$, siis $ax \mathcal{L} x$. Kuna $x \mathcal{L} ab$ (sest $x \mathcal{H} ab$), siis transitiivsuse tõttu $ax \mathcal{L} ab$. Sellega oleme näidanud, et $ax \mathcal{H} ab$ ehk $ax \in H_{ab} = H$. Järelikult λ_a on tõepoolest kujutus $H \to H$.

Veendume, et ka

$$\lambda_v : H \to H, \quad y \mapsto vy$$

on kujutus. Kui $y \in H = H_{ab} = H_b$, siis $y \mathcal{R} ab$, seega $y = abt$ mingi $t \in S^1$ korral ja

$$avy = av(abt) = a(vab)t = abt = y. \tag{6.2}$$

Kuna $\mathcal{R}$ on vasakpoolne kongruents, siis $vy \mathcal{R} vab = b$. Et $avy = y$, siis $vy \mathcal{L} y$. Kuna $y \mathcal{L} b$ (sest $y \mathcal{H} b$), siis transitiivsuse tõttu $vy \mathcal{L} b$ ning seega $vy \mathcal{H} b$ ehk $vy \in H_b = H$. Järelikult λ_v on kujutus $H \to H$.

Võrdustest (6.1) ja (6.2) näeme, et λ_a ja λ_v on teineteise pöörkujutused, seega bijektiivsed. □

Lemma 6.37 *Mittetühi poolrühm S on rühm parajasti siis, kui $aS = S$ ja $Sa = S$ iga $a \in S$ korral.*

TÕESTUS. TARVILIKKUS. Seda on lihtne kontrollida.

PIISAVUS. Fikseerime mingi elemendi $a \in S$. Siis $aS = S$. Muuhulgas leidub selline element $e \in S$, et $a = ae$. Kui $s \in S = Sa$, siis $s = ua$ mingi $u \in S$ korral ja seega $se = uae = ua = s$. Niisiis $se = s$ iga $s \in S$ korral. Analoogiliselt saab leida elemendi $f \in S$ nii, et $fs = s$ iga $s \in S$ korral. Järelikult

$$f = fe = e$$

ja S on monoid ühikelemendiga e.

Kui $s \in S$, siis võrdustest $S = sS$ ja $S = Ss$ järeldub, et $e = su$ ja $e = vs$ mingite $u, v \in S$ korral. Siis aga

$$v = ve = v(su) = (vs)u = eu = u,$$

s.t. u on elemendi s pöördelement. □

Üldiselt poolrühma $\mathcal{H}$-klassid ($\mathcal{L}$-klassid, $\mathcal{R}$-klassid, $\mathcal{D}$-klassid, $\mathcal{J}$-klassid) ei pruugi olla alampoolrühmad. Vaatleme ühte olukorda, kus $\mathcal{H}$-klassid on alampoolrühmad.

Lause 6.38 *Järgmised väited poolrühma S $\mathcal{H}$-klassi H kohta on samaväärsed.*

1. *Leidub $e^2 = e \in H$.*
2. *Leiduvad $a, b \in H$ nii, et $ab \in H$.*
3. *H on poolrühma S alampoolrühm, mis on rühm.*

TÕESTUS. 1. $\Rightarrow$ 2. Võtame $a = b = e$.

2. $\Rightarrow$ 3. Olgu $a, b \in H$ sellised, et $ab \in H$. Lemma 6.36 põhjal on kujutus

$$\lambda_a : H \to H, \quad x \mapsto ax$$

bijektiivne. Kuna λ_a on kujutus, siis $ac \in H$ iga $c \in H$ korral ning kuna λ_a on sürjektiivne, siis $H = aH$. Nüüd iga $c \in H$ korral $a \mathcal{H} ac$ ja seega $H = H_a = H_{ac}$. Lemmaga 6.36 duaalne tulemus (mille tõestus on täiesti analoogiline) ütleb, et ka

$$\rho_c : H \to H, \quad x \mapsto xc$$

on bijektiivne kujutus. Seega $Hc = H$ iga $c \in H$ korral. Kuna $dc \in H$ mistahes $d, c \in H$ korral, siis H on kinnine korrutamise suhtes, s.t. alampoolrühm. Muuhulgas $cc \in H$ iga $c \in H$ korral. Võttes a ja b ossa c ja kasutades tõestuse alguse mõttekäiku näeme, et ka $H = cH$ iga $c \in H$ korral Kokkuvõttes $cH = H = Hc$ iga $c \in H$ korral. Me oleme juba näidanud, et H on S alampoolrühm, järelikult ka ise poolrühm. Et $a \in H$, siis H on mittetühi. Lemma 6.37 kohaselt on H rühm.

3. $\Rightarrow$ 1. Idempotendiks e sobib rühma H ühikelement. □

Lause 6.39 *Täiesti lihtsa poolrühma kõik $\mathcal{H}$-klassid on rühmad.*

TÕESTUS. Olgu S täiesti lihtne poolrühm ja e tema primitiivne idempotent. Näitame, et Se on minimaalne vasakpoolne ideaal. Selleks oletame, et $I \neq \emptyset$ on vasakpoolne ideaal ja $I \subseteq Se$. Võtame mingi elemendi $a \in I$. Kuna $a \in Se$, siis leidub selline $s \in S$, et $a = se$. Järelikult $ae = see = se = a$. Et S on lihtne, siis $S^1 a S^1 = S$ ning seega $e = uav$ mingite $u, v \in S^1$ korral. Tähistame $f := eveua$. Kasutades võrdusi $ae = a$ ja $uav = e$ saame, et

$$\begin{aligned} f^2 &= (eveua)(eveua) = (eveu)(ae)(veua) = (eveu)a(veua) = (eve)(uav)(eua) \\ &= eveeeua = eveua = f, \\ ef &= eeveua = eveua = f, \\ fe &= eveuae = eveua = f. \end{aligned}$$

Kuna e on primitiivne idempotent, siis $e = f$ ehk $e = eveua \in I$, sest $a \in I$ ja I on vasakpoolne ideaal. Seega iga $t \in S$ korral $te = teveua \in I$. Järelikult $Se \subseteq I$ ning kokkuvõttes oleme saanud, et $I = Se$. Sellega on näidatud, et Se on minimaalne vasakpoolne ideaal.

Lause 6.35 põhjal on S on oma minimaalsete vasakpoolsete ideaalide ühend. Olgu $a \in S$. Siis leidub minimaalne vasakpoolne ideaal L nii, et $a \in L$. Siis ka $a^2 \in L$. Lemma 6.33 põhjal on L poolrühma S $\mathcal{L}$-klass, seega $a\mathcal{L}a^2$. Analoogiliselt saab näidata, et $a\mathcal{R}a^2$. Järelikult $a\mathcal{H}a^2$ ehk $a^2 \in H_a$. Tänu lausele 6.38 on H_a rühm. □

Järgnev lause annab piisava tingimuse selleks, et poolrühm oleks täiesti lihtne.

Lause 6.40 *Olgu S lihtne poolrühm, mis sisaldab vähemalt ühte minimaalset vasakpoolset ideaali ning vähemalt ühte minimaalset parempoolset ideaali. Siis poolrühma S iga minimaalse vasakpoolse ideaali L ja iga minimaalse parempoolse ideaali R korral kehtivad tingimused:*

1. *$LR = S$;*
2. *RL on rühm;*
3. *rühma RL ühikelement e on primitiivne idempotent.*

Seega S on täiesti lihtne.

Tõestus. 1. Olgu L poolrühma S minimaalne vasakpoolne ideaal ja R minimaalne parempoolne ideaal. Siis on hulk $LR = \{xy \mid x \in L, y \in R\}$ ideaal ja seega poolrühma S lihtsuse tõttu $LR = S$.

2. Paneme tähele, et $RL \subseteq R \cap L$. Näitamaks, et see on rühm, peavad iga $a \in RL$ korral kehtima võrdused $RLa = RL = aRL$ (vt. lemmat 6.37). Kuna L on vasakpoolne ideaal, siis ka hulk $La = \{xa \mid x \in L\}$ on vasakpoolne ideaal. Samas $La \subseteq L$, sest $a \in RL \subseteq L$. Siit L minimaalsuse tõttu $La = L$, millest järeldub võrdus $RLa = RL$. Võrduse $aRL = RL$ tõestus on analoogiline.

3. Olgu e rühma RL ühikelemenet ja eeldame, et f on poolrühma S idempotent, mille korral $ef = fe = f$. Nüüd kuna $e \in R \cap L$, siis lause 6.34 põhjal $R = eS$ ning $L = Se$. Järelikult

$$f = f^2 = (ef)(fe) \in (eS)(Se) = RL\,.$$

Kuna rühmas leidub täpselt üks idempotent, siis $e = f$. Seega e on primitiivne idempotent poolrühmas S. □

Käesoleva paragrahvi põhitulemus on järgmine teoreem.

Teoreem 6.41 *Olgu S lihtne poolrühm. Siis järgmised väited on samaväärsed:*

1. *S on täiesti lihtne;*
2. *S on rühmade ühend;*
3. *S kõik vasakpoolsed ja parempoolsed peaideaalid on minimaalsed;*

4. *S sisaldab vähemalt ühte minimaalset vasakpoolset ideaali ja vähemalt ühte minimaalset parempoolset ideaali.*

TÕESTUS. 1. $\Rightarrow$ 2. See järeldub lausest 6.39, sest S on oma $\mathcal{H}$-klasside lõikumatu ühend ja kõik $\mathcal{H}$-klassid on rühmad.

2. $\Rightarrow$ 3. Eeldame, et S on rühmade ühend. Vaatame vasakpoolset peaideaali S^1b, kus $b \in S$. Olgu $I \subseteq S^1b$ mingi mittetühi vasakpoolne ideaal ja $a \in I$. Siis $S^1a \subseteq I \subseteq S^1b$. Kui näitame, et $S^1a = S^1b$, siis ka $S^1b = I$ ja seega S^1b on minimaalne vasakpoolne ideaal.

Niisiis, on vaja näidata, et

$$S^1b \subseteq S^1a.$$

Selleks piisab, kui tõestame, et $b \in S^1a$. Kuna $a \in S^1b$, siis leidub selline $u \in S^1$, et $a = ub$. Lihtsuse tõttu leiduvad poolrühmas S^1 elemendid x, y nii, et $b = xay$. Seega

$$b = (xu)by.$$

Eelduse põhjal kuulub element $g = xu \in S$ mingisse alampoolrühma G, mis on rühm. Olgu G ühikelement e. Selles alamrühmas G leidub elemendil g pöördelement g^{-1}.
Siis

$$b = gby = egby = eb = g^{-1}gb = g^{-1}(xu)b = g^{-1}x(ub) = g^{-1}xa,$$

mis tähendab, et $b \in S^1a$. Seda oligi vaja.

Analoogiliselt on kõik S parempoolsed peaideaalid minimaalsed.

3. $\Rightarrow$ 4. See on ilmne.

4. $\Rightarrow$ 1. See järeldub lausest 6.40. □

Järeldus 6.42 *Lõplik poolrühm on täiesti lihtne parajasti siis, kui ta on lihtne.*

TÕESTUS. Lõplik poolrühm peab sisaldama minimaalset vasakpoolset ideaali ja minimaalset parempoolset ideaali. □

6.5 Reesi maatrikspoolrühmad

Osutub, et täiesti lihtsad poolrühmad on võimalik saada suhteliselt lihtsa konstruktsiooni abil rühmadest. Seda konstruktsiooni kirjeldas esimesena David Rees[2].

Olgu G rühm ühikelemendiga 1 ning olgu I, Λ mittetühjad hulgad. Võtame ühe $(\Lambda \times I)$-maatriksi $P = (p_{\lambda i})$, mille elemendid kuuluvad rühma G. Sellist maatriksit võib vaadelda kujutusena $\Lambda \times I \longrightarrow G, (\lambda, i) \mapsto p_{\lambda i}$.

Olgu $S = I \times G \times \Lambda$ ja defineerime hulka S kuuluvate järjestatud kolmikute korrutamise järgmiselt:

$$(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda j}h, \mu),$$

$(i, g, \lambda), (j, h, \mu) \in S$. Märgime, et korrutis $gp_{\lambda j}h$ leitakse rühmas G.

[2]David Rees (1918–2013) — briti matemaatik

Lemma 6.43 *S on poolrühm.*

TÕESTUS. Kontrollime kas hulgal S defineeritud korrutamine on assotsiatiivne. Tõepoolest:

$$\begin{aligned}((i,g,\lambda)(i',g',\lambda'))(i'',g'',\lambda'') &= (i, gp_{\lambda,i'}g', \lambda')(i'',g'',\lambda'')\\ &= (i, (gp_{\lambda,i'}g')p_{\lambda',i''}g'', \lambda'')\\ &= (i, gp_{\lambda,i'}(g'p_{\lambda',i''}g''), \lambda'')\\ &= (i,g,\lambda)(i', g'p_{\lambda',i''}g'', \lambda'')\\ &= (i,g,\lambda)((i',g',\lambda')(i'',g'',\lambda'')).\end{aligned}$$

□

Niimoodi konstrueeritud poolrühma tähistatakse $\mathcal{M}[G; I, \Lambda; P]$ ja nimetatakse $I \times \Lambda$ Reesi maatrikspoolrühmaks üle rühma G "sändvitšmaatriksiga" P.

Ülesanne 6.44 Olgu $I = \{i, j\}$, $\Lambda = \{\lambda, \mu\}$ ja $G = (\mathbb{Z}_2, +)$. Anname kujutuse $P : \Lambda \times I \longrightarrow G$ maatriksiga

	i	j
λ	$\overline{1}$	$\overline{0}$
μ	$\overline{1}$	$\overline{0}$

.

Kirjutage välja Reesi maatrikspoolrühma $\mathcal{M}[G; I, \Lambda; P]$ korrutamistehte Cayley tabel.

Lause 6.45 *Poolrühm $\mathcal{M} = \mathcal{M}[G; I, \Lambda; P]$ on täiesti lihtne.*

TÕESTUS. Kontrollimaks, et poolrühm $\mathcal{M}$ on lihtne, võib tähele panna, et poolrühma $\mathcal{M}$ iga kahe elemendi (i, a, λ) ja (j, b, μ) korral

$$(j, a^{-1}p_{\lambda i}^{-1}, \lambda)(i, a, \lambda)(i, p_{\lambda i}^{-1}b, \mu) = (j, a^{-1}p_{\lambda i}^{-1}p_{\lambda i}ap_{\lambda i}p_{\lambda i}^{-1}b, \mu) = (j, b, \mu).$$

Lause 6.18 põhjal on poolrühm $\mathcal{M}$ lihtne.

Näitame, et $\mathcal{M}$ on täiesti lihtne poolrühm, see tähendab, et temas leidub primitiivne idempotent. Selleks vaatame elementi $(i, a, \lambda) \in \mathcal{M}$. Paneme tähele, et

$$\begin{aligned}(i,a,\lambda) \in E(\mathcal{M}) &\iff (i,a,\lambda)(i,a,\lambda) = (i,a,\lambda)\\ &\iff (i, ap_{\lambda i}a, \lambda) = (i,a,\lambda)\\ &\iff ap_{\lambda,i}a = a\\ &\iff p_{\lambda,i}a = 1\\ &\iff a = p_{\lambda,i}^{-1}.\end{aligned}$$

Seega poolrühma $\mathcal{M}$ idempotentide hulk

$$E(\mathcal{M}) = \{(i, p_{\lambda i}^{-1}, \lambda) \mid i \in I, \lambda \in \Lambda\}.$$

Võtame kaks idempotenti $e = (i, p_{\lambda i}^{-1}, \lambda)$ ja $f = (j, p_{\mu j}^{-1}, \mu)$ ning oletame, et $ef = fe = e$ ehk

$$(i, p_{\lambda i}^{-1}p_{\lambda j}p_{\mu j}^{-1}, \mu) = (j, p_{\mu j}^{-1}p_{\mu i}p_{\lambda i}^{-1}, \lambda) = (i, p_{\lambda i}^{-1}, \lambda),$$

Siis $j = i$ ja $\lambda = \mu$, kust järeldub, et $e = f$, sest ka $p_{\lambda i} = p_{\mu j}$ ja $p_{\lambda i}^{-1} = p_{\mu j}^{-1}$. Seega näeme, et kõik idempotendid on primitiivsed. Järelikult on poolrühm $\mathcal{M}$ täiesti lihtne. □

Teoreem 6.46 (Reesi teoreem) *Poolrühm on täiesti lihtne siis ja ainult siis, kui ta on isomorfne Reesi maatrikspoolrühmaga üle rühma.*

TÕESTUS. PIISAVUS. Järeldub lausest 6.45.
TARVILIKKUS. Seda tõestust me käesolevas kursuses anda ei jõua. □

6.6 Regulaarsed ja inverssed poolrühmad

Definitsioon 6.47 Poolrühma S nimetatakse **regulaarseks**, kui

$$(\forall a \in S)(\exists x \in S)\ a = axa.$$

Kui a ja x on sellised elemendid, et $a = axa$, siis $ax = axax$ ja $xa = xaxa$, mis tähendab, et ax ja xa on idempotendid. Seega regulaarsetes poolrühmades on üldiselt "palju" idempotente.

Näide 6.48 1. Kui poolrühma kõik elemendid on idempotendid, siis see poolrühm on regulaarne.

2. Kui X on mittetühi hulk, siis tema teisenduste poolrühm $\mathcal{T}(X)$ on regulaarne. Kui $f \in \mathcal{T}(X)$, siis defineerime teisenduse $g \in \mathcal{T}(X)$ nii, et ta viib iga elemendi hulgast $\mathrm{Im}\,(f)$ mingiks selle elemendi originaaliks f suhtes, ja kõigil teistel X elementidel on g defineeritud suvaliselt. Siis $f = fgf$.

3. Poolrühm $(\mathrm{Mat}_n(K), \cdot)$, kus K on korpus, on regulaarne. Ruutmaatriksi A Moore'i-Penrose'i pöördmaatriks A^+ rahuldab muuhulgas võrdust $AA^+A = A$.

Definitsioon 6.49 Poolrühma S elementi a' nimetatakse elemendi a **inversseks elemendiks**, kui $a = aa'a$ ja $a' = a'aa'$.

Lause 6.50 *Regulaarse poolrühma igal elemendil leidub vähemalt üks inversne element.*

TÕESTUS. Olgu S regulaarne poolrühm ja $a \in S$. Siis leidub $x \in S$ nii, et $a = axa$. Tähistame $a' := xax$. Siis

$$aa'a = a(xax)a = (axa)xa = axa = a$$

ja

$$a'aa' = (xax)a(xax) = x(axa)xax = x(axa)x = xax = a'.$$

□

Definitsioon 6.51 Poolrühma nimetatakse **inversseks**, kui tema igal elemendil leidub täpselt üks inversne element.

Edaspidi tähistame inversse poolrühma elemendi a üheselt määrtaud inversset elementi sümboliga a'. Definitsioonist järeldub, et $(a')' = a$. Kuna iga idempotent e on iseenda inversne element, siis inversses poolrühmas $e' = e$.

Näide 6.52 Iga rühm on inversne poolrühm, kus $a' = a^{-1}$.

On selge, et iga inversne poolrühm on regulaarne. Järgmine tulemus ütleb, millised regulaarsed poolrühmad on inverssed.

Teoreem 6.53 *Regulaarne poolrühm on inversne parajasti siis, kui tema idempotendid kommuteeruvad.*

TÕESTUS. TARVILIKKUS. Olgu S inversne poolrühm ja olgu $e, f \in S$ idempotendid. Siis korrutise ef inversne element x rahuldab võrdusi

$$efxef = ef \quad \text{ja} \quad xefx = x.$$

Kuna

$$(fxe)(fxe) = f(xefx)e = fxe,$$

siis fxe on idempotent ja seega iseenda inversne element. Näitame, et ka ef on fxe inversne element. Tõepoolest,

$$effxeef = efxef = ef$$

ja

$$fxeeffxe = fxefxe = fxe.$$

Kuna S on inversne poolrühm, siis $ef = fxe$. Siit järeldub, et $fef = ef$ ja $efe = ef$. Vahetades ära e ja f rollid saame, et peavad kehtima ka võrdused

$$efe = fe \quad \text{ja} \quad fef = fe.$$

Järelikult $ef = fe$.

PIISAVUS. Olgu S regulaarne poolrühm, mille idempotendid kommuteeruvad ja olgu $a \in S$ suvaline. Oletame, et $a', a'' \in S$ on mõlemad elemendi a inverssed elemendid. Siis

$$a = aa'a,\ a' = a'aa',\ a = aa''a,\ a'' = a''aa''$$

ning $aa', aa'', a'a, a''a$ on idempotendid. Järelikult

$$aa' = (aa''a)a' = (aa'')(aa') = (aa')(aa'') = (aa'a)a'' = aa''.$$

Analoogiliselt saab näidata, et $a'a = a''a$. Neid võrdusi kasutades saame, et

$$a' = a'aa' = (a'a)a' = (a''a)a' = a''(aa') = a''(aa'') = a''aa'' = a''.$$

□

Näide 6.54 Kommutatiivne poolrühm, mille kõik elemendid on idempotendid, on inversne. Näiteks $(\mathbb{Z}, \min)$ on selline poolrühm.

Peatükk 7

Polügoonid

7.1 Põhimõisted

Polügoone on võimalik vaadelda nii üle poolrühmade kui monoidide. Selles kursuses vaatleme ainult polügoone üle monoidide ja selle paragrahvi jooksul eeldame kõikjal, et S on monoid ühikelemendiga 1.

Definitsioon 7.1 Hulka A nimetatakse **parempoolseks polügooniks üle monoidi** S ehk **parempoolseks** S**-polügooniks**, kui on antud kujutus $A \times S \to A, (a, s) \mapsto as$, nii, et

1. $(as)t = a(st)$,
2. $a1 = a$

mistahes $a \in A$ ja $s, t \in S$ korral. Kujutust $A \times S \to A$ nimetatakse ka monoidi S **toimeks** hulgal A.

Parempoolset S-polügooni tähistatakse harilikult nii: A_S. Analoogiliselt saab defineerida vasakpoolsed S-polügoonid. Selles kursuses vaatleme enamasti parempoolseid S-polügoone.

Näide 7.2 1. Olgu $(R, +, \cdot)$ ring. Siis iga parempoolne R-moodul on polügoon üle selle ringi multiplikatiivse monoidi $(R, \cdot)$.

2. Olgu S monoid. Siis S on polügoon üle iseenda, kui toime defineerida monoidi S korrutamise abil. Seda polügooni tähistatakse S_S.

3. Olgu A mittetühi hulk ja $\mathcal{T}$ selle hulga kõigi teisenduste monoid järjestrakendamise suhtes. Defineerides vasakpoolse toime $\mathcal{T} \times A \longrightarrow A$ võrdusega

$$fa := f(a)$$

$a \in A$, $f \in \mathcal{T}$, saame vasakpoolse polügooni ${}_{\mathcal{T}}A$.

4. Automaatide teoorias vaadeldavad automaadid on polügoonid. Selles teoorias tõlgendatakse hulka A kui automaadi olekute hulka, hulka S kui sisendite hulka ja toimet

mõistetakse nii, et olekus a oleva automaadi mõjutamisel sisendiga s läheb see automaat üle uude olekusse as. Automaatide teoorias võetakse monoidiks S tihti mõni vaba monoid.

5. Geomeetriast tuntud afiinsed ruumid on polügoonid. Afiinne ruum on punktide hulk, millele saab liita mingist vektorruumist V pärit vektoreid nii, et tulemuseks on punkt. See polügoon on üle vektoruumi aditiivse monoidi $(V, +)$.

Definitsioon 7.3 Alamhulka B nimetatakse polügooni A_S **alampolügooniks**, kui iga $b \in B$ ja $s \in S$ korral $bs \in B$.

Näide 7.4 Olgu S monoid. Siis S iga parempoolne ideaal on polügooni S_S alampolügoon. Muuhulgas parempoolsed peaideaalid sS, kus $s \in S$, on polügooni S_S alampolügoonid.

Mistahes S-polügoonil A_S on olemas triviaalsed alampolügoonid $\emptyset$ ja A.

Definitsioon 7.5 Polügooni nimetatakse **lahutumatuks**, kui teda ei saa esitada kahe mittetühja lõikumatu alampolügooni ühendina.

Näide 7.6 Olgu $s \in S$. Näitame, et sS on lahutumatu polügoon. Oletame vastuväiteliselt, et $sS = C_S \sqcup D_S$, kus C_S ja D_S on mittetühjad alampolügoonid. Oletame, et $s \in C$. Siis $sS \subseteq C$ ja seega $C \sqcup D = sS \subseteq C$, kust $D \subseteq C$, mis on vastuolus C ja D lõikumatusega. Analoogiliselt saaksime vastuolu siis, kui oletaksime, et $s \in D$. Rohkem võimalusi s jaoks ei ole.

Näide 7.7 Olgu S suvaline monoid ja $A = \{a_1, \ldots, a_n\}$, kus $n \geq 2$, mingi hulk. Defineerime S-toime järgmiselt:

$$a_i s := a_i$$

iga $i \in \{1, \ldots, n\}$ ja iga $s \in S$ korral. On selge, et nii saame parempoolse S-polügooni, kus iga alamhulk on alampolügoon. Kuna näiteks

$$A_S = \{a_1\} \sqcup \{a_2, \ldots, a_n\},$$

siis see polügoon on lahutuv.

Lause 7.8 *Iga mittetühi polügoon on esitatav mittetühjade lahutumatute alampolügoonide lõikumatu ühendina.*

Tõestus. Vaatleme polügooni A_S. Defineerime hulgal A binaarse seose ρ järgmiselt: $a \rho b$ parajasti siis, kui leiduvad sellised $b_1, \ldots, b_n \in A$ ja $s_1, \ldots, s_n, t_1, \ldots, t_n \in S$, et

$$\begin{array}{rcl} a & = & b_1 s_1 \\ b_1 t_1 & = & b_2 s_2 \\ b_2 t_2 & = & b_3 s_3 \\ & \cdots & \\ b_n t_n & = & b. \end{array} \tag{7.1}$$

Saab näidata, et seos ρ on ekvivalentsiseos. Seega A on ρ-klasside lõikumatu ühend. Paneme veel tähele, et kui $as = bt$, $a, b \in A$, $s, t \in S$, siis $a \rho b$. Tõepoolest,

$$\begin{array}{rcl} a & = & a1 \\ as & = & bt \\ b1 & = & b. \end{array}$$

Muuhulgas, kuna $as \cdot 1 = a \cdot s$, siis $as\rho a$ iga $a \in A$ ja $s \in S$ korral. Oletame, et $b \in [a]_\rho$. Siis $a\rho b$ ja sobivate elementide korral kehtivad võrdused (7.1). Korrutades kõiki võrdusi paremalt suvalise S elemendiga s saame võrdused

$$\begin{aligned} as &= b_1 s_1 s \\ b_1 t_1 s &= b_2 s_2 s \\ b_2 t_2 s &= b_3 s_3 s \\ &\dots \\ b_n t_n s &= bs, \end{aligned}$$

kust näeme, et $as\rho bs$. Et $a\rho as$, siis transitiivsuse tõttu $a\rho bs$ ehk $bs \in [a]_\rho$. See tähendab, et iga ρ-klass $[a]_\rho$ on alampolügoon.

Tõestuse lõpetamiseks näitame, et ρ-klassid on lahutumatud. Oletame vastuväiteliselt, et

$$[a]_\rho = C \sqcup D\,,$$

kus C ja D on polügooni A_S mittetühjad alampolügoonid. Valime mingid elemendid $c \in C$ ja $d \in D$. Siis $c\rho a\rho d$ ja seega $c\rho d$. Järelikult leiduvad sellised $b_1, \dots, b_n \in A$ ja $s_1, \dots, s_n, t_1, \dots, t_n \in S$, et

$$\begin{aligned} c &= b_1 s_1 \\ b_1 t_1 &= b_2 s_2 \\ b_2 t_2 &= b_3 s_3 \\ &\dots \\ b_n t_n &= d. \end{aligned}$$

Siit näeme, et

$$a\rho c\rho b_1 \rho b_2 \rho \dots \rho b_n \rho d.$$

Järelikult $b_1, \dots, b_n, d \in [a]_\rho = C \sqcup D$. Kui $b_1 \in D$, siis $c = b_1 s_1 \in C \cap D$, mis on vastuolus eeldusega, et $C \cap D = \emptyset$. Seega $b_1 \in C$. Analoogiliselt näeme, et ka $b_2, \dots, b_n, d \in C$. Viimane ($d \in C$) on aga samuti vastuolus sellega, et $C \cap D = \emptyset$. □

7.2 Vabad polügoonid

Definitsioon 7.9 Kujutust $f : A_S \to B_S$ nimetatakse **polügoonide homomorfismiks**, kui ta säilitab monoidi toime, s.t.

$$f(as) = f(a)s$$

iga $a \in A$ ja $s \in S$ korral. **Isomorfism** on bijektiivne homomorfism.

Definitsioon 7.10 Ütleme, et polügoon B_S on polügooni A_S **epimorfne kujutis**, kui leidub sürjektiivne homomorfism $f : A_S \to B_S$.

Definitsioon 7.11 Polügooni A_S alamhulka X nimetatakse **baasiks**, kui iga $a \in A$ korral leiduvad üheselt määratud $x \in X$ ja $s \in S$ nii, et $a = xs$.

Definitsioon 7.12 Polügooni nimetatakse **vabaks**, kui temas leidub baas.

Näide 7.13 Polügoon S_S on vaba, tema baas on $\{1\}$.

Anname vabade polügoonide kirjelduse. See on mingis mõttes sarnane teoreemis 1.55 antud vektorruumide kirjeldusega.

Teoreem 7.14 *Polügoon F_S on vaba parajasti siis, kui leidub hulk I nii, et*

$$F = \bigsqcup_{i \in I} F_i,$$

kus $F_i \cong S_S$ iga $i \in I$ korral.

TÕESTUS. TARVILIKKUS. Olgu X polügooni F_S baas. Baasi definitsiooni tõttu $F = \bigcup_{x \in X} xS$, kus hulk $xS = \{xs \mid s \in S\}$ on polügooni F_S alampolügoon iga $x \in X$ korral. Kui $x \neq y$, siis $xS \cap yS = \emptyset$, sest vastasel korral $xs = yt$ mingite $s, t \in S$ korral, mis on vastuolus ühesuse nõudega baasi definitsioonis. Seega

$$F = \bigsqcup_{x \in X} xS.$$

Kujutus

$$f : S \to xS, \quad s \mapsto xs$$

on ilmselt parempoolsete S-polügoonide sürjektiivne homomorfism. Kui $xs = xt$, $s, t \in S$, siis baasi definitsiooni tõttu $s = t$. Seega f on ka injektiivne, mis tähendab, et f on isomorfism. Niisiis $xS \cong S_S$ iga $x \in X$ korral.

PIISAVUS. Olgu $f_i : S_S \to F_i$, $i \in I$, parempoolsete S-polügoonide isomorfismid. Tähistame $x_i := f_i(1) \in F_i$. Et F on alampolügoonide F_i, $i \in I$, ühend, siis iga $a \in F$ korral leiduvad $i \in I$ ja $s \in S$ nii, et

$$a = f_i(s) = f_i(1)s = x_i s.$$

Kui $a = x_i s = x_j t \in F_i \cap F_j$, kus $i, j \in I$ ja $s, t \in S$, siis lõikumatuse tõttu $i = j$. Kuna

$$f_i(s) = x_i s = x_i t = f_i(t),$$

siis f_i injektiivsuse tõttu $s = t$. Seega iga $a \in F$ esitub üheselt kujul $a = x_i s$, kus $i \in I$ ja $s \in S$. See tähendab, et $\{x_i \mid i \in I\}$ on polügooni F_S baas ja F_S on vaba. □

Sellest teoreemist on näha, et polügoonide vabadus on väga tugev omadus, s.t. selliseid polügoone on väga vähe.

Lause 7.15 *Iga polügoon on vaba polügooni epimorfne kujutis.*

TÕESTUS. Olgu A_S polügoon. Defineerime hulgal $A \times S$ toime järgmiselt:

$$(a, s)t := (a, st),$$

$a \in A$, $s, t \in S$. Lihtne on veenduda, et tulemuseks on parempoolne S-polügoon. Tähistame seda polügooni sümboliga F_S. Nüüd

$$F_S = A \times S = \bigsqcup_{a \in A} \{a\} \times S,$$

kusjuures alampolügoonid $\{a\} \times S = \{(a, s) \mid s \in S\}$ on isomorfsed polügooniga S_S. Seega F_S on vaba polügoon teoreemi 7.14 põhjal. Defineerime kujutuse $f : F \to A$ võrdusega

$$f(a, s) := as.$$

See kujutus on homomorfism, sest

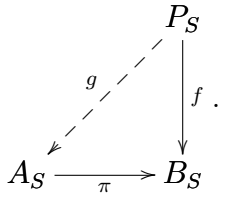
$$f((a, s)t) = f(a, st) = a(st) = (as)t = f(a, s)t$$

iga $a \in A$ ja $s, t \in S$ korral. Kujutus f on ka sürjektiivne, sest $f(a, 1) = a1 = a$ iga $a \in A$ korral. Seega A_S on vaba polügooni F_S epimorfne kujutis. □

7.3 Projektiivsed polügoonid

Selles paragrahvis vaatleme polügoonide projektiivsuse omadust. Osutub, et see on mõnevõrra nõrgem kui vabaduse omadus.

Definitsioon 7.16 Polügooni P_S nimetatakse **projektiivseks**, kui iga sürjektiivse homomorfismi $\pi : A_S \to B_S$ ja iga homomorfismi $f : P_S \to B_S$ korral leidub homomorfism $g : P_S \to A_S$ nii, et $\pi g = f$, s.t. järgmine diagramm on kommutatiivne:

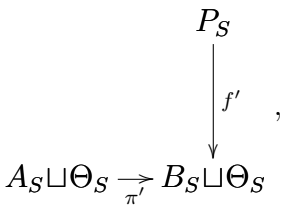


Näide 7.17 Tühi polügoon $\emptyset_S$ on projektiivne, sest ainuke homomorfism $\emptyset_S \longrightarrow B_S$ on tühi kujutus ja seega ka g ossa sobib tühi kujutus.

Edasises kirjeldame ära mittetühjad projektiivsed S-polügoonid.

Lause 7.18 *Olgu polügoon P_S oma mittetühjade alampolügoonide P_i, $i \in I$, lõikumatu ühend, s.t. $P_S = \bigsqcup_{i \in I} P_i$. Polügoon P_S on projektiivne parajasti siis, kui iga $i \in I$ korral polügoon P_i on projektiivne.*

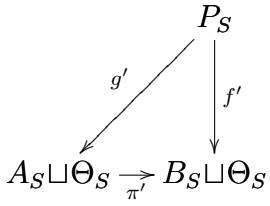
TÕESTUS. TARVILIKKUS. Olgu P_S projektiivne ning $j \in J$. Näitame, et P_j on projektiivne. Olgu $f : P_j \to B_S$ homomorfism ja $\pi : A_S \to B_S$ sürjektiivne homomorfism. Vaatleme diagrammi



kus $\Theta_S = \{\theta\}$ on üheelemendiline polügoon (s.t. $\theta s = \theta$ iga $s \in S$ korral) ja kujutused π', f' on defineeritud võrdustega

$$\pi'(x) = \begin{cases} \pi(x), & \text{kui } x \in A, \\ \theta, & \text{kui } x = \theta, \end{cases}$$
$$f'(y) = \begin{cases} f(y), & \text{kui } y \in P_j, \\ \theta, & \text{kui } y \in P \setminus P_j. \end{cases}$$

Lihtne on aru saada, et π' ja f' on homomorfismid ning π' on sürjektiivne. Kuna P_S on projektiivne, siis leidub homomorfism $g' : P_S \to A_S \sqcup \Theta_S$ nii, et $\pi' g' = f'$.



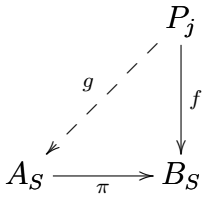
Olgu $y \in P_j$. Kui oletaksime, et $g'(y) = \theta$, siis

$$f(y) = f'(y) = \pi'(g'(y)) = \pi'(\theta) = \theta\,,$$

mis ei ole võimalik. Seega $g'(y) \in A$. See lubab meil defineerida kujutuse $g : P_j \to A$ võrdusega

$$g(y) := g'(y).$$

Ilmselt g on homomorfism.

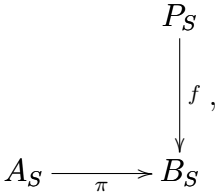


Iga $y \in P_j$ korral

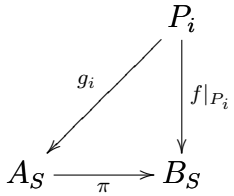
$$(\pi g)(y) = \pi(g'(y)) = \pi'(g'(y)) = f'(y) = f(y).$$

Järelikult $\pi g = f$, nagu vaja.

Piisavus. Eeldame, et kõik alampolügoonid P_i, $i \in I$, on projektiivsed. Vaatleme diagrammi



kus π on sürjektiivne. Siis iga $i \in I$ korral leidub homomorfism $g_i : P_i \to A_S$ nii, et diagramm



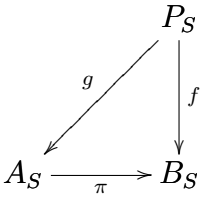
on kommutatiivne. Defineerime kujutuse $g : P \to A$ võrdusega

$$g(x) := g_i(x),$$

kus $x \in P_i$ (iga $x \in P$ peab kuuluma mingisse alampolügooni P_i). Siis iga $i \in I$ ja iga $x \in P_i$ korral

$$\pi(g(x)) = \pi(g_i(x)) = f|_{P_i}(x) = f(x)$$

ehk diagramm



on kommutatiivne. □

Märgime, et kui $e \in S$ on idempotent, siis $eS = \{es \mid s \in S\}$ on polügooni S_S alampolügoon (vt. näidet 7.4) ja seega ise ka parempoolne S-polügoon. Tuleb välja, et mittetühjad projektiivsed S-polügoonid on parajasti seda tüüpi polügoonide lõikumatud ühendid.

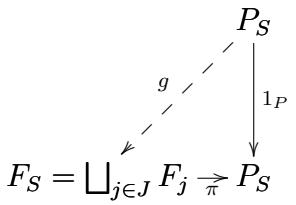
Teoreem 7.19 *Mittetühi polügoon P_S on projektiivne parajasti siis, kui*

$$P = \bigsqcup_{i \in I} P_i,$$

kusjuures iga $i \in I$ korral leidub idempotent $e_i \in S$ nii, et $P_i \cong e_i S$.

TÕESTUS. TARVILIKKUS. Olgu A_S mittetühi projektiivne polügoon. Kasutades lauset 7.8 saab polügooni A_S esitada mittetühjade lahutumatute alampolügoonide A_i, $i \in I$, lõikumatu ühendina. Vastavalt lausele 7.18 on polügoonid A_i projektiivsed. Seega piisab näidata, et iga lahutumatu projektiivne polügoon P_S on isomorfne polügooniga eS, kus $e \in S$ on mingi idempotent.

Vastavalt lausele 7.15 on P_S mingi vaba polügooni F_S epimorfne kujutis. Kasutades teoreemi 7.14 näeme, et $F_S = \bigsqcup_{j \in J} F_j$, kus $F_j \cong S_S$ iga $j \in J$ korral. Olgu $\pi : F_S \to P_S$ sürjektiivne homomorfism. Kuna P_S on projektiivne, siis leidub homomorfism $g : P_S \to F_S$ nii, et $1_P = \pi g$.

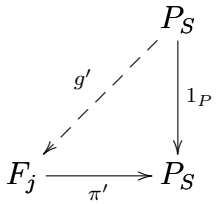


Kuna P_S on lahutumatu, siis tema ainus ρ-klass (vt. lause 7.8) on P ise. Fikseerime mingi elemendi $a \in P$ ja olgu $g(a) \in F_j$. Siis iga $b \in P$ korral peavad leiduma sellised elemendid $b_1, \ldots, b_n \in P$, $s_1, \ldots, s_n, t_1, \ldots, t_n \in S$, et kehtivad võrdused (7.1). Siis lõikumatuse tõttu $g(b_1) \in F_j$, $g(b_2) \in F_j, \ldots, g(b_n) \in F_j$ ja seega ka $g(b) \in F_j$. Järelikult $g(P) \subseteq F_j$.

Tänu sellele saame defineerida homomorfismid

$$g' : P_S \longrightarrow F_j, \quad x \mapsto g(x)$$

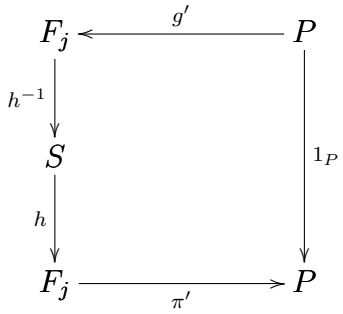
ja $\pi' = \pi|_{F_j}$ nii, et diagramm



on kommutatiivne. Järelikult π' on sürjektiivne.

Olgu $h : S_S \to F_j$ isomorfism ja tähistame

$$a := (\pi h)(1) \in P.$$



Et $\pi' h$ on sürjektiivne homomorfism, siis

$$P = (\pi' h)(S) = (\pi' h)(1)S = aS.$$

Tähistame

$$e := (h^{-1} g')(a) \in S.$$

Siis

$$a = 1_P(a) = (\pi' g')(a) = (\pi' h)((h^{-1} g')(a)) = (\pi' h)(e)$$

ja

$$\begin{aligned} e &= (h^{-1} g')(a) = (h^{-1} g' \pi' h)(e) = (h^{-1} g' \pi' h)(1e) = ((h^{-1} g' \pi' h)(1))e \\ &= ((h^{-1} g')((\pi' h)(1)))(e) = ((h^{-1} g')(a))e = ee = e^2. \end{aligned}$$

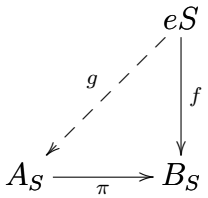
Võrdusest $\pi' g' = 1_P$ järeldub, et g' on üksühene ja seega ka $h^{-1} g' : P \to S$ on üksühene. Kuna

$$(h^{-1} g')(P) = (h^{-1} g')(aS) = ((h^{-1} g')(a))S = eS,$$

siis $eS = \mathrm{Im}\,(h^{-1} g')$ ja $eS \cong P_S$.

PIISAVUS. Arvestades lauset 7.18 on piisav, kui me näitame, et polügoonid eS, kus e on idempotent, on projektiivsed. Vaatleme homomorfismi $f : eS \to B_S$ ja sürjektiivset homomorfismi $\pi : A_S \to B_S$. Olgu $b := f(e) \in B$. Sürjektiivsuse tõttu saame valida $a \in A$ nii, et $\pi(a) = b$. Defineerime kujutuse $g : eS \to A$ võrdusega

$$g(es) := aes.$$



Siis g on korrektselt defineeritud homomorfism ja

$$\pi(g(es)) = \pi(aes) = \pi(a)es = bes = f(e)es = f(ees) = f(es)$$

iga $s \in S$ korral. Järelikult $\pi g = f$. □

Järeldus 7.20 *Vaba polügoon on projektiivne.*

TÕESTUS. See järeldub teoreemidest 7.14 ja 7.19, sest $S_S = 1S_S$ ja 1 on idempotent. □

Peatükk 8

Lõplikud korpused

Selles peatükis uurime lõplikke korpusi. Kõige lihtsamaks näiteks lõplikest korpustest on jäägiklassikorpused $\mathbb{Z}_p$, kuid osutub, et on ka teisi lõplikke korpusi. Lõplikud korpused on väga olulised tööriistad teoreetilises informaatikas, eelkõige kodeerimisteoorias ja krüptograafias. Samuti on neil tihedad seosed arvuteooria ja lineaaralgebraga (muuhulgas polünoomidega).

8.1 Lõplike korpuste ehitus

Definitsioon 8.1 Korpus on kommutatiivne ring, mille nullist erinevad elemendid moodustavad korrutamise suhtes rühma.

Korpuse K ühikelementi tähistame $\mathbf{1}$ ja nullelementi $\mathbf{0}$. Me tähistame ka $K^* := K \setminus \{\mathbf{0}\}$ ja ütleme, et $(K^*, \cdot)$ on korpuse K **multiplikatiivne rühm**.

Tuletame meelde, et iga Abeli rühma on võimalik vaadelda $\mathbb{Z}$-moodulina (vt. paragrahvi 3.1). Muuhulgas ka $(K, +)$ on $\mathbb{Z}$-moodul, kui defineerida mistahes naturaalarvu m ja elemendi $a \in K$ korral

$$ma = \underbrace{a + a + \ldots + a}_{m \text{ liidetavat}},$$

$0a = \mathbf{0}$ ning $(-m)a = -(ma)$. Lihtne on kontrollida, et lisaks mooduli omadustele kehtivad

- $(\forall m \in \mathbb{Z})(\forall a, b \in K)(m(ab) = (ma)b)$;
- $(\forall m, k \in \mathbb{Z})(\forall a, b \in K)((ma)(kb) = (mk)(ab))$.

Kuna hulk K on lõplik, siis $(K, +)$ on lõplik rühm ja seega peavad kõik tema elemendid olema lõplikku järku. Olgu p ühikelemendi $\mathbf{1} \in K$ järk aditiivses rühmas $(K, +)$, s.t. vähim selline naturaalarv p, et $p\mathbf{1} = \mathbf{0}$. Siis öeldakse, et korpuse K **karakteristika** on p ja tähistatakse $\mathrm{char}K = p$. Definitsioonist järeldub, et kui $\mathrm{char}K = p$, siis iga $a \in K$ korral $pa = \mathbf{0}$, sest

$$pa = p(\mathbf{1} \cdot a) = (p\mathbf{1})a = \mathbf{0}a = \mathbf{0}.$$

Lause 8.2 *Lõpliku korpuse karakteristika on algarv.*

TÕESTUS. Olgu p elemendi $\mathbf{1} \in K$ järk rühmas $(K, +)$. Näitame, et p on algarv. Selleks oletame vastuväiteliselt, et $p = kl$, kus $1 < k, l < p$. Siis $k\mathbf{1} \neq \mathbf{0}$ ja $l\mathbf{1} \neq \mathbf{0}$, kuid

$$(k\mathbf{1}) \cdot (l\mathbf{1}) = (kl)(\mathbf{1} \cdot \mathbf{1}) = (kl)\mathbf{1} = p\mathbf{1} = \mathbf{0}.$$

Korrutades selle võrduse pooli elemendiga $(k\mathbf{1})^{-1}$ saame vastuolu $l\mathbf{1} = \mathbf{0}$. Seega p on algarv. □

Definitsioon 8.3 Korpuse L alamringi K nimetatakse **alamkorpuseks**, kui $a^{-1} \in K$ iga $a \in K \setminus \{\mathbf{0}\}$ korral.

Definitsioon 8.4 Kui korpus K on korpuse L alamkorpus, siis öeldakse, et korpus L on korpuse K **laiend**.

Näiteks korpused $\mathbb{R}$ ja $\mathbb{C}$ on korpuse $\mathbb{Q}$ laiendid.

Lause 8.5 *Korpuse iga laiendi karakteristika on võrdne selle korpuse karakteristikaga.*

TÕESTUS. Olgu L korpuse K laiend ja $\mathrm{char}K = p$. Siis K kui korpuse L alamkorpus peab sisaldama korpuse L ühikelementi $\mathbf{1}$, mis on seega ka K ühikelemendiks. Kuna elemendi $\mathbf{1}$ järk rühmas $(K, +)$ on p, siis tema järk rühmas $(L, +)$ on samuti p ja seega $\mathrm{char}L = p$. □

Lause 8.6 *Korpuse K iga laiendit L võib vaadelda vektorruumina üle korpuse K. Kui L on lõplik ja $|K| = q$, siis $|L| = q^m$, kus $m \in \mathbb{N}$.*

TÕESTUS. Vaatleme hulka L vektorruumina, kus liitmine on korpuse L liitmine ning vektori $a \in L$ ja skalaari $\alpha \in K$ korrutis on lihtsalt nende elementide korrutis αa korpuses L. Vektorruumi aksioomide täidetus järeldub kohe korrutamise assotsiatiivsusest ja distributiivsuse seadustest korpuses L. Kui L on lõplik, siis on ta lõplikumõõtmeline vektorruum üle korpuse K ning seega, nagu hästi teada, omab lõplikku baasi ([1], teoreem 3.2.3). Olgu $e_1, \ldots, e_m$ baas vektorruumis L üle korpuse K. Siis iga $a \in L$ esitub üheselt lineaarkombinatsioonina $a = \alpha_1 e_1 + \ldots + \alpha_m e_m$, kus $\alpha_1, \ldots, \alpha_m \in K$. Et iga kordaja α_i valikuks on q võimalust, siis selliseid lineaarkombinatsioone on q^m tükki, s.t. $|L| = q^m$. □

Teoreem 8.7 *Lõpliku korpuse elementide arv on algarvu aste.*

TÕESTUS. Olgu K lõplik korpus, mille karakteristika on p. Vaatleme hulka

$$P = \{\mathbf{1}, \mathbf{1}+\mathbf{1}, \mathbf{1}+\mathbf{1}+\mathbf{1}, \ldots, (p-1)\mathbf{1}, p\mathbf{1} = \mathbf{0}\} \subseteq K.$$

Iga täisarvu m korral leiduvad $q, r \in \mathbb{Z}$ nii, et $m = pq + r$ ja $0 \leqslant r < p$. Seega

$$m\mathbf{1} = (pq)\mathbf{1} + r\mathbf{1} = q(p\mathbf{1}) + r\mathbf{1} = q\mathbf{0} + r\mathbf{1} = r\mathbf{1}$$

ja $P = \{m\mathbf{1} \mid m \in \mathbb{Z}\}$. Me näeme, et P on korpuse K alamkorpus, sest mistahes $k, l \in \{1, \ldots, p\}$ korral

- $k\mathbf{1} + l\mathbf{1} = (k+l)\mathbf{1} \in P$,
- $-(k\mathbf{1}) = (p-k)\mathbf{1} \in P$,
- $(k\mathbf{1}) \cdot (l\mathbf{1}) = (kl)\mathbf{1} \in P$,
- kui $k \neq p$, siis $(k\mathbf{1})^{-1} = u\mathbf{1} \in P$, kus $ku \equiv 1 \pmod{p}$ (ehk $\overline{u} = \overline{k}^{-1}$ korpuses $\mathbb{Z}_p$).

Märgime, et korpus P on isomorfne korpusega $\mathbb{Z}_p$, kusjuures isomorfismi realiseerib kujutus $f : P \longrightarrow \mathbb{Z}_p$,

$$f(k\mathbf{1}) = \overline{k}.$$

Lause 8.6 põhjal leidub selline naturaalarv n, et $|K| = p^n$. □

Selle teoreemi tõestuse käigus näitasime, et kehtib järgmine väide.

Järeldus 8.8 *Kui korpuse K karakteristika on p, siis see korpus sisaldab jäägiklassikorpusega $\mathbb{Z}_p$ isomorfset alamkorpuset.*

Edasises läheb meil vaja järgmisi abitulemusi.

Lemma 8.9 *Kui korpuse K karakteristika on p, siis iga $a, b \in K$ ja $n \in \mathbb{N}$ korral*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

TÕESTUS. Tõestame väite induktsiooniga n järgi. Olgu $n = 1$. Kuna K korrutamine on kommutatiivne, siis

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i.$$

Olgu $i \in \{1, \ldots, p-1\}$. Kuna

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-i+1)}{i!},$$

siis

$$p \cdot (p-1) \cdot \ldots \cdot (p-i+1) = \binom{p}{i} \cdot i!.$$

Et p jagab viimase võrduse vasakut poolt, aga ei jaga arvu $i!$ (sest selle algtegurite hulgas ei esine p), siis $p \mid \binom{p}{i}$, s.t. leidub selline $k_i \in \mathbb{N}$, et $k_i p = \binom{p}{i}$. Järelikult iga $i \in \{1, \ldots, p-1\}$ korral

$$\binom{p}{i} a^{p-i} b^i = (k_i p)(a^{p-i} b^i) = k_i (p(a^{p-i} b^i)) = k_i \mathbf{0} = \mathbf{0},$$

seega $(a+b)^p = a^p + b^p$ ning induktsiooni alus on tõestatud.

Oletame nüüd, et $(a+b)^{p^k} = a^{p^k} + b^{p^k}$. Kasutades äsjatõestatut saame

$$(a+b)^{p^{k+1}} = \left((a+b)^{p^k}\right)^p = \left(a^{p^k} + b^{p^k}\right)^p = \left(a^{p^k}\right)^p + \left(b^{p^k}\right)^p = a^{p^{k+1}} + b^{p^{k+1}}.$$

□

Järgmise lemma üheks erijuhuks on Fermat' väike teoreem.

Lemma 8.10 *Kui K on lõplik korpus ning $|K| = q$, siis*

1. *iga $a \in K^*$ korral $a^{q-1} = \mathbf{1}$,*

2. *iga $a \in K$ korral $a^q = a$.*

TÕESTUS. 1. Olgu m elemendi a järk korpuse K multiplikatiivses rühmas K^*. Siis $m \mid q-1 = |K^*|$ ehk $mk = q-1$ mingi naturaalarvu k korral. Järelikult

$$a^{q-1} = a^{mk} = (a^m)^k = \mathbf{1}^k = \mathbf{1}.$$

2. Võrdus $a^q = a$ kehtib nii nullelemendi kui nullist erinevate elementide korral. □

Lõplikud korpused konstrueeritakse enamasti polünoomide ringide faktorringidena. Vaatleme seda konstruktsiooni lähemalt.

Olgu K korpus ja vaatleme polünoomide ringi $K[x]$. See polünoomide ring on kommutatiivne. Kui $p(x) \in K[x]$ on mingi polünoom üle korpuse K, siis selle polünoomi poolt tekitatud peaideaal

$$p(x)K[x] = \{p(x)h(x) \mid h(x) \in K[x]\}$$

koosneb kõigist polünoomidest ringis $K[x]$, mis jaguvad polünoomiga $p(x)$. Kõrvalklass esindajaga $f(x) \in K[x]$ ideaali $p(x)K[x]$ järgi on hulk

$$[f(x)] = f(x) + p(x)K[x] = \{f(x) + p(x)h(x) \mid h(x) \in K[x]\}.$$

Muuhulgas $[0] = p(x)K[x]$. Saab näidata, et

$$[f(x)] = [g(x)] \iff f(x) - g(x) \in p(x)K[x] \iff p(x) \mid f(x) - g(x). \tag{8.1}$$

Näiteks $[p(x)] = [0]$, sest $p(x) \mid p(x)$. Kui kõrvalklasside hulgal defineerida tehted esindajate abil, s.t.

$$\begin{aligned} [f(x)] + [g(x)] &= [f(x) + g(x)], \\ [f(x)] \cdot [g(x)] &= [f(x)g(x)], \end{aligned}$$

saame ringi, mida nimetatakse ringi $K[x]$ **faktorringiks** ideaali $p(x)K[x]$ järgi (vt. [1], def. 6.5.11) ning mida tähistatakse

$$K[x]/p(x)K[x] = \{[f(x)] \mid f(x) \in K[x]\}.$$

Definitsioon 8.11 Mittekonstantset polünoomi $p(x) \in K[x]$ nimetatakse **taandumatuks**, kui teda ei saa esitada kahe mittekonstantse polünoomi korrutisena, s.t. kui võrdusest $p(x) = f(x)g(x)$ järeldub, et kas polünoom $f(x)$ on konstantne või $g(x)$ on konstantne.

Lause 8.12 *Olgu K korpus ja $p(x) \in K[x]$ taandumatu polünoom, mille aste $d \geqslant 2$. Siis faktorring $L = K[x]/p(x)K[x]$ on korpus, mis sisaldab korpusega K isomorfset alamkorpust ning milles polünoomil $p(x)$ on olemas juur. Kui $|K| = p^m$, siis $|L| = p^{md}$.*

TÕESTUS. Olgu

$$L = K[x]/p(x)K[x] = \{[f(x)] \mid f(x) \in K[x]\}$$

ringi $K[x]$ faktorring ideaali $p(x)K[x]$ järgi. Esimene väide on tõestatud raamatus [1] lausena 7.3.1. Meenutame, et elemendi $[0] \neq [f(x)] \in L$ pööratavus järeldub sellest, et $p(x)$ ei jaga polünoomi $f(x)$ ja $p(x)$ on taandumatu (seega $\text{SÜT}(p(x), f(x)) = 1$), korpusega K isomorfseks alamkorpuseks korpuses L on konstantsete polünoomide kõrvalklasside hulk $K' = \{[k] \mid k \in K\}$ ning polünoomi $p(x)$ üheks juureks korpuses L on lineaarpolünoomi x kõrvalklass $[x]$ (s.t. $p([x]) = [0]$).

Näitame veel, et korpuses L on p^{md} elementi. Selleks tõestame, et

$$K[x]/p(x)K[x] = \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}.$$

Tuleb veenduda, et

$$\{[f(x)] \mid f(x) \in K[x]\} \subseteq \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}$$

(vastupidine sisalduvus on ilmne). Võttes $g(x) \in K[x]$ võime selle polünoomi jagada jäägiga polünoomiga $p(x)$, s.t. leida sellised $q(x), r(x) \in K[x]$, et

$$g(x) = p(x)q(x) + r(x) \quad \text{ja} \quad \deg r(x) < \deg p(x) = d.$$

Järelikult

$$\begin{aligned}[g(x)] &= [p(x)][q(x)] + [r(x)] = [0][q(x)] + [r(x)] \\ &= [r(x)] \in \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}.\end{aligned}$$

Seega iga kõrvalklassi esindajaks saab valida sellise polünoomi, mille aste on väiksem kui d:

$$L = \{[k_{d-1}x^{d-1} + \ldots + k_1x + k_0] \mid k_0, \ldots, k_{d-1} \in K\}. \tag{8.2}$$

Erinevaid selliseid polünoome on $|K|^d$ tükki ning erinevatele sellistele polünoomidele vastavad erinevad kõrvalklassid, sest kui $f(x), g(x) \in K[x]$, $f(x) \neq g(x), \deg f(x) < d$ ja $\deg g(x) < d$, siis $f(x) - g(x) \neq 0$, $\deg(f(x) - g(x)) < d$, mistõttu $p(x)$ ei jaga polünoomi $f(x) - g(x)$ ja seega (8.1) põhjal $[f(x)] \neq [g(x)]$. Sellega oleme tõestanud, et $|L| = |K|^d = p^{md}$. □

Lauset 8.12 kasutades saab tõestada järgmise teoreemi.

Teoreem 8.13 ([1], teoreem 7.3.3) *Olgu $f(x) \in K[x]$ polünoom kordajatega korpusest K ning olgu $f(x)$ aste $n \geqslant 1$. Siis leidub korpuse K selline laiend L, milles polünoomil $f(x)$ on n juurt.*

Kui need teoreemis 8.13 mainitud juured on $a_1, \ldots, a_n \in L$, siis $f(x)$ lahutub lineaartegurite korrutiseks üle korpuse L: $f(x) = b(x - a_1) \ldots (x - a_n)$, kus $b \in K$ on x^n kordaja polünoomis $f(x)$.

Definitsioon 8.14 Korpuse K laiendit L nimetatakse polünoomi $f(x) \in K[x]$ **lahutuskorpuseks**, kui $f(x)$ lahutub lineaartegurite korrutiseks üle L,

$$f(x) = b(x - a_1) \dots (x - a_n),$$

kus $a_1, \dots, a_n, b \in L$, ning korpuse L iga alamkorpuse M korral, mis sisaldab korpust K ja elemente $a_1, \dots, a_n$, kehtib võrdus $M = L$.

Teoreem 8.13 ütleb, et igal mittekonstantsel polünoomil üle korpuse K on lahutuskorpus olemas. Kui K on lõplik, siis ka $f(x)$ lahutuskorpus L on lõplik. Veelgi enam, kehtib järgmine teoreem, mida me siinkohal ei tõesta.

Teoreem 8.15 *Polünoomi lahutuskorpus on isomorfismi täpsuseni üheselt määratud.*

Teoreem 8.7 väitis, et lõpliku korpuse elementide arv on algarvu aste. Järgnevalt veendume, et kehtib ka selle teoreemi pöördteoreem.

Teoreem 8.16 *Iga algarvu p ja naturaalarvu n korral leidub korpus, milles on p^n elementi. See korpus on isomorfismi täpsuseni üheselt määratud.*

TÕESTUS. Olgu $q = p^n$. Vaatleme polünoomi $x^q - x \in \mathbb{Z}_p[x]$. Olgu L polünoomi $x^q - x$ lahutuskorpus ning olgu

$$x^q - x = (x - a_1) \dots (x - a_q),$$

kus $a_1, \dots, a_q \in L$. Kuna $\mathbb{Z}_p \subseteq L$ on alamkorpus, siis lause 8.5 põhjal on korpuse L karakteristika p, s.t. $p\mathbf{1} = \mathbf{0}$ ja seega ka $q\mathbf{1} = \mathbf{0}$. Järelikult

$$(x^q - x)' = q\mathbf{1}x^{q-1} - \mathbf{1} = -\mathbf{1} \in L[x]$$

ning seega polünoomi $x^q - x$ ja tema tuletise suurim ühistegur ringis $L[x]$ on

$$\text{SÜT}((x^q - x), (x^q - x)') = \text{SÜT}((x^q - x), -\mathbf{1}) = \mathbf{1}.$$

Näitame, et sellest järeldub, et polünoomil $x^q - x$ ei ole kordseid juuri. Oletame vastuväiteliselt, et $a \in L$ on polünoomi $x^q - x$ kordne juur, s.t.

$$x^q - x = (x - a)^k g(x),$$

kus $k \geqslant 2$ ja $g(x) \in L[x]$. Siis korrutise tuletise leidmise reegli põhjal

$$(x^q - x)' = k\mathbf{1}(x-a)^{k-1}g(x) + (x-a)^k g'(x) = (x-a)\left(k\mathbf{1}(x-a)^{k-2}g(x) + (x-a)^{k-1}g'(x)\right).$$

Kuna $x - a \mid x^q - x$ ja $x - a \mid (x^q - x)'$, siis

$$(x - a) \mid \text{SÜT}((x^q - x), (x^q - x)') = \mathbf{1}$$

ringis $L[x]$. Lineaarpolünoom ei saa jagada konstantset polünoomi, seega oleme saanud vastuolu. Järelikult tõesti polünoomil $x^q - x$ pole kordseid juuri, s.t. elemendid $a_1, \dots, a_q$ on erinevad.

Vaatleme q-elemendilist alamhulka

$$K = \{a_1, \ldots, a_q\} \subseteq L.$$

Paneme tähele, et

$$K = \{a \in L \mid a^q = a\}.$$

Tõepoolest, kuna $a_1, \ldots, a_q$ on polünoomi $x^q - x$ juured, siis nad peavad kuuluma hulka $\{a \in L \mid a^q = a\}$. Kui aga $a^q = a$, siis a on polünoomi $x^q - x$ juur. Kuna q-nda astme polünoomil ei saa olla rohkem kui q juurt, siis $a \in \{a_1, \ldots, a_q\}$.

Näitame, et K on korpuse L alamkorpus. Selleks näitame, et K on kinnine tehete suhtes. Olgu $a, b \in K$, s.t. $a^q = a$ ja $b^q = b$.

- Lemma 8.9 põhjal

$$(a+b)^q = (a+b)^{p^n} = a^{p^n} + b^{p^n} = a^q + b^q = a + b,$$

  s.t. $a + b \in K$.

- Kui $p = 2$, siis $a + a = \mathbf{0}$ ehk $-a = a \in K$. Kui aga $p > 2$, siis q on paaritu ja

$$(-a)^q = ((-\mathbf{1})a)^q = (-\mathbf{1})^q a^q = (-\mathbf{1})\, a = -a,$$

  s.t. $-a \in K$.

- Korrutamise kommutatiivsuse tõttu ka $(ab)^q = a^q b^q = ab$, s.t. $ab \in K$.

- Olgu $a \neq \mathbf{0}$. Siis $(a^{-1})^q = (a^q)^{-1} = a^{-1}$, s.t. $a^{-1} \in K$.

Seega K on alamkorpus. Lisaks sellele $\mathbb{Z}_p \subseteq K$, sest iga $\overline{c} \in \mathbb{Z}_p$ korral

$$\overline{c}^{p^n} = (\overline{c}^p)^{p^{n-1}} = \overline{c}^{p^{n-1}} = \ldots = \overline{c}.$$

Kuna L on korpuse L vähim alamkorpus, mis sisaldab korpust $\mathbb{Z}_p$ ja elemente $a_1, \ldots, a_q$, siis $L = K$, järelikult $|L| = |K| = q$.

Ühesuse näitamiseks paneme tähele, et mistahes q-elemendilise korpuse L' korral on lemma 8.10 tõttu kõik tema elemendid polünoomi $x^q - x \in \mathbb{Z}_p[x]$ juured. Kuna sellel polünoomil ei saa olla üle q juure, siis on L' selle polünoomi lahutuskorpus. Kuna polünoomi mistahes kaks lahutuskorpust on isomorfsed, siis on ka korpus L' isomorfne korpusega L. □

Korpust, milles on $q = p^n$ elementi, tähistatakse tihti kas $\mathbb{F}_q$ või $\mathrm{GF}(q)$ (GF=*Galois field*). Sellise korpuse konstrueerimiseks on otstarbekas kasutada lauset 8.12. Võtame näiteks korpuse $\mathbb{Z}_p$, leiame mingi n-nda astme taandumatu polünoomi üle $\mathbb{Z}_p$ ning moodustame faktorringi $\mathbb{Z}_p[x]/p(x)\mathbb{Z}_p[x]$. Tulemus on p^n-elemendiline korpus, mis tänu teoreemile 8.16 ongi $\mathbb{F}_q$.

8.2 Multiplikatiivse rühma tsüklilisus

Definitsioon 8.17 Rühma G nimetatakse **tsükliliseks**, kui leidub element $g \in G$ nii, et kõik G elemendid on esitatavad elemendi g astmetena. Sellisel juhul öeldakse, et g on rühma G **tekitaja** või **moodustaja** ja kirjutatakse $G = \langle g \rangle$.

Kui $|G| = n$ ja g on selle rühma tekitaja, siis

$$G = \{g, g^2, \ldots, g^{n-1}, g^n = 1\}.$$

Teiste sõnadega võib öelda, et n-elemendiline rühm on tsükliline parajasti siis, kui temas leidub element, mille järk on n.

Arvuteooria konspektist võib leida järgmise teoreemi tõestuse.

Teoreem 8.18 *Lõpliku korpuse multiplikatiivne rühm on tsükliline.*

Lõpliku korpuse multiplikatiivse rühma tekitajaid nimetatakse selle korpuse **primitiivseteks elementideks**. Korpuse $\mathbb{Z}_p$ (p on algarv) primitiivseid elemente nimetatakse **algjuurteks** mooduli p järgi.

8.3 Aritmeetika lõplikes korpustes

Lõpliku korpuse elementide esitamiseks on mitmeid võimalusi. Üks viis on kasutada faktorringi $\mathbb{Z}_p[x]/p(x)\mathbb{Z}_p[x]$, kus $p(x)$ on taandumatu polünoom üle $\mathbb{Z}_p$. Teine võimalus on kasutada fakti, et rühm $\mathbb{F}_q^*$ on tsükliline ja seega tema elemendid on esitatavad tekitaja (primitiivse elemendi) astmetena. On selge, et liita on lihtsam elemente, mis on esitatud polünoomidena ning korrutada on lihtsam rühma moodustaja astmeid. Osutub, et neid kahte viisi saab omavahel kombineerida, mis annab võimaluse aritmeetiliste tehete efektiivseks sooritamiseks lõplikus korpuses.

Näide 8.19 Vaatleme lõplikku korpust $\mathbb{F}_{16}$ kui korpuse $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ ($\overline{0}$ ja $\overline{1}$ asemel kirjutame 0 ja1) laiendit.

Näitame, et polünoom $p(x) = x^4 + x + 1$ on taandumatu üle $\mathbb{F}_2$. Selleks paneme tähele, et kui $p(x)$ oleks taanduv, siis ta peaks omama kas lineaar- või ruuttegurit. Kuna $p(0) \neq 0$ ja $p(1) \neq 0$, siis polünoomil $p(x)$ pole lineaartegureid. Veendumaks, et polünoom $p(x)$ ei jagu ühegi ruutpolünoomiga, märgime, et üle $\mathbb{F}_2$ on täpselt neli erinevat ruutpolünoomi

$$x^2,\ x^2 + 1,\ x^2 + x,\ x^2 + x + 1$$

ning vahetu kontroll näitab, et neid polünoome omavahel korrutades me ei saa polünoomi $p(x)$.

Kuna polünoomi $p(x)$ aste on 4, siis lause 8.12 põhjal

$$\mathbb{F}_2[x]/(x^4 + x + 1)\mathbb{F}_2[x] = \mathbb{F}_{16}.$$

Tähistame $a = [x]$ ning samastame kõrvlaklassid $[0]$ ja $[1]$ esindajatega 0 ja 1. Kui vaatleme polünoomile $p(x)$ vastavat polünoomi $\tilde{p}(y) = y^4 + y + 1 \in \mathbb{F}_{16}[y]$, siis a on polünoomi $\tilde{p}(y)$ juur, sest

$$\tilde{p}(a) = a^4 + a + 1 = [x]^4 + [x] + [1] = [x^4 + x + 1] = [0].$$

Tänu võrdusele (8.2) võib korpuse $\mathbb{F}_{16}$ elemente esitada kui ülimalt kolmanda astme polünoome a suhtes:

konstantsed	$0, 1,$
lineaarsed	$a, a+1,$
ruutpolünoomid	$a^2, a^2+1, a^2+a, a^2+a+1$
kuuppolünoomid	$a^3, a^3+1, a^3+a, a^3+a^2, a^3+a+1,$
	$a^3+a^2+1, a^3+a^2+a, a^3+a^2+a+1.$

Sellisel kujul elementide liitmine on lihtne, sest see on lihtsalt polünoomide liitmine. Korrutamine nõuab taandamist "mooduli $p(x)$ järgi", s.o. jäägiga jagamist polünoomiga $x^4 + x + 1$, kuid võib kasutada ka seost $a^4 + a + 1 = 0$ ehk $a^4 = a + 1$. Näiteks

$$\begin{aligned} a^{14} &= (a^4)^3 a^2 = (a+1)^3 a^2 = (a^3 + a^2 + a + 1)a^2 = a^5 + a^4 + a^3 + a^2 \\ &= (a+1)a + a + 1 + a^3 + a^2 = a^2 + a + a + 1 + a^3 + a^2 = a^3 + 1. \end{aligned}$$

Kuna $a \neq 0$, siis $a \in \mathbb{F}_{16}^*$. Samuti $a \neq 1$. Elemendi a järk multiplikatiivses rühmas $\mathbb{F}_{16}^*$ peab olema rühma järgu (s.t. arvu 15 jagaja). Seega $\mathrm{ord}(a) \in \{3, 5, 15\}$. Et $a^3 \neq 1$ ja $a^5 = a^2 + a \neq 1$, siis $\mathrm{ord}(a) = 15$, s.t. element a on rühma $\mathbb{F}_{16}^*$ tekitaja. Seega

$$\mathbb{F}_{16} = \{0, 1, a, a^2, \ldots, a^{14}\}.$$

Sellisel viisil esitatud elementide korrutamine on lihtne, kuid liitmine on tülikas.

Need kaks esitust saab omavahel siduda, kui arvutada välja tabel, mis näitab, kuidas element a^k esitub ülimalt kolmanda astme polünoomina a suhtes. Kasutades seost $a^4 = a + 1$ saame

$$\begin{aligned} a^4 &= a + 1, \\ a^5 &= a \cdot a^4 = a(a+1) = a^2 + a, \\ a^6 &= a \cdot a^5 = a^3 + a^2, \\ a^7 &= a \cdot a^6 = a^4 + a^3 = a^3 + a + 1 \end{aligned}$$

ja nii edasi. Tulemused võtame kokku alljärgneva tabelina, kus elemendi a^k asemel kirjutame lihtsalt k ning polünoomi $k_3a^3 + k_2a^2 + k_1a + k_0$ asemel kirjutame tema kordajate jada $k_3k_2k_1k_0$.

0	0001
1	0010
2	0100
3	1000
4	0011
5	0110
6	1100
7	1011
8	0101
9	1010
10	0111
11	1110
12	1111
13	1101
14	1001

Selle tabeli ning seose $a^{15} = 1$ abil võime nüüd näiteks arvutada

$$\begin{aligned}(a^8 + a^4 + 1)(a^3 + a) &= (0101 + 0011 + 0001)(1000 + 0010) = (0111)(1010) \\ &= a^{10} \cdot a^9 = a^{19} = a^4 = a + 1.\end{aligned}$$

Seega arvutamiseks (liitmiseks ja korrutamiseks) lõplikus korpuses on kasulik teada tema multiplikatiivse rühma moodustajat koos mingi taandumatu polünoomiga, mille juureks ta on. Üldjuhul pole taandumatu polünoomi leidmine lihtne. Siiski on paljude konkreetsete korpuste jaoks leitud taandumatud polünoomid ja tabelid.

Peatükk 9

Võred

9.1 Kaks vaatenurka võredele

Võret on võimalik defineerida kahel erineval viisil, üks neist on järjestusteoreetiline ja teine puhtalt algebraline. Osutub, et need kaks definitsiooni on samaväärsed. Alustame järjestusteoreetilisest definitsioonist.

Definitsioon 9.1 Järjestatud hulga $(P, \leq)$ elementi c nimetatakse elementide a ja b ülemiseks **tõkkeks**, kui $a \leq c$ ja $b \leq c$. Elementide a ja b **ülemine raja** on nende elementide vähim ülemine tõke. Analoogiliselt saab defineerida alumised tõkked ja alumised rajad. Ülemist raja tähistatakse $a \vee b$ ja alumist raja $a \wedge b$.

Definitsioon 9.2 Võre on järjestatud hulk, mille igal kahel elemendil leidub ülemine ja alumine raja.

Näide 9.3

1. Hulga A kõigi alamhulkade hulk $\mathcal{P}(A)$ koos sisalduvusseosega $\subseteq$ on võre. Selles võres on A alamhulkade X ja Y alumiseks rajaks ühisosa $X \cap Y$ ja ülemiseks rajaks ühend $X \cup Y$.

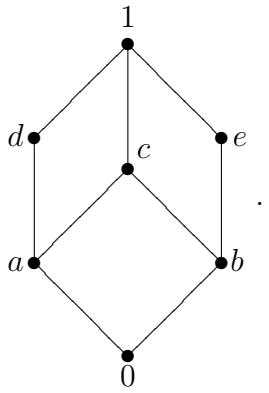
2. Öeldakse, et järjestatud hulk on **lineaarselt järjestatud**, kui mistahes kahe elemendi a ja b korral kas $a \leq b$ või $b \leq a$. Iga lineaarselt järjestatud hulk on võre, kus $a \wedge b = \min(a, b)$ ja $a \vee b = \max(a, b)$. Näiteks hulk $\mathbb{Z}$ on lineaarselt järjestatud.

3. Naturaalarvude hulk, mida vaatleme järjestatud hulgana jaguvusseose $|$ suhtes, on võre, kus alumine raja on SÜT ja ülemine raja on VÜK.

4. Vektorruumi V kõigi alamruumide hulk $\mathsf{Sub}(V)$ on võre, kus alamruumide V_1 ja V_2 alumine raja on $V_1 \cap V_2$ ja ülemine raja on $V_1 + V_2$.

Näide 9.4 Lõplike järjestatud hulkade (muuhulgas lõplike võrede) kujutamiseks kasutatakse tihti teatud graafe, kus punktid (tipud) märgivad hulga elemente ja kaks punkti on ühendatud joonega (servaga) kui üks elementidest on teisest väiksem ja nende kahe vahel

ei ole järjestusseose mõttes kolmandaid elemente. Kokkuleppeliselt asuvad suuremas elemendid joonisel kõrgemal (sellisel juhul öeldakse ka, et üks element katab teist). Näiteks on võimalik vaadelda 7-elemendilist võret



Selles võres näiteks $a < d$ ja $d < 1$, aga ka $a < 1$. Jooniselt on näha, et näiteks $a \vee b = c$, $a \vee e = 1$ ja $d \wedge c = a$.

Võret võib defineerida ka kui kahe kahekohalise algebralise tehtega struktuuri.

Definitsioon 9.5 Võre on mittetühi hulk L, millel on defineeritud kaks algebralist tehet $+$ ja $\cdot$ (liitmine ja korrutamine) nii, et mistahes $a, b, c \in L$ korral

$$\begin{array}{rclrcll} (a+b)+c & = & a+(b+c) & (ab)c & = & a(bc) & \text{(assotsiatiivsus)} \\ a+b & = & b+a & ab & = & ba & \text{(kommutatiivsus)} \\ a+a & = & a & aa & = & a & \text{(idempotentsus)} \\ (a+b)a & = & a & ab+a & = & a & \text{(neelduvus).} \end{array}$$

On lihtne aru saada, et esimese tulba omadused on duaalsed teise tulba omadega selles mõttes, et kui liitmine asendada korrutamisega ja vastupidi, siis saame esimese tulba omadusest samas reas asuva teise tulba omaduse.

Lause 9.6 *Olgu $(L, +, \cdot)$ võre definitsiooni 9.5 mõttes. Siis mistahes $a, b \in L$ korral*

$$a = ab \iff b = a + b.$$

Tõestus. Tarvilikkus. Kui $a = ab$, siis kommutatiivsuse ja neelduvuse tõttu $a + b = ab + b = ba + b = b$.
Piisavus. Kui $b = a + b$, siis $ab = a(a + b) = (a + b)a = a$. □

Teoreem 9.7 *1. Kui $(L, \leq)$ on võre definitsiooni 9.2 mõttes ja defineerime kahekohalised tehted $+$ ja $\cdot$ võrdustega*

$$\begin{aligned} a + b &:= a \vee b, \\ ab &:= a \wedge b, \end{aligned}$$

siis $(L, +, \cdot)$ on võre definitsiooni 9.5 mõttes.

2. Kui $(L, +, \cdot)$ on võre definitsiooni 9.5 mõttes ja defineerime seose $\leq$ järgmiselt:

$$a \leq b \Longleftrightarrow a = ab,$$

siis $(L, \leq)$ on võre definitsiooni 9.2 mõttes. Selles võres

$$a \leq b \implies ac \leq bc \quad ja \quad a + c \leq b + c \tag{9.1}$$

mistahes $a, b, c \in L$ korral.

TÕESTUS. 1. Näitame, et kehtivad definitsiooni 9.5 parempoolses tulbas toodud samasused. Vasakpoolse tulba omaduste kontroll on sarnane.

Assotsiatiivsus. Veendume, et $(ab)c = a(bc)$ ehk $(a \wedge b) \wedge c = a \wedge (b \wedge c)$. Tähistame $d := (a \wedge b) \wedge c$ ja $e := a \wedge (b \wedge c)$. Siis $d \leq a \wedge b$ ja $d \leq c$, järelikult ka $d \leq a$ ja $d \leq b$. Seega $d \leq b \wedge c$ ning koos võrratusega $d \leq a$ saame, et $d \leq a \wedge (b \wedge c) = e$. Võrratuse $e \leq d$ tõestus on analoogiline. Järjestusseose antisümmeetria põhjal $e = d$.

Kommutatiivsus. On selge, et $a \wedge b = b \wedge a$.

Idempotentsus. On ilmne, et $a \wedge a = a$.

Neelduvus. Tõestame võrduse $a = ab + a$ ehk $a = (a \wedge b) \vee a$. Kuna $a \wedge b \leq a$ ja $a \leq a$, siis a on elementide $a \wedge b$ ja a ülemine tõke. Olgu nüüd $a \wedge b \leq x$ ja $a \leq x$. Võrratus $a \leq x$ ütleb kohe, et a on väiksem või võrdne elementide $a \wedge b$ ja a iga ülemise tõkkega. Seega a on elementide $a \wedge b$ ja a ülemine raja, $a = (a \wedge b) \vee a$.

2. Veendume, et $\leq$ on järjestusseos.

Refleksiivsus. Kuna $aa = a$, siis $a \leq a$.

Antisümmeetria. Olgu $a \leq b$ ja $b \leq a$. Siis $a = ab$ ja $b = ba$. Järelikult $a = ab = ba = b$.

Transitiivsus. Olgu $a \leq b$ ja $b \leq c$. Siis $a = ab$ ja $b = bc$. Järelikult $a = ab = a(bc) = (ab)c = ac$, kust $a \leq c$.

Tõestame nüüd, et $a \wedge b = ab$, s.t. et ab on elementide a ja b alumine raja. Kasutame selleks alumise raja definitsiooni.

1) Kuna $(ab)a = a(ba) = a(ab) = (aa)b = ab$, siis $ab \leq a$. Et $(ab)b = a(bb) = ab$, siis $ab \leq b$.

2) Oletame, et $x \leq a$ ja $x \leq b$. Siis $x = xa$ ja $x = xb$. Järelikult $x(ab) = (xa)b = xb = x$ ehk $x \leq ab$. Sellega on näidatud, et $a \wedge b = ab$.

Kasutades seda, et $a \leq b$ parajasti siis, kui $b = a + b$ (vt. lauset 9.6), saab tõestada, et $a \vee b = a + b$. Kuna mistahes kahel elemendil leidub nii alumine kui ülemine raja, siis $(L, \leq)$ on võre definitsiooni 9.2 mõttes.

Tõestuse lõpetamiseks näitame, et kehtib implikatsioon (9.1). Olgu $a \leq b$. Siis $a = ab$, kust $(ac)(bc) = abcc = ac$ ehk $ac \leq bc$.

Võrratusest $a \leq b$ järeldub ka, et $b = a + b$, kust $(a + c) + (b + c) = a + b + c + c = b + c$ ehk $a + c \leq b + c$. □

Järgnevas tutvume põgusalt kolme olulise võrede klassiga, need on täielikud võred, modulaarsed võred ja distributiivsed võred.

9.2 Täielikud võred

Definitsioon 9.8 Osaliselt järjestatud hulka L nimetatakse **täielikuks võreks**, kui selle mistahes alamhulgal on olemas nii ülemine kui alumine raja.

Definitsiooni järgi peab leiduma ka tühja alamhulga alumine ja ülemine raja. Kui $a := \wedge\emptyset$, siis iga element $b \in L$ on tühja hulga alumine tõke ja seega $b \leq a$. See tähendab, et a on järjestatud hulga L suurim element. Analoogiliselt saab näidata, et $\vee\emptyset$ on järjestatud hulga L vähim element. Seega igas täielikus võres peab leiduma suurim element (seda tähistatakse sümboliga 1) ja vähim element (tähistatakse sümboliga 0). Muuhulgas $1 = \vee L$ ja $0 = \wedge L$.

Näide 9.9

1. Kõik lõplikud võred on täielikud.
2. Hulga X alamhulkade võre $(\mathcal{P}(X), \cup, \cap)$ on täielik.
3. Naturaalarvude hulk SÜT ja VÜK võtmise suhtes on võre, mis ei ole täielik, sest puudub suurim element.
4. Reaalarvude järjestatud hulk $[0, 1]$ on täielik võre.
5. Ratsionaalarvude hulk $\mathbb{Q}$ ei ole täielik võre. Näiteks hulgal $\{a \in \mathbb{Q} \mid 2 < a^2\}$ on lõpmata palju alumisi tõkkeid, aga puudub suurim alumine tõke ehk alumine raja.
6. Abeli rühma A kõigi alamrühmade hulk on täielik võre alamrühmade summa (ülemine raja) ja ühisosa (alumine raja) suhtes.
7. Topoloogia (lahtiste hulkade hulk) $\bigcup$ ja $(\cap)^\circ$ suhtes, kus $^\circ$ tähistab sisepunktide hulga võtmist.
8. Poolrühma kõigi ideaalide hulk on täielik võre $\cap$ ja $\cup$ suhtes.
9. Ringi kõigi ideaalide hulk on täielik võre $\cap$ ja $+$ suhtes.

Lause 9.10 *Järjestatud hulga L korral on järgmised väited samaväärsed.*

1. *L on täielik võre.*
2. *Hulga L igal alamhulgal on olemas alumine raja.*
3. *Hulga L igal mittetühjal alamhulgal on olemas alumine raja ning hulk L sisaldab suurimat elementi.*

Tõestus. $1 \Rightarrow 2 \Rightarrow 3$. See on ilmne.

$3 \Rightarrow 1$. Peame näitama, et mistahes alamhulgal leidub ülemine raja. Olgu $A \subseteq L$ ja vaatleme selle hulga kõigi ülemiste tõkete hulka $A^\triangle$. Kuna $1 \in L$, siis $A^\triangle \neq \emptyset$ ja sellel hulgal peab leiduma alumine raja. Olgu $x = \wedge A^\triangle \in L$. Näitame, et $x = \vee A$. Selleks kasutame ülemise raja definitsiooni.

Kui $a \in A$, siis iga $d \in A^{\triangle}$ korral $a \leqslant d$. Seega a on hulga $A^{\triangle}$ alumine tõke. Järelikult $a \leqslant x$, sest x on alumine raja hulgale $A^{\triangle}$. Kuna see võrratus kehtib iga $a \in A$ korral, siis x on hulga A ülemine tõke ja $x \in A^{\triangle}$.

Tesiest küljest $x \leqslant d$ iga $d \in A^{\triangle}$ korral. Seega oleme tõestanud, et $x = \vee A$. □

Tõestatud lause on väga kasulik, sest tihti on tingimust 3 lihtsam kontrollida kui tingimust 1.

Teoreem 9.11 *Täieliku võre L ja mistahes järjestust säilitava teisenduse $f : L \to L$ korral leidub element $x_0 \in L$ nii, et $f(x_0) = x_0$.*

TÕESTUS. Vaatleme hulka

$$P = \{x \in L \mid x \leq f(x)\} \subseteq L\,.$$

Olgu $x_0 = \bigvee P$. Kuna f säilitab järjestust, siis iga $x \in P$ korral

$$x \leq x_0 \;\Rightarrow\; f(x) \leq f(x_0) \;\Rightarrow\; x \leq f(x_0)\,.$$

See tähendab, et $f(x_0)$ on hulga P ülemine tõke. Ülemise raja definitsiooni kohaselt nüüd $x_0 \leq f(x_0)$ ja veelkord kujutust f rakendades ka $f(x_0) \leq f(f(x_0))$. Seega $f(x_0) \in P$ ja kokkuvõttes $f(x_0) \leq \bigvee P = x_0 \leq f(x_0)$, kust $f(x_0) = x_0$. □

Elementi x_0 nimetatakse teisenduse f **püsipunktiks**.

9.3 Modulaarsed võred

Lause 9.12 *Mistahes võre L ja elementide $a, b, c \in L$ korral*

1. $a + bc \leq (a + b)(a + c)$;
2. *kui* $a \leq c$, *siis* $a + bc \leq (a + b)c$.

TÕESTUS. 1. Tähistame $u := (a + b)(a + c)$. Kuna $a \leq a + b$ ja $a \leq a + c$, siis $a \leq u$. Et $b \leq a + b$ ja $c \leq a + c$, siis $bc \leq (a + b)c \leq (a + b)(a + c) = u$. Seega u on elementide a ja bc ülemine tõke. Järelikult

$$a + bc \leq u = (a + b)(a + c)\,.$$

2. See järeldub eelmisest väitest, sest kui $a \leq c$, siis $a + c = c$. □

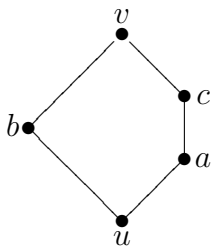
Kui lause 9.12 viimase võrratuse asemel kehtib võrdus, siis kutsutakse võret modulaarseks.

Definitsioon 9.13 Võret L nimetatakse **modulaarseks**, kui mistahes $a, b, c \in L$ korral

$$a \leq c \Longrightarrow (a + b)c = a + bc.$$

Näide 9.14 1. Saab näidata, et rühma kõigi normaaljagajate võre tehete $\cdot$ ja $\cap$ suhtes on modulaarne.

2. Viieelemendiline võre



ei ole modulaarne. Tõepoolest, selles võres $a \leq c$, $(a+b)c = vc = c$ ja $a + bc = a + u = a$, seega $(a+b)c \neq a + bc$. Seda võret tähistatakse sümboliga N_5.

Lause 9.15 *Mooduli M_R (R on ring) alammoodulite võre $(\mathsf{Sub}(M), +, \cap)$ on modulaarne.*

TÕESTUS. Olgu $A, B, C \in \mathsf{Sub}(M)$ ja $A \subseteq C$. Peame näitama, et

$$(A + B) \cap C = A + B \cap C.$$

Võtame elemendi $c \in (A + B) \cap C$. Siis leiduvad $a \in A$ ja $b \in B$ nii, et $c = a + b$. Siis $a \in C$ ja $b = c - a \in C$. Seega $b \in B \cap C$ ja $c \in A + B \cap C$.

Oletame nüüd, et $x \in A + B \cap C$. Siis leiduvad $a \in A$ ja $y \in B \cap C$ nii, et $x = a + y$. Kuna $y \in B$, siis $x \in A+B$. Et $a \in A \subseteq C$ ja $y \in C$, siis ka $x \in C$. Seega $x \in (A+B)\cap C$. □

Teoreem 9.16 *Võre L jaoks on järgmised väited samaväärsed.*

1. *L on modulaarne.*
2. *Kui $a, b, c \in L$, $a \geq b$, $a + c = b + c$ ja $ac = bc$, siis $a = b$.*
3. *L ei sisalda võrega N_5 isomorfset alamvõret.*

TÕESTUS. 2. $\Rightarrow$ 1. Olgu $a, b, c \in L$ ja $a \leq c$. Siis

$$a + b = (a + b)a + b \leq (a + b)c + b \leq (a + b)c + (a + b) = a + b,$$
$$bc = (a + bc)bc \leq (a + bc)b \leq (c + bc)b = cb = bc.$$

Tänu järjestusseose antisümmeetriale saame võrdused

$$(a + b)c + b = a + b,$$
$$(a + bc)b = bc.$$

Lisaks sellele

$$(a + bc) + b = a + (bc + b) = a + b,$$
$$(a + b)cb = (a + b)bc = ((a + b)b)c = bc.$$

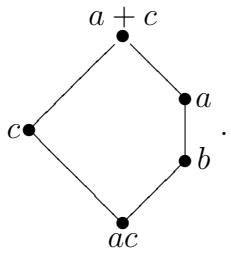
Seega

$$(a + b)c + b = (a + bc) + b, \tag{9.2}$$
$$(a + bc)b = (a + b)cb. \tag{9.3}$$

Lause 9.12(2) ütleb, et $a + bc \leq (a + b)c$. Rakendades nüüd tingimust 2 võrdustele (9.2) ja (9.3) saame järeldada, et $(a + b)c = a + bc$.

1. $\Rightarrow$ 3. Kui võre L sisaldaks võrega N_5 isomorfset alamvõret, siis ta ei saaks olla modulaarne.

3. $\Rightarrow$ 2. Oletame vastuväiteliselt, et leiduvad elemendid $a, b, c \in L$ nii, et $a > b$, $a + c = b + c$ ja $ac = bc$. Vaatleme elemente $a, b, c, a + c, ac \in L$. Kui nad oleksid paarikaupa erinevad, siis L sisaldaks võrega N_5 isomorfset alamvõret



Seega tõestuse lõpetamiseks piisab näidata, et tehtud eeldustel peavad need 5 elementi olema paarikaupa erinevad.

- Kuna $a > b$, siis $a \neq b$.
- Oletame, et $a = c$. Siis $c = cc = ac = bc$, kust $c \leq b$ ehk $a \leq b$, mis on vastuolus võrratusega $a > b$. Seega $a \neq c$.
- Oletame, et $a = a + c$. Siis

$$c \leq a \;\Rightarrow\; c = ac = bc \;\Rightarrow\; c \leq b \;\Rightarrow\; b = b + c = a + c = a,$$

  mis on vastuolus võrratusega $a > b$.
- Oletame, et $a = ac$. Siis võrratustest $b < a$ ja $a \leq c$ järeldub, et $b \leq c$. Seega $b = bc = ac = a$, vastuolu.
- Oletame, et $b = c$. Siis $a + c = b + c = c + c = c$ ehk $a \leq c$. Järelikult $a = ac$ ja me saame vastuolu sarnaselt eelneva juhuga.
- Ka ülejäänud juhtudel tekib vastuolu. Jätame selle läbimõtlemiseks lugejale.

□

9.4 Distributiivsed võred

Definitsioon 9.17 Võret L nimetatakse **distributiivseks**, kui mistahes $a, b, c \in L$ korral

$$(a + b)c = ac + bc.$$

Lemma 9.18 *Iga distributiivne võre on modulaarne.*

TÕESTUS. Olgu L distributiivne võre ja $a \leq c$, $a, b, c \in L$. Siis

$$(a + b)c = ac + bc = a + bc.$$

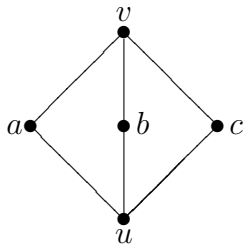
□

Näide 9.19 1. Hulga X alamhulkade võre $(\mathcal{P}(X), \cup, \cap)$ on distributiivne.

2. Naturaalarvude hulk suurima ühisteguri ja vähima ühiskordse võtmise suhtes on distributiivne võre.

3. Ahelad on distributiivsed võred.

4. Võre



ei ole distributiivne, sest

$$(a + b)c = vc = c \neq u = u + u = ac + bc.$$

Seda võret tähistatakse lühidalt sümboliga M_3.

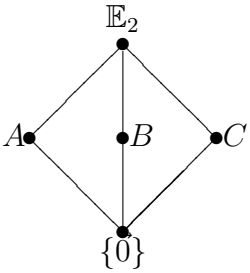
5. Vektorruumi V alamruumide võre $(\mathsf{Sub}(V), +, \cap)$ ei ole üldjuhul distributiivne. Vaatleme näiteks tasandi vabavektorite vektorruumis $\mathbb{E}_2$ kolme mittekollineaarset vektorit $\vec{a}, \vec{b}, \vec{c}$ ja nende poolt tekitatud alamruume A, B, C. Siis

$$A \cap B = A \cap C = B \cap C = \{\vec{0}\}$$

ja

$$A + B = A + C = B + C = \mathbb{E}_2.$$

Seega $\mathbb{E}_2$ alamruumide võre sisaldab võrega M_3 isomorfset alamvõret



ja ei saa olla distributiivne.

Järgmise kahe teoreemi tõestust me käesolevas kursuses anda ei jõua.

Teoreem 9.20 *Võre L on distributiivne parajasti siis, kui ta ei sisalda võredega N_5 ja M_3 isomorfseid alamvõresid.*

Teoreem 9.21 *Võre on distributiivne parajasti siis, kui ta on isomorfne mingi hulga X kõigi alamhulkada võre $(\mathcal{P}(X), \cup, \cap)$ mingi alamvõrega.*

Peatükk 10

Universaalalgberad ja nende muutkonnad

10.1 Universaalalgberad

Definitsioon 10.1 **Universaalalgebraks** nimetatakse kolmikut (A, Ω, ψ), kus A on hulk, $\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$ on loenduva arvu (võib-olla tühjade) hulkade lõikumatu ühend (universaalalgebra **signatuur**) ja ψ on selline kujutus

$$\psi : \Omega \to \{f : A^n \to A \mid n \in \mathbb{N} \cup \{0\}\},$$

et kui $\omega \in \Omega_n$, siis $\psi(\omega)$ on n-aarne algebraline tehe hulgal A (vt ka definitsiooni 1.1).

Hulka A nimetatakse universaalalgebra **kandjaks**, **põhihulgaks** või ka **universumiks**. Universaalalgebrat ennast tähistatakse tavaliselt sümboliga $\mathbf{A}$, et teda oma kandjast eristada. Traditsiooniliselt loetakse universaalalgebratest rääkides, et põhihulk on mittetühi. Selles kursuses me sellist kitsendust ei tee.

Seda algebra osa, mis tegeleb universaalalgebrate ja nende omaduste uurimisega üldiselt vaatekohalt (st nõudes *a priori* ainult teatava hulga tehete olemasolu ilma neile lisakitsendusi seadmata), nimetatakse samuti universaalalgebraks. Traditsiooniliselt kutsutakse universaalalgebraid sellises üldises kontekstis lihtsalt algebrateks. Loengukonspektis on seni tarvitatud terminit "algebraline struktuur", aga edaspidi kasutame samuti nimetust "algebra" või "Ω-algebra".

Algebra signatuurist võib mõelda kui kõigi sellel antud tehete jaoks kasutatavate tehtemärkide hulgast. Öeldakse, et universaalalgebrad on **sama tüüpi**, kui nende signatuurid on võrdsed. Kui $\omega \in \Omega_n$, siis n-aarset algebralist tehet $\psi(\omega)$ tähistame sümboliga ω^A või lihtsalt ω, kui hulk A on kontekstist selge. Sama tüüpi algebrate $\mathbf{A}$ ja $\mathbf{B}$ korral võib sümbol ω seetõttu tähistada korraga nii tehtemärki hulgast Ω_n, kujutust $A^n \to A$ ja kujutust $B^n \to B$, mis on üldiselt kõik erinevad.

Näide 10.2 Toome mõned näited eri tüüpi algebratest.

1. Iga hulk on algebra signatuuriga $\Omega = \emptyset$.

2. Rühmoidid ja poolrühmad on algebrad signatuuriga $\Omega = \Omega_2$, kus $\Omega_2 = \{\cdot\}$ (korrutamine).
3. Abeli rühmad on algebrad signatuuriga $\Omega = \Omega_0 \sqcup \Omega_1 \sqcup \Omega_2$, kus $\Omega_0 = \{0\}$ (nullelemendi fikseerimine), $\Omega_1 = \{\text{-}\}$ (vastandelemendi võtmine) ja $\Omega_2 = \{+\}$ (liitmine).
4. Ringid on algebrad signatuuriga $\Omega = \Omega_0 \sqcup \Omega_1 \sqcup \Omega_2$, kus Ω_0 ja Ω_1 on samad, mis Abeli rühmade korral ning $\Omega_2 = \{+, \cdot\}$ (lisandub korrutamine).
5. Parempoolsed moodulid üle ringi R on algebrad signatuuriga $\Omega = \Omega_0 \sqcup \Omega_1 \sqcup \Omega_2$, kus Ω_0 ja Ω_2 on samad, mis Abeli rühmade korral ning $\Omega_1 = \{\text{-}\} \cup \{\cdot r \mid r \in R\}$ (lisandub $|R|$ korrutamistehet ringi R elementidega).
6. Võred on algebrad signatuuriga $\Omega = \Omega_2 = \{\wedge, \vee\}$ (alumise ja ülemise raja võtmine).

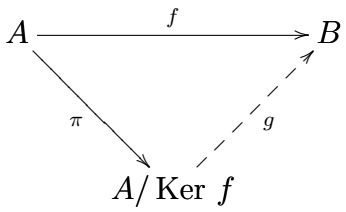
Universaalalgebrate alamalgebrad, homomorfismid, isomorfismid, kongruentsid, faktoralgebrad ja korrutised on 1. peatükis juba sisuliselt defineeritud (vt definitsioone 1.9, 1.12, 1.20, 1.26, lausele 1.28 järgnevat ja lausele 1.54 eelnevat lõiku). Defineerime üldisemal kujul homomorfismi tuuma mõiste.

Definitsioon 10.3 Olgu $\mathbf{A}$ ja $\mathbf{B}$ sama tüüpi algebrad. Homomorfismi $f : \mathbf{A} \to \mathbf{B}$ **tuum** $\operatorname{Ker} f$ on binaarne seos

$$\operatorname{Ker} f = \{(a, a') \in A \times A \mid f(a) = f(a')\}.$$

On lihtne veenduda, et homomorfismi tuum on alati kongruents. Algebrate jaoks kehtivad järgmised teoreemi 1.35 ja järelduse 1.36 analoogid, mille tõestus on praktiliselt sama.

Teoreem 10.4 (Homomorfismiteoreem) *Olgu $f : \mathbf{A} \to \mathbf{B}$ sama tüüpi algebrate homomorfism. Siis leidub üksühene homomorfism $g : \mathbf{A}/\operatorname{Ker} f \to \mathbf{B}$ nii, et $f = g\pi$, kus $\pi : \mathbf{A} \to \mathbf{A}/\operatorname{Ker} f$ on loomulik projektsioon.*



Järeldus 10.5 *Kui homomorfism $f : \mathbf{A} \to \mathbf{B}$ on sürjektiivne, siis $\mathbf{A}/\operatorname{Ker} f \cong \mathbf{B}$.*

Universaalalgebra on tihedalt seotud võreteooriaga. Näiteks algebra $\mathbf{A}$ kõigi alamalgebrate hulk $\mathsf{Sub}(\mathbf{A})$ on võre, kus alumiseks rajaks on ühisosa võtmine ja ülemiseks rajaks on vähima mõlemat alamalgebrat sisaldava alamalgebra leidmine. Teatud juhtudel saab võre $\mathsf{Sub}(\mathbf{A})$ struktuurist välja lugeda informatsiooni algebra $\mathbf{A}$ omaduste kohta.

Mistahes algebra kõigi kongruentside hulk $\mathsf{Con}(\mathbf{A})$ on samuti võre. Kongruentside ρ ja τ alumine raja $\rho \wedge \tau$ defineeritakse seosega

$$a \; (\rho \wedge \tau) \; a' \iff (a \; \rho \; a') \wedge (a \; \tau \; a')$$

(s.t. $\rho \wedge \tau = \rho \cap \tau$) ning ülemine raja $\rho \vee \tau$ seosega

$$a\ (\rho \vee \tau)\ a' \Longleftrightarrow \exists a_1, \ldots, a_n \in A : (a\ \rho\ a_1) \wedge (a_1\ \tau\ a_2) \wedge \ldots \wedge (a_{n-1}\ \rho\ a_n) \wedge (a_n\ \tau\ a'),$$

mistahes $a, a' \in A$ jaoks. Neile tehetele vastav järjestusseos $\leq$ hulgal $\mathsf{Con}(\mathbf{A})$ on sisalduvusseos $\subseteq$ ehk

$$\rho \leq \tau \Longleftrightarrow (\forall a, a' \in A)(a\ \rho\ a' \Rightarrow a\ \tau\ a').$$

Kongruentside võred on algebrate uurimisel väga olulised abivahendid ja annavad tavaliselt algebra kohta tunduvalt rohkem informatsiooni kui alamalgebrate võred.

Sama tüüpi algebrate **otsekorrutised** on defineeritud alapeatükis 1.8.

10.2 Muutkonnad

Olgu $\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$ signatuur ja X mittetühi hulk. Me mõtleme X elementidest kui muutujatest (selles tähenduses nagu muutuja esineb polünoomi definitsioonis), vahel ütleme nende kohta ka "täht".

Definitsioon 10.6 (Ω, X)**-termid** defineeritakse järgmiste kolme tingimuse abil.

1. Hulga $\Omega_0 \cup X$ elemendid on 0-astme (Ω, X)-termid.
2. Kui $n, m \in \mathbb{N}, \omega \in \Omega_n$ ja $t_1, \ldots, t_n$ on ülimalt $(m-1)$-astme (Ω, X)-termid, kusjuures vähemalt üks neist on täpselt $(m-1)$-astme (Ω, X)-term, siis "sõna" $\omega(t_1, \ldots, t_n)$ on m-astme (Ω, X)-term.
3. Rohkem (Ω, X)-terme ei ole.

Termid on seega teatud reeglite abil tähestikus $\Omega \cup X \cup \{(\} \cup \{)\} \cup \{,\}$ kirja pandud sõnad ehk sümbolite järjendid.

Märkus 10.7 Iga (Ω, X)-term definitsiooni 10.6 mõttes on term ka kursuse "Diskreetne matemaatika I" mõttes. Nimelt

- hulga Ω_0 elemente saame tõlgendada konstantsümbolitena,
- hulga $\bigsqcup_{n=1}^{\infty} \Omega_n$ elemendid loeme funktsionaalsümboliteks,
- predikaatsümbolid meil praegu signatuuris puuduvad.

Kõigi (Ω, X)-termide hulka tähistame sümboliga $F(X)$ (kasutusel on ka $T(X)$ ja $T(\Omega, X)$). Hulga $F(X)$ saab muuta Ω-algebraks, kui defineerida iga $\omega \in \Omega_0$ jaoks

$$\omega^{F(X)} = \omega \in F(X)$$

ning mistahes $\omega \in \Omega_n$, $n \in \mathbb{N}$ ja $t_1, \ldots, t_n \in F(X)$ korral võtta

$$\omega^{F(X)}(t_1, \ldots, t_n) = \omega(t_1, \ldots, t_n) \in F(X)\,. \tag{10.1}$$

Saadud algebrat $\mathbf{F(X)}$ nimetatakse **termide algebraks** või **absoluutselt vabaks algebraks** baasiga X ja signatuuriga Ω. Hulka X nimetatakse tihti selle algebra **tähestikuks** ning tema elemente tähtedeks.

Näide 10.8 Olgu Ω ühikuga ringi signatuur, s.t. $\Omega = \{0, 1\} \cup \{\text{-}\} \cup \{+, \cdot\}$, ja $X = \{x, y\}$. Siis $F(X)$ elemendid on näiteks

$$((x + y) \cdot (x + 1)) + (-(y + x)),\ x + y,\ y + x.$$

Isegi kui me vaatleksime ainult kommutatiivseid ringe, on kaks viimast $F(X)$ elementi erinevad. Formaalselt peaksime definitsiooni 10.6 järgides $x+y$ asemel kirjutama $+(x, y)$, aga üldlevinud kokkuleppe kohaselt kirjutatakse kahekohaline tehtemärk argumentide vahele.

0-astme termid on $0, 1, x, y$, esimese astme termiks on näiteks $y + x$ ja teise astme termiks $-(y + x)$.

Algebras $\mathbf{F(X)}$ on näiteks elementide $x + y$ ja $y + x$ korrutiseks term $(x + y) \cdot (y + x)$.

Konkreetse termi $t \in F(X)$ korral on tihti otstarbekas välja tuua need tähed, mis selles termis esineda võivad. Edaspidi kirjutame $t = t(x_1, \ldots, x_n)$, kui tähed hulgast $X \setminus \{x_1, \ldots, x_n\}$ termis t kindlasti ei esine. Tähed $x_1, \ldots, x_n$ võivad, aga ei pea seal esinema. Näiteks saame ühikuga ringi signatuuris kirjutada, et

$$t_1(x, y, z) = t_2(x, y) = ((x + y) \cdot (x + 1)) + (-(y + x)) .$$

Kui termis t on ülimalt n tähte, siis seda termi nimetatakse **n-aarseks**. Märgime, et nullaarsed termid on olemas ainult siis, kui $\Omega_0 \neq \emptyset$.

Kui $\mathbf{A}$ on Ω-algebra, siis iga n-aarne (Ω, X)-term tekitab loomulikul viisil ühe n-aarse funktsiooni $A^n \longrightarrow A$. Kuna termid defineeriti induktiivselt, tuleb siin samamoodi teha.

Definitsioon 10.9 Kui $t = t(x_1, \ldots, x_n) \in F(X) = T(\Omega, X)$ ja $\mathbf{A}$ on Ω-algebra, siis n-aarne funktsioon $t^A : A^n \to A$ defineeritakse järgmiselt:

1. kui $t = \omega \in \Omega_0$, siis mistahes $a_1, \ldots, a_n \in A$ korral $t^A(a_1, \ldots, a_n) = 0^A_\omega$, kus 0^A_ω on nullaarse tehte ω poolt fikseeritud element hulgas A,

2. kui $t = x \in X$, siis $x = x_i$ mingi $i \in \{1 \ldots, n\}$ korral, ja mistahes $a_1, \ldots, a_n \in A$ jaoks saame võtta funktsiooniks t^A **projektsiooni** i-ndale komponendile, s.t.

$$t^A(a_1, \ldots, a_n) = a_i ,$$

3. kui $t = \omega(t_1, \ldots, t_s) \in F(X)$ on m-astme term, s.t. $t_1, \ldots, t_s$ on ülimalt $(m - 1)$ astme termid ja $\omega \in \Omega_s$, siis mistahes $a_1, \ldots, a_n \in A$ korral

$$t^A(a_1, \ldots, a_n) = \omega^A(t^A_1(a_1, \ldots, a_n), \ldots, t^A_s(a_1, \ldots, a_n)) .$$

   Paneme siin tähele, et eelmises lõigus sisse toodud "fiktiivsete" muutujate lisamine võimaldab meil muuta termid $t, t_1, \ldots, t_s$ sama aarsusega n ja samade tähtedega $x_1, \ldots, x_n$ termideks, sest termides t_i ei tohi esineda tähti hulgast $X \setminus \{x_1, \ldots, x_n\}$.

Edaspidi kirjutame jällegi $t^A(a_1, \ldots, a_n)$ asemel lihtsalt $t(a_1, \ldots, a_n)$. Funktsioone t^A nimetatakse **termfunktsioonideks** algebral $\mathbf{A}$. Kõigi termfunktsioonide hulka algebral $\mathbf{A}$ tähistatakse sümboliga T^A.

Märkus 10.10 Termfunktsioonide kohta saab teha järgmised tähelepanekud:

1. Kuna igas termis saab sisalduda vaid lõplik arv tähti, siis T^A sisaldab juba loenduva tähestiku X korral kõiki võimalikke termfunktsioone.

2. Kõik algebra $\mathbf{A}$ tehted ja kõik projektsioonid on termfunktsioonid.

3. Kui vaatleme muutujat $x \in X$ unaarse termina $t = x$, siis tema poolt tekitatud unaarne termfunktsioon (projektsioon) on samasusteisendus, $x^A(a) = a$ iga $a \in A$ korral.

4. Termfunktsioonide hulk on kinnine (mitmemuutuja) funktsioonide kompositsiooni suhtes.

Näide 10.11 Vaatleme täisarvude ringi $\mathbb{Z}$ Ω-algebrana signatuuris $\Omega = \{0,1\} \cup \{\text{-}\} \cup \{+,\cdot\}$. Olgu $X = \{x_1, x_2, x_3\}$.

1. Term $t_1 = ((1+1)+1)\cdot(x_1 \cdot x_1)$ tekitab unaarse termfunktsiooni
$$t_1^{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad a \mapsto 3a^2\,.$$

2. Term $t_2 = x_1 + x_2$ tekitab binaarse termfunktsiooni
$$t_2^{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (a,b) \mapsto a+b\,.$$
See termfunktsioon langeb kujutusena kokku ringi $\mathbb{Z}$ liitmistehtega.

3. Term $t_3(x_1,x_2,x_3) = x_2$ tekitab ternaarse termfunktsiooni
$$t_3^{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (a,b,c) \mapsto b$$
(see on projektsioon teisele komponendile).

4. Erinevatele termidele vastavad termfunktsioonid võivad olla võrdsed. Näiteks $t_4^{\mathbb{Z}} = t_5^{\mathbb{Z}}$, kus
$$t_4 = x_1 + x_2, \quad t_5 = x_2 + x_1\,,$$
sest täisarvude liitmine on kommutatiivne. Sellisel juhul saame rääkida samasusest, s.t. algebra $\mathbb{Z}$ rahuldab samasust $x_1 + x_2 = x_2 + x_1$ (vt definitsiooni 10.13).

Lause 10.12 *Iga algebra on isomorfne mingi sama tüüpi absoluutselt vaba algebra faktoralgebraga.*

TÕESTUS. Vaatleme Ω-algebrat $\mathbf{A}$. Võtame mingi hulga X, mille võimsus ei ole väiksem kui A võimsus. (Selliseid hulki kindlasti leidub, näiteks võib võtta $X := A$.) Siis leidub sürjektiivne kujutus $\rho : X \longrightarrow A$. Olgu $\mathbf{F}(\mathbf{X})$ absoluutselt vaba Ω-algebra baasiga X. Defineerime kujutuse $f : F(X) \to A$ järgmiselt:
$$f(t(x_1,\ldots,x_s)) = t^A(\rho(x_1),\ldots,\rho(x_s)) \in A$$
iga termi $t(x_1,\ldots,x_s) \in F(X)$ korral. See kujutus on sürjektiivne, sest iga $a \in A$ korral leidub $x \in X$ nii, et
$$a = \rho(x) = x^A(\rho(x)) = f(x)\,,$$
kus kasutasime seda, et termi $t = x$ poolt tekitatud termfunktsioon $x^A : A \longrightarrow A$ on samasusteisendus (vt. märkust 10.10).

Näitame, et kujutus f on Ω-algebrate homomorfism. Esiteks, iga $w \in \Omega_0$ korral $w^{F(X)} = w \in F(X)$ ja
$$f(w^{F(X)}) = f(w) = w^A = 0_\omega^A\,,$$
seega f säilitab null-aarseid tehteid. Olgu nüüd $n \in \mathbb{N}$, $w \in \Omega_n$ ja $t_1,\ldots,t_n \in F(X)$. Eelneva kokkuleppe kohaselt võib termi aarsust alati suurendada. Seega kui $\{x_1,\ldots,x_s\}$

on kõik tähed, mis esinevad vähemalt ühes termidest $t_1, \ldots, t_n$, siis saame kirjutada, et $t_i = t_i(x_1, \ldots, x_s)$, $i = 1, \ldots, n$, ning järelikult

$$\begin{aligned} f(\omega^{F(X)}(t_1, \ldots, t_n)) &= f(\omega(t_1, \ldots, t_n)) && ((10.1)) \\ &= \omega^A(t_1^A(\rho(x_1), \ldots, \rho(x_s)), \ldots, t_n^A(\rho(x_1), \ldots, \rho(x_s))) && (f \text{ def.}) \\ &= \omega^A(f(t_1(x_1, \ldots, x_s)), \ldots, f(t_n(x_1, \ldots, x_s))) && (f \text{ def.}) \\ &= \omega^A(f(t_1), \ldots, f(t_n))\,. \end{aligned}$$

Seega f säilitab ka n-aarseid tehteid ja on homomorfism. Järelduse 10.5 põhjal $\mathbf{A} \cong \mathbf{F}(\mathbf{X})/\operatorname{Ker} f$. □

Defineerime nüüd samasused ja muutkonnad. Muutkondade uurimine on universaalalgebra üks kesksemaid probleeme.

Definitsioon 10.13 Olgu Ω signatuur ja $u, v \in F(X) = T(\Omega, X)$, kus $X = \{x_1, x_2, \ldots\}$ on loenduv hulk. Öeldakse, et Ω-algebral $\mathbf{A}$ kehtib **samasus** $u = v$, kui termidele u ja v vastavad termfunktsioonid on võrdsed, s.t. $u^A = v^A$.

Formaalselt on samasus tegelikult termide paar (u, v), aga sisulise arusaamise lihtsustamiseks kirjutame selle üles kujul $u = v$. Paneme veel tähele, et termfunktsioonide võrduseks peavad termide u ja v aarsused kokku langema. Kui nad seda ei tee, siis me võime vastavalt varasemale kokkuleppele väiksema aarsusega termi aarsust sobivalt suurendada, lisades vajaliku arvu "fiktiivseid" muutujaid x_i. Siit on ka näha, miks me nõudsime loenduvat tähtede arvu: me tahame, et oleks võimalik mistahes lõpliku aarsusega terme ja termfunktsioone võrrelda.

Definitsioon 10.14 Ω-algebrate klassi $\mathcal{K}$ nimetatakse **muutkonnaks**, kui leidub selline samasuste hulk S, et klassi $\mathcal{K}$ kuuluvad need ja ainult need algebrad, mis rahuldavad kõiki hulka S kuuluvaid samasusi.

Paljud varem kursuses käsitletud algebralised struktuurid moodustavad muutkonna (vt tabelit järgmisel lehel). Samas nii mitmedki tuntud struktuurid ei moodusta (üldiselt) muutkonda, näiteks lõplikud, jaguvad ja lahenduvad rühmad, korpused, injektiivsed ja projektiivsed moodulid.

Muutkonnaks olek on teatud mõttes formaalne, sest see sõltub vaadeldavast signatuurist. Näiteks moodustavad kõik rühmad muutkonna signatuuris $\Omega = \{1\} \cup \{^{-1}\} \cup \{\cdot\}$, aga nad ei moodusta kõigi monoidide muutkonna alammuutkonda signatuuris $\Omega' = \{1\} \cup \{\cdot\}$.

Muutkond	Signatuur	Samasused
Poolrühmad	$\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$
Inverssed poolrühmad	$\Omega_1 = \{'\}$ $\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $x \cdot x' \cdot x = x$, $x' \cdot x \cdot x' = x'$
Monoidid	$\Omega_0 = \{1\}$ $\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $1 \cdot x_1 = x_1$, $x_1 \cdot 1 = x_1$
Rühmad	$\Omega_0 = \{1\}$ $\Omega_1 = \{^{-1}\}$ $\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $1 \cdot x_1 = x_1$, $x_1 \cdot 1 = x_1$ $x_1 \cdot x_1^{-1} = 1$, $x_1^{-1} \cdot x_1 = 1$
Abeli rühmad	$\Omega_0 = \{0\}$ $\Omega_1 = \{-\}$ $\Omega_2 = \{+\}$	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ $0 + x_1 = x_1$, $x_1 + 0 = x_1$ $x_1 + (-x_1) = 0$, $(-x_1) + x_1 = 0$ $x_1 + x_2 = x_2 + x_1$
Ringid	$\Omega_0 = \{0, 1\}$ $\Omega_1 = \{-\}$ $\Omega_2 = \{+, \cdot\}$	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ $0 + x_1 = x_1$, $x_1 + 0 = x_1$ $x_1 + (-x_1) = 0$, $(-x_1) + x_1 = 0$ $x_1 + x_2 = x_2 + x_1$ $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $1 \cdot x_1 = x_1$, $x_1 \cdot 1 = x_1$ $x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$ $(x_1 + x_2) \cdot x_3 = x_1 \cdot x_3 + x_2 \cdot x_3$
Võred	$\Omega_2 = \{\wedge, \vee\}$	$x_1 \vee (x_2 \vee x_3) = (x_1 \vee x_2) \vee x_3$ $x_1 \vee x_2 = x_2 \vee x_1$ $x_1 \vee x_1 = x_1$ $(x_1 \vee x_2) \wedge x_1 = x_1$ $x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3$ $x_1 \wedge x_2 = x_2 \wedge x_1$ $x_1 \wedge x_1 = x_1$ $(x_1 \wedge x_2) \vee x_1 = x_1$
S-polügoonid	$\Omega_1 = \{\cdot s \mid s \in S\}$	$(x_1 \cdot s) \cdot t = x_1 \cdot (st)$ ($\lvert S\rvert^2$ samasust) $x_1 \cdot 1 = x_1$
R-moodulid	$\Omega_1 = \{r\cdot \mid r \in R\}$ $\Omega_2 = \{+\}$	$x_1+(x_2+x_3) = (x_1+x_2)+x_3$ $0 + x_1 = x_1, x_1 + 0 = x_1$ $x_1 + (-x_1) = 0$, $-x_1+x_1 = 0$ $x_1 + x_2 = x_2 + x_1$ $r \cdot (x_1 + x_2) = r \cdot x_1 + r \cdot x_2$ ($\lvert R\rvert$ samasust) $(r + s) \cdot x_1 = r \cdot x_1 + s \cdot x_1$ ($\lvert R\rvert^2$ samasust) $r \cdot (s \cdot x_1) = (rs) \cdot x_1$ ($\lvert R\rvert^2$ samasust) $1 \cdot x_1 = x_1$
Üheelemendilised algebrad	Ω	$x_1 = x_2$
Kõik algebrad signatuuriga Ω	Ω	$x_1 = x_1$

Järgmine teoreem on universaalalgebra üks olulisemaid tulemusi, mis ütleb, et muutkondi võib defineerida kahel samaväärsel viisil:

- samasuste abil,
- kinnisuse abil teatavate operatsioonide suhtes.

Märgime, et Ω-algebrate klassi nimetatakse **triviaalseks**, kui see koosneb ainult triviaalsetest algebratest, s.t. üheelemendilistest algebratest ja tühjast algebrast.

Teoreem 10.15 (Birkhoff) *Mittetriviaalne Ω-algebrate klass on muutkond parajasti siis, kui see on kinnine alamalgebrate, homomorfsete kujutiste ja (mistahes võimsusega) otsekorrutiste võtmise suhtes.*

Birkhoffi teoreemi kutsutakse operatsioonide nimede järgi mõnikord ka HSP-teoreemiks (need tähed tulevad terminitest *homomorphic image, subalgebra, direct product*).

Mistahes Ω-algebra $\mathbf{A}$ puhul leidub vähim Ω-algebrate muutkond $\mathrm{Var}\,(\mathbf{A})$, mis seda algebrat sisaldab. On võimalik näidata, et

$$\mathrm{Var}\,(\mathbf{A}) = HSP(\mathbf{A}),$$

s.t. see muutkond koosneb $\mathbf{A}$ otseastmete alamalgebrate homomorfsetest kujutistest (faktoralgebratest).

Peatükk 11

Kategooriad

11.1 Kategooria mõiste

11.1.1 Objektid ja morfismid

Kategooria koosneb kahte sorti asjadest: objektidest ja nendevahelistest morfismidest, mida saab teatud juhtudel korrutada. Objektid võivad olla nt. (teatud struktuuriga, nt. algebralise, topoloogilise vm.) hulgad ja morfismideks kujutused (mis on kooskõlas struktuuriga). Formaalne definitsioon on järgmine.

Definitsioon 11.1 **Kategooria** $\mathcal{C}$ koosneb järgmistest komponentidest:

1. klass $\mathcal{C}_0$, mille elemente kutsume selle kategooria **objektideks**;
2. iga objektipaari (A, B) jaoks on olemas hulk $\mathcal{C}(A, B)$, mille elemente nimetame **morfismideks** objektist A objekti B;
3. iga objektikolmiku (A, B, C) jaoks on olemas kujutus (**komponeerimine** ehk **korrutamine**)
$$\mathcal{C}(A, B) \times \mathcal{C}(B, C) \longrightarrow \mathcal{C}(A, C);$$
paari (f, g) kujutist (morfismide f ja g **kompositsiooni** ehk **korrutist**) tähistame $g \circ f$ või lühidalt gf;
4. iga objekti A jaoks on olemas morfism $1_A \in \mathcal{C}(A, A)$, mida kutsutakse objekti A **ühikmorfismiks**.

Need andmed peavad rahuldama järgmisi aksioome.

1. Kui $(A, B) \neq (A', B')$, siis $\mathcal{C}(A, B) \cap \mathcal{C}(A', B') = \emptyset$.
2. **Assotsiatiivsuse aksioom:** mistahes morfismide $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$, $h \in \mathcal{C}(C, D)$ korral kehtib võrdus
$$h(gf) = (hg)f.$$
3. **ühiku aksioom:** mistahes morfismide $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$ korral kehtivad võrdused $1_B f = f$ ja $g1_B = g$.

Morfismi $f \in \mathcal{C}(A,B)$ jaoks kasutatakse tihti tähistusi $f : A \to B$ ja $A \xrightarrow{f} B$; üheselt määratud objekti A kutsutakse morfismi f **lähteobjektis** ehk domeeniks (tähistus: $\mathrm{dom}\, f$) ning objekti B kutsutakse f **sihtobjektiks** ehk kodomeeniks (tähistus: $\mathrm{cod}\, f$). Morfismi $f : A \to A$ nimetatakse objekti A **endomorfismiks** ja hulka $\mathsf{End}(A) = \mathcal{C}(A,A)$ nimetatakse objekti A endomorfismide hulgaks. On selge, et $(\mathsf{End}(A), \circ)$ on monoid. Kategooria $\mathcal{C}$ objektide klassi tähistatakse ka $\mathrm{Ob}(\mathcal{C})$ või $|\mathcal{C}|$, morfismide klassi aga $\mathrm{Mor}(\mathcal{C})$ või $\mathcal{C}_1$. Morfismide hulka objektist A objekti B tähistatakse veel ka sümboliga $\mathrm{Mor}(A,B)$ või $\hom(A,B)$.

Märkused 11.2 1. Osutub, et 1_A on objekti A ainus ühikmorfism, sest kui $i_A \in \mathcal{C}(A,A)$ on veel mingi morfism, mis rahuldab ühiku aksioomi, siis $1_A = 1_A i_A = i_A$.

2. Samamoodi nagu poolrühmade korral järeldub assotsiatiivsuse aksioomist, et lõpliku arvu morfismide komponeerimisel võib sulge paigutada mistahes (mõttekal) viisil ja seega võib nad üldse ära jätta.

Definitsioon 11.3 Kategooria on **väike** kui tema objektide klass on hulk, vastasel korral kutsutakse kategooriat **suureks**.

Näide 11.4 Paljud matemaatilised struktuurid ja nendevahelised kujutused või homomorfismid moodustavad kategooria. Järgnevas tabelis on toodud mõned selliste kategooriate näited.

Tähis	objektid	morfismid
Set	hulgad	kujutused
Rel	hulgad	binaarsed seosed hulkade vahel
Mon	monoidid	monoidide homomorfismid
Gr	rühmad	rühmade homomorfismid
Ab	Abeli rühmad	rühmade homomorfismid
Rng	assotsiatiivsed ringid	ringide homomorfismid
$\mathsf{Vec}_{\mathbb{R}}$	vektorruumid üle reaalarvude	lineaarkujutused
Mod_R	parempoolsed moodulid üle ringi R	moodulite homomorfismid
Ban_∞	Banachi ruumid üle reaalarvude	tõkestatud lineaarkujutused
Ban_1	Banachi ruumid üle reaalarvude	ahendavad lineaarkujutused
Top	topoloogilised ruumid	pidevad kujutused
Pos	järjestatud hulgad	järjestust säilitavad kujutused
Lat	võred	võrede homomorfismid
Graph	graafid	graafide homomorfismid
Sgraph	graafid	tugevad graafide homomorfismid
$\mathbf{0}$	ei ole	ei ole
$\mathbf{1}$	A	1_A
$\mathbf{2}$	A, B	$A \to B, 1_A, 1_B$

Enamasti on morfismide komponeerimiseks tavaline kujutuste komponeerimine (järjestrakendamine) ja ühikmorfismid on samasusteisendused. Kategoorias Rel on seoste kompositsiooniks nende korrutis ja ühikmorfism on võrdusseos. Kategooriat $\mathbf{0}$ nimetatakse **tühjaks kategooriaks**.

Näide 11.5 1. Kategooria, kus objektid on naturaalarvud, morfismid m-st n-i on kõik maatriksid (üle fikseeritud korpuse), millel on m rida ja n veergu, morfismide komponeerimine on maatriksite korrutamine ja ühikmorfismideks on vastavat järku ühikmaatriksid.

2. Osaliselt järjestatud hulka $(P, \leqslant)$ võib vaadelda kategooriana $\mathcal{P}$, mille objektide hulk on P. Kui $x, y \in P$, siis hulk $\mathcal{P}(x, y)$ koosneb täpselt ühest morfismist, kui $x \leqslant y$, ning on tühi vastasel juhul. (Tegelikult piisab kategooria saamiseks sellest, et $\leqslant$ on eeljärjestus, s.t. refleksiivne ja transitiivne seos hulgal P.)

3. Iga hulka võib vaadelda kui **diskreetset kategooriat**, s.t. kui kategooriat, mille objektid on selle hulga elemendid ja ainsad morfismid on ühikmorfismid.

4. Iga monoid $(M, \cdot)$ tekitab kategooria $\mathcal{M}$, kus $\mathcal{M}_0 = \{*\}$, ja $\mathcal{M}(*, *) = M$; morfismide komponeerimine on monoidi M korrutamine $\cdot$ ja objekti $*$ ühikmorfism on monoidi ühikelement 1. Ka vastupidi: iga üheobjektilise kategooria kõigi morfismide hulk on monoid.

11.1.2 Alam- ja korrutiskategooriad

Olemasolevatest kategooriatest saab teatud konstruktsioonide abil luua uusi.

Definitsioon 11.6 Kategooria $\mathcal{A}$ **alamkategooria** koosneb

1. kategooria $\mathcal{A}$ objektide klassi $\mathcal{A}_0$ alamklassist $\mathcal{B}_0$;

2. iga objektipaari $(B, B') \in \mathcal{B}_0 \times \mathcal{B}_0$ jaoks leiduvast hulgast $\mathcal{B}(B, B') \subseteq \mathcal{A}(B, B')$, nii et

   (a) kui $f \in \mathcal{B}(B, B')$ ja $g \in \mathcal{B}(B', B'')$, siis $gf \in \mathcal{B}(B, B'')$,

   (b) $1_B \in \mathcal{B}(B, B)$ iga $B \in \mathcal{B}_0$ korral.

Definitsioon 11.7 Kategooria $\mathcal{A}$ alamkategooriat $\mathcal{B}$ nimetatakse **täielikuks alamkategooriaks**, kui

$$B, B' \in \mathcal{B}_0 \Longrightarrow \mathcal{B}(B, B') = \mathcal{A}(B, B'),$$

s.t. $\mathcal{B}$ sisaldab koos iga kahe objektiga kõik nende objektide vahel kategoorias $\mathcal{A}$ leiduvad morfismid.

Näide 11.8 1. Kategooria Ab on kategooria Gr täielik alamkategooria.
2. Gr on Mon täielik alamkategooria.
3. Mon on poolrühmade kategooria Sgr alamkategooria, mis ei ole täielik.
4. Kategooria Ban_∞ on $\mathsf{Vec}_\mathbb{R}$ alamkategooria, kuid mitte täielik alamkategooria.

11.2 Morfismide liigid.

Nii nagu hulkade korral on tähtsal kohal üksühesed kujutused ja pealekujutused, nii ka kategooriates võib vaadelda teatud eriomadustega morfisme.

Definitsioon 11.9 Morfismi $f : A \to B$ kategoorias $\mathcal{C}$ nimetatakse

- **monomorfismiks**, kui ta on vasakult taandatav, s.t. iga morfismide paari $g, h : C \to A$ korral
$$fg = fh \;\Rightarrow\; g = h;$$
- **koretraktsiooniks** (või lõikeks), kui ta on vasakult pööratav, s.t. leidub selline morfism $g : B \to A$, et $gf = 1_A$. Sellisel juhul nimetatakse objekti A objekti B **retraktiks**.

Lause 11.10 *Kategoorias $\mathcal{C}$*

1. *iga koretraktsioon on monomorfism;*
2. *iga ühikmorfism on koretraktsioon;*
3. *kahe monomorfismi (koretraktsiooni) korrutis on monomorfism (koretraktsioon);*
4. *kui kahe morfismi korrutis kf monomorfism (koretraktsioon), siis f on monomorfism (koretraktsioon).*

Tõestus. 1. Oletame, et $kf = 1_A$ ja $fg = fh$ kus $f : A \to B$, $k : B \to A$ ja $g, h : C \to A$. Siis
$$g = 1_A g = (kf)g = k(fg) = k(fh) = (kf)h = 1_A h = h.$$

2. Iga $A \in \mathcal{C}_0$ korral $1_A = 1_A 1_A$.

3. Eeldame, et $k : B \to D$ ja $f : A \to B$ on monomorfismid ja oletame, et $(kf)g = (kf)h$, kus $g, h : C \to A$. Olukorda iseloomustab järgmine diagramm:
$$C \underset{h}{\overset{g}{\rightrightarrows}} A \xrightarrow{f} B \xrightarrow{k} D\,.$$
Siis $k(fg) = k(fh)$ ja seega $fg = fh$, sest k on monomorfism. Kuna f on monomorfism, siis viimasest võrdusest järeldub $g = h$. Sellega oleme näidanud, et kf on monomorfism.

Kui $k : B \to D$ ja $f : A \to B$ on koretraktsioonid, s.t. $sk = 1_B$ ja $tf = 1_A$ mingite $s : D \to B$ ja $t : B \to A$ korral, siis võrduste ahel
$$(ts)(kf) = t(sk)f = t1_B f = tf = 1_A$$
näitab, et kf on koretraktsioon.

$$A \underset{t}{\overset{f}{\rightleftarrows}} B \underset{s}{\overset{k}{\rightleftarrows}} D$$

4. Oletame, et kf on monomorfism ja $fg = fh$, kus $f : A \to B$, $k : B \to D$ ja $g, h : C \to A$. Siis

$$(kf)g = k(fg) = k(fh) = (kf)h,$$

millest järeldub võrdus $g = h$. Seega f on monomorfism.

Kui kf on koretraktsioon, s.t. $s(kf) = 1_A$ mingi $s : D \to A$ korral, siis $(sk)f = 1_A$ tähendab seda, et ka f on koretraktsioon. □

Definitsioon 11.11 Morfismi $f : A \to B$ kategoorias $\mathcal{C}$ nimetatakse

- **epimorfismiks** kui ta on paremalt taandatav, s.t. iga morfismipaari $g, h : B \to C$ korral
$$gf = hf \quad \Rightarrow \quad g = h;$$
- **retraktsiooniks**, kui ta on paremalt pööratav, s.t. leidub $g : B \to A$ nii, et $fg = 1_B$.

Analoogiliselt lausega 11.10 saab tõestada järgmise lause.

Lause 11.12 *Kategoorias $\mathcal{C}$*

1. *iga retraktsioon on epimorfism;*
2. *iga ühikmorfism on retraktsioon;*
3. *kahe epimorfismi (retraktsiooni) korrutis on epimorfism (retraktsioon);*
4. *kui kahe morfismi korrutis kf on epimorfism (retraktsioon), siis k on epimorfism (retraktsioon).*

Näide 11.13 Hulkade kategoorias Set on monomorfismideks parajasti injektiivsed kujutused ja epimorfismideks sürjektiivsed kujutused. Veelgi enam, iga sürjektiivne kujutus on retraktsioon.

Näide 11.14 Kategooriates Gr ja Ab on monomorfismideks parajasti injektiivsed rühmade homomorfismid.

Definitsioon 11.15 Morfismi nimetatakse **bimorfismiks**, kui ta on nii monomorfism kui ka epimorfism, s.t. kui ta on taandatav.

Definitsioon 11.16 Morfismi nimetatakse **isomorfismiks**, kui ta on nii koretraktsioon kui ka retraktsioon, s.t. kui ta on pööratav. Kategooria $\mathcal{C}$ objektid A ja B on **isomorfsed** kui leidub isomorfism $f : A \to B$. Objektide A ja B isomorfsust tähistatakse $A \cong B$.

Lause 11.17 *Kategoorias $\mathcal{C}$*

1. *iga isomorfism on bimorfism;*
2. *iga ühikmorfism on isomorfism;*
3. *kahe bimorfismi (isomorfismi) korrutis on bimorfism (isomorfism).*

TÕESTUS. See järeldub lausest 11.10 ja lausest 11.12. □

Järeldus 11.18 *Objektide isomorfsusseos on ekvivalentsiseos.*

Lause 11.19 *Kui epimorfism on koretraktsioon, siis on ta isomorfism.*

TÕESTUS. Jätame lugejale läbimõtlemiseks. □

Näide 11.20 Kategoorias Set on isomorfismideks bijektiivsed kujutused.

Näide 11.21 Kategooriates Gr, Ab ja Rng on isomorfismideks bijektiivsed homomorfismid.

Näide 11.22 Kategoorias $\mathsf{Vec}_{\mathbb{R}}$ on isomorfismideks bijektiivsed lineaarkujutused.

Näide 11.23 Iga rühma võib vaadelda kui üheobjektilist kategooriat, kus kõik morfismid on isomorfismid.

Näide 11.24 Meenutame, et iga järjestatud hulka võib vaadelda kategooriana (vaata näidet 11.5). Sellises kategoorias on iga morfism bimorfism, sest mistahes kahe objekti vahel leidub ülimalt üks morfism. Isomorfismid on aga ainult ühikmorfismid.

11.3 Objektide liigid

Nii nagu kategooriates saab vaadelda eri tüüpi morfisme, on võimalik uurida ka erinevate omadustega objekte.

Definitsioon 11.25 Kategooria $\mathcal{C}$ objekti $\mathbf{1}$ nimetatakse **lõppobjektiks**, kui $\mathcal{C}$ igast objektist C leidub täpselt üks morfism objekti $\mathbf{1}$. Kategooria $\mathcal{C}$ objekt $\mathbf{0}$ on **algobjekt**, kui objektist $\mathbf{0}$ leidub täpselt üks morfism $\mathcal{C}$ igasse objekti. Objekt on **nullobjekt**, kui ta on korraga nii lõpp- kui algobjekt.

Lause 11.26 *Kategooria mistahes kaks lõpp-(alg-, null-)objekti on isomorfsed.*

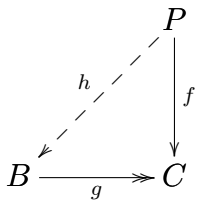
TÕESTUS. Kui $C, C' \in \mathcal{C}_0$ on lõppobjektid, siis $\mathcal{C}(C,C) = \{1_C\}$ ja $\mathcal{C}(C',C') = \{1_{C'}\}$. Samuti leiduvad morfismid $f : C \to C'$ ja $g : C' \to C$. Kuna $gf : C \to C$, siis $gf = 1_C$ ja samamoodi $fg = 1_{C'}$. Seega $C \cong C'$. Alg- ja nullobjektide jaoks on tõestus analoogiline. □

Näide 11.27 Kategoorias Set on tühi hulk algobjekt ja üheelemendilised hulgad on lõppobjektid. Sama kehtib kategooria Top korral.

Näide 11.28 Kategooriates Ab, $\mathsf{Vec}_{\mathbb{R}}$ ja Ban_1 on $\{0\}$ nii alg- kui ka lõppobjekt, seega nullobjekt.

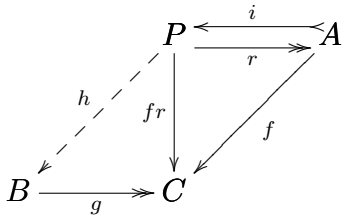
Näide 11.29 Ühikuga assotsiatiivsete ringide kategoorias Ring on $\{0\}$ lõppobjekt ja $\mathbb{Z}$ algobjekt.

Definitsioon 11.30 Kategooria $\mathcal{C}$ objekti P nimetatakse **projektiivseks**, kui iga epimorfismi $g : B \to C$ ja iga morfismi $f : P \to C$ jaoks leidub selline morfism $h : P \to B$, et $gh = f$.



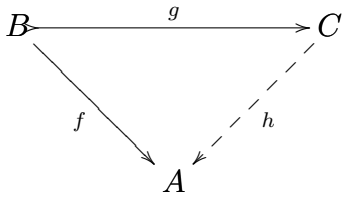
Lause 11.31 *Projektiivse objekti retrakt on projektiivne.*

Tõestus. Järgmises diagrammis olgu P projektiivne ja olgu A tema retrakt, s.t. $ri = 1_A$ mingite $r : P \to A$ ja $i : A \to P$ korral (vt. definitsiooni 11.9).



Kui $f : A \to C$, siis P projektiivsuse tõttu leidub selline $h : P \to B$, et $gh = fr$. Seega $ghi = fri = f1_A = f$. □

Definitsioon 11.32 Kategooria $\mathcal{C}$ objekti A nimetatakse **injektiivseks**, kui iga monomorfismi $g : B \to C$ ja iga morfismi $f : B \to A$ korral leidub selline morfism $h : C \to A$, et $hg = f$.



Näide 11.33 Kategooria Set iga objekt on projektiivne. Kasutades fakti, et iga epimorfism on retraktsioon kategoorias Set ja definitsiooni 11.30 tähistusi saame leida sellise $p : C \to B$, et $gp = 1_C$. Võttes $h := pf$ saame, et $gh = gpf = f$.

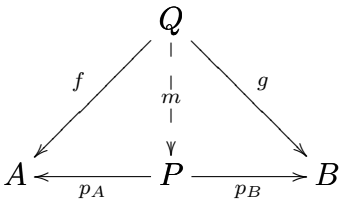
Näide 11.34 Abeli rühm on injektiivne parajasti siis, kui ta on jaguv (vt. lauset 5.23).

Näide 11.35 Projektiivsed ja injektiivsed objektid mängivad tähtsat rolli moodulite teoorias (üle ringi). Saab näidata, et moodul projektiivne parajasti siis, kui ta on vaba mooduli otseliidetav (vt. teoreemi 5.19).

11.4 Korrutised ja kokorrutised

Hulkade otsekorrutise projektsioonide omadustest on motiveeritud järgmine üldine definitsioon.

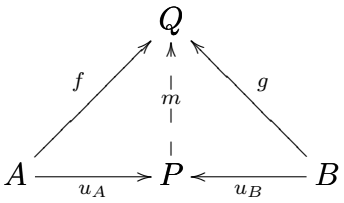
Definitsioon 11.36 Kategooria $\mathcal{C}$ objektide A, B **korrutis** on kolmik (P, p_A, p_B), kus $P \in \mathcal{C}_0$ ja $p_A : P \to A$, $p_B : P \to B$ on morfismid kategoorias $\mathcal{C}$ (mida nimetatakse **projektsioonideks**), mis rahuldavad tingimust, et kui $Q \in \mathcal{C}_0$ on objekt ja $f : Q \to A$, $g : Q \to B$ on morfismid, siis leidub üheselt määratud morfism $m : Q \to P$ nii, et järgmine diagramm kommuteerub:



Harilikult kirjutatakse P asemel $A \times B$. Üheselt määratud m leidumise omadust kutsutakse tihti korrutiste **universaalomaduseks**.

Korrutise definitsiooni dualiseerimisel saadakse kokorrutise mõiste, mis üldistab hulkade lõikumatu ühendi konstruktsiooni.

Definitsioon 11.37 Kategooria $\mathcal{C}$ objektide A ja B **kokorrutis** (ehk **summa**) on järjestatud kolmik (P, u_A, u_B), kus $P \in \mathcal{C}_0$ ja $u_A : A \to P$, $u_B : B \to P$ on kategooria $\mathcal{C}$ morfismid (mida nimetatakse **sisestusteks**), mis rahuldavad tingimust, et kui $Q \in \mathcal{C}_0$ on mistahes objekt ja $f : A \to Q$, $g : B \to Q$ on morfismid, siis leidub üheselt määratud morfism $m : P \to Q$ nii, et järgmine diagramm kommuteerub:



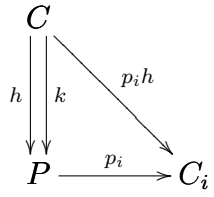
Harilikult kirjutatakse P asemel $A \coprod B$.

Korrutiste ja kokorrutiste definitsiooni võib üldistada mistahes arvu objektide jaoks. Harilikult kirjutatakse P asemel siis vastavalt $\prod_{i \in I} C_i$ ja $\coprod_{i \in I} C_i$.

Tõestame korrutiste mõned omadused.

Lause 11.38 *Kui $(P, (p_i)_{i \in I})$ on kategooria $\mathcal{C}$ objektide süsteemi $(C_i)_{i \in I}$ korrutis ja $h, k : C \to P$ on sellised morfismid, et iga $i \in I$ korral $p_i h = p_i k$, siis $h = k$.*

Tõestus. Nii h kui ka k muudavad kõik kolmnurgad

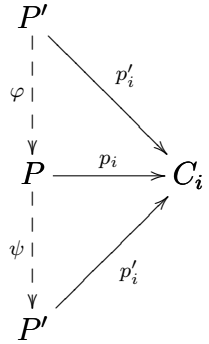


kommutatiivseks, seega peavad nad korrutise universaalomaduse põhjal võrdsed olema. □

Lause 11.38 väidet võib sõnastada ka nii, et korrutise projektsioonid on korraga vasakult taandatavad.

Lause 11.39 *Kui $(P,(p_i)_{i\in I})$ ja $(P',(p'_i)_{i\in I})$ on kategooria $\mathcal{C}$ objektide süsteemi $(C_i)_{i\in I}$ korrutised, siis P ja P' on isomorfsed.*

TÕESTUS. Kuna P ja P' on objektide C_i, $i \in I$, korrutised siis leiduvad morfismid φ ja ψ, mis muudavad nii ülemise kui alumise kolmnurga diagrammis



kommutatiivseks iga $i \in I$ korral. Sellest, et

$$p'_i 1_{P'} = p'_i = p_i\varphi = p'_i\psi\varphi,$$
$$p_i 1_P = p_i = p'_i\psi = p_i\varphi\psi,$$

iga $i \in I$ korral, järeldub lause 11.38 põhjal, et $\psi\varphi = 1_{P'}$ ja $\varphi\psi = 1_P$. Seega $P \cong P'$. □

Öeldakse, et kategoorias $\mathcal{C}$ **on (ko)korrutised**, kui igal $\mathcal{C}$ objektide süsteemil $(C_i)_{i\in I}$ on olemas (ko)korrutis. Kategoorias $\mathcal{C}$ **on lõplikud (ko)korrutised**, kui igal lõplikul objektide süsteemil on olemas (ko)korrutis.

On lihtne näha, et tühja objektide süsteemi korrutis on lõppobjekt ja $(A, 1_A)$ on ühestainsast objektist A koosneva süsteemi korrutis.

Lause 11.40 *Kategoorias on lõplikud korrutised parajasti siis, kui temas on binaarsed korrutised ja lõppobjekt.*

Toome mõned korrutiste näited.

Näide 11.41 Kategoorias Set on süsteemi $(C_i)_{i\in I}$ korrutiseks otsekorrutis

$$\prod_{i\in I} C_i = \{(x_i)_{i\in I} \mid x_i \in C_i\}$$

koos projektsioonidega $p_k\left((x_i)_{i\in I}\right) = x_k$, $k \in I$.

Näide 11.42 Algebraliste struktuuride kategooriates (nt. rühmad, Abeli rühmad, ringid, moodulid, vektorruumid, võred jne.) on objektide süsteemi korrutis nende otsekorrutis, mis on varustatud komponenthaavaliste tehetega.

Näide 11.43 Kui me vaatleme järjestatud hulka $(P, \leqslant)$ kategooriana (vt. näidet 11.5), siis korrutised (kui nad leiduvad) on täpselt alumised rajad.

Vaatleme kokorrutiste näiteid.

Näide 11.44 Kategoorias Set on süsteemi $(C_i)_{i\in I}$ kokorrutis sinna kuuluvate hulkade lõikumatu ühend. Selle lõikumatu ühendi võib konstrueerida kui hulga

$$\bigsqcup_{i\in I} C_i := \bigcup_{i\in I}(C_i \times \{i\}) = \{(x,i) \mid i \in I,\ x \in C_i\}.$$

Sisestused $u_i : C_i \to \bigsqcup_{i\in I} C_i$ on defineeritud võrdusega $u_i(x) := (x,i)$, $x \in C_i$.

Näide 11.45 Kategoorias Ab on süsteemi $(A_i)_{i\in I}$ kokorrutiseks Abeli rühmade otsesumma

$$\coprod_{i\in I} A_i := \{(x_i)_{i\in I} \mid x_i \in A_i,\ \text{ hulk } \{i \in I \mid x_i \neq 0\} \text{ on lõplik } \} \leqslant \prod_{i\in I} A_i,$$

kus liitmine on defineeritud komponenthaaval. Sisestused $u_k : A_k \to \coprod_{i\in I} A_i$ on defineeritud võrdusega $u_k(x) := (x_i)_{i\in I}$, kus $x_k = x$ ja kõik teised komponendid on nullid. Kui B on teine Abeli rühm ja $q_i : A_i \to B$, $i \in I$, on rühmade homomorfismide süsteem, siis üheselt määratud kujutused $m : \coprod_{i\in I} A_i \to B$ on defineeritud võrdusega $m((x_i)_{i\in I}) := \sum_{i\in I} q_i(x_i)$, kus viimases summas on lõpliku arv nullist erinevaid liidetavaid ja me summeerime neid.

Näide 11.46 Kui vaatleme järjestatud hulka $(P, \leqslant)$ kategooriana (vt. näidet 11.5), siis kokorrutised (kui nad leiduvad) on ülemised rajad.

Korrutise konstruktsioon on erijuhuks ühest üldisemast kategoorsest konstruktsioonist, mida kutsutakse piiri leidmiseks. On ka teisi loomulikke piiride näiteid, nagu võrdsustajad, tagasitõmbajad ja muud, aga neid me siin kursuses ei käsitle. Piiridega duaalsed on kopiirid.

Nii kategooriateooria kui universaalalgebra on üldised teooriad, mis võimaldavad meil vaadelda suuri algebraliste struktuuride kogumeid tervikuna. Näiteks võime vaadelda nii kõigi rühmade kategooriat kui ka muutkonda. Kui universaalalgebra vaatepunktist huvitab meid tihti algebralise struktuuri siseehitus (millised on tema alamalgebrad ja kongruentsid, milliseid samasusi tema elemendid rahuldavad), siis kategooriateoorias objekti sisse ei vaadata, oluline on see, kuidas käituvad objektidevahelised morfismid, muuhulgas on väga oluline roll kommutatiivsetel diagrammidel. Ükskõik milliste konkreetsete algebraliste struktuuride uurimisel on kasulik mõlemast üldisest teooriast üht-teist teada. Kategooriateooria põhimõistete tundmine tuleb kasuks ka kõigile neile, kes tegelevad funktsionaalanalüüsi, topoloogia või diferentsiaalgeomeetriaga.

Väike eesti-inglise algebrasõnastik

Abeli rühm — *abelian group*
ahel — *chain*
alamalgebra — *subalgebra*
alampolügoon — *subact*
alamruum — *subspace*
algebra — *algebra*
algebraline struktuur — *algebraic structure*
algebraline tehe — *algebraic operaion*
algobjekt — *initial object*
alumine raja — *meet*
automorfism — *automorphism*
baas — *basis*
bimorfism — *bimorphism*
distributiivne võre — *distributive lattice*
distributiivsus — *distributivity*
duaalne kategooria — *opposite category*
endomorfism — *endomorphism*
epimorfism — *epimorphism*
epimorfne kujutis — *epimorphic image*
faktorhulk — *quotient set*
faktoriseeruv — *factorisable*
faktorrühm — *quotient group, factor group*
Greeni seosed — *Green's relations*
homomorfism — *homomorphism*
homomorfismiteoreem — *homomorphism theorem*
ideaal — *ideal*
idempotent — *idempotent*
injektiivne — *injective*
isomorfism — *isomorphism*
isomorfismiteoreem — *isomorphism theorem*
jada — *sequence*
jagamisega ring — *division ring*
jagatis — *quotient*
jaguv — *divisible*
juur — *root*
järjend — *tuple*
järk — *order*
kategooria — *category*
kokorrutis — *coproduct*
kommutatiivne diagramm — *commutative diagram*
kongruents — *congruence*
kordaja — *coefficient*

koretratktsioon — *coretraction*
korpus — *field*
korrutis — *product*
kujutis — *image*
kõrvalklass — *coset*
lahutumatu — *indecomposable*
lahutuskorpus — *splitting field*
lihtne — *simple*
lineaarkombinatsioon — *linear combination*
lineaarkujutus — *linear mapping*
lineaarselt järjestatud hulk — *linearly ordered set*
lineaarselt sõltumatu — *linearly independent*
lineaarselt sõltuv — *linearly dependent*
lineaarteisendus — *linear transformation*
loomulik projektsioon — *natural projection*
lõplik korpus — *finite field*
lõppobjekt — *terminal object*
lühike täpne jada — *short exact sequence*
maksimaalne element — *maximal element*
minimaalne ideaal — *minimal ideal*
modulaarne võre — *modular lattice*
monoid — *monoid*
monomorfism — *monomorphism*
moodul — *module*
morfism — *morphism*
muutkond — *variety*
n-kohaline tehe — *n-ary operation*
normaaljagaja — *normal subgroup*
nullelement — *zero element*
nullobjekt — *zero object*
nullvektor — *null vector*
objekt — *object*
osaliselt järjestatud hulk — *partially ordered set, poset*
otseaste — *direct power*
otsekorrutis — *direct product*
otsesumma — *direct sum*
peaideaal — *principal ideal*
pere — *family*
perioodiline osa — *torsion subgroup*
perioodiline rühm — *periodic group*
permutatsioon — *permutation*
polügoon — *act*
poolrühm — *semigroup*
primitiivne idempotent — *primitive idempotent*
projektiivne — *projective*

pärisideaal — *proper ideal*
pöördelement — *inverse element*
püsipunkt — *fixed point*
Reesi maatrikspoolrühm — *Rees matrix semigroup*
retraktsioon — *retraction*
ring — *ring*
rühm — *group*
samasus — *identity*
signatuur — *signature*
sisemine otsesumma — *internal direct sum*
skalaar — *scalar*
substitutsioon — *permutation*
sõltumatud tsüklid — *independent cycles*
tehe — *operation*
term — *term*
termfunktsioon — *term function*
termide algebra — *term algebra*
toime — *action*
transpositsioon — *transposition*
tsükkel — *cycle*
tuum — *kernel*
tõke — *bound*
täielik alamkategooria — *full subcategory*
täielikult lihtne poolrühm — *completely simple semigroup*
täielik võre — *complete lattice*
täpne — *exact*
täpne jada — *exact sequence*
tüüp — *type*
universaalalgebra — *universal algebra*
vaba — *free*
vastandelement — *additive inverse*
vektor — *vector*
vektorruum — *vector space, linear space*
võre — *lattice*
väline otsesumma — *(external) direct sum*
väändeta Abeli rühm — *torsion-free abelian grouo*
ühikelement — *identity element*
ühiksubstitutsioon — *identity permutation*
ülemine raja — *join*
ülemine tõke — *upper bound*

Kasutatud kirjandus

1. M. Kilp, Algebra I, Eesti Matemaatika Selts, Tartu, 2005.
2. M. Kilp, Algebra II, Tartu, 1998.
3. K. Kaarli, Sissejuhatus universaalalgebrasse, Tartu, 1989.