Sissejuhatus algebra struktuuridesse

Kevad 2018

Lektor: Lauri Tart

Konspekt: Valdis Laan

Sisukord

Eessõna **2**

1 Vektorruum **7**
1.1 Algebraline tehe . . . 7
1.2 Alamstruktuurid . . . 9
1.3 Homomorfismid . . . 10
1.4 Isomorfismid . . . 12
1.5 Faktorstruktuurid . . . 13
1.6 Homomorfismiteoreem . . . 17
1.7 Baasi olemasolu . . . 18
1.8 Otsekorrutised ja otsesummad . . . 20

2 Rühm **23**
2.1 Rühm, alamrühm . . . 23
2.2 Normaaljagaja, faktorrühm . . . 25
2.3 Isomorfismiteoreemid . . . 26
2.4 Lihtsad rühmad . . . 29

3 Abeli rühm **33**
3.1 Põhimõisted . . . 33
3.2 Jaguvate Abeli rühmade lihtsamad omadused . . . 34
3.3 Elementide järkudest . . . 37
3.4 Väändeta jaguvad rühmad . . . 38
3.5 Jaguvad p-rühmad . . . 40
3.6 Jaguvate Abeli rühmade kirjeldus . . . 43

4 Ringid **45**
4.1 Põhimõisted . . . 45
4.2 Lihtsad minimaalset parempoolset ideaali sisaldavad ringid . . . 47

5 Moodulid **53**
5.1 Mooduli definitsioon . . . 53
5.2 Täpsed jadad . . . 54
5.3 Projektiivsed moodulid . . . 56
5.4 Injektiivsed moodulid . . . 57

6 Poolrühmad **59**
6.1 Põhidefinitsioonid 59
6.2 Lihtsad poolrühmad 60
6.3 Greeni seosed 61
6.4 Täiesti lihtsad poolrühmad ja minimaalsed ühepoolsed ideaalid 62
6.5 Reesi maatrikspoolrühmad 67

7 Polügoonid **69**
7.1 Põhimõisted 69
7.2 Vabad polügoonid 71
7.3 Projektiivsed polügoonid 72

8 Võred **77**
8.1 Kaks vaatenurka võredele 77
8.2 Täielikud võred 79
8.3 Modulaarsed võred 79
8.4 Distributiivsed võred 81

9 Universaalalgberad ja nende muutkonnad **83**
9.1 Universaalalgberad 83
9.2 Muutkonnad 85

10 Kategooriad **91**
10.1 Kategooria mõiste 91
10.1.1 Objektid ja morfismid 91
10.1.2 Alam- ja korrutiskategooriad 93
10.2 Morfismide liigid. 94
10.3 Objektide liigid. Duaalsus 96
10.3.1 Objektide liigid 96
10.3.2 Duaalsus 97
10.4 Korrutised ja kokorrutised 98

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.

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

Loengukonspekt tugineb peamiselt raamatutele [2] ja [1].

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).

Illustreerime neid mõisteid vektorruumi näite varal. Tuletame meelde, kuidas harilikult defineeritakse vektorruum üle korpuse K. (Kes ei ole kuulnud, mis on korpus, võib järgnevas võtta K ossa reaalarvude hulga $\mathbb{R}$. Selles kursuses eeldame, et korpuse korrutamine on kommutatiivne.)

Definitsioon 1.3 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).

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 põhitehteks) 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.

Lause 1.4 *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.*

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 1.5 Algebralise struktuuri A alamhulka A' nimetatakse selle struktuuri **alamstruktuuriks**, kui A' on kinnine kõigi struktuuril A defineeritud tehete suhtes. See tähendab, et

1. $\omega(a_1, a_2, \ldots, a_n) \in A'$ mistahes $n \in \mathbb{N}$, struktuuril A defineeritud n-kohalise algebralise tehte ω ja elementide $a_1, a_2, \ldots, a_n \in A'$ korral,

2. $0_\omega^A \in A'$ iga nullkohalise algebralise tehte ω korral.

Vaatame jälle vektorruumide näidet.

Lause 1.6 *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 1.5 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 1.4(4) tõttu $0 = 0a \in V'$. Kui $a \in V'$, siis lause 1.4 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 1.7 *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 1.8 Öeldakse, et algebralised struktuurid A ja B on **sama tüüpi**, kui iga $n \in \mathbb{N} \cup \{0\}$ korral on neil sama palju n-kohalisi tehteid.

Näiteks kõik vektorruumid üle sama korpuse on sama tüüpi.

Sama tüüpi algebraliste struktuuride puhul saab korraldada üksühese vastavuse neil defineeritud tehete vahel. Tihti tähistatakse üksteisele vastavaid tehteid sama märgiga, kuigi kujutustena võivad need tehted olla väga erinevad. Ka meie kasutame järgmises defintsioonis vastavuses olevate tehete tähistamiseks sama sümbolit.

Näide 1.9 Vaatleme näiteks $(m \times n)$-maatriksite vektoruumi $\mathrm{Mat}_{m,n}(\mathbb{R})$ üle korpuse $\mathbb{R}$ ja kolmemõõtmelise ruumi vabavektorite hulka $\mathbb{E}_3$, mis on samuti vektorruum üle korpuse $\mathbb{R}$. Need on sama tüüpi algebralised struktuurid, kus mõlemas on olemas üks kahekohaline tehe (liitmine), mida tähistatakse sümboliga $+$. Samas kujutused

$$+ : \mathrm{Mat}_{mn}(\mathbb{R}) \times \mathrm{Mat}_{mn}(\mathbb{R}) \to \mathrm{Mat}_{mn}(\mathbb{R}) \quad \text{ja} \quad + : \mathbb{E}_3 \times \mathbb{E}_3 \to \mathbb{E}_3$$

on täiesti erinevad.

Märgime veel, et vektorruumid $\mathrm{Mat}_{m,n}(\mathbb{R})$ ja $\mathrm{Mat}_{m,n}(\mathbb{Z}_5)$ ($\mathbb{Z}_5$ on jäägiklassikorpus mooduli 5 järgi) ei ole sama tüüpi, sest neist esimesel on lõpmata palju ühekohalisi tehteid, aga teisel on ainult 6 ühekohalist tehet.

Definitsioon 1.10 Olgu A ja B sama tüüpi algebralised struktuurid. Kujutust $f : A \to B$ nimetatakse **homomorfismiks**, kui f säilitab kõik nendel struktuuridel defineeritud tehted. See tähendab, et

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

$$f(\omega(a)) = \omega(f(a))$$

iga $a \in A$ korral.

Definitsioon 1.11 Homomorfismi algebralisest struktuurist A algebralisse struktuuri A nimetatakse struktuuri A **endomorfismiks**.

Kõigi homomorfismide hulka struktuurist A struktuuri B tähistatakse sümboliga $\mathrm{Hom}(A, B)$. Algebralise struktuuri A kõigi endomorfismide hulka tähistatakse sümboliga $\mathrm{End}(A)$.

Lause 1.12 *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 liitmise);*

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

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

Definitsiooni 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 1.13 Vektorruumide homomorfisme nimetatakse **lineaarkujutusteks** ja vektoruumide endomorfisme nimetatakse **lineaarteisendusteks**.

Meenutame nüüd hulgateooriast kujutise mõistet.

Definitsioon 1.14 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 1.15 *Kui $f : A \to B$ on homomorfism sama tüüpi algebraliste struktuuride vahel, siis* $\operatorname{Im} f$ *on struktuuri B alamstruktuur.*

TÕESTUS. Kontrollime alamstruktuuri definitsiooni tingimusi.
1. Olgu ω n-kohaline tehe 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

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

kust näeme, et $\omega(b_1, \ldots, b_n) \in \operatorname{Im} f$.
2. Kui ω on nullkohaline tehe, 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 1.16 *Sama tüüpi algebraliste struktuuride homomorfismide korrutis on homomorfism.*

TÕESTUS. Olgu $f : A \to B$ ja $g : B \to C$ homomorfismid sama tüüpi algebraliste struktuuride vahel. Näitame, et $gf : A \to C$ on homomorfism.
1. Olgu ω n-kohaline tehe ($n \in \mathbb{N}$) ja $a_1, \ldots, a_n \in A$. Siis

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

2. Kui ω on nullkohaline tehe, siis

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

□

Lause 1.17 *Algebralise struktuuri A endomorfismide hulk* $\operatorname{End}(A)$ *on monoid kujutuste korrutamise suhtes.*

TÕESTUS. Lause 1.16 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 1.18 Olgu A ja B sama tüüpi algebralised struktuurid. Kujutust $f : A \to B$ nimetatakse **isomorfismiks** struktuurist A struktuuri B, kui f on bijektiivne homomorfism. Struktuure A ja B nimetatakse **isomorfseteks**, kui leidub isomorfism $f : A \to B$. Sellisel juhul kirjutatakse $A \cong B$.

Definitsioon 1.19 Isomorfismi algebralisest struktuurist samasse algebralisse struktuuri nimetatakse **automorfismiks**. Struktuuri A kõigi automorfismide hulka tähistatakse sümboliga $\mathrm{Aut}(A)$.

Näide 1.20 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 algebralistel struktuuridel on samasugused algebralised omadused. Näiteks kui A ja B on isomorfsed struktuurid, millel on üks kahekohaline tehe ja struktuuril A on see tehe kommutatiivne, siis ka struktuuril B on see tehe kommutatiivne. Või kui A ja B on isomorfsed struktuurid ja struktuuril A on kolmteist alamstruktuuri, siis ka struktuuril B on kolmteist alamstruktuuri.

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

Lause 1.21 *Isomorfismide korrutis on isomorfism.*

Tõestus. Hulgateooriast teame, et bijektiivsete kujutuste korrutis on bijektiivne. Lause 1.16 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 1.22 *Isomorfismi pöördkujutus on isomorfism.*

Tõestus. Olgu A ja B sama tüüpi algebralised struktuurid ja olgu $f : A \to B$ 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 f^{-1} on bijektiivne. Seega jääb veel näidata, et f^{-1} on kooskõlas tehetega.
1. Olgu ω n-kohaline tehe ($n \in \mathbb{N}$) 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

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

2. Kui ω on nullkohaline tehe, siis

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

□

Lause 1.23 *Algebralise struktuuri A automorfismide hulk* $\mathrm{Aut}(A)$ *on rühm kujutuste korrutamise suhtes.*

TÕESTUS. Lause 1.21 põhjal on tegu algebralise tehtega. Mistahes kujutuste korrutamine on assotsiatiivne, samasusteisendus 1_A on ilmselt automorfism ja lause 1.22 tõttu leidub igal automorfismil pöördelement hulgas $\mathrm{Aut}(A)$, nimelt selle pöördkujutus. □

Sama tüüpi algebraliste struktuuride klassil võib vaadelda isomorfismiseost $\cong$. Osutub, et sellel seosel on ekvivalentsiseoselt nõutavad omadused.

Lause 1.24 *Olgu A, B ja C sama tüüpi algebralised struktuurid. 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 1.22 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 1.21 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?

1.5 Faktorstruktuurid

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

Definitsioon 1.25 Algebralise struktuuri A **kongruents** on selline ekvivalentsiseos ρ hulgal A, mis on kooskõlas tehetega. See tähendab, et

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

mistahes $n \in \mathbb{N}$, n-kohalise tehte ω ja elementide $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in A$ korral.

Kooskõla kahekohalise tehtega $*$ tähendab seda, et

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

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

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

Lause 1.26 *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 1.6 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 algebralisel struktuuril A. Vaatleme faktorhulka

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

Iga struktuuril A defineeritud n-kohalise tehte ω jaoks defineerime ka hulgal A/ρ vastava tehte võrdusega

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

Kongruentsi kooskõla tehtega ω 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 faktorstruktuuri A/ρ, mis on esialgse struktuuriga 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 1.26 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 1.27 *Kui V' on vektorruumi V (üle korpuse K) alamruum, siis V/V' on ka vektorruum üle korpuse K eelpool defineeritud tehete suhtes.*

Tõestus. Nagu juba öeldud, need 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 1.28 *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

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

□

Lauses 1.28 defineeritud kujutust π nimetatakse vektoruumi V **loomulikuks projektsiooniks** faktorruumile V/V'.

Näide 1.29 Vaatleme vektorruumi $V := \mathbb{R}^2$ üle $\mathbb{R}$ ja selle alamruumi $V' := \{(z, 0) \mid z \in \mathbb{R}\}$. Faktorruumi V/V' saab kirjeldada kahel viisil. Kui lähtuda alamruumist V', siis

$$V/V' = \{a+V' \mid a \in V\} = \{(x,y)+\{(z,0) \mid z \in \mathbb{R}\} \mid (x,y) \in \mathbb{R}^2\} = \{\{(x+z,y) \mid z \in \mathbb{R}\} \mid (x,y) \in \mathbb{R}^2\}.$$

Kuna $\{x + z \mid z \in \mathbb{R}\} = \mathbb{R}$ sõltumata punkti x valikust, siis võime teha asenduse $z' = x + z$:

$$V/V' = \{\{(z', y) \mid z' \in \mathbb{R}\} \mid y \in \mathbb{R}\}.$$

Seega faktorruum V/V' koosneb x-teljega paralleelsetest tasanditest, millest üks on muuseas V'. Teisalt, kasutades lauses 1.26 antud seost, võime lähtuda kongruentsist

$$\begin{aligned} \rho &= \{(a,b) \in V \times V \mid a - b \in V'\} = \{((x_1,y_1),(x_2,y_2)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid y_1 - y_2 = 0\} \\ &= \{((x_1,y),(x_2,y)) \in \mathbb{R}^2 \times \mathbb{R}^2\}. \end{aligned}$$

Faktorhulk osutub täpselt samaks, mis varem:

$$V/\rho = \{\overline{a} \mid a \in V\} = \{\{(x', y') \in \mathbb{R}^2 \mid y' = y\} \mid (x,y) \in \mathbb{R}^2\} = \{\{(x', y) \mid x' \in \mathbb{R}\} \mid y \in \mathbb{R}\}.$$

Ükskõik, kummal viisil kirjeldatud hulgal V/V' on defineeritud tehted

$$\{(x_1, y_1) \mid x_1 \in \mathbb{R}\} + \{(x_1, y_2) \mid x_2 \in \mathbb{R}\} = \{(x, y_1 + y_2) \mid x \in \mathbb{R}\},$$

$$k \cdot \{(x,y) \mid x \in \mathbb{R}\} = \{(x', ky) \mid x' \in \mathbb{R}\},$$

$$-\{(x,y) \mid x \in \mathbb{R}\} = \{(x', -y) \mid x' \in \mathbb{R}\}$$

ja

$$0^{V/V'} = V',$$

mille suhtes V/V' osutub tänu lausele 1.27 ka ise vektorruumiks.

1.6 Homomorfismiteoreem

Definitsioon 1.30 Olgu V ja U vektorruumid üle korpuse K. Lineaarkujutuse $f : V \to U$ **tuum** Ker f defineeritakse järgmiselt:

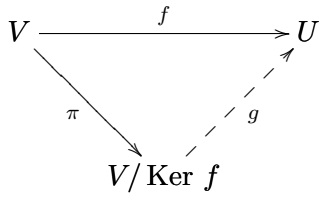
$$\text{Ker } f = \{a \in V \mid f(a) = 0\}.$$

Lihtne on veenduda, et kehtivad järgmised tulemused tuumade kohta.

Lause 1.31 *Kui $f : V \to U$ on lineaarkujutus, siis* Ker f *on vektorruumi V alamruum.*

Lause 1.32 *Lineaarkujutus $f : V \to U$ on üksühene parajasti siis, kui* Ker $f = \{0\}$.

Teoreem 1.33 (Homomorfismiteoreem) *Olgu $f : V \to U$ lineaarkujutus. Siis leidub üksühene lineaarkujutus $g : V/\text{Ker } f \to U$ nii, et $f = g\pi$, kus $\pi : V \to V/\text{Ker } f$ on loomulik projektsioon.*



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

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

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 $g\pi = f$. □

Nagu näeme, ütleb Homomorfismiteoreem seda, et iga lineaarkujutuse saab esitada injektiivse lineaarkujutuse ja sürjektiivse lineaarkujutuse korrutisena.

Järeldus 1.34 *Kui lineaarkujutus $f : V \to U$ on sürjektiivne, siis $V/\text{Ker } f \cong U$.*

Tõestus. Näitame, et lineaarkujutus $g : V/\text{Ker } f \to U$ 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 1.35 *Kui mittetriviaalses vektoruumis leidub 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 1.36 Osaliselt järjestatud hulk on hulk, millel on antud osalise järjestuse seos, s.t. binaarne seos, mis on refleksiivne, antisümmeetriline ja transitiivne.

Definitsioon 1.37 Ahel ehk **lineaarselt järjestatud hulk** on selline osaliselt järjestatud hulk $(P, \leqslant)$, kus $a \leqslant b$ või $b \leqslant a$ iga $a, b \in P$ korral (s.t. mistahes kaks elementi on võrreldavad).

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

Näide 1.38 Hulk $\mathbb{Q}$ on ahel osaliselt järjestatud hulgas $(\mathbb{R}, \leqslant)$. Samuti hulk, mis koosneb elementidest $-5 \leqslant -1 \leqslant 2 \leqslant 13$.

Definitsioon 1.39 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 1.40 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 1.41 (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 1.42 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 ja kasutame vastavat sümboolikat.

Definitsioon 1.43 Vektorruumi V (üle korpuse K) vektorite hulka $\{a_1, a_2, \ldots, a_s\}$, $s \in \mathbb{N}$, nimetatakse **lineaarselt sõltumatuks**, kui mistahes $k_1, k_2, \ldots, k_s \in K$ korral võrdusest

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

järeldub, et

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

Lõpmatut vektorite hulka nimetatakse **lineaarselt sõltumatuks**, kui tema iga lõplik mittetühi alamhulk on lineaarselt sõltumatu.

Definitsioon 1.44 Vektorite süsteemi nimetatakse **lineaarselt sõltuvaks**, kui ta ei ole lineaarselt sõltumatu

Lause 1.45 *Ühestainsast vektorist a koosnev hulk on lineaarselt sõltumatu parajasti siis, kui $a \neq 0$.*

Lause 1.46 *Lineaarselt sõltumatu vektorite hulga iga alamhulk on ka lineaarselt sõltumatu.*

Lause 1.47 *Nullist erinevate vektorite lõplik hulk, mis sisaldab vähemalt kaks vektorit, on lineaarselt sõltuv parajasti siis, kui selle hulga vektorite mistahes järjestuse korral leidub vektor, mis avaldub eelnevate vektorite lineaarkombinatsioonina.*

Definitsioon 1.48 Vektorruumi V vektorite hulka B nimetatakse **baasiks**, kui

1. hulk B on lineaarselt sõltumatu,
2. vektoruumi V iga vektor avaldub hulka B kuuluvate vektorite lineaarkombinatsioonina.

Teoreem 1.49 *Igas mittetriviaalses vektorruumis leidub baas.*

Tõestus. Olgu $V \neq \{0\}$ vektorruum üle korpuse K. 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 suhtes. Olgu $a \in V \setminus \{0\}$. Siis lause 1.45 tõttu on hulk $\{a\}$ lineaarselt sõltumatu. Seega $\{a\} \in P$ ja $P \neq \emptyset$.

Olgu nüüd $\{A_\alpha \mid \alpha \in I\}$ mingi ahel hulgas P. 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}, kõik ülejäänud hulgad ning seega ka $a_1, \ldots, a_s \in A_{\alpha_k}$. Kuna $A_{\alpha_k} \in P$, siis on ta lineaarselt sõltumatu ja seega ka alamhulk $\{a_1, \ldots, a_s\}$ on lineaarselt sõltumatu tänu lausele 1.46. Sellega on näidatud, et A on lineaarselt sõltumatu, ning järelikult $A \in P$. Et $A_\alpha \subseteq A$ iga $\alpha \in I$ korral, siis A on ahela $\{A_\alpha \mid \alpha \in I\}$ ülemine tõke hulgas P. Sellega oleme näidanud, et Zorni lemma eeldus 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 iga V vektor avaldub B elementide lineaarkombinatsioonina. Olgu $a \in V$ suvaline vektor. 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 $B \cup \{a\}$ on 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 süsteemi S vektorid nii, et a on viimane. Siis lause 1.47 põhjal avaldub mingi süsteemi 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 näidata. □

1.8 Otsekorrutised ja otsesummad

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). 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 $I = \mathbb{N}$, 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 $\prod_{i=1}^{n} X_i$.

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.

Olgu X_i, $i \in I$ sama tüüpi algebralised struktuurid. Defineerime hulkade otsekorrutisel $X := \prod_{i\in I} X_i$ tehted n.ö. komponenthaaval:

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

kui ω on n-kohaline tehe ($n \in \mathbb{N}$) ja

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

kui ω on null-kohaline tehe. Nii saame sama tüüpi algebralise struktuuri nagu olid esialgsed struktuurid.

Lause 1.50 *Vektorruumide otsekorrutis on vektorruum.*

Tõestus. Olgu V_i, $i \in I$ vektorruumid üle sama kmorpuse 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 1.7 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 $V_1 \oplus V_2 \oplus \ldots \oplus V_n$. 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.

Teoreem 1.51 *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 1.49 põhjal leidub vektoruumis V baas. Indekseerime selle baasi vektorid ära mingi hulga I elelementidega, s.t. olgu see baas $\{e_i \mid i \in I\}$. 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.

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

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

Näitame nüüd, et f on pealekujutus. Olgu $a \in V$. Kuna $\{e_i \mid i \in I\}$ on baas, siis leidub naturaalarv n, indeksid $i_1, \ldots, i_n$ 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 1.32. 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 $\operatorname{Ker} f = \{0\}$ ning seega f on üksühene. □

Järeldus 1.52 *Kui n on naturaalarv ja V on n-mõõtmeline vektorruum üle korpuse K, siis $V \cong K^n$.*

Tõestus. See järeldub teoreemist 1.51 ja võrdusest (1.3). □

Peatükk 2

Rühm

2.1 Rühm, alamrühm

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).

Lihtne on veenduda, et kehtib järgmine tulemus.

Lause 2.2 *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 2.3 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 2.4 *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 $bH \subseteq aH$. Samuti $a^{-1} = hb^{-1}$ ehk $a = (hb^{-1})^{-1} = bh^{-1} \in bH$, millest järeldub, et $aH \subseteq bH$. Kokkuvõttes $aH = bH$.

Väidete 1 ja 3 samaväärsuse saab tõestada analoogiliselt. □

Järeldus 2.5 *Kui H on rühma G alamrühm ja $b \in G$, siis $H = bH$ parajasti siis, kui $b \in H$.*

Lause 2.6 *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 2.4 põhjal $aH = bH$. Sellega oleme näidanud, et tegemist on tükeldusega. □

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

Lause 2.7 *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 2.8 Lõpliku rühma **järguks** nimetatakse tema elementide arvu.

Teoreem 2.9 (Lagrange'i teoreem) *Lõpliku rühma iga alamrühma järk jagab rühma järku.*

TÕESTUS. Lause 2.7 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 2.10 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 2.11 *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 2.12 Iga rühma G korral on alamrühmad G ja $\{1\}$ normaalsed. Neid normaaljagajaid nimetatakse **triviaalseteks**.

Näide 2.13 Kommutatiivse rühma kõik alamrühmad on normaaljagajad.

Näide 2.14 Rühma $GL_n(\mathbb{R})$ alamrühm $SL_n(\mathbb{R})$ on normaaljagaja.

Märkus 2.15 Üldiselt ei pruugi gH ja Hg võrdsed olla. Selle kohta võib näite leida raamatust [1] (näide 6.1.8).

Analoogiliselt lausega 1.12 saab tõestada järgmise tulemuse.

Lause 2.16 *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 2.17 Olgu $f : G \to G'$ rühmade homomorfism. Hulka

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

nimetatakse homomorfismi f **tuumaks**.

Lause 2.18 *Rühmade homomorfismi tuum on normaaljagaja.*

Tõestus. Olgu $f : G \to G'$ rühmade homomorfism, $a \in \text{Ker } f$ 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. $g^{-1}ag \in \text{Ker } f$. Järelikult $\text{Ker } f \trianglelefteq G$. □

Saab näidata, et analoogiliselt vektorruumidega on rühma kongruentsid üksüheses vastavuses normaaljagajatega, kusjuures konguentsiklassideks on kõrvalklassid selle normaaljagaja järgi.

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 $\pi : G \to G/H$ on rühmade homomorfism. Seda kujutust nimetatakse **loomulikuks projektsiooniks** faktorrühmale G/H.

Analoogiliselt teoreemiga 1.33 saab näidata, et kehtib järgmine teoereem.

Teoreem 2.19 (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 2.20 *Kui $f : G \to G'$ on sürjektiivne rühmade homomorfism, siis $G' \simeq G/\operatorname{Ker} f$.*

2.3 Isomorfismiteoreemid

Kui H ja K on rühma G mingid alamhulgad siis tähistatakse

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

Isomorfismiteoreemide tõestamisel läheb meil vaja järgmisi abitulemusi.

Lemma 2.21 *Kui G on rühm, $H \leq G$ ja $K \trianglelefteq G$, siis $HK \leq G$.*

Tõestus. 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 2.22 *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 $K \trianglelefteq H$. □

Tõestame nüüd kolm klassikalist teoreemi, mis käivad isomorfismide kohta teatud faktorrühmade vahel.

Teoreem 2.23 (Esimene isomorfismiteoreem) *Olgu G rühm, $H \leq G$ ja $K \trianglelefteq G$. Siis*

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

Tõestus. Lemma 2.21 põhjal $HK \leq G$. Kuna $K \trianglelefteq G$ ja $K \subseteq HK$, siis lemma 2.22 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 $f(h) = hK = (hk)K$, mis tähendab, et f on pealekujutus. Kasutades järeldust 2.20 võime öelda, et

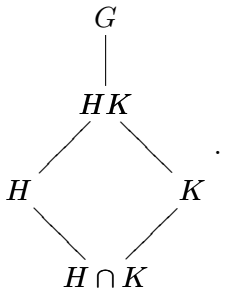
$$H/\operatorname{Ker} f \cong HK/K.$$

Tõestuse lõpetamiseks tuleb näidata, et $\operatorname{Ker} f = H \cap K$.

Tänu tuuma definitsioonile $\operatorname{Ker} f \subseteq H$. Kui $x \in \operatorname{Ker} f$, siis $f(x) = K$. Teisest küljest f definitsiooni põhjal $f(x) = xK$. Seega $xK = K$, kust $x \in K$. Järelikult $\operatorname{Ker} f \subseteq K$ ja oleme näidanud, et $\operatorname{Ker} f \subseteq H \cap K$.

Olgu nüüd $x \in H \cap K$. Siis $f(x) = xK = K$ ehk $x \in \operatorname{Ker} f$. Seega $H \cap K \subseteq \operatorname{Ker} f$ ja kokkuvõttes $H \cap K = \operatorname{Ker} f$. □

Märkus 2.24 Eelmises teoreemis esinevate alamrühmade vahelisi sisalduvusseoseid illustreerib järgmine diagramm (suuremad alamrühmad on ülevalpool):



Teoreem 2.25 (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 $hK, h'H \in H/K$. 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 $g_2^{-1}g_1 \in K \subseteq H$. Järelikult $g_1H = g_2H$, mis näitab, et f on korrektselt defineeritud. Lihtne on näha, et f on sürjektiivne homomorfism. Järelduse 2.20 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 võrdus tõestatud. □

Teoreem 2.26 (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 ($M = \pi^{-1}(N)$), 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 nüüd

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

□

Märkus 2.27 Seoseid eelmises teoreemis esinevate alamrühmade vahel illustreerib järgnev diagramm:

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

2.4 Lihtsad rühmad

Definitsioon 2.28 Rühma nimetatakse **lihtsaks**, kui tal ei ole mittetriviaalseid normaaljagajaid.

Ülesanne 2.29 Näidake, et kui p on algarv, siis rühm $(\mathbb{Z}_p, +)$ on lihtne.

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

Substitutsiooni 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. Põhikursusest on teada, et S_n on rühm substitutsioonide korrutamise suhtes.

Definitsioon 2.30 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

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

tähistatame lühidalt

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

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

Definitsioon 2.31 Tsükleid $(i_1, i_2, \ldots, i_k)$ ja $(j_1, j_2, \ldots, j_l)$ nimetatakse **sõltumatuteks**, kui $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_l\} = \emptyset$.

Lause 2.32 *Iga substitutsiooni saab esitada sõltumatute tsüklite korrutisena.*

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.

Definitsioon 2.33 **Transpositsioon** on tsükkel pikkusega 2.

Lause 2.34 *Transpositsioon on paaritu substitutsioon.*

Tõestus. Transpositsiooni

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

puhul on permutatsioon $\langle 1, \ldots, j, \ldots, i, \ldots, n \rangle$ saadud loomulikust permutatsioonist ühe transpositsiooni abil, seega on $\langle 1, \ldots, j, \ldots, i, \ldots, n \rangle$ paaritu permutatsioon. □

Lause 2.35 *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. Kuna transpositsioon muudab permutatsiooni paarsust, siis 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. 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 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 2.36 *Olgu $n \geq 2$. Siis on paaris- ja paarituid substitutsioone n elemendist ühepalju.*

Lause 2.37 *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 2.34 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. □

Lause 2.38 *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 2.37 põhjal on tsükkel $(i_1, i_2, \dots, i_k)$ ja arv $k - 1$ sama paarsusega. □

Lause 2.39 *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 2.35 põhjal saab σ ja τ esitada paarisarvu transpositsioonide korrutisena. Siis ka $\sigma\tau$ on paarisarvu transpositsioonide korrutis. Tänu lausele 2.37 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 2.40 *Kui $n \geq 3$, siis S_n ei ole lihtne.*

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

Ülesanne 2.41 Millise rühmaga on isomorfne faktorrühm S_n/A_n?

Teoreem 2.42 *Olgu A_n kõigi paarissubstitutsioonide hulk n elemendist. 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.

Kõigepäält 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:

$$\varphi = (i_1, i_2, \ldots, i_{s-2}, i_{s-1}, i_s) \cdot \ldots,$$

kus $s \geq 4$. Võtame $\psi := (i_{s-2}, i_{s-1}, i_s) \in S_n$. Tänu lausele 2.38 on 3-elemendilised tsüklid paarissubstitutsioonid, seega $\psi \in A_n$. Järelikult

$$\psi\varphi^{-1}\psi^{-1}\varphi = (i_{s-3}, i_s, i_{s-2}) \in N.$$

2) Lahutuses leidub vähemalt kaks 3-elemendilist tsüklit:

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

Olgu $\psi := (i_3, j_1, j_2) \in A_n$. Siis

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

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

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

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 mingi 3-elemendilise tsükli (i,j,k).

Järgmiseks näitame, et N sisaldab *kõik* 3-elemendilised tsüklid. 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, 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 kõik 3-elemendilised tsüklid.

Tõestuse lõpetamiseks näitame, et $A_n \subseteq N$. Olgu $\psi \in A_n$ suvaline paarissubstitutsioon. Lause 2.35 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 $(i,j)(i,k) = (i,j,k)$. 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 2.43 Saab näidata, et A_2 ja A_3 on lihtsad rühmad, aga A_4 ei ole.

Peatükk 3

Abeli rühm

3.1 Põhimõisted

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.

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.

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

Definitsioon 3.2 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 3.3 1. Rühma $(\mathbb{Z}, +)$ ei ole jaguv.
2. Rühm $(\mathbb{Q}, +)$ on jaguv.

Lemma 3.4 *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 $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, kus $p_1, p_2, \dots, p_s$ on paarikaupa erinevad algarvud ja $k_1, k_2, \dots, k_n \in \mathbb{N}$. Siis leiduvad elemendid $b_1, \dots, b_{k_1} \in A$ nii, et

$$p_1 b_1 = a,\ p_1 b_2 = b_1,\ \dots,\ p_1 b_{k_1} = b_{k_1 - 1}.$$

Järelikult $p_1^{k_1} b_{k_1} = a$. Edasi jagame b_{k_1} algarvuga p_2, ja nii edasi, kuni jõuame soovitud tulemuseni. □

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

Lemma 3.5 *Jaguva Abeli rühma epimorfne kujutis on jaguv.*

Tõestus. Vt. [1, lemma 2.3]. □

Lemma 3.6 *Jaguvate Abeli rühmade otsekorrutis ja väline otsesumma on jaguvad.*

Tõestus. Vt. [1, lemma 2.4]. □

Meenutame nüüd Abeli rühma alamrühmade sisemise otsesumma mõistet.

Definitsioon 3.7 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 alamrühmade elemendid, s.t.

$$\sum_{i \in I} A_i = \{a \in A \mid a = a_{i_1} + \dots + a_{i_k}, k \in \mathbb{N}, i_1, \dots, i_k \in I, a_{i_1} \in A_{i_1}, \dots, a_{i_k} \in A_{i_k}\}.$$

Alamrühmade summat $\sum_{i \in I} A_i$ nimetatakse **sisemiseks otsesummaks**, kui iga element $a \in A$ on üheselt esitatav kujul

$$a = a_{i_1} + \dots + a_{i_k},$$

kus $k \in \mathbb{N}, i_1, \dots, i_k \in I, a_{i_1} \in A_{i_1}, \dots, a_{i_k} \in A_{i_k}$. Kui alamrühmade $A_i, i \in I$ summa on sisemine otsesumma, siis kirjutatakse

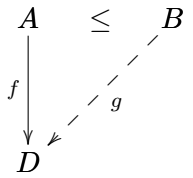
$$\sum_{i \in I} A_i = \dot{\sum_{i \in I}} A_i.$$

Teoreem 3.8 ([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 3.9 ([1], lause 2.7.12) *Abeli rühma A alamrühmade B ja C summa on otsesumma parajasti siis, kui $B \cap C = \{0\}$.*

Lause 3.10 *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

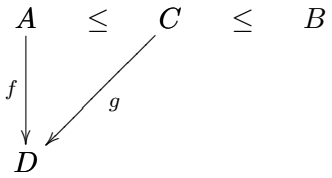
$$P = \{(X, h) \mid A \leq X \leq B, h \in \hom(X, D), h|_A = f\}.$$

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.

Olgu $b \in B \setminus C$. Vaatleme alamrühma $\mathbb{Z}b = \{zb \mid z \in \mathbb{Z}\} \leq B$. Siis $C < C + \mathbb{Z}b \leq B$. Vastuolu saame, kui õnnestub defineerida homomorfism $g' : C + \mathbb{Z}b \to D$ nii, et $g'|_C = g$, sest siis ka $g'|_A = f$.

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

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

$c \in C$, $z \in \mathbb{Z}$, ning nõutavad omadused on g' puhul täidetud.

2) Oletame, et $C + \mathbb{Z}b$ ei ole alamrühmade C ja $\mathbb{Z}b$ otsesumma. Siis $C \cap \mathbb{Z}b \neq \emptyset$. Olgu n vähim naturaalarv, mille korral $nb \in C$. Kuna $g(nb) \in D$ ja D on jaguv, siis leidub $d \in D$ nii, et $nd = g(nb)$. 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:

$$z_1 - z_2 = qn + r, \quad 0 \leq r < n.$$

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

$$g(c_2) - g(c_1) = g(c_2 - c_1) = g((z_1 - z_2)b) = g(qnb) = q \cdot g(nb) = qnd = (z_1 - z_2)d = z_1 d - z_2 d,$$

kust

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

Seega 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

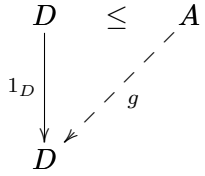
$$\begin{aligned} g'((c_1 + z_1 b) + (c_2 + z_2 b)) &= g'((c_1 + c_2) + (z_1 + z_2)b) = g(c_1 + c_2) + (z_1 + z_2)d \\ &= g(c_1) + g(c_2) + z_1 d + z_2 d = g(c_1) + z_1 d + g(c_2) + z_2 d \\ &= g'(c_1 + z_1 b) + g'(c_2 + z_2 b). \end{aligned}$$

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

TÕESTUS. Lause 3.10 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 3.12 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 3.13 *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:

$$m = nq + r, \;\; 0 \leq r < n.$$

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 3.14 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 3.15 Kui A on Abeli rühm ja p on algarv, siis hulka

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

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 3.16 *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 $\mathrm{ord}(a) = p^k$, kus $k \in \mathbb{N}$. Siis $p(p^{k-1}a) = 0$. Olgu $n = \mathrm{ord}(p^{k-1}a)$. Siis lemma 3.13 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 $\mathrm{ord}(a) = p^k$. Järelikult $n = p$, mis tähendab, et otsitavaks p-ndat järku elemendiks sobib $p^{k-1}a$. □

Saab näidata, et kehtib järgmine teoreem.

Teoreem 3.17 ([1], teoreem 11.2.5) *Perioodiline Abeli rühm on oma p-komponentide sisemine otsesumma.*

Näide 3.18 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 $A = A_2 \dotplus A_3$, 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

Definitsioon 3.19 Öeldakse, et Abeli rühm on **väändeta**, kui kõik tema nullist erinevad elemendid on lõpmatut järku.

Lemma 3.20 *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 $-(xb) = (-x)b = 0$, kus $-x > 0$, ning jällegi oleks tegemist vastuoluga. Seega $x = 0$.

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 3.20 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 3.21 *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 3.20 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 3.22 *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 $f : \mathbb{Q} \to Q(b)$ 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

$$\frac{x}{n} = \frac{y}{m} \iff mx = ny \iff (mx)b = (ny)b \iff m(xb) = nyb \iff (nyb)/m = xb$$
$$\iff n \cdot (yb)/m = xb \iff (xb)/n = (yb)/m,$$

siis näeme, et f on korrektselt defineeritud ja injektiivne. On selge, et f on sürjektiivne.

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

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

siis f on homomorfism. Seega f on isomorfism ja $Q(b) \cong \mathbb{Q}$. Niisiis B sisaldab rühmaga $\mathbb{Q}$ isomorfset alamrühma. □

Teoreem 3.23 *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 3.22 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. Me peame veenduma, et hulka X kuuluvate alamrühmade summa on otsesumma.

Võtame mingi elemendi x sellest summast. Oletame, et

$$x = x_{i_1} + x_{i_2} + \ldots + x_{i_n} = y_{j_1} + y_{j_2} + \ldots + y_{j_m},$$

kus

$$i_1, \ldots, i_n \in I \text{ on paarikaupa erinevad}, \quad x_{i_k} \in Q_{i_k} \leq B, \ \mathbb{Q} \cong Q_{i_k} \in X_{i_k},$$
$$j_1, \ldots, j_m \in I \text{ on paarikaupa erinevad}, \quad y_{j_l} \in Q_{j_l} \leq B, \ \mathbb{Q} \cong Q_{j_l} \in X_{j_l}.$$

Kuna hulgad $X_{i_1}, \ldots, X_{i_n}, X_{j_1}, \ldots, X_{j_m}$ moodustavad lõpliku ahela, siis selles ahelas leidub suurim element, s.t. leidub selline $r \in \{i_1, \ldots, i_n, j_1, \ldots, j_m\}$, et $X_{i_k}, X_{j_l} \subseteq X_r$ iga $k \in \{1, \ldots, n\}$ ja $l \in \{1, \ldots, m\}$ korral. Siis ka $Q_{i_k}, Q_{j_l} \in X_r$ iga $k \in \{1, \ldots, n\}$ ja $l \in \{1, \ldots, m\}$ korral. Et X_r on temasse kuuluvate B alamrühmade otsesumma, siis ka

$$Q_{i_1} + \ldots + Q_{i_n} + Q_{j_1} + \ldots + Q_{j_m} = Q_{i_1} \dotplus \ldots \dotplus Q_{i_n} \dotplus Q_{j_1} \dotplus \ldots \dotplus Q_{j_m}.$$

Järelikult $\{x_{i_1}, \ldots, x_{i_n}\} = \{y_{j_1}, \ldots, y_{j_m}\}$, s.t. x avaldub summana üheselt. Seega hulka X kuuluvate alamruumide summa on otsesumma.

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 $\mathbb{Q} \cong Q \leq B$ korral summa $D + Q$ ei ole otsesumma. Kuna $\mathbb{Q}$ on jaguv ja jaguvate rühmade otsesumma on ka jaguv, siis D on jaguv. Vastavalt lausele 3.11 leidub alamrühm $C \leq B$ nii, et

$$B = D \dotplus C.$$

Kuna C on jaguva rühma B epimorfne kujutis (võib vaadelda homomorfismi $B \to C,\ d+c \mapsto c$), siis C on jaguv tänu lemmale 3.5. Olles väändeta rühma B alamrühm on ka C väändeta. Kui $C \neq \{0\}$, siis ta peaks lause 3.22 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 3.24 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, $\mathbb{Q} \times \mathbb{Q} = Q_1 \dot{+} Q_2$.

3.5 Jaguvad p-rühmad

Uurime nüüd veel ühte rühmade klassi. Iga algarvu p korral vaatleme hulka

$$\mathbb{Q}_p := \left\{ \frac{x}{p^k} \mid x \in \mathbb{Z}, k \in \mathbb{N} \cup \{0\} \right\} \subseteq \mathbb{Q}.$$

Lihtne on veenduda, et $\mathbb{Q}_p$ on rühma $(\mathbb{Q}, +)$ alamrühm ja seega ise ka rühm liitmise suhtes. Hulk $\mathbb{Z} = \{\frac{x}{p^0} \mid x \in \mathbb{Z}\}$ on omakorda rühma $\mathbb{Q}_p$ alamrühm. Seega on võimalik vaadelda faktorrühma

$$\mathbb{Q}_p/\mathbb{Z} = \left\{ \frac{x}{p^k} + \mathbb{Z} \mid x \in \mathbb{Z}, k \in \mathbb{N} \cup \{0\} \right\}.$$

Definitsioon 3.25 Rühma nimetatakse **Prüferi p-rühmaks** ehk **p^∞-tüüpi rühmaks**, kui ta on isomorfne rühmaga $\mathbb{Q}_p/\mathbb{Z}$.

Võib veenduda, et ka näiteks kompleksarvuliste ühejuurte multiplikatiivne rühm

$$\left\{ \cos\frac{2u\pi}{p^k} + i \sin\frac{2u\pi}{p^k} \mid u \in \mathbb{Z}, k \in \mathbb{N} \right\} \subseteq \mathbb{C}$$

on Prüferi p-rühm.

Teeme veel mõned tähelepanekud rühma $\mathbb{Q}_p/\mathbb{Z}$ kohta. Tähistame kõrvalklasse alamrühma $\mathbb{Z}$ järgi lühidalt

$$\left[\frac{x}{p^k}\right] := \frac{x}{p^k} + \mathbb{Z}.$$

1. Iga $x \in \mathbb{Z}$ korral $[x] = \left[\frac{x}{p^0}\right] = [0] = \mathbb{Z}$, sest $x - 0 \in \mathbb{Z}$.
2. Iga $x \in \mathbb{Z}$ ja $k \in \mathbb{N}$ korral $\left[\frac{x}{p^k}\right] = x\left[\frac{1}{p^k}\right]$. Tähistades

$$a_k := \left[\frac{1}{p^k}\right]$$

võime öelda, et $\{a_k \mid k \in \mathbb{N}\}$ on rühma $\mathbb{Q}_p/\mathbb{Z}$ moodustajate süsteem. Täpsemalt

$$\mathbb{Q}_p/\mathbb{Z} = \{z a_k \mid z \in \mathbb{Z}, k \in \mathbb{N}\}.$$

3. Kehtivad seosed

$$pa_1 = p\left[\frac{1}{p}\right] = \left[\frac{p}{p}\right] = [1] = [0],$$

$$pa_2 = p\left[\frac{1}{p^2}\right] = \left[\frac{p}{p^2}\right] = \left[\frac{1}{p}\right] = a_1,$$

ja analoogiliselt

$$pa_{k+1} = a_k$$

iga $k \in \mathbb{N}$ korral. Seega

$$\mathbb{Z}a_1 \subseteq \mathbb{Z}a_2 \subseteq \mathbb{Z}a_3 \subseteq \dots$$

ja $\mathbb{Q}_p/\mathbb{Z}$ on oma alamrühmade $\mathbb{Z}a_k, k \in \mathbb{N}$ ahela ühend,

$$\mathbb{Q}_p/\mathbb{Z} = \bigcup_{k\in\mathbb{N}} \mathbb{Z}a_k.$$

Lemma 3.26 *Rühm $\mathbb{Q}_p/\mathbb{Z}$ on p-rühm.*

Tõestus. Me näitame, et

$$(\forall k \in \mathbb{N})(\mathrm{ord}(a_k) = p^k).$$

Teeme seda matemaatilise induktsiooniga k järgi. Induktsiooni aluse tõestamiseks näitame, et $\mathrm{ord}(a_1) = p$. Kõigepäält paneme tähele, et $pa_1 = [0]$. Näitame, et p on vähim selline naturaalarv. Oletame, et $ma_1 = [0]$, kus $m \in \mathbb{N}$. Jagame arvu m jäägiga arvuga p:

$$m = pq + r, \;\; 0 \le r < p, \;\; q, r \in \mathbb{Z}.$$

Siis

$$[0] = ma_1 = (pq + r)a_1 = qpa_1 + ra_1 = [0] + ra_1 = ra_1.$$

Kui $r > 0$, siis saame, et $[0] = ra_1 = \left[\frac{r}{p}\right]$. Seega $\frac{r}{p} \in \mathbb{Z}$, mis on vastuolu. Järelikult $r = 0$ ehk $m = pq$, kust näeme, et $p \le m$. Sellega on tõestatud, et $\mathrm{ord}(a_1) = p$.

Viime nüüd läbi induktsiooni sammu. Eeldame, et $\mathrm{ord}(a_{k-1}) = p^{k-1}$. Siis

$$p^k a_k = p^{k-1}a_{k-1} = [0].$$

Olgu $m = \mathrm{ord}(a_k)$. Siis lemma 3.13 põhjal $m \mid p^k$ ning järelikult leidub selline $l \in \mathbb{N}$, et $l \le k$ ja $m = p^l$. Oletame vastuväiteliselt, et $l < k$. Siis

$$[0] = ma_k = p^l a_k = p^{l-1}(pa_k) = p^{l-1}a_{k-1},$$

kus $l - 1 < k - 1$, mis on vastuolus induktsiooni eeldusega. Järelikult $l = k$ ja $\mathrm{ord}(a_k) = p^k$.

Rühma $\mathbb{Q}_p/\mathbb{Z}$ suvalise elemendi za_k ($z \in \mathbb{Z}$, $k \in \mathbb{N}$) korral $p^k(za_k) = zp^k a_k = [0]$, mis tähendab, et elemendi za_k järk jagab arvu p^k ning on seetõttu ise ka p aste. Seega $\mathbb{Q}_p/\mathbb{Z}$ on tõepoolest p-rühm. □

Lemma 3.27 *Prüferi p-rühm on jaguv.*

TÕESTUS. Olgu $za_k \in \mathbb{Q}_p/\mathbb{Z}$. Tänu lemmale 3.4 piisab kontrollida elemendi za_k jaguvust kõigi algarvudega. Kuna

$$p(za_{k+1}) = zpa_{k+1} = za_k,$$

siis za_k jagub algarvuga p. Olgu nüüd q selline algarv, mis ei ole p. Kuna $\text{SÜT}(p^k, q) = 1$, siis leiduvad täisarvud u, v nii, et $1 = p^k u + qv$. Järelikult

$$za_k = z(p^k u + qv)a_k = zup^k a_k + zqva_k = [0] + zqva_k = q(zva_k).$$

Seega rühm $\mathbb{Q}_p/\mathbb{Z}$ on jaguv. Lihnte on aru saada, et jaguva rühmaga isomorfne rühm peab ka olema jaguv. □

Lause 3.28 *Mittetriviaalne jaguv p-rühm sisaldab alamrühma, mis on Prüferi p-rühm.*

TÕESTUS. Olgu $C \neq \{0\}$ jaguv p-rühm. Siis vastavalt lemmale 3.16 leidub rühmas C element c_1 nii, et $\text{ord}(c_1) = p$. Tähistades $c_0 := 0$ võime kirjutada

$$pc_1 = c_0.$$

Jaguvuse tõttu leiduvad elemendid $c_2, c_3, \ldots \in C$ nii, et

$$pc_2 = c_1,\ pc_3 = c_2,\ \ldots,\ pc_k = c_{k-1},\ \ldots.$$

Näitame matemaatilise induktsiooni abil, et

$$(\forall k \in \mathbb{N})(\text{ord}(c_k) = p^k).$$

Kui $k = 1$, siis väide kehtib. Oletame, et $k > 1$ ja iga $0 < m < k$ korral $\text{ord}(c_m) = p^m$. Siis muuhulgas $\text{ord}(c_{k-1}) = p^{k-1}$ ja

$$p^k c_k = p^{k-1}(pc_k) = p^{k-1}c_{k-1} = 0.$$

Kui $n = \text{ord}(c_k)$, siis $n \mid p^k$, seega $n = p^l$, kus $1 \leq l \leq k$. Kui $l < k$, siis $0 = p^l c_k = c_{k-l}$, mis on vastuolus induktiivse eeldusega, et $\text{ord}(c_{k-l}) = p^{k-l}$. Järelikult $l = k$ ja $\text{ord}(c_k) = n = p^k$.

Defineerime nüüd kujutuse $f : \mathbb{Q}_p \to C$ võrdusega

$$f\left(\frac{x}{p^k}\right) := xc_k,$$

$x \in \mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$. Kui $\frac{x}{p^k} = \frac{y}{p^{k+r}}$, kus $x, y \in \mathbb{Z}$, $k, r \in \mathbb{N} \cup \{0\}$, siis $xp^{k+r} = yp^k$. Taandades naturaalarvu p^k saame võrduse $xp^r = y$. Järelikult $yc_{k+r} = xp^r c_{k+r} = xc_k$. Seega f on korrektselt defineeritud.

Veendume, et f on rühmade homomorfism. Tõepoolest, iga $x, y \in \mathbb{Z}$, $k, l \in \mathbb{N} \cup \{0\}$ korral

$$\begin{aligned} f\left(\frac{x}{p^k} + \frac{y}{p^l}\right) &= f\left(\frac{xp^l + yp^k}{p^{k+l}}\right) = (xp^l + yp^k)c_{k+l} = xp^l c_{k+l} + yp^k c_{k+l} = xc_k + yc_l \\ &= f\left(\frac{x}{p^k}\right) + f\left(\frac{y}{p^l}\right). \end{aligned}$$

Näitame, et $\text{Ker}\,(f) = \mathbb{Z}$. Oletame, et $\frac{x}{p^k} \in \text{Ker}\,(f)$, s.t. $xc_k = 0$. Siis $p^k = \text{ord}(c_k) \mid x$, kust $\frac{x}{p^k} \in \mathbb{Z}$. Vastupidi, kui $x \in \mathbb{Z}$, siis

$$f(x) = f\left(\frac{x}{p^0}\right) = xc_0 = x0 = 0,$$

s.t. $x \in \operatorname{Ker}(f)$. Seega tõesti $\operatorname{Ker}(f) = \mathbb{Z}$. Homomorfismiteoreemi põhjal

$$\operatorname{Im}(f) \cong \mathbb{Q}_p / \operatorname{Ker}(f) = \mathbb{Q}_p/\mathbb{Z}$$

ehk $\operatorname{Im}(f)$ on rühma C alamrühm, mis on Prüferi p-rühm. □

Teoreem 3.29 *Mittetriviaalne jaguv p-rühm on Prüferi p-rühmade otsesumma.*

TÕESTUS. Olgu T mittetriviaalne jaguv p-rühm. Võtame hulga P, mille elementideks on sellised rühma T alamrühmade hulgad, millesse kuuluvad alamrühmad on Prüferi p-rühmad ja millesse kuuluvate alamrühmade summa on otsesumma. Vaatleme hulka P osaliselt järjestatud hulgana sisalduvusseose suhtes. Tänu lausele 3.28 on hulk P mittetühi. Saab näidata, et ta rahuldab Zorni lemma eeldusi. Ülejäänud tõestus on analoogiline Teoreemi 3.23 tõestusega. □

3.6 Jaguvate Abeli rühmade kirjeldus

Teoreem 3.30 *Abeli rühm on jaguv parajasti siis kui ta on isomorfne teatud arvu ratsionaalarvude rühmade ja teatud arvu Prüferi p-rühmade välise otsesummaga.*

TÕESTUS. TARVILIKKUS. Olgu A jaguv rühm ja olgu T selle rühma perioodiline osa, s.t.

$$T = \{a \in A \mid \operatorname{ord}(a) < \infty\} = \{a \in A \mid (\exists m \in \mathbb{N})(ma = 0)\}.$$

Tänu lausele 11.5.2 raamatust [1] on see hulk alamrühm rühmas A. Näitame, et T on jaguv rühm. Olgu $a \in T$ ja $n \in \mathbb{N}$. Siis leidub selline $m \in \mathbb{N}$, et $ma = 0$. Kuna A on jaguv, siis leidub $b \in A$ nii, et $nb = a$. Järelikult $0 = ma = m(nb) = (mn)b$, kus $mn \in \mathbb{N}$. Siit näeme, et b järk on lõplik, järelikult $b \in T$. Sellega on tõestatud, et T on jaguv.

Lause 3.11 põhjal esitub rühm A sisemise otsesummana

$$A = T \dotplus B,$$

kus B on mingi alamrühm. On selge, et B on väändeta, sest vastasel juhul ei kehtiks võrdus $T \cap B = \{0\}$. Kuna $A = T \dotplus B$, siis rühma A iga element avaldub üheselt summana $t + b$, kus $t \in T$ ja $b \in B$. Kujutus $\pi : A \to B$, mis on defineeritud võrdusega

$$\pi(t + b) := b$$

on sürjektiivne homomorfism. Seega on B jaguv, sest ta on jaguva rühma epimorfne kujutis (vt. lauset 3.5). Kui $B \neq \{0\}$, siis tänu teoreemile 3.23 on B rühmaga $\mathbb{Q}$ isomorfsete alamrühmade sisemine otsesumma.

Vastavalt teoreemile 3.17 on perioodiline rühm T oma p-komponentide sisemine otsesumma:

$$T = \dot{\sum_{p \in \mathbb{P}}} T_p.$$

Kuna iga algarvu p korral on p-komponent T_p jaguva rühma T epimorfne kujutis, siis on ka T_p jaguv rühm. Kasutades teoreemi 3.29 saame öelda, et kui $T_p \neq \{0\}$, siis on ta Prüferi p-rühmade sisemine otsesumma.

Seega A on selliste alamrühmade sisemine otsesumma, mis on isomorfsed kas rühmaga $\mathbb{Q}$ või Prüferi p-rühmaga mõne algarvu p-korral. Tänu teoreemile 3.8 on see sisemine otsesumma aga isomorfne nendesamade alamrühmade välise otsesummaga.

PIISAVUS. Kuna rühm $\mathbb{Q}$ ja Prüferi p-rühmad on jaguvad, siis on seda lemma 3.6 põhjal ka nende väline otsesumma. □

Näide 3.31 Rühm

$$\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}_2/\mathbb{Z} \times \mathbb{Q}_{11}/\mathbb{Z}$$

on jaguv Abeli rühm. Kuna siin on tegemist lõpliku otsekorrutisega, siis see lõplik otsekorrutis on võrdne vastavate rühmade välise otsesummaga. Milline on selles rühmas elemendi

$$\left(6, -12, \frac{3}{5}, \left[\frac{1}{8}\right], \left[\frac{4}{11}\right]\right)$$

ja naturaalarvu 2 jagatis?

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. $f(1) = 1$.

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**.

Lause 4.9 *Ringide homomorfismi tuum on ideaal.*

Tõestus. .... □

Lemma 4.10 *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. .... □

Lihtne on veenduda, et kehtib järgmine tulemus.

Lemma 4.11 *Ringi parempoolsete ideaalide (vasakpoolsete ideaalide, ideaalide) ühisosa on samuti parempoolne ideaal (vasakpoolne ideaal, ideaal).*

Lause 4.12 ([1], lause 6.5.5) *Ringis, mis sisaldab vähemalt kahte elementi, ei ole mittetriviaalseid parempoolseid ideaale parajasti siis, kui see ring on jagamisega ring.*

Definitsioon 4.13 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 4.14 *Olgu D jagamisega ring ja $n \in \mathbb{N}$. Siis ring $\mathrm{Mat}_n(D)$ on lihtne.*

TÕESTUS. Olgu I ringi $\mathrm{Mat}_n(D)$ nullit 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 $(E_{ik}A)E_{lj} \in I$, kus element a_{kl} asub kohal (i, j). Korrutame viimase maatriksi vasakult maatriksiga $b_{ij}a_{kl}^{-1}E$, kus E on ühikmaatriks. Saame maatriksi

$$B_{ij} := (b_{ij}a_{kl}^{-1}E)(E_{ik}AE_{lj}) \in I.$$

Kuna I on kinnine liitmise suhtes, siis ka

$$B = \sum_{i,j=1}^{n} B_{ij} \in I.$$

□

4.2 Lihtsad minimaalset parempoolset ideaali sisaldavad ringid

Definitsioon 4.15 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 4.16 *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. Lihtne on aru saada, et I on 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

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

Seega $I \subseteq J$, kust $I = J$. □

Teoreem 4.17 *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 4.14 ja lausest 4.16.
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 $1 = \sum_{i=1}^{n} x_i x y_i$ mingite $n \in \mathbb{N}$, $x_i, y_i \in R$ korral. Et

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

siis leidub mingi $k \in \{1, \ldots, n\}$ nii, et $x x_k x y_k \neq 0$. 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 4.11 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

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

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

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

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.

Olgu $0 \neq exe \in D$. Kuna $M = eR$, siis $exe \in M$ ja $(exe)R \subseteq M$, 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. 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 $m\varphi$. Hulgal $\mathrm{End}_D(M)$ defineerime liitmise ja korrutamistehte $\bullet$ järgmiselt:

$$m(\varphi + \psi) := m\varphi + m\psi,$$
$$m(\varphi \bullet \psi) := (m\varphi)\psi$$

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

$$\begin{aligned} mg(r_1r_2) &= m\rho_{r_1r_2} = m(r_1r_2) = (mr_1)r_2 = (mr_1)\rho_{r_2} \\ &= (m\rho_{r_1})\rho_{r_2} = m(\rho_{r_1} \bullet \rho_{r_2}) = m(g(r_1) \bullet g(r_2)), \end{aligned}$$

kust $g(r_1r_2) = g(r_1) \bullet g(r_2)$.

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 $\varphi \in \mathrm{End}_D(M)$. Kuna ringi R lihtsuse tõttu $R = ReR$, siis leiduvad selline $n \in \mathbb{N}$ ja elemendid $x_i, y_i \in R$ nii, et

$$1 = \sum_{i=1}^{n} x_i e y_i.$$

Olgu

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

Kasutades seda, et $m = em$ iga $m \in M$ korral, ning seda, et φ on lineaarteisendus, saame, et

$$\begin{aligned} m\rho_r = mr &= m\left(\sum_{i=1}^{n}(x_i e)((ey_i)\varphi)\right) = \sum_{i=1}^{n}(mx_i e)((ey_i)\varphi) = \sum_{i=1}^{n}(emx_i e)((ey_i)\varphi) \\ &= \sum_{i=1}^{n}((emx_i e)(ey_i))\varphi = \left(\sum_{i=1}^{n}(emx_i e)(ey_i)\right)\varphi = \left(m\left(\sum_{i=1}^{n}(x_i e)(ey_i)\right)\right)\varphi \\ &= (m1)\varphi = m\varphi. \end{aligned}$$

Seega $\varphi = \rho_r = g(r)$ ja g on pealekujutus. Oleme tõestanud, et g on 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 $\{e_i \mid i \in I\}$ vektorruumi M baas (eelduse tõttu peab see olema lõpmatu). Fikseerime selles ühe vektori e_k, $k \in I$. Iga vektor $m \in M$ peab üheselt avalduma kujul

$$m = d_1 e_{i_1} + \ldots + d_n e_{i_n},$$

kus $n \in \mathbb{N}$, $d_1, \ldots, d_n \in D$ ja $e_{i_1}, \ldots, e_{i_n}$ on paarikaupa erinevad baasivektorid. Defineerime teisenduse $\varphi : M \to M$ võrdusega

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

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

Näitame, et I on 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 $\{e'_1, \ldots, e'_n\}$. Olgu $m \in \mathrm{Im}(\varphi\psi)$. Siis leidub $m' \in M$ nii, et $m = (m'\varphi)\psi$. Kuna $m'\varphi \in \mathrm{Im}(\varphi)$, siis leiduvad $d_1 \ldots, d_n \in D$ nii, et $m'\varphi = d_1e'_1 + \ldots + d_ne'_n$. Järelikult

$$m = (d_1e'_1 + \ldots + d_ne'_n)\psi = d_1(e'_1\psi) + \ldots + d_n(e'_n\psi).$$

Siit näeme, et alamruumil $\mathrm{Im}(\varphi\psi)$ leidub lõplik moodustajate süsteem $e'_1\psi, \ldots, e'_n\psi$, seega leidub tal ka lõplik baas. Järelikult $\varphi\psi \in I$. Kuna $\mathrm{Im}(\psi\varphi) \subseteq \mathrm{Im}(\varphi)$, siis ka alamruum $\mathrm{Im}(\psi\varphi)$ on lõplikumõõtmeline. Järelikult $\psi\varphi \in I$. Sellega on tõestatud, et I on 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 $\left(A^B_\varphi\right)^T$ on nullmaatriks, kust järeldub, et ka A^B_φ 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 $X^T = A^B_\varphi$. Siis aga

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

Sellega oleme näidanud, 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) ja tähistatakse ${}_RA$. Analoogiliselt saab defineerida parempoolsed moodulid.

Alammoodul, moodulite homomorfism jm. mõisted defineeritakse sarnaselt vastavate mõistetega vektorruumide korral.

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

2. Iga Abeli rühma saab loomulikul viisil vaadelda moodulina üle ringi $\mathbb{Z}$.

3. Ringi R iga vasakpoolne ideaal I on moodul üle ringi R.

4. Olgu $R = \mathrm{Mat}_n(D)$, kus D on jagamisega ring. Siis hulk $A = \mathrm{Mat}_{n,1}(D)$ on 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 alapeatükis on kõik vaadeldavad moodulid vasakpoolsed ja 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.

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

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

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

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

Definitsioon 5.4 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. $\operatorname{Ker}(f) = \operatorname{Im}(0) = 0$, st f on injektiivne;
2. $\operatorname{Im}(g) = \operatorname{Ker}(0) = C$, st g on sürjektiivne;
3. $C \cong B/\operatorname{Ker}(g) = B/\operatorname{Im}(f)$ tänu järelduse 1.34 analoogile moodulite jaoks;
4. kui samastada A ja sellega isomorfne $\operatorname{Im}(f)$, siis $C \cong B/A$.

Teoreem 5.5 *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 $\operatorname{Im}(f) = \operatorname{Im}(\iota)$.*

(iii) *Kehtib $B = \operatorname{Im}\iota \dotplus H$ mingi mooduli B alammooduli H korral.*

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

Tõestus. (i) $\Rightarrow$ (ii) Võtame $f = \iota\varphi : B \to B$. Kohe saame, et

$$f^2 = (\iota\varphi)(\iota\varphi) = \iota(\varphi\iota)\varphi = \iota\varphi.$$

Jääb üle veenduda, et $\operatorname{Im}(f) = \operatorname{Im}(\iota)$. Kuna mistahes $x \in B$ korral $f(x) = \iota(\varphi(x))$, siis ilmselt $\operatorname{Im}(f) \subseteq \operatorname{Im}(\iota)$. Teisipidi, iga $y \in A$ korral $y = 1_A(y) = \varphi(\iota(y))$, mistõttu $\iota(y) = \iota(\varphi(\iota(y))) = f(\iota(y))$ ja $\operatorname{Im}(\iota) \subseteq \operatorname{Im}(f)$ ning tõepoolest $\operatorname{Im}(\iota) = \operatorname{Im}(f)$.

(ii) $\Rightarrow$ (iii) Veendume, et väide kehtib, kui võtta $H = \mathrm{Ker}\,(f)$, st $B = \mathrm{Im}\,(\iota) \dotplus \mathrm{Ker}\,(f)$. Fikseerime $b \in B$ ja näitame esmalt, et $B = \mathrm{Im}\,(\iota) + \mathrm{Ker}\,(f)$. Selleks paneme tähele, et $b - f(b) \in B$ ning

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

st $b - f(b) \in \mathrm{Ker}\,(f)$ ja tõepoolest $b \in \mathrm{Im}\,(f) + \mathrm{Ker}\,(f) = \mathrm{Im}\,(\iota) + \mathrm{Ker}\,(f)$.
Olgu nüüd $b \in \mathrm{Im}\,(f) \cap \mathrm{Ker}\,(f)$, st $f(b) = 0$ ja $b = f(b')$ mingi $b' \in B$ korral. Siis $b = f(b') = f^2(b') = f(f(b')) = f(b) = 0$. Järelikult kehtibki $B = \mathrm{Im}\,(\iota) \dotplus \mathrm{Ker}\,(f)$.

(iii) $\Rightarrow$ (i) Olgu $B = \mathrm{Im}\ \iota \dotplus H$, kus H on B alammoodul. Siis iga $b \in B$ esitub üheselt kujul $b = \iota(x) + y$, $x \in A$, $y \in H$. 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 homomorfism. Viimaks, 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

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

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 leiame, et iga $c \in C$ korral

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

Seega tõesti $\pi\psi = 1_C$.

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

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

Ilmselt on tegu homomorfismiga, ja

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

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

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

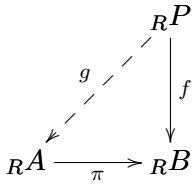
kust on näha, et $\mathrm{Im}\,(\iota) \subseteq \mathrm{Im}\,(f)$. Teisipidi, kui $b \in B$, siis

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

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

5.3 Projektiivsed moodulid

Definitsioon 5.6 Moodulit ${}_RP$ nimetatakse **projektiivseks**, kui mistahes sürjektiivse homomorfismi $\pi : {}_RA \to {}_RB$ ja mistahes homomorfismi $f : {}_RP \to {}_RB$ korral leidub homomorfism $g : {}_RP \to {}_RA$ nii, et $f = \pi g$.



Definitsioon 5.7 Moodulit nimetatakse vabaks kui temas leidub baas, st lineaarselt sõltumatu moodustajate süsteem.

Lause 5.8 *Mistahes vaba moodul ${}_RF$ on isomorfne otsesummaga sellistest moodulitest A_α, kus $A_\alpha \cong {}_RR$ iga $\alpha \in I$ korral:*

$$ {}_RF \cong \oplus \sum_{\alpha \in I} A_\alpha.$$

Tõestus. ... □

Lause 5.9 *Mistahes vaba moodul ${}_RF$ on projektiivne.*

Tõestus. ... □

Lause 5.10 *Mistahes moodul on vaba mooduli sürjektiivne kujutis (faktormoodul).*

Tõestus. ... □

Järeldus 5.11 *Mistahes moodul on projektiivse mooduli sürjektiivne kujutis (faktormoodul).*

Lause 5.12 *Olgu ${}_RP = \oplus \sum_{\alpha \in I} P_\alpha$. Moodul ${}_RP$ on projektiivne parajasti siis, kui moodulid P_α, $\alpha \in I$, on kõik projektiivsed.*

Tõestus. ... □

Teoreem 5.13 *Järgmised väited on samaväärsed.*

(i) *Moodul ${}_RP$ on projektiivne.*

(ii) *Mistahes lühikese täpse jada*

$$0 \longrightarrow {}_RA \xrightarrow{\iota} {}_RB \xrightarrow{\pi} {}_RP \longrightarrow 0$$

korral leidub homomorfism $\psi : {}_RP \to {}_RB$ nii, et $\pi\psi = 1_P$.

(iii) *Leidub vaba moodul ${}_RF$ nii, et $F = {}_RA \dot{+} {}_RB$, kusjuures üks otseliidetavatest on isomorfne mooduliga ${}_RP$.*

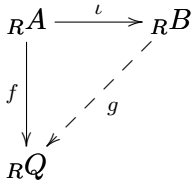
TÕESTUS. (i) $\Rightarrow$ (ii) Rakendame ${}_RP$ projektiivsust kujutustele $\pi :{}_R B \to {}_RP$ ja $1_P : {}_RP \to {}_RP$. Siis leidub selline homomorfism $\psi : {}_RP \to {}_RB$, et $\pi\psi = 1_P$, mida oligi tarvis tõestada.
(ii) $\Rightarrow$ (iii) Lause 5.10 tõttu on meil lühike täpne jada

$$0 \longrightarrow \mathrm{Ker}\,(\pi) \xrightarrow{\iota} {}_RF \xrightarrow{\pi} {}_RP \longrightarrow 0\,,$$

kus ${}_RF$ on vaba moodul ja ι on sisestus. Eelduse (i) kohaselt leidub homomorfism $\psi : {}_RP \to {}_RF$ nii, et $\pi\psi = 1_P$, mis teoreemist 5.5 tulenevalt annab meile, et ${}_RF = \mathrm{Im}\,(\iota) \dotplus {}_RB$ mingi ${}_RF$ alammooduli ${}_RB$ korral. Viimasest saab järeldada, et ${}_RB \cong {}_RF/\,\mathrm{Ker}\,(\pi)$. Homomorfismi π sürjektiivsuse ja homomorfismiteoreemi tõttu kehtibki, et ${}_RP \cong {}_RF/\,\mathrm{Ker}\,(\pi) \cong {}_RB$.
(iii) $\Rightarrow$ (i) Vaba moodul ${}_RF = {}_RA \dotplus {}_RP$ on projektiivne lause 5.9 tõttu. Lause 5.12 annabki nüüd, et nii ${}_RA$ kui ${}_RP$ on projektiivsed. □

5.4 Injektiivsed moodulid

Definitsioon 5.14 Moodulit ${}_RQ$ nimetatakse **injektiivseks**, kui mistahes injektiivse homomorfismi $\iota : {}_RA \to {}_RB$ ja mistahes homomorfismi $f : {}_RA \to {}_RQ$ korral leidub homomorfism $g : {}_RB \to {}_RQ$ nii, et $f = g\iota$.



Lause 5.15 *Moodul ${}_RQ$ on injektiivne parajasti siis, kui mistahes 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. ... □

Teoreem 5.16 *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 $g|_I = f$.*

TÕESTUS. ... □

Lause 5.17 *Abeli rühm vaadelduna vasakpoolse $\mathbb{Z}$-moodulina on injektiivne parajasti siis kui see Abeli rühm on jaguv.*

TÕESTUS. ... □

Lemma 5.18 *Olgu A ja B Abeli rühmad ja $C \leq A \leq B$. Siis $A/C \leq B/C$.*

TÕESTUS. ... □

Lause 5.19 *Iga Abeli rühm on isomorfne mingi jaguva rühma alamrühmaga.*

TÕESTUS. ... □

Lemma 5.20 *Olgu R ring ja A Abeli rühm. Siis hulka*

$$\mathrm{Hom}(R, A) = \{f : R \to A \mid f \text{ on Abeli rühmade homomorfism}\}$$

saab vaadelda vasakpoolse moodulina üle ringi R.

TÕESTUS. ... □

Lause 5.21 *Kui A on jaguva Abeli rühm, siis vasakpoolne R-moodul $\mathrm{Hom}(R, A)$ on injektiivne.*

TÕESTUS. ... □

Teoreem 5.22 *Iga moodul on isomorfne mingi injektiivse mooduli alammooduliga.*

TÕESTUS. Olgu ${}_RA$ suvaline vasakpoolne R-moodul. Lause 5.19 põhjal leidub jaguv Abeli rühm D ja selle alamrühm D' nii, et $A \cong D'$ kui Abeli rühmad. Olgu $\alpha : A \to D'$ Abeli rühmade isomorfism. Lause 5.21 põhjal on vasakpoolne R-moodul $\mathrm{Hom}(R, D)$ injektiivne. Defineerime kujutuse

$$\iota : A \to \mathrm{Hom}(R, D)$$

võrdusega

$$(x)(\iota(a)) := \alpha(x \cdot a).$$

Siis $\iota(a) : R \to D$. Veendume, et $\iota(a)$ on Abeli rühmade homomorfism. Tõepoolest,

$$(x + y)(\iota(a)) = \alpha((x + y) \cdot a) = \alpha(x \cdot a + y \cdot a) = \alpha(xa) + \alpha(ya) = (x)(\iota(a)) + (y)(\iota(a)).$$

mistahes $x, y \in R$ korral.

Kuna mistahes $r, x \in R$ ja $a, b \in A$ korral

$$\begin{aligned}(x)(\iota(a + b)) &= \alpha(x(a + b)) = \alpha(xa + xb) = \alpha(xa) + \alpha(xb) = (x)(\iota(a)) + (x)(\iota(b)) \\ &= (x)(\iota(a) + \iota(b)), \\ (x)(r \cdot \iota(a)) &= (xr)(\iota(a)) = \alpha((xr)a) = \alpha(x(ra)) = (x)(\iota(ra)),\end{aligned}$$

siis ι on R-moodulite homomorfism.

Tõestuse lõpetamiseks näitame, et kujutus ι on üksühene (siis $A \cong \mathrm{Im}\,(\iota)$, kus $\mathrm{Im}\,(\iota)$ on injektiivse mooduli alammmoodul). Selleks näitame, et $\mathrm{Ker}\,(\iota) = \{0\}$. Olgu $a \in \mathrm{Ker}\,(\iota)$. Siis $\iota(a) : R \to D$ on nullkujutus, see tähendab, et $(x)(\iota(a)) = 0$ iga $x \in R$ korral. Järelikult $\alpha(xa) = 0$ iga $x \in R$ korral. Muuhulgas $\alpha(a) = \alpha(1a) = 0$. Et α on Abeli rühmade isomorfism, siis $a = 0$. Seega $\mathrm{Ker}\,(\iota) = \{0\}$. □

Peatükk 6

Poolrühmad

6.1 Põhidefinitsioonid

Definitsioon 6.1 **Poolrühmaks** nimetatakse mittetühja 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 nimetatakse **monoidiks**, kui temas leidub ühikelement.

Definitsioon 6.3 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 6.4 Poolrühmade **isomorfismiks** nimetatakse homomorfismi, mis on bijektiivne.

Definitsioon 6.5 Poolrühma S mittetühja alamhulka U nimetatakse **alampoolrühmaks**, kui ta on kinnine korrutamise suhtes.

Nii nagu ringiteooriaski, on ka poolrühmateoorias oluline roll ideaalidel.

Definitsioon 6.6 Mittetühja 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.

On selge, et poolrühma ideaal on alampoolrühm. Vastupidine üldjuhul ei kehti.

Näide 6.7 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 $3 \cdot 2 \notin U$.

Definitsioon 6.8 Poolrühma S ideaali I nimetatakse **minimaalseks ideaaliks**, kui see on minimaalne element poolrühma S kõigi ideaalide sisalduvusseose suhtes järjestatud hulgas.

Definitsioon 6.9 Poolrühma S **vähimaks ideaaliks** nimetatakse ideaali, mis sisaldub poolrühma S igas ideaalis.

Analoogiliselt saab defineerida minimaalsed ja vähimad vasak- ja parempoolsed ideaalid.

Definitsioon 6.10 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**.

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 6.11 *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 6.12 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 6.13 Poolrühma S ideaali I nimetatakse **pärisideaaliks**, kui $I \neq S$.

Definitsioon 6.14 Poolrühma S nimetatakse **lihtsaks,** kui ta ei sisalda pärisideaale.

Lause 6.15 *Poolrühm S on lihtne parajasti siis, kui $SaS = S$ iga $a \in S$ korral.*

TÕESTUS. Tarvilikkus. Oletame, et S on lihtne poolrühm. 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. Kuna S on lihtne, siis $SaS = S$.

Piisavus. Oletame, et $SaS = S$ iga $a \in S$ korral ja olgu I poolrühma S 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 ideaal poolrühmas S ja $a \in I$, siis ka $s \in I$. Seega $I = S$ ning S 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 6.16 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 6.17 *Lihtne poolrühm on faktoriseeruv.*

TÕESTUS. Kuna S^2 on poolrühma S ideaal, siis lihtsuse tõttu $S^2 = S$. □

Lause 6.18 *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 6.15 põhjal on M lihtne poolrühm. □

6.3 Greeni seosed

Definitsioon 6.19 Olgu $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ ja $\mathcal{D}$ seosed poolrühmal S, mis on defineeritud järgmiselt:

$$a\mathcal{J}b \iff S^1aS^1 = S^1bS^1$$

$$a\mathcal{R}b \iff aS^1 = bS^1$$

$$a\mathcal{L}b \iff S^1a = S^1b$$

$$\mathcal{H} = \mathcal{L} \wedge \mathcal{R}$$

$$\mathcal{D} = \mathcal{L} \vee \mathcal{R}$$

mistahes $a, b \in S$ korral. Seoseid $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ ja $\mathcal{D}$ nimetatakse **Greeni seosteks** poolrühmal S.

Märkus 6.20 Lihtne on aru saada, et $\mathcal{R}$, $\mathcal{L}$ ja $\mathcal{J}$ on ekvivalentsiseosed hulgal S. Alumine ja ülemine raja $\mathcal{R}$ ja $\mathcal{L}$ vahel leitakse hulga S kõigi ekvivalentsiseoste hulgas, mis on järjestatud hulk sisalduvusseose suhtes.

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 6.21 *Mistahes poolrühma S ja elementide $a, b \in S$ korral*

$$a\mathcal{R}b \iff (\exists u, v \in S^1)(a = bu \wedge b = av);$$
$$a\mathcal{L}b \iff (\exists u, v \in S^1)(a = ub \wedge b = va);$$
$$a\mathcal{J}b \iff (\exists u, v, s, t \in S^1)(a = ubv \wedge b = sat).$$

Lause 6.22 *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 6.21 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 6.21 põhjal võime öleda, et $ca\mathcal{R}cb$.

Analoogiliselt saab näidata, et $\mathcal{L}$ on parempoolne kongruents. □

Definitsioon 6.23 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 6.24 *Kui S on rühm, siis temas on täpselt üks idempotent.*

6.4 Täiesti lihtsad poolrühmad ja minimaalsed ühepoolsed ideaalid

Definitsioon 6.25 Poolrühma S idempotenti e nimetatakse **primitiivseks,** kui iga $f \in E(S)$ korral:

$$ef = fe = f \;\Rightarrow\; e = f.$$

Definitsioon 6.26 Lihtsat poolrühma S, mis sisaldab primitiivset idempotenti, nimetatakse **täiesti lihtsaks.**

Üks võimalik lähenemisviis täiesti lihtsatele poolrühmadele on kasutada minimaalseid ühepoolseid ideaale.

Lemma 6.27 *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 $L = L_a$. □

Lause 6.28 *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 $Sa \subseteq L$. Tõepoolest iga elemendi $s \in S$ korral, sa kuulub hulka L, sest L on vasakpoolne ideaal. 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 6.29 *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 $s \in S$, tähistatame $Ls = \{as \mid a \in L\}$. Siis hulk Ls on vasakpoolne ideaal poolrühmas S. Näitame, et Ls on minimaalne vasakpoolne ideaal. Oletame, et B on vasakpoolne ideaal poolrühmas S ja $B \subseteq Ls$. Siis hulk

$$A = \{a \in L | as \in B\} \subseteq L$$

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 6.30 *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. Kuna $ab\,\mathcal{H}\,b$, siis $ab\,\mathcal{L}\,b$. Lause 6.21 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 $x\,\mathcal{L}\,ab$, 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

$$avy = avabt = abt = y. \tag{6.2}$$

Kuna $\mathcal{R}$ on vasakpoolne kongruents, siis $vy\,\mathcal{R}\,vab = b$. Et $avy = y$, siis $vy\,\mathcal{L}\,y$. Kuna $y\,\mathcal{L}\,b$, 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 6.31 *Poolrühm S on rühm parajasti siis, kui $aS = S$ ja $Sa = S$ iga $a \in S$ korral.*

TÕESTUS. Tarvilikkus on ilmne.

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. □

Lause 6.32 *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 alamrühm.*

TÕESTUS. 1. $\Rightarrow$ 2. See on ilmne.

2. $\Rightarrow$ 3. Olgu $a, b \in H$ sellised, et $ab \in H$. Lemma 6.30 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 $c \in H = H_a$ korral $a\,\mathcal{H}\,ac$. Lemmaga 6.30 duaalne tulemus ütleb, et ka

$$H \to H, \quad x \mapsto xc$$

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. 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 ja

$$H \to H, \quad x \mapsto cx$$

on bijektiivne kujutus. Kokkuvõttes $cH = H = Hc$ iga $c \in H$ korral. Lemma 6.31 kohaselt on H rühm, sest me oleme juba näidanud, et H on S alampoolrühm, järelikult ka ise poolrühm. □

Lause 6.33 *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 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 $S^1aS^1 = S$ 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 6.29 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 6.27 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 6.32 on H_a rühm. □

Järgnev lause annab piisava tingimuse selleks, et poolrühm oleks täiesti lihtne.

Lause 6.34 *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 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 $RLa = RL = aRL$. Lause 6.29 tõestuses nägime, et La on minimaalne vasakpoolne ideaal. Samas $La \subseteq L$, kuna $a \in RL \subseteq L$. Siit $La = L$ ja sellest järeldub $RLa = RL$. 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 6.28 põhjal $R = eS$ ning $L = Se$. Lause 6.17 tõttu

$$eSe = eS^2e = (eS)(Se) = RL$$

ning $f = efe \in RL$. Kuna rühmas leidub täpselt üks idempotent, siis $e = f$. Seega e on ainuke primitiivne idempotent rühmas RL. □

Käesoleva paragrahvi põhitulemus on järgmine teoreem.

Teoreem 6.35 *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. järeldub lausest 6.33, 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 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 alamrühma G, mille ühikelement olgu e. Selles alamrühmas 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 6.34. □

Järeldus 6.36 *Lõplik poolrühm on täiesti lihtne parajasti siis, kui ta on lihtne.*

Tõestus. Lõplik poolrühm peab sisaldama minimaalset vasakpoolset ideaali. □

6.5 Reesi maatrikspoolrühmad

Osutub, et täiesti lihtsad poolrühmad on võimalik saada suhteliselt lihtsa konstruktsiooni abil rühmadest. Seda konstruktsiooni kirjeldas esimesena briti matemaatik David Rees.

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 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.

Lemma 6.37 *S on poolrühm.*

Tõestus. Kontrollime kas hulgal S defineeritud korrutamine on assotsiatiivne. Näitame, et

$$((i, g, \lambda)(i', g', \lambda'))(i'', g'', \lambda'') = (i, g, \lambda)((i', g', \lambda')(i'', g'', \lambda'')).$$

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.

Lause 6.38 *Poolrühm $\mathcal{M} = \mathcal{M}[G; I, \Lambda; P]$ on täiesti lihtne.*

Tõestus. Kontrollimaks, et poolrühm $\mathcal{M}$ on lihtne, võib tähele panna, et iga kahe elemendi (i, a, λ) ja (j, b, μ) korral, mis kuuluvad poolrühma $\mathcal{M}$, saab valida $v \in \Lambda$ ja $k \in I$ nii, et

$$(j, a^{-1}p_{vi}^{-1}, v)(i, a, \lambda)(k, p_{\lambda k}^{-1}b, \mu) = (j, a^{-1}p_{vi}^{-1}p_{vi}ap_{\lambda k}p_{\lambda k}^{-1}b, \mu) = (j, b, \mu).$$

Lause 6.15 põhjal on poolrühm $\mathcal{M}$ lihtne.

Näitame, et S 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

$$E(\mathcal{M}) = \{(i, p_{\lambda i}^{-1}, \lambda) \mid i \in I, \lambda \in \Lambda\}.$$

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 6.39 (Reesi teoreem) *Poolrühm on täiesti lihtne siis ja ainult siis, kui ta on isomorfne Reesi maatrikspoolrühmaga üle rühma.*

Tõestus. **Piisavus**. Järeldub lausest 6.38.
Tarvilikkus. Seda tõestust me käesolevas kursuses anda ei jõua. □

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 Mittetühja 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.

Näide 7.2 1. Olgu $(R, +, \cdot)$ ring. Siis iga parempoolne R-moodul on polügoon üle 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. Defineerides toime võrdusega

$$af := f(a)$$

$a \in A$, $f \in \mathcal{T}$, saame parempoolse polügooni.

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 pärit vektoreid nii, et tulemuseks on punkt. See polügoon on üle vektoruumi aditiivse monoidi.

Definitsioon 7.3 Mittetühja 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.

Definitsioon 7.5 Polügooni nimetatakse **lahutumatuks**, kui teda ei saa esitada kahe lõikumatu alampolügooni ühendina.

Näide 7.6 Olgu $s \in S$. Näitame, et sS on lahutumatu polügoon. Oletame vastuvïteliselt, et $sS = C_S \sqcup D_S$, kus C_S ja D_S on alampolügoonid. Oletame, et $s \in C_S$. Siis $sS \subseteq C$ ja seega $C_S \sqcup D_S = sS \subseteq C_S$, kust $D_S \subseteq C_S$, vastuolu.

Lause 7.7 *Iga polügoon on esitatav lahutumatute alampolügoonide lõikumatu ühendina.*

TÕESTUS. Vaatleme polügooni A_S. Defineerime hulgal A binaaarse 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

$$\begin{array}{rcl} a & = & b_1 s_1 \\ b_1 t_1 & = & b_2 s_2 \\ b_2 t_2 & = & b_3 s_3 \\ & \ldots & \\ b_n t_n & = & b. \end{array} \tag{7.1}$$

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

$$\begin{array}{rcl} as & = & b_1 s_1 s \\ b_1 t_1 s & = & b_2 s_2 s \\ b_2 t_2 s & = & b_3 s_3 s \\ & \ldots & \\ b_n t_n s & = & bs, \end{array}$$

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

$$[a]_\rho = C_S \sqcup D_S.$$

Valime mingid $c \in C$ ja $d \in D$. Siis $c\rho a\rho d$ ja seega $c\rho d$. Järelikult leiduvad sellised $b_1, \ldots, b_n \in A$ ja $s_1, \ldots, s_n, t_1, \ldots, t_n \in S$, et

$$\begin{array}{rcl} c & = & b_1 s_1 \\ b_1 t_1 & = & b_2 s_2 \\ b_2 t_2 & = & b_3 s_3 \\ & \ldots & \\ b_n t_n & = & d. \end{array}$$

Siit näeme, et

$$a\rho c\rho b_1\rho b_2\rho\ldots\rho b_n\rho d.$$

Järelikult $b_1,\ldots,b_n,d\in C\sqcup D$. Kui $b_1\in D$, siis $c=b_1s_1\in C\cap D$, mis on vastuolus eeldusega, et $C\cap D=\emptyset$. Seega $b_1\in C$. Analoogiliselt näeme, et ka $b_2,\ldots,b_n,d\in C$. Viimane ($d\in C$) on aga vastuolus d valikuga. □

7.2 Vabad polügoonid

Definitsioon 7.8 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 7.9 Ütleme, et polügoon B_S on polügooni A_S **epimorfne kujutis**, kui leidub sürjektiivne homomorfism $f:A_S\to B_S$.

Definitsioon 7.10 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 7.11 Polügooni nimetatakse **vabaks**, kui temas leidub baas.

Näide 7.12 Polügoon S_S on vaba, tema baas on $\{1\}$.

Teoreem 7.13 *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. Siis $F=\bigcup_{x\in X}xS$. Kui $x\neq y$, siis $xS\cap yS=\emptyset$, sest vastasel korral $xs=yt$ mingite $s,t\in S$ korral, mis on vastuolus baasi definitsiooniga. Seega

$$F=\bigsqcup_{x\in X}xS.$$

Kujutus $f:S\to xS, s\mapsto xs$ on ilmselt 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 $f_i:S_S\to F_i$ isomorfismid, $i\in I$. Tähistame $x_i:=f_i(1)\in F_i$. Siis iga $a\in F$ korral leiduvad $i\in I$ ja $s\in S$ nii, et

$$a=f_i(s)=f_i(1)s=x_is.$$

Kui $a=x_is=x_jt$, kus $i,j\in I$, $s,t\in S$, siis lõikumatuse tõttu $i=j$. Kuna $f_i(s)=x_is=x_it=f_i(t)$, siis f_i injektiivsuse tõttu $s=t$. Seega iga $a\in F$ esitub üheselt kujul $a=x_is$, kus $i\in I$ ja $s\in S$. See tähendab, et $\{x_i\mid i\in I\}$ on polügooni F_S baas. □

Lause 7.14 *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 7.13 põhjal. Defineerime kujutuse $f : F \to A$ võrdusega

$$f(a, s) := as.$$

See kujutus on homomorfism, sest

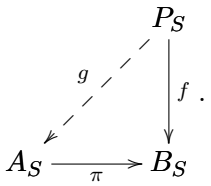
$$f((a, s)t) = f(a, st) = a(st) = (as)t = f(a, s)t$$

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. □

7.3 Projektiivsed polügoonid

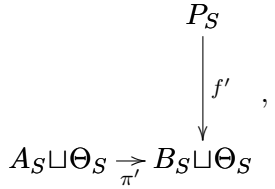
Projektiivsuse mõiste on duaalne injektiivsuse mõistega.

Definitsioon 7.15 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:



Lause 7.16 *Olgu polügoon P_S oma 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.*

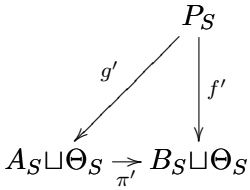
TÕESTUS. TARVILIKKUS. Olgu P_S projektiivne ning $j \in J$. Näitame, et P_j on projektiivne. Olgu $f : P_j \to B_S$ homomorfism ja $\pi : A_S \to B_S$ sürjektiivne homomorfism. Vaatleme diagrammi



kus $\Theta_S = \{\theta\}$ on üheelemendiline polügoon,

$$\pi'(x) = \begin{cases} \pi(x), & \text{kui } x \in A, \\ \theta, & \text{kui } x = \theta, \end{cases}$$
$$f'(y) = \begin{cases} f(y), & \text{kui } y \in P_j, \\ \theta, & \text{kui } y \in P \setminus P_j. \end{cases}$$

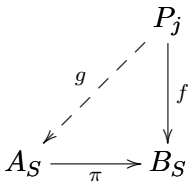
Lihnte on aru saada, et π' ja f' on homomorfismid ning π' on sürjektiivne. Kuna P_S on projektiivne, siis leidub homomorfism $g' : P_S \to A_S \sqcup \Theta_S$ nii, et $\pi' g' = f'$.



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.

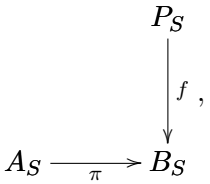


Iga $y \in P_j$ korral

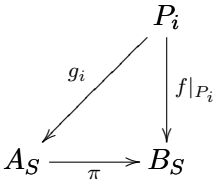
$$(\pi g)(y) = \pi(g'(y)) = \pi'(g'(y)) = f'(y) = f(y).$$

Järelikult $\pi g = f$.

Piisavus. Eeldame, et polügoonid 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



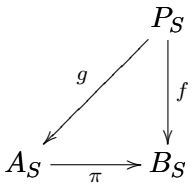
on kommutatiivne. Defineerime kujutuse $g : P \to A$ võrdusega

$$g(x) := g_i(x),$$

kus $x \in P_i$. 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. □

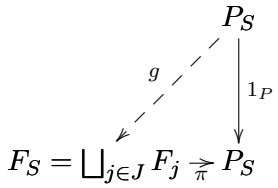
Teoreem 7.17 *Polügoon P_S on projektiivne parajasti siis, kui*

$$P = \bigsqcup_{i \in I} P_i,$$

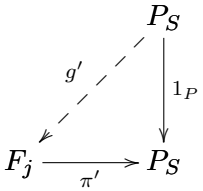
kusjuures iga $i \in I$ korral leidub idempotent $e_i \in S$ nii, et $P_i \cong e_i S$.

Tõestus. Tarvilikkus. Olgu A_S projektiivne polügoon. Kasutades lauset 7.7 saab polügooni A_S esitada lahutumatute alampolügoonide A_i, $i \in I$, lõikumatu ühendina. Vastavalt lausele 7.16 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 7.14 on P_S mingi vaba polügooni F_S epimorfne kujutis. Kasutades teoreemi 7.13 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 $1_P = \pi g$.



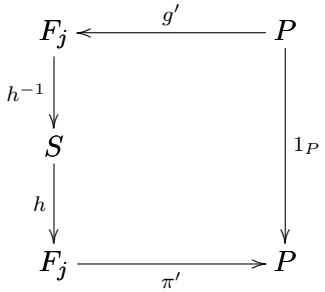
Kuna P_S on lahutumatu, siis leidub mingi $j \in J$ nii, et $g(P) \subseteq F_j$. Siis ka diagramm



on kommutatiivne, kus $g'(x) = g(x)$ iga $x \in P$ korral ja $\pi' = \pi|_{F_j}$. 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

$$\begin{aligned} e &= (h^{-1}g')(a) = (h^{-1}g'\pi' h)(e) = (h^{-1}g'\pi' h)(1e) = ((h^{-1}g'\pi' h)(1))e \\ &= ((h^{-1}g')((\pi' h)(1)))(e) = ((h^{-1}g')(a))e = ee = e^2. \end{aligned}$$

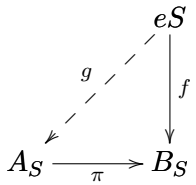
Võrdusest $\pi' g' = 1_P$ järeldub, et g' on üksühene ja seega ka $h^{-1}g' : P \to S$ on üksühene. Kuna

$$(h^{-1}g')(P) = (h^{-1}g')(aS) = ((h^{-1}g')(a))S = eS,$$

siis $eS = \mathrm{Im}\,(h^{-1}g')$ ja $eS \cong P_S$.

Piisavus. Arvestades lauset 7.16 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 7.18 *Vaba polügoon on projektiivne.*

Peatükk 8

Võred

8.1 Kaks vaatenurka võredele

Definitsioon 8.1 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 8.2 Võre on järjestatud hulk, mille igal kahel elemendil leidub ülemine ja alumine raja.

Näide 8.3

1. Hulga A kõigi alamhulkade hulk $\mathcal{P}(A)$ koos sisalduvusseosega $\subseteq$ on võre. Selles võres A alamhulkade X ja Y alumiseks rajaks on $X \cap Y$ ja ülemiseks rajaks on $X \cup Y$.
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 $a \vee b = \max a, b$.
3. Vektorruumi V kõigi alamruumide hulk $\mathcal{A}(V)$ on võre, kus alamruumide V_1 ja V_2 alumine raja on $V_1 \cup V_2$ ja ülemine raja on $V_1 + V_2$.

Definitsioon 8.4 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

$$\begin{array}{rclcrcl} (a+b)+c & = & a+(b+c) & \qquad & (ab)c & = & a(bc) \quad \text{(assotsiatiivsus)} \\ a+b & = & b+a & & ab & = & ba \quad \text{(kommutatiivsus)} \\ a+a & = & a & & aa & = & a \quad \text{(idempotentsus)} \\ (a+b)a & = & a & & ab+a & = & a \quad \text{(neelduvus).} \end{array}$$

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 8.5 *Olgu $(L, +, \cdot)$ võre definitsiooni 8.4 mõttes. Siis mistahes $a, b \in L$ korral*

$$a = ab \iff b = a + b.$$

Tõestus. Tarvilikkus. Kui $a = ab$, siis neelduvuse tõttu $a + b = ab + b = b$.
Piisavus. Kui $b = a + b$, siis $ab = a(a + b) = a$. □

Teoreem 8.6 *1. Kui $(L, \leq)$ on võre, definitsiooni 8.2 mõttes ja defineerime*

$$a + b := a \vee b,$$
$$ab := a \wedge b,$$

siis $(L, +, \cdot)$ on võre definitsiooni 8.4 mõttes.

2. Kui $(L, +, \cdot)$ on võre, definitsiooni 8.4 mõttes ja defineerime

$$a \leq b \Longleftrightarrow a = ab,$$

siis $(L, \leq)$ on võre definitsiooni 8.2 mõttes. Selles võres

$$a \leq b \implies ac \leq bc \quad ja \quad a + c \leq b + c \tag{8.1}$$

mistahes $a, b, c \in L$ korral.

Tõestus. 1. Näitame, et kehtivad definitsiooni 8.4 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. 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 $a = (a \wedge b) \vee a$.

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 $b = a + b$, saab tõestada, et $a \vee b = a + b$.

Tõestuse lõpetamiseks näitame, et kehtib implikatsioon (8.1). 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 $a + c \leq b + c$. □

8.2 Täielikud võred

Definitsioon 8.7 Osaliselt järjestatud hulka L nimetatakse **täielikuks võreks**, kui selle mistahes alamhulgal on olemas nii ülemine kui alumine raja.

Märgime, et definitsiooni järgi peavad eksisteerima ka $1 := \bigcup L$ ja $0 := \bigcap L$, mis osutuvad täieliku võre suurimaks ja vähimaks elemendiks.

Näide 8.8 1. Kõik lõplikud võred on täielikud.

2. Hulga X alamhulkade võre $(\mathcal{P}(X), \cap, \cup)$ on täielik.

3. Naturaalarvude hulk SÜT ja VÜK võtmise suhtes on täielik võre.

4. Reaalarvude järjestatud hulk $[0, 1]$ on täielik võre.

5. Rühma alamrühmade hulk $\cap$ ja $\langle - \rangle$ suhtes, ringi ideaalide ja mooduli alammoodulite hulgad $\cap$ ja $+$ suhtes on täielikud võred.

6. Topoloogia (lahtiste hulkade hulk) $\bigcup$ ja $(\cap)^\circ$ suhtes, kus $^\circ$ tähistab sisepunktide hulga võtmist.

7. Reaalarvude hulk hariliku järjestuse suhtes ei ole täielik.

Teoreem 8.9 *Täieliku võre L ja mistahes järjestust säilitava teisenduse $f : L \to L$ korral leidub element $x_0 \in L$ nii, et $f(x_0) = x_0$. Elementi x_0 nimetatakse sel juhul teisenduse f* ***püsipunktiks****.*

Tõestus. Vaatleme hulka $P = \{x \in L \mid x \leq f(x)\}$. Olgu $x_0 = \bigvee P$. Siis f säilitab järjestuse $x \leq x_0$, st $f(x) \leq f(x_0)$, kust $x \leq f(x_0)$ iga $x \in P$ korral. Ülemise raja definitsiooni kohaselt nüüd $x_0 \leq f(x_0)$ ja veel kord kujutust f rakendades ka $f(x_0) \leq f(f(x_0))$. Seega $f(x_0) \in P$ ja kokkuvõttes $f(x_0) \leq \bigvee P = x_0 \leq f(x_0)$ ehk $f(x_0) = x_0$. □

8.3 Modulaarsed võred

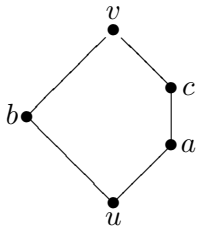
Definitsioon 8.10 Võret L nimetatakse **modulaarseks**, kui mistahes $a, b, c \in L$ korral

$$a \leq c \Longrightarrow (a + b)c = a + bc.$$

Näide 8.11 1. Vektorruumi V kõigi alamruumid võre $(\mathcal{V}, +, \cap)$ on modulaarne.

2. Rühma normaaljagajate võre on $(\mathcal{N}, \cdot, \cap)$ modulaarne.

3. 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.

Teoreem 8.12 *Võre L jaoks on järgmised väited samaväärsed.*

1. *L on modulaarne.*
2. *Mistahes $a, b, c \in L$ korral*
$$(ab + c)a = ab + ca.$$
3. *Kui $a, b, c \in L$, $a \geq b$, $a + c = b + c$ ja $ac = bc$, siis $a = b$.*
4. *L ei sisalda võrega N_5 isomorfset alamvõret.*

TÕESTUS. 1. $\Rightarrow$ 2. Olgu $a, b, c \in L$. Siis $ab \leq a$ ja modulaarsuse tõttu $(ab + c)a = ab + ca$.

2. $\Rightarrow$ 1. Olgu $a, b, c \in L$ ja $a \leq c$. Siis $a = ac$ ja
$$(a + b)c = (ac + b)c = ac + bc = a + bc.$$

1. $\Rightarrow$ 3. Olgu $a, b, c \in L$, $a \geq b$, $a + c = b + c$ ja $ac = bc$. Siis
$$a = a(a + c) = a(b + c) = b + ac = b + bc = b.$$

3. $\Rightarrow$ 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
$$(a + bc) + b = a + (bc + b) = a + b,$$
$$(a + b)cb = (a + b)bc = ((a + b)b)c = bc.$$

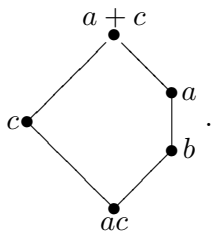
Seega
$$(a + b)c + b = (a + bc) + b,$$
$$(a + bc)b = (a + b)cb.$$

Kuna $a \leq c$, $a \leq a + b$ ja $b \leq b + c$, siis $a \leq (a + b)c$ ning $bc \leq (a + b)c$. Järelikult
$$a + bc \leq c + bc = c \leq (a + b)c.$$

Kasutades nüüd tingimust 3 saame järeldada, et $(a + b)c = a + bc$.

1. $\Rightarrow$ 4. Kui võre L sisaldaks võrega N_5 isomorfset alamvõret, siis ta ei saaks olla modulaarne.

4. $\Rightarrow$ 3. 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 tuleks vaadelda erinevaid juhtumeid.

- Eelduse põhjal $a \neq b$.
- Oletame, et $a = c$. Siis $c = cc = ac = bc$, kust $c \leq b$ ehk $a \leq b$, mis on vastuolus võrratusega $a > b$.
- 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 $a \leq c$, vastuolu.
- Ka ülejäänud juhtudel tekib vastuolu. Jätame selle läbimõtlemiseks lugejale.

□

8.4 Distributiivsed võred

Definitsioon 8.13 Võret L nimetatakse **distributiivseks**, kui mistahes $a, b, c \in L$ korral

$$(a + b)c = ac + bc.$$

Lemma 8.14 *Iga distributiivne võre on modulaarne.*

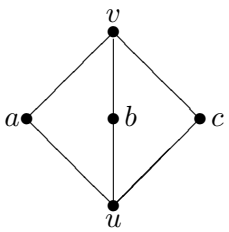
Tõestus. Olgu L distributiivne võre ja $a \leq c$, $a, b, c \in L$. Siis

$$(a + b)c = ac + bc = a + bc.$$

□

Näide 8.15 1. Hulga X alamhulkade võre $(\mathcal{P}(X), \cap, \cup)$ on distributiivne.

2. Naturaalarvude hulk suurima ühisteguri ja vähima ühiskordse võtmise suhtes on distributiivne võre.
3. Ahelad on distributiivsed võred.
4. Boole'i algebrad (täienditega distributiivsed võred) ja Heytingi algebrad (suurima ja vähima elemendiga võred, milles on defineeritud lisatehe "implikatsioon") on distributiivsed võred.
5. Võre



ei ole distributiivne, sest

$$(a+b)c = vc = c \neq u = u+u = ac+bc.$$

Seda võret tähistatakse lühidalt sümboliga M_3.

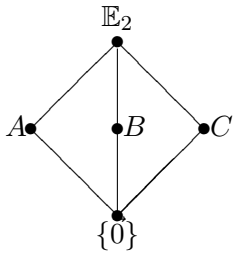
6. Vektorruumi V alamruumide võre $(\mathcal{A}(V), \cap, +)$ ei ole üldjuhul distributiivne. Vaatleme näiteks tasandi vabavektorite vektorruumis $\mathbb{E}_2$ kolme mittekollineaarset vektorit $\vec{a}, \vec{b}, \vec{c}$ ja nende poolt tekitatud alamruume A, B, C. Siis

$$A \cap B = A \cap C = B \cap C = \{\vec{0}\}$$

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.

Distributiivsete võrede kirjeldus on mingis mõttes sarnane modulaarsete võrede kirjeldusega.

Teoreem 8.16 *Võre L jaoks on järgmised väited samaväärsed.*

1. *L on distributiivne.*
2. *Mistahes $a, b, c \in L$ korral*
$$ab + c = (a+c)(b+c).$$
3. *Mistahes $a, b, c \in L$ korral*
$$ab + bc + ca = (a+b)(b+c)(c+a).$$
4. *Kui $a, b, c \in L$, $a + c = b + c$ ja $ac = bc$, siis $a = b$.*
5. *L ei sisalda võredega N_5 ja M_3 isomorfseid alamvõresid.*

Selle ja järgmise teoreemi tõestust me käesolevas kursuses anda ei jõua.

Teoreem 8.17 *Võre on distributiivne parajasti siis, kui ta on isomorfne mingi hulga X kõigi alamhulkada võre $(\mathcal{P}(X), \cap, \cup)$ mingi alamvõrega.*

Peatükk 9

Universaalalgberad ja nende muutkonnad

9.1 Universaalalgberad

Definitsioon 9.1 **Universaalalgebraks** nimetatakse kolmikut (A, Ω, ψ), kus A on mittetühi 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 **universumiks**. Universaalalgebrat ennast tähistatakse tavaliselt sümboliga $\mathbf{A}$, et teda oma kandjast eristada. 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 9.2 Mõned näited eri tüüpi algebratest:

1. Iga mittetühi hulk on algebra signatuuriga $\Omega = \emptyset$.
2. Rühmoidid (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).

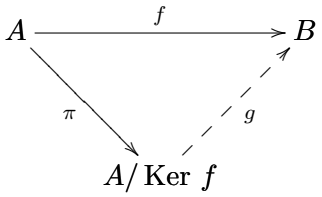
Universaalalgebrate alamalgebrad, homomorfismid, isomorfismid, kongruentsid, faktoralgebrad ja korrutised on 1. peatükis juba sisuliselt defineeritud (vt definitsioone 1.5, 1.10, 1.18, 1.25, lausele 1.26 järgnevat ja lausele 1.50 eelnevat lõiku). Defineerime üldisemal kujul homomorfismi tuuma mõiste:

Definitsioon 9.3 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 1.33 ja järelduse 1.34 analoogid, mille tõestus on praktiliselt sama.

Teoreem 9.4 (Homomorfismiteoreem) *Olgu $f : \mathbf{A} \to \mathbf{B}$ sama tüüpi algebrate homomorfism. Siis leidub üksühene homomorfism $g : \mathbf{A}/\mathbf{Ker\,f} \to \mathbf{B}$ nii, et $f = g\pi$, kus $\pi : \mathbf{A} \to \mathbf{A}/\mathbf{Ker\,f}$ on loomulik projektsioon.*



Järeldus 9.5 *Kui homomorfism $f : \mathbf{A} \to \mathbf{B}$ on sürjektiivne, siis $\mathbf{A}/\mathbf{Ker\,f} \cong \mathbf{B}$.*

Olgu algebra $\mathbf{A}$ selline, et tema alamalgebrate ühisosa ei ole kunagi tühi (näiteks Abeli rühmade korral sisaldab see ühisosa alati nullelementi). Sel juhul on algebra $\mathbf{A}$ kõigi **alamalgebrate** hulk $\mathcal{A}(\mathbf{A})$ **võre**, kus alumiseks rajaks on ühisosa võtmine ja ülemiseks rajaks on vähima mõlemat alamalgebrat sisaldava alamalgebra leidmine. Teatud juhtudel saab võre $\mathcal{A}(\mathbf{A})$ struktuurist välja lugeda informatsiooni algebra $\mathbf{A}$ omaduste kohta.

Mistahes algebra kõigi **kongruentside** hulk $\operatorname{Con}(A)$ on samuti **võre**. Kongruentside ρ ja τ alumine raja $\rho \wedge \tau$ defineeritakse seosega

$$a\ (\rho \wedge \tau)\ a' \iff (a\ \rho\ a') \wedge (a\ \tau\ a')$$

ning ülemine raja $\rho \vee \tau$ seosega

$$a\ (\rho \vee \tau)\ a' \iff \exists a_1, \ldots, a_m \in A : (a\ \rho\ a_1) \wedge (a_1\ \tau\ a_2) \wedge \ldots \wedge (a_{n-1}\ \tau\ a_n) \wedge (a_n\ \tau\ a'),$$

mistahes $a, a' \in A$ jaoks. Neile tehetele vastav järjestusseos $\leq$ hulgal $\operatorname{Con}(A)$ on $\subseteq$ ehk

$$\rho \leq \tau \iff (\forall a, a' \in A)(a\ \rho\ a' \Rightarrow a\ \tau\ a').$$

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.

9.2 Muutkonnad

Olgu $\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$ signatuur ja X mittetühi hulk.

Definitsioon 9.6 (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. Kõigi (Ω, X)-termide hulka tähistame sümboliga $F(X)$ (kasutusel on ka $T(X)$ ja $T(\Omega, X)$). Kui $F(X) \neq \emptyset$, siis saab selle muuta algebraks signatuuriga Ω, 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 $t_1, \ldots, t \in F(X)$ korral võtta

$$\omega^{F(X)}(t_1, \ldots, t_n) = \omega(t_1, \ldots, t_n) \in F(X).$$

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 9.7 Olgu Ω ühikuga ringi signatuur, st $\Omega = \{0,1\} \cup \{\text{-}\} \cup \{+, \cdot\}$, 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 formaalselt erinevad.

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 $X \setminus \{(x_1, \ldots, x_n\}$ termis t kindlasti ei esine. Tähed $x_1, \ldots, x_n$ võivad, aga ei pea seal esinema. Näiteks saame 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 $\Omega_0 \neq \emptyset$.

Seame nüüd igale n-aarsele termile vastavusse teatud n-aarse funktsiooni kõigil sama signatuuriga algebratel $\mathbf{A}$. Kuna termid defineeriti induktiivselt, tuleb siin samamoodi teha.

Definitsioon 9.8 Kui $t = t(x_1, \ldots, x_n) \in F(X) = T(\Omega, X)$ ja $\mathbf{A}$ on algebra signatuuriga Ω, siis n-aarne funktsioon $t^A : A^n \to A$ defineeritakse järgmiselt:

1. kui $t \in \Omega_0$, siis mistahes $a_1, \ldots, a_n \in A$ korral $t^A(a_1, \ldots, a_n) = t^A$, kus t^A on nullaarse tehte t 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, st

$$t^A(a_1, \ldots, a_n) = a_i,$$

3. kui $t = \omega(t_1, \ldots, t_s) \in X$ on m-astme term, st $t_1, \ldots, t_s$ on ülimalt $(m-1)$ astme termid ja $\omega \in \Omega_s$, siis mistahes $a_1, \ldots, a_n \in A$ korral

$$t^A(a_1, \ldots, a_n) = \omega^A(t_1^A(a_1, \ldots, a_n), \ldots, t_s^A(a_1, \ldots, a_n)).$$

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 9.9 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. Termfunktsioonide hulk on kinnine (mitmemuutuja) funktsioonide kompositsiooni suhtes.

Lause 9.10 *Iga algebra on mõne sama tüüpi absoluutselt vaba algebra faktoralgebra.*

TÕESTUS. Olgu $\mathbf{A}$ algebra signatuuriga Ω ja $\mathbf{F}(\mathbf{A})$ sama signatuuriga absoluutselt vaba algebra baasiga A. Defineerime kujutuse $f : F(A) \to A$ järgmiselt: kui $t = t(a_1, \ldots, a_n) \in F(A)$, siis

$$f(t(a_1, \ldots, a_n)) = t^A(a_1, \ldots, a_n).$$

Ilmselt on tegu sürjektsiooniga, sest iga $a \in A$ korral projektsioonid $a(a) \in F(A)$ ja $a^A(a) = a$. Näitame, et kujutus f on homomorfism. Esiteks, iga $w \in \Omega_0$ korral $w^{F(A)} = w$ ja

$$f(w^{F(A)}) = f(w) = w^A.$$

Olgu nüüd $n \in \mathbb{N}$, $w \in \Omega_n$ ja $t_1, \ldots, t_n \in F(A)$. Eelneva kokkuleppe kohaselt võib termi aarsust alati suurendada, seega olgu $\{a_1, \ldots, a_s\}$ kõik tähed, mis esinevad vähemalt ühes termidest $t_1, \ldots, t_n$. Siis saame kirjutada, et $t_i = t_i(a_1, \ldots, a_s)$, $i = 1, \ldots, n$, ja järelikult

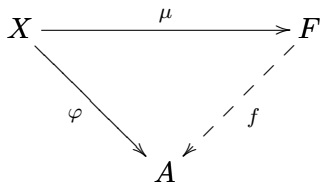
$$\begin{aligned} f(\omega^{F(A)}(t_1, \ldots, t_n)) &= f(\omega(t_1, \ldots, t_n)) = \omega^A(t_1^A(a_1, \ldots, a_n), \ldots, t_n^A(a_1, \ldots, a_n)) \\ &= \omega^A(f(t_1(a_1, \ldots, a_n)), \ldots, f(t_n(a_1, \ldots, a_n))). \end{aligned}$$

Järelduse 9.5 kohaselt $\mathbf{A} \cong \mathbf{F}(\mathbf{A})/\mathbf{Ker}\,\mathbf{f}$. □

Definitsioon 9.11 Olgu $\mathcal{K}$ sama tüüpi algebrate klass. Algebrat $\mathbf{F} \in \mathcal{K}$ nimetatakse klassi $\mathcal{K}$ **vabaks algebraks** baasiga X, kui

(i) leidub kujutus $\mu : X \to F$ nii, et $\mathrm{Im}\,(\mu)$ on algebra $\mathbf{F}$ moodustajate süsteem, st kõik hulga F elemendid on avaldatavad hulga $\mathrm{Im}\,(\mu)$ elementide kaudu, kasutades algebra $\mathbf{F}$ tehteid;

(ii) iga algebra $\mathbf{A} \in \mathcal{K}$ ja kujutuse $\varphi : X \to A$ korral leidub homomorfism $f : \mathbf{F} \to \mathbf{A}$ nii, et $\varphi = f\mu$.



Lause 9.12 *Absoluutselt vaba algebra signatuuriga Ω ja baasiga X on vaba algebra baasiga X kõigi nende algebrate klassis, mille signatuur on Ω.*

TÕESTUS. Kuna hulk $F(X)$ on defineeritud induktiivselt tehete $\omega \in \Omega_n$ rakendamisega tähtedele $x \in X$ ja konstantidele $\omega_0 \in \Omega_0$, siis vabaks algebraks oleku tingimus 1. on ilmselt täidetud, võttes kujutuseks μ sisestuse $X \hookrightarrow F(X)$. Tingimuse 2. rahuldamiseks sobib kujutus $f : F(X) \to A$, mis on defineeritud järgmiselt: kui $t = t(x_1, \ldots, x_n) \in F(X)$, siis

$$f(t(x_1, \ldots, x_n)) = t^A(\varphi(x_1), \ldots, \varphi(x_1)).$$

On selge, et mistahes $x \in X$ korral $(f\mu)(x) = f(x) = x^A(\varphi(x)) = \varphi(x)$. Kujutuse f homomorfismiks oleku kontroll on samasugune, nagu lauses 9.10. □

Lause 9.13 *Olgu algebrate klass $\mathcal{K}$ kinnine alamalgebrate ja otsekorrutiste võtmise suhtes, kusjuures vähemalt üks selle klassi algebra on vähemalt kaheelemendiline. Siis iga $X \neq \emptyset$ korral leidub klassis $\mathcal{K}$ vaba algebra baasiga X.*

TÕESTUS. Näitame esiteks, et kui $|X| > 1$ ja vaba algebra $\mathbf{F}$ baasiga X on tõepoolest olemas, siis definitsioonis 9.11 esinev kujutus μ peab olema injektiivne. Oletame vastuväiteliselt, et $\mu(x_1) = \mu(x_2)$ mingite tähtede $x_1 \neq x_2$ korral. Olgu $\mathbf{A} \in \mathcal{K}$ selline, et $|A| \geq 2$. Siis on võimalik defineerida kujutus $\varphi : X \to A$ nii, et $\varphi(x_1) \neq \varphi(x_2)$. Aga nüüd ei saa ühegi kujutuse $\psi : F \to A$ korral kehtida $\varphi = \psi\mu$, sest sel juhul

$$\varphi(x_1) = (\psi\mu)(x_1) = (\psi\mu)(x_2) = \varphi(x_2).$$

Vaatleme nüüd klassi $\mathcal{K}$ alamklassi, mille moodustavad kõikvõimalikud algebrad, millel on olemas moodustajate süsteem, mille võimsus on ülimalt $|X|$. Valime selle klassi kõigi isomorfsmiklasside seast välja ühe esindaja, st moodustame paarikaupa mitteisomorfsetest algebratest koosneva alamklassi $\mathcal{A} \subseteq \mathcal{K}$. Olgu iga $\mathbf{A} \in \mathcal{A}$ korral M_A selle moodustajate süsteem. Siis $|M_A| \leq |X|$ ja me saame leida sürjektiivse kujutuse $\iota_A : X \to M_A$. Kuna M_A on moodustajate süsteem, siis leidub mistahes $a \in A$ korral $t(x_1, \ldots, x_n) \in F(X)$ nii, et $a = t^A(a_1, \ldots, a_n)$, kus $a_1, \ldots, a_n \in M_A$. Lause 9.10 tõestuse põhjal on algebra $\mathbf{A}$ absoluutselt vaba algebra $\mathbf{F(X)}$ faktoralgebra. Tõepoolest, me võime muuta kujutuse $f : F(X) \to A$ definitsiooni järgmiseks:

$$f(t(x_1, \ldots, x_n)) = t^A(\iota_A(x_1), \ldots, \iota_A(x_n)).$$

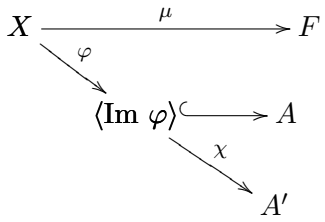
Kujutuse f sürjektiivsus järeldub ι_A sürjektiivsusest ja sellest, et M_A on moodustajate süsteem.

Eelneva põhjal saame öelda, et klassis $\mathcal{A}$ ei ole rohkem elemente, kui on olemas $\mathbf{F(X)}$ faktoralgebraid, st kongruentse hulgal $F(X)$. Kuna selliseid kongruentse ei ole rohkem, kui hulga $F(X) \times F(X)$ alamhulki, mis moodustavad hulga, siis on klass $\mathcal{A}$ tegelikult samuti hulk. Vaatleme nüüd kõikvõimalikke paare kujul $(\mathbf{A}_i, f_i : X \to A_i)$, kus $\mathbf{A}_i \in \mathcal{A}$, $i \in I$ (erinevate indeksitele i võib siin vastata üks ja sama algebra $\mathbf{A}$). Kuna $\mathcal{A}$ ja I on hulgad, siis korrutis $\mathfrak{A} := \prod_{i \in I} \mathbf{A}_i$

eksisteerib ja kuulub eelduse kohaselt klassi $\mathcal{K}$. Defineerime kujutuse $\mu : X \to \mathfrak{A}$ iga $x \in X$ korral seosega

$$(\mu(x))_i = f_i(x).$$

Olgu $\mathbf{F}$ vähim $\mathfrak{A}$ alamalgebra, mis sisaldab hulka $\operatorname{Im}\mu$, st $\mathbf{F} = \langle \operatorname{Im}\mu \rangle$. Kuna $\mathcal{K}$ on kinnine alamalgebrate võtmise suhtes, siis $\mathbf{F} \in \mathcal{K}$. Näitame, et $\mathbf{F}$ ongi otsitav vaba algebra. Kuna $\operatorname{Im}\mu$ on ilmselt $\mathbf{F}$ moodustajate süsteem, peame kontrollima ainult definitsiooni 2. tingimust.



Valime vabalt $\mathbf{A} \in \mathcal{K}$ ja $\varphi : X \to A$. Kuna $|\operatorname{Im}\varphi| \leq |X|$ ja otsekorrutis $\mathfrak{A}$ ammendab kõik paarid $(\mathcal{A}, f : X \to A)$, siis leidub selline $\mathbf{A}' = \mathbf{A}_{i_0} \in \mathcal{A}$, $i_0 \in I$, et $\langle \operatorname{Im}\varphi \rangle \cong \mathbf{A}'$. Veelgi enam, kui vastav isomorfism tähistada $\chi : \langle \operatorname{Im}\varphi \rangle \to \mathbf{A}'$, peab kehtima ka võrdus $\chi\varphi = f_{i_0}$. Võtame i_0-nda projektsiooni ahendi $\tau = \pi_{i_0}|_F : \mathbf{F} \to \mathbf{A}' = \mathbf{A}_{i_0}$ (meenutame, et $\mathbf{F} \subseteq \mathfrak{A} = \prod_{i \in I} \mathbf{A}_i$) ja paneme tähele, et $f_{i_0} = \tau\mu$. Ilmselt on $\psi = \chi^{-1}\tau : \mathbf{F} \to \langle \operatorname{Im}\varphi \rangle \leq \mathbf{A}$ homomorfism ja

$$\psi\mu = (\chi^{-1}\tau)\mu = \chi^{-1}f_{i_0} = \chi^{-1}(\chi\varphi) = \varphi.$$

□

Definitsioon 9.14 Olgu Ω signatuur ja $u, v \in F(X) = T(\Omega, X)$, kus $X = \{x_1, x_2, \ldots\}$ on loenduv hulk. Öeldakse, et algebral $\mathbf{A}$ signatuuriga Ω kehtib **samasus** $u = v$, kui neile vastavad termfunktsioonid on võrdsed, st $u^A = v^A$.

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 9.15 Signatuuriga Ω algebrate klassi $\mathcal{K}$ nimetatakse **muutkonnaks**, kui leidub selline samasuste hulk $S = \{u = v \mid u, v \in T(\Omega, X)\}$, kus X on loenduv hulk, 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 klassid ei ole (üldiselt) muutkonnad, 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 ole kõigi monoidide muutkonna alammuutkond signatuuris $\Omega' = \{1\} \cup \{\cdot\}$.

Lause 9.16 *Mistahes Ω-algebrate muutkondade hulga ühisosa on samuti Ω-algebrate muutkond.*

Tõestus. On lihtne tähele panna, et ühisosa koosneb täpselt neist algebratest, mis rahuldavad kõiki samasusi, mis kehtivad vähemalt ühes vaadeldavatest muutkondadest. □

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	$\Omega_1 = \{'\}$ $\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $xx'x = x$, $x'xx' = x'$
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	$\Omega_2 = \{\wedge, \vee\}$	$x_1 \vee (x_2 \vee x_3) = (x_1 \vee x_2) \vee x_3$ $x_1 \vee x_2 = x_2 \vee x_1$ $x_1 \vee x_1 = x_1$ $(x_1 \vee x_2) \wedge x_1 = x_1$ $x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3$ $x_1 \wedge x_2 = x_2 \wedge x_1$ $x_1 \wedge x_1 = x_1$ $(x_1 \wedge x_2) \vee x_1 = x_1$
Distributiivsed võred	$\Omega_2 = \{\wedge, \vee\}$	$x_1 \vee (x_2 \vee x_3) = (x_1 \vee x_2) \vee x_3$ $x_1 \vee x_2 = x_2 \vee x_1$ $x_1 \vee x_1 = x_1$ $(x_1 \vee x_2) \wedge x_1 = x_1$ $x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3$ $x_1 \wedge x_2 = x_2 \wedge x_1$ $x_1 \wedge x_1 = x_1$ $(x_1 \wedge x_2) \vee x_1 = x_1$ $(x_1 \vee x_2) \wedge x_3 = (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$
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	$\Omega_1 = \{r\cdot \mid r \in R\}$ $\Omega_2 = \{+\}$	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ $0 + x_1 = x_1, x_1 + 0 = x_1$ $x_1 + (-x_1) = 0$, $-x_1 + x_1 = 0$ $x_1 + x_2 = x_2 + x_1$ $r \cdot (x_1 + x_2) = r \cdot x_1 + r \cdot x_2$ ($\lvert S\rvert$ samasust) $(r + s) \cdot x_1 = r \cdot x_1 + s \cdot x_1$ ($\lvert S\rvert^2$ samasust) $r \cdot (s \cdot x_1) = (rs) \cdot x_1$ ($\lvert S\rvert^2$ samasust) $1 \cdot x_1 = x_1$
Üheelemendilised algebrad	Ω	$x_1 = x_2$
Kõik algebrad signatuuriga Ω	Ω	$x_1 = x_1$

Järeldus 9.17 *Iga Ω-algebrate klassi $\mathcal{K}$ jaoks leidub vähim klassi $\mathcal{K}$ sisaldav Ω-algebrate muutkond.*

TÕESTUS. Võtame kõigi klassi $\mathcal{K}$ sisaldavate muutkondade hulga ühisosa. Tegu on hulgaga, sest samasusi ei ole rohkem, kui absoluutselt vaba algebra võimsuse ruut. Eelneva lause põhjal on tegu muutkonnaga, mis ilmselt sisaldab klassi $\mathcal{K}$. Paneme siin tähele, et me ei võta ühisosa tühjast hulgast, sest vähemalt samasuse $x_1 = x_1$ abil defineeritud muutkond sisaldab klassi $\mathcal{K}$. □

Definitsioon 9.18 Eelnevas järelduses konstrueeritud muutkonda nimetatakse **klassi $\mathcal{K}$ poolt moodustatud muutkonnaks** ja tähistatakse $\mathrm{Var}(\mathcal{K})$. Kui $|\mathcal{K}| = 1$, st $\mathcal{K} = \{\mathbf{A}\}$, siis nimetatakse seda **algebra A poolt moodustatud muutkonnaks** ja tähistatakse $\mathrm{Var}(\mathbf{A})$.

Ei ole raske näha, et $\mathrm{Var}(\mathcal{K})$ koosneb täpselt kõigist neist Ω-algebratest, mis rahuldavad kõiki klassis $\mathcal{K}$ kehtivaid samasusi.

Järgmine teoreem on universaalalgebra üks olulisemaid tulemusi, mis ütleb, et muutkondi võib defineerida kahel viisil:

- samasuste abil,
- kinnisuse abil teatavate operatsioonide suhtes.

Märgime, et Ω-algebrate klassi nimetatakse **triviaalseks**, kui see koosneb ainult triviaalsetest, st üheelemendilistest algebratest.

Teoreem 9.19 (Birkhoff) *Mittetriviaalne Ω-algebrate klass on muutkond parajasti siis, kui see on kinnine alamalgebrate, homomorfsete kujutiste ja (mistahes võimsusega) otsekorrutiste võtmise suhtes.*

TÕESTUS. TARVILIKKUS. Olgu $\mathcal{K}$ muutkond definitsiooni 9.15 mõttes. On selge, et iga muutkonda $\mathcal{K}$ kuuluva algebra mistahes alamalgebra rahuldab samuti kõiki samasusi, mis kehtivad muutkonnas $\mathcal{K}$. Järelikult on klass $\mathcal{K}$ kinnine alamalgebrate võtmise suhtes.

Vaatleme järgmiseks suvalist sürjektiivset homomorfismi $f : \mathbf{A} \to \mathbf{B}$, kus $\mathbf{A} \in \mathcal{K}$. Olgu $u(x_1, \ldots, x_m) = v(x_1, \ldots, x_m)$ samasus algebral $\mathbf{A}$ ja $b_1, \ldots, b_m \in B$. Kujutuse f sürjektiivsuse tõttu leiduvad $a_1, \ldots, a_m \in A$ nii, et $f(a_i) = b_i$ iga $i = 1, \ldots, m$ korral. Seega $u(a_1, \ldots, a_m) = v(a_1, \ldots, a_m)$ ja kuna f on homomorfism, mis kommuteerub kõigi tehetaga ning termid u ja v on moodustatud induktiivselt signatuuri Ω kuuluvatest tehetest, siis

$$\begin{aligned} u^{\mathbf{B}}(b_1, \ldots, b_m) &= u^{\mathbf{B}}(f(a_1), \ldots, f(a_m)) = f(u^{\mathbf{A}}(a_1, \ldots, a_m)) = f(v^{\mathbf{A}}(a_1, \ldots, a_m)) \\ &= v^{\mathbf{B}}(f(a_1), \ldots, f(a_m)) = v^{\mathbf{B}}(b_1, \ldots, b_m). \end{aligned}$$

Oleme saanud, et klass $\mathcal{K}$ on kinnine homomorfsete kujutiste võtmise suhtes.

Olgu viimaks $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$, $\mathbf{A}_i \in \mathcal{K}$ ja kehtigu igal algebral $\mathbf{A}_i$ samasus $u(x_1, \ldots, x_m) = v(x_1, \ldots, x_m)$. Valime vabalt $({}_j a_i)_{i \in I} \in \mathbf{A}$, kus $j = 1, \ldots, m$. Kuna termid u ja v koosnevad järjestikustest tehetest, mis on korrutisel $\mathbf{A}$ defineeritud komponentide kaupa, siis

$$\begin{aligned} u^{\mathbf{A}}(({}_1 a_i)_{i \in I}, \ldots, ({}_m a_i)_{i \in I}) &= (u^{\mathbf{A}_i}({}_1 a_i, \ldots, {}_m a_i))_{i \in I} \\ &= (v^{\mathbf{A}_i}({}_1 a_i, \ldots, {}_m a_i))_{i \in I} = v^{\mathbf{A}}(({}_1 a_i)_{i \in I}, \ldots, ({}_m a_i)_{i \in I}). \end{aligned}$$

Järelikult kehtib samasus $u = v$ ka korrutisel $\mathbf{A}$ ja me olemegi näidanud, et klass $\mathcal{K}$ on kinnine ka suvaliste otsekorrutiste võtmise suhtes.

PIISAVUS. Selle teoreemi täielik tõestus ei mahu samuti käesolevasse kursusesse. □

Birkhoffi teoreemi kutsutakse operatsioonide nimede järgi mõnikord ka HSP-teoreemiks.

Peatükk 10

Kategooriad

10.1 Kategooria mõiste

10.1.1 Objektid ja morfismid

Definitsioon 10.1 **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: $\operatorname{dom} f$) ning objekti B kutsutakse f **sihtobjektiks** ehk kodomeeniks (tähistus: $\operatorname{cod} f$). 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 10.2 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 10.3 Kategooria on **väike** kui tema objektide klass on hulk, vastasel korral kutsutakse kategooriat **suureks**.

Näide 10.4 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	ühikelemendiga 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
0	ei ole	ei ole
1	A	1_A
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 **0** nimetatakse **tühjaks kategooriaks**.

Näide 10.5 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 $\mathcal{P}(x,y)$ koosneb täpselt ühest morfismist, kui $x \leqslant y$, ning on tühi vastasel juhul. (Tegelikult piisab 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.

10.1.2 Alam- ja korrutiskategooriad

Olemasolevatest kategooriatest saab teatud konstruktsioonide abil luua uusi.

Definitsioon 10.6 Kategooria $\mathcal{A}$ **alamkategooria** koosneb

1. kategooria $\mathcal{A}$ objektide klassi $\mathcal{A}_0$ alamklassist $\mathcal{B}_0$;
2. iga objektipaari $(B, B') \in \mathcal{B}_0^2$ 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 10.7 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 10.8 Kategooria Ab on kategooria Gr täielik alamkategooria, Gr on Mon täielik alamkategooria, Mon on poolrühmade kategooria Sgr alamkategooria, mis ei ole täielik. Kategooria Ban_∞ on $\mathsf{Vec}_\mathbb{R}$ alamkategooria, kuid mitte täielik alamkategooria.

Definitsioon 10.9 Kategooriate $\mathcal{A}$ ja $\mathcal{B}$ **korrutis** on kategooria $\mathcal{A} \times \mathcal{B}$, mis on defineeritud järgmiselt.

1. $(\mathcal{A} \times \mathcal{B})_0 = \mathcal{A}_0 \times \mathcal{B}_0$.
2. $(\mathcal{A} \times \mathcal{B})((A, B), (A', B')) = \{(a, b) \mid a \in \mathcal{A}(A, A'), b \in \mathcal{B}(B, B')\}$.
3. Kategooria $\mathcal{A} \times \mathcal{B}$ morfismide komponeerimine on indutseeritud $\mathcal{A}$ ja $\mathcal{B}$ komponeerimiste poolt, nimelt
$$(a', b')(a, b) = (a'a, b'b).$$

10.2 Morfismide liigid.

Nii nagu hulkade korral on tähtsal kohal üksühesed kujutused ja pealekujutused, nii ka kategooriates võib vaadelda teatud eriomadustega morfisme.

Definitsioon 10.10 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
$$fg = fh \quad \Rightarrow \quad g = h;$$
- **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 10.11 *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. Oletame, et $k : B \to D$ ja $f : A \to B$ on monomorfismid ja $(kf)g = (kf)h$, kus $g, h : C \to A$.

$$C \underset{h}{\overset{g}{\rightrightarrows}} A \xrightarrow{f} B \xrightarrow{k} D$$

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 $g = h$. 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, et ka f on koretraktsioon. □

Definitsioon 10.12 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 10.11 saab tõestada järgmise lause.

Lause 10.13 *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 10.14 Hulkade kategoorias Set on monomorfismideks parajasti injektiivsed kujutused ja epimorfismideks sürjektiivsed kujutused Veelgi enam, iga sürjektiivne kujutus on retraktsioon.

Näide 10.15 Kategooriates Gr ja Ab on monomorfismideks injektiivsed rühmade homomorfismid.

Definitsioon 10.16 Morfismi nimetatakse **bimorfismiks**, kui ta on nii monomorfism kui epimorfism, s.t. kui ta on taandatav.

Definitsioon 10.17 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 10.18 *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 10.11 ja lausest 10.13. □

Järeldus 10.19 *Objektide isomorfsusseos on ekvivalentsiseos.*

Lause 10.20 *Kui epimorfism on koretraktsioon, siis on ta isomorfism.*

TÕESTUS. Jätame lugejale läbimõtlemiseks. □

Näide 10.21 Kategoorias Set on isomorfismideks bijektiivsed kujutused.

Näide 10.22 Kategooriates Gr, Ab ja Rng on isomorfismideks bijektiivsed homomorfismid.

Näide 10.23 Kategoorias $\mathsf{Vec}_{\mathbb{R}}$ on isomorfismideks bijektiivsed lineaarkujutused.

Näide 10.24 Iga rühma võib vaadelda kui üheobjektilist kategooriat, kus kõik morfismid on isomorfismid.

Näide 10.25 Meenutame, et iga järjestatud hulka võib vaadelda kategooriana (näide 10.5). Sellises kategoorias on iga morfism bimorfism, sest mistahes kahe objekti vahel leidub ülimalt üks morfism. Isomorfismid on aga ainult ühikmorfismid.

10.3 Objektide liigid. Duaalsus

10.3.1 Objektide liigid

Definitsioon 10.26 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 10.27 *Kategooria mistahes kaks lõpp-(alg-, null-)objekti on isomorfsed.*

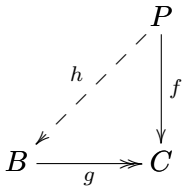
Tõestus. Kui $C, C' \in \mathcal{C}_0$ on lõppobjektid, siis $\mathcal{C}(C,C) = \{1_C\}$ ja $\mathcal{C}(C',C') = \{1_{C'}\}$. Samuti leiduvad morfismid $f : C \to C'$ ja $g : C' \to C$. Kuna $gf : C \to C$, siis $gf = 1_C$ ja samamoodi $fg = 1_{C'}$. Seega $C \cong C'$. Alg- ja nullobjektide jaoks on tõestus analoogiline. □

Näide 10.28 Kategoorias Set on tühi hulk algobjekt ja üheelemendilised hulgad on lõppobjektid. Sama kehtib kategooria Top korral.

Näide 10.29 Kategooriates Ab, $\mathsf{Vec}_{\mathbb{R}}$ ja Ban_1 on $\{0\}$ nii alg- kui ka lõppobjekt, seega nullobjekt.

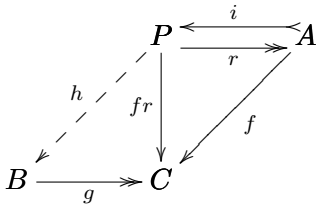
Näide 10.30 Ühikuga assotsiatiivsete ringide kategoorias Rng on $\{0\}$ lõppobjekt ja $\mathbb{Z}$ algobjekt.

Definitsioon 10.31 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 $gh = f$.



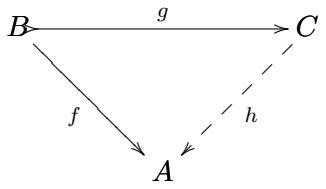
Lause 10.32 *Projektiivse objekti retrakt on projektiivne.*

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 10.10).



Kui $f : A \to C$, siis P projektiivsuse tõttu leidub selline $h : P \to B$, et $gh = fr$. Seega $ghi = fri = f$. □

Definitsioon 10.33 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 10.34 Kategooria Set iga objekt on projektiivne. Kasutades fakti, et iga epimorfism on retraktsioon kategoorias Set ja definitsiooni 10.31 tähistusi saame leida sellise $p : C \to B$, et $gp = 1_C$. Võttes $h := pf$ saame, et $gh = gpf = f$.

Näide 10.35 Lause 5.17 kohaselt on Abeli rühm on injektiivne parajasti siis, kui ta on jaguv.

Näide 10.36 Projektiivsed ja injektiivsed objektid mängivad tähtsat rolli moodulite teoorias (üle ringi). Teoreemi 5.13 põhjal on moodul projektiivne parajasti siis, kui ta on vaba mooduli otseliidetav.

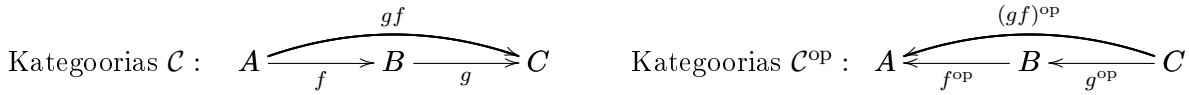
10.3.2 Duaalsus

Lihtsustatult tähendab kategoorne duaalsus "kõigi noolte ümberpööramist".

Definitsioon 10.37 Kategooria $\mathcal{C}$ **duaalne kategooria** $\mathcal{C}^{\mathrm{op}}$ defineeritakse järgmiselt.

1. Kategooriatel $\mathcal{C}$ ja $\mathcal{C}^{\mathrm{op}}$ on samad objektid, $\mathcal{C}_0^{\mathrm{op}} = \mathcal{C}_0$.
2. Iga $A, B \in \mathcal{C}_0^{\mathrm{op}}$ korral $\mathcal{C}^{\mathrm{op}}(A, B) = \mathcal{C}(B, A)$, s.t. $\mathcal{C}^{\mathrm{op}}$ morfismid on $\mathcal{C}$ morfismid, mida "kirjutatakse vastupidises suunas". Segaduse vältimiseks kirjutame $f^{\mathrm{op}} : A \to B$, kui vaatleme $\mathcal{C}$ morfismi $f : B \to A$ kui $\mathcal{C}^{\mathrm{op}}$ morfismi.
3. Komponeerimine kategoorias $\mathcal{C}^{\mathrm{op}}$ defineeritakse võrdusega

$$f^{\mathrm{op}} g^{\mathrm{op}} := (gf)^{\mathrm{op}}.$$



Iga kategooriate jaoks defineeritud mõiste jaoks leidub duaalne mõiste (mille nimi tekitatakse harilikult eesliite 'ko-' abil), mis saadakse definitsioonis kõigi morfismide suuna muutmisel vastupidiseks ja kompositsioonide fg asendamisel kompositsioonidega gf. Samuti on iga väite jaoks olemas duaalne väide.

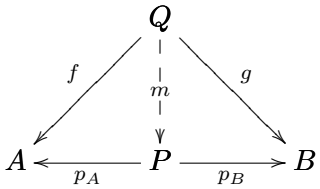
Duaalsusprintsiip ütleb, et kui mingi väide on tõene kõigis kategooriates, siis ka selle väite duaalne väide on tõene kõigis kategooriates.

Me näeme, et lõppobjektid on duaalsed algobjektidega, epimorfismid monomorfismidega, projektiivsus on injektiivsuse duaalne mõiste jne. Samuti näiteks, kui me teame, et lõppobjektid on igas kategoorias määratud üheselt isomorfismi täpsusega, siis duaalsusprintsiibi põhjal ka algobjektid on määratud üheselt isomorfismi täpsusega.

10.4 Korrutised ja kokorrutised

Hulkade otsekorrutise projektsioonide omadustest on motiveeritud järgmine üldine definitsioon.

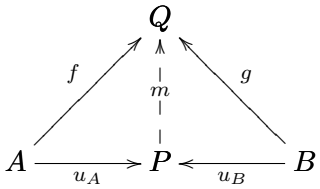
Definitsioon 10.38 Kategooria $\mathcal{C}$ objektide A, B **korrutis** on kolmik (P, p_A, p_B), kus $P \in \mathcal{C}_0$ ja $p_A : P \to A$, $p_B : P \to B$ on morfismid kategoorias $\mathcal{C}$ (mida nimetatakse **projektsioonideks**), mis rahuldavad tingimust, et kui $Q \in \mathcal{C}_0$ on objekt 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**. Morfismi m asemel kirjutatakse mõnikord $\langle f, g \rangle$.

Korrutise definitsiooni dualiseerimisel saadakse kokorrutise mõiste, mis üldistab hulkade lõikumatu ühendi konstruktsiooni.

Definitsioon 10.39 Kategooria $\mathcal{C}$ objektide A, B **kokorrutis** (ehk **summa**) on 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:



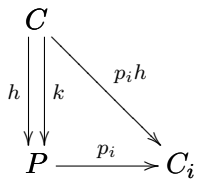
Harilikult kirjutatakse P asemel $A \coprod B$.

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 10.40 *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

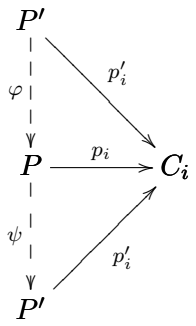


kommutatiivseks, seega peavad nad definitsiooni põhjal võrdsed olema. □

Lause 10.40 väidet võib sõnastada ka nii, et korrutise projektsioonid on korraga vasakult taandatavad. Selle kohta öeldakse ka, et projektsioonid moodustavad **monomorfse pere**.

Lause 10.41 *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 φ ja ψ, mis muudavad nii ülemise kui alumise kolmnurga diagrammis



kommutatiivseks iga $i\in I$ korral. Sellest, et

$$\begin{aligned} p'_i &= p_i\varphi = p'_i\psi\varphi, \\ p_i &= p'_i\psi = p_i\varphi\psi, \end{aligned}$$

iga $i\in I$ korral, järeldub lause 10.40 põhjal, et $\psi\varphi = 1_{P'}$ ja $\varphi\psi = 1_P$. Seega $P\cong P'$. □

Loomulikult kehtivad duaalsed väited kokorrutiste jaoks, muuseas moodustavad sisestused **epimorfse pere**.

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.

Lause 10.42 *Kui kategoorias $\mathcal{C}$ on binaarsed korrutised (kõigi objektipaaride jaoks), siis on temas ka ternaarsed korrutised. Veelgi enam, iga $A,B,C\in\mathcal{C}_0$ korral*

$$\begin{gathered} (A\times B)\times C\cong A\times(B\times C), \\ A\times B\cong B\times A, \end{gathered}$$

ja kui kategoorias $\mathcal{C}$ on lõppobjekt $\mathbf{1}$, siis

$$A\times\mathbf{1}\cong A,\quad \mathbf{1}\times A\cong A.$$

Tõestus. ... □

Eelmist tulemust üldistades saame, et kui kategoorias on binaarsed korrutised, siis on temas n objekti korrutised iga $n\geq 2$ korral. Samuti on lihtne näha, et tühja objektide süsteemi korrutis on lõppobjekt ja $(A,1_A)$ on ühestainsast objektist A koosneva süsteemi korrutis.

Lause 10.43 *Kategoorias on lõplikud korrutised parajasti siis, kui temas on binaarsed korrutised ja lõppobjekt.*

Toome mõned korrutiste näited.

Näide 10.44 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 10.45 Algebraliste struktuuride kategooriates (nt. rühmad, Abeli rühmad, ringid, moodulid, vektorruumid, Boole'i algebrad jne.) on objektide süsteemi korrutis nende otsekorrutis, mis on varustatud komponenthaavaliste tehetega.

Näide 10.46 Kui me vaatleme järjestatud hulka $(P, \leqslant)$ kategooriana (vt. näidet 10.5), siis korrutised (kui nad leiduvad) on täpselt alumised rajad.

Vaatleme kokorrutiste näiteid.

Näide 10.47 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 10.48 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 viimane summa on tegelikult lõpliku arvu nullist erinevate elementide summa.

Näide 10.49 Kui vaatleme järjestatud hulka $(P, \leqslant)$ kategooriana (vt. näidet 10.5), siis kokorrutised (kui nad leiduvad) on ülemised rajad.

Indeks

n-kohaline algebraline tehe, 7

alamkategooria, 93
    täielik, 93
algobjekt, 96

bimorfism, 95

diskreetne kategooria, 92
distributiivsuse seadused, 45
duaalne kategooria, 97

endomorfism, 91
epimorfism, 95

injektiivne objekt, 96
isomorfism, 95
isomorfsed objektid, 95

kategooria, 91
    diskreetne, 92
    suur, 92
    väike, 92
kategooriate korrutis, 93
kokorrutis, 98
kokorrutise sisestused, 98
koretraktsioon, 94
korpus, 45
korrutis, 98
korrutise projektsioon, 98

lõige, 94
lõppobjekt, 96
lineaarkombinatsioon, 18
lineaarkombinatsiooni
    kordajad, 18
lineaarkujutus, 11
lineaarne
    sõltumatus, 18
    sõltuvus, 19
lineaarne ruum, 7

monomorfism, 94
moodul, 53
morfismide kompositsioon, 91

nullobjekt, 96
nullvektor, 8

projektiivne objekt, 96

rühm, 23
retrakt, 94
retraktsioon, 95
ring, 45

skalaar, 8
summa, 98
suur kategooria, 92

täielik alamkategooria, 93
tühi kategooria, 92

väike kategooria, 92
vastandvektor, 8
vektor, 8
vektorruum, 7

Kasutatud kirjandus

1. M. Kilp, Algebra I, Eesti Matemaatika Selts, Tartu, 2005.
2. M. Kilp, Algebra II, Tartu, 1998.