

Algebra struktuurid

Sügis 2026

Lektor: Valdis Laan

3. september 2026. a.

Sisukord

Eessõna	2
1 Kategooriad	11
1.1 Kategooria mõiste	11
1.2 Morfismide liigid	13
1.3 Objektide liigid	15
1.4 Funktorid	16
1.5 Loomulikud teisendused	19
1.6 Korrutised ja kokorrutised	21
2 Vektorruum	25
2.1 Algebraalne tehe	25
2.2 Alamstruktuurid	28
2.3 Homomorfismid	29
2.4 Isomorfismid	31
2.5 Faktorstruktuurid	32
2.6 Homomorfismiteoreem	36
2.7 Baasi olemasolu	37
2.8 Otsekorrutised ja välised otsesummad	40
2.9 Vektorruumide kirjeldus	43
3 Rühm	45
3.1 Rühm, alamrühm	45
3.2 Normaaljagaja, faktorrühm	47
3.3 Tsüklilised rühmad	50
3.4 Rühma elemendi järk	51
3.5 Lihtsad rühmad	53
4 Abeli rühm	59
4.1 Põhimõisted	59
4.2 Sisemised otsesummad	60
4.3 Perioodilised Abeli rühmad	63
4.3.1 Lõplikud Abeli p -rühmad	65

5	Ringid	69
5.1	Põhimõisted	69
5.2	Ideaalid	71
5.3	Lihtsad minimaalse parempoolse ideaaliga ringid	74
5.4	Algebra üle korpuse	80
5.5	Kvaternioonide algebra	83
6	Moodulid	85
6.1	Mooduli definitsioon	85
6.2	Morfismid ja välised otsesummad	86
6.3	Täpsed jadad	88
6.4	Vabad moodulid	91
6.5	Projektiivsed moodulid	97
6.6	Tensorkorrutise definitsioon ja konstruktsioon	100
6.7	Tensorkorrutise omadused	104
6.8	Tensorfunktorid	106
6.9	Lamedad moodulid	108
7	Poolrühmad	113
7.1	Põhimõisted	113
7.2	Lihtsad poolrühmad	116
7.3	Greeni seosed	117
7.4	Täiesti lihtsad poolrühmad	119
7.5	Reesi maatrikspoolrühmad	122
7.6	Reesi teoreem	123
7.7	Regulaarsed ja inverssed poolrühmad	125
8	Polügonid	127
8.1	Põhimõisted	127
8.2	Lahutumatud polügonid	129
8.3	Projektiivsed polügonid	131
8.4	Polügonide tensorkorrutis	135
8.5	Poolrühmade Morita teooria	138
9	Korpused	145
9.1	Korpuse karakteristika	145
9.2	Lihtsad korpused	147
9.3	Lõplike korpuste ehitus	149
9.4	Aritmeetika lõplikes korpustes	154
10	Võred	157
10.1	Kaks vaatenurka võredele	157
10.2	Täielikud võred	160
10.3	Modulaarsed võred	162
10.4	Distributiivsed võred	165

11	Universaalalgeberad ja nende muutkonnad	167
11.1	Põhimõisted	167
11.2	Muutkonnad	168

Eessõna

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

Kursuse jooksul eeldame, et üliõpilane on tuttav põhiliste mõistete ja tulemustega hulgateooriast (tehted hulkadega, kujutused, ekvivalentsiseosed), lineaaralgebrast (maatriksid, vektorruumid ja lineaarteisendused) ja abstraktsest algebrast (rühmad, ringid, polünoomid). Selles kursuses loeme, et $\mathbb{N} = \{1, 2, 3, \dots\}$. Sümbol $\mathbb{P}$ tähistab kõigi algarvude hulka.

Suurema osa loengukonspektist on kirjutanud Valdis Laan, täiendusi ja parandusi on teinud Lauri Tart ja Ülo Reimaa. Põhiliselt on tuginetud raamatutele [2] ja [1]. Lause 5.18 tõestus on pärit Hendrik Vijalt. Soovin tänada ka Simmo Saani, kes leidis konspektist mitmeid vigu.

Loengute ajakava

1. Kategooriad, morfismide liigid, objektide liigid.
2. Funktorid, loomulikkud teisendused, korrutised ja kokorrutised.
3. Algebraline tehe. Algebraline struktuur. Alamstruktuur. Homomorfism. Isomorfism.
4. Faktorstruktuur. Vektorruumi faktorruum. Vektorruumi baasi olemasolu (üldjuht).
5. Otsekorrutised ja otsesummad.
6. Rühm, normaaljagaja, kongruents.
7. Tsükliline rühm. Rühma elemendi järk.
8. Lihtsad rühmad.
9. Abeli rühmad. Sisemised otsesummad. Perioodilised Abeli rühmad.
10. Lõplikud Abeli rühmad.
11. Ringid. Ideaalid.
12. Lihtsad ringid.
13. Lihtsad ringid
14. Algebrad üle korpuse.
15. Moodulid üle ringi. Täpsed jadad.
16. Vabad moodulid.
17. Projektiivsed moodulid.
18. Moodulite tensorkorrutis.
19. Moodulite tensorkorrutis.
20. Lamedad moodulid.
21. Poolrühmad. Lihtsad poolrühmad. Greeni seosed.
22. Täiesti lihtsad poolrühmad.

23. Reesi teoreem. Regulaarsed ja inverssed poolrühmad.
24. Polügonid üle poolrühma. Lahutumatud polügonid.
25. Projektiivsed polügonid. Polügonide tensorkorrutis.
26. Poolrühmade Morita teooria.
27. Korpuse karakteristika. Lihtsad korpused.
28. Lõplikud korpused.
29. Lõplikud korpused.
30. Kaks vaatekohta võrele. Täielikud võred.
31. Modulaarsed ja distributiivsed võred.
32. Universaalalgebrad ja nende muutkonnad.

Peatükk 1

Kategooriad

1.1 Kategooria mõiste

Kategooria koosneb kahte sorti asjadest: objektidest ja nendevahelistest morfismidest, mida saab teatud juhtudel korrutada. Objektid võivad olla näiteks (teatud struktuuriga: algebralise, topoloogilise vm.) hulgad ja morfismideks kujutused (mis on kooskõlas struktuuriga). Formaalne definitsioon on järgmine.

Definitsioon 1.1 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 $\text{id}_A \in \mathcal{C}(A, A)$, 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

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

3. **ühiku aksioom:** mistahes morfismide $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$ korral kehtivad võrdsused $\text{id}_B \circ f = f$ ja $g \circ \text{id}_B = g$.

Morfismi $f \in \mathcal{C}(A, B)$ jaoks kasutatakse tihti tähistusi $f : A \rightarrow B$ ja $A \xrightarrow{f} B$; üheselt määratud objekti A kutsutakse morfismi f **lähteobjektis** ning objekti B kutsutakse f **sihtobjektiks**. Morfismi $f : A \rightarrow A$ nimetatakse objekti A **endomorfismiks** ja hulka $\text{End}(A) = \mathcal{C}(A, A)$ nimetatakse objekti A endomorfismide hulgaks. On selge, et $(\text{End}(A), \circ)$ on monoid. Kategooria $\mathcal{C}$ objektide klassi tähistatakse ka $\text{Ob}(\mathcal{C})$ või $|\mathcal{C}|$, morfismide klassi aga $\text{Mor}(\mathcal{C})$ või $\mathcal{C}_1$. Morfismide hulka objektist A objekti B tähistatakse veel ka sümboliga $\text{Mor}(A, B)$ või $\text{hom}(A, B)$.

- Märkused 1.2** 1. Osutub, et id_A on objekti A ainus ühikmorfism, sest kui $i_A \in \mathcal{C}(A, A)$ on veel mingi morfism, mis rahuldab ühiku aksioomi, siis $\text{id}_A = \text{id}_A \circ i_A = i_A$.
2. Samamoodi nagu poolrühmade korral järeldeb assotsiatiivsuse aksioomist, et lõpliku arvu morfismide komponeerimisel võib sulge paigutada mistahes (mõttekal) viisil ja seega võib nad üldse ära jätta.

Definitsioon 1.3 Kategooria on **väike** kui tema objektide klass on hulk, vastasel korral öeldakse, et kategooria on **suur**.

Näide 1.4 Paljud matemaatilised struktuurid ja nende vahelised kujutused või homomorfismid moodustavad kategooria. Järgnevas tabelis on toodud mõned selliste kategooriate näited.

Tähis	objektid	morfismid
Set	hulgad	kujutused
Rel	hulgad	binaarsed seosed hulkade vahel
Mon	monoidid	monoidide homomorfismid
Gr	rühmad	rühmade homomorfismid
Ab	Abeli rühmad	rühmade homomorfismid
Rng	assotsiatiivsed ringid	ringide homomorfismid
$\text{Vec}_{\mathbb{R}}$	vektorruumid üle reaalarvude	lineaarkujutused
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
Graph	graafid	graafide homomorfismid

Enamasti on morfismide komponeerimiseks tavaline kujutuste komponeerimine (järjest-rakendamine) ja ühikmorfismid on samasusteisendused. Kategoorias Rel on seoste kompositsiooniks nende korrutis ja ühikmorfism on võrdusseos.

Näide 1.5 On olemas 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.

Näide 1.6 Igat osaliselt järjestatud hulka $(P, \leq)$ võib vaadelda kategooriana $\mathcal{P}$, mille objektide hulk on P . Kui $x, y \in P$, siis hulk $\mathcal{P}(x, y)$ koosneb täpselt ühest morfismist, kui $x \leq y$, ning on tühi vastasel juhul.

Definitsioon 1.7 Kategooria $\mathcal{A}$ alamkategooria koosneb

1. kategooria $\mathcal{A}$ objektide klassi $\mathcal{A}_0$ alamklassist $\mathcal{B}_0$;
2. iga objektipaari $(B, B') \in \mathcal{B}_0 \times \mathcal{B}_0$ jaoks leiduvast hulgast $\mathcal{B}(B, B') \subseteq \mathcal{A}(B, B')$, nii et
 - (a) kui $f \in \mathcal{B}(B, B')$ ja $g \in \mathcal{B}(B', B'')$, siis ka $g \circ f \in \mathcal{B}(B, B'')$,
 - (b) $\text{id}_B \in \mathcal{B}(B, B)$ iga $B \in \mathcal{B}_0$ korral.

Definitsioon 1.8 Kategooria $\mathcal{A}$ alamkategooriat $\mathcal{B}$ nimetatakse **täielikuks alamkategooriaks**, kui

$$B, B' \in \mathcal{B}_0 \implies \mathcal{B}(B, B') = \mathcal{A}(B, B'),$$

s.t. $\mathcal{B}$ sisaldab koos iga kahe objektiga kõik nende objektide vahel kategoorias $\mathcal{A}$ leiduvad morfismid.

Näide 1.9 1. Kategooria $\mathbf{Ab}$ on kategooria $\mathbf{Gr}$ täielik alamkategooria.

2. $\mathbf{Mon}$ on poolrühmade kategooria $\mathbf{Sgr}$ alamkategooria, mis ei ole täielik.

1.2 Morfismide liigid

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

Definitsioon 1.10 Morfismi $f : A \rightarrow B$ kategoorias $\mathcal{C}$ nimetatakse **monomorfismiks**, kui ta on vasakult taandatav, s.t. iga morfismipaari $g, h : C \rightarrow A$ korral

$$f \circ g = f \circ h \implies g = h;$$

Pöörates definitsioonis 1.10 kõik nooled ümber ehk *dualiseerides* saadakse epimorfismi mõiste.

Definitsioon 1.11 Morfismi $f : A \rightarrow B$ kategoorias $\mathcal{C}$ nimetatakse **epimorfismiks** kui ta on paremalt taandatav, s.t. iga morfismipaari $g, h : B \rightarrow C$ korral

$$g \circ f = h \circ f \implies g = h;$$

Lihtne on veenduda, et kahe monomorfismi korrutis on monomorfism ja kahe epimorfismi korrutis on epimorfism. Lisaks harilikele monomorfismidele on veel olemas terve rida eri tüüpi monomorfisme (regulaarsed, ranged, tugevad jne) ja epimorfisme, aga selles kursuses me neid ei vaatle.

Definitsioon 1.12 Kategooriat nimetatakse **konkreetses kategooriaks**, kui tema objektid on hulgad (harilikult mingi struktuuriga), morfismid on kujutused (mis harilikult säilitavad vaadeldavat struktuuri), morfismide komponeerimine on kujutuste järjestordenamine ja ühikmorfismid on samasusteisendused.

Set , Gr , Rng , Top , Ban_∞ , Pos ja paljud teised on konkreetsete kategooriate näideteks. Rel ei ole konkreetne kategooria, sest mitte kõik binaarsed seosed ei ole kujutused. Konkreetsetes kategooriates kehtib järgmine lause.

Lause 1.13 *Konkreetses kategoorias on iga injektiivne morfism monomorfism ja iga sürjektiivne morfism epimorfism.*

TÕESTUS. Oletame, et $f : A \rightarrow B$ on injektiivne morfism ja $f \circ g = f \circ h$, kus $g, h : C \rightarrow A$. Siis iga $c \in C$ korral $f(g(c)) = f(h(c))$, millest järeldub, et $g(c) = h(c)$ iga $c \in C$ korral. Järelikult $g = h$ ja me oleme näidanud, et f on monomorfism.

Oletame, et $f : A \rightarrow B$ on sürjektiivne morfism ja $g \circ f = h \circ f$, kus $g, h : B \rightarrow C$. Siis iga $b \in B$ jaoks leidub $a \in A$ nii, et $f(a) = b$ ning seega $g(b) = g(f(a)) = h(f(a)) = h(b)$. Järelikult $g = h$ ja me oleme näidanud, et f on epimorfism. $\square$

Näide 1.14 Hulkade kategoorias Set on monomorfismideks parajasti injektiivsed kujutused ja epimorfismideks sürjektiivsed kujutused. Tõestuse jätame läbimõtlemiseks lugejale.

Paljudes kategooriates (aga mitte kõigis) langevad injektiivsed morfismid kokku monomorfismidega ja sürjektiivsed morfismid epimorfismidega. Selles kursuses tõestame selle moodulite jaoks üle ringi R lauses 6.4. Sama kehtib Abeli rühmade ja vektorruumide korral, mis mõlemad on moodulite erijuhuks.

Definitsioon 1.15 Morfismi $f : A \rightarrow B$ nimetatakse **isomorfismiks**, kui ta on pööratav, s.t. leidub morfism $g : B \rightarrow A$ nii, et $g \circ f = \text{id}_A$ ja $f \circ g = \text{id}_B$. Kategooria $\mathcal{C}$ objektid A ja B on **isomorfsed** kui leidub isomorfism $f : A \rightarrow B$. Objektide A ja B isomorfsust tähistatakse $A \cong B$.

Lause 1.16 *Objektide isomorfsusseos on ekvivalentsiseos.*

TÕESTUS. Kuna iga objekti ühikmorfism on isomorfism, siis iga objekt on isomorfne iseendaga, seega seos $\cong$ on refleksiivne.

Lihtne on näha, et kahe isomorfismi korrutis on isomorfism, seega seos $\cong$ on transitiivne.

Kui $A \cong B$ ehk leidub isomorfism $f : A \rightarrow B$, siis leidub morfism $g : B \rightarrow A$ nii, et $g \circ f = \text{id}_A$ ja $f \circ g = \text{id}_B$. Siis ka g on isomorfism ja järelikult $B \cong A$. See tähendab, et $\cong$ on sümmeetriline. $\square$

Näide 1.17 Kategoorias Set on isomorfismideks bijektiivsed kujutused.

Näide 1.18 Kategooriates Gr , Ab ja Rng on isomorfismideks bijektiivsed homomorfismid.

Näide 1.19 Kategoorias $\text{Vec}_\mathbb{R}$ on isomorfismideks bijektiivsed lineaarkujutused.

Näide 1.20 Iga rühma võib vaadelda kui üheobjektilist kategooriat, kus kõik morfismid on isomorfismid.

1.3 Objektide liigid

Nii nagu kategooriates saab vaadelda eri tüüpi morfisme, on võimalik uurida ka erinevate omadustega objekte.

Definitsioon 1.21 Kategooria $\mathcal{C}$ objekti **1** nimetatakse **lõppobjektiks**, kui $\mathcal{C}$ igast objektist C leidub täpselt üks morfirm objekti **1**. Kategooria $\mathcal{C}$ objekt **0** on **algobjekt**, kui objektist **0** leidub täpselt üks morfirm $\mathcal{C}$ igasse objekti. Objekt on **nullobjekt**, kui ta on korraga nii lõpp- kui algobjekt.

Lause 1.22 Kategooria mistahes kaks lõpp-(alg-, null-)objekti on isomorfsed.

TÕESTUS. Kui $C, C' \in \mathcal{C}_0$ on lõppobjektid, siis $\mathcal{C}(C, C) = \{\text{id}_C\}$ ja $\mathcal{C}(C', C') = \{\text{id}_{C'}\}$. Samuti leiduvad morfismid $f : C \rightarrow C'$ ja $g : C' \rightarrow C$. Kuna $g \circ f : C \rightarrow C$, siis $g \circ f = \text{id}_C$ ja samamoodi $f \circ g = \text{id}_{C'}$. Seega $C \cong C'$. Alg- ja nullobjektide jaoks on tõestus analoogiline. $\square$

Näide 1.23 Kategoorias **Set** on tühi hulk algobjekt ja üheelemendilised hulgad on lõppobjektid.

Näide 1.24 Kategooriates **Ab**, **Vec $_{\mathbb{R}}$** ja **Ban $_1$** on $\{0\}$ nii alg- kui ka lõppobjekt, seega nullobjekt.

Näide 1.25 Ühikelemendiga assotsiatiivsete ringide kategoorias **Ring** on $\{0\}$ lõppobjekt ja $\mathbb{Z}$ algobjekt.

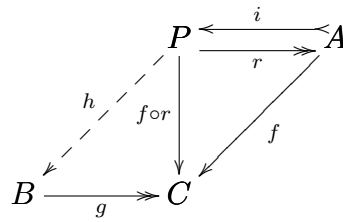
Definitsioon 1.26 Kategooria $\mathcal{C}$ objekti P nimetatakse **projektiivseks**, kui iga epimorfismi $g : B \rightarrow C$ ja iga morfismi $f : P \rightarrow C$ jaoks leidub selline morfirm $h : P \rightarrow B$, et $gh = f$.

$$\begin{array}{ccc}
 & P & \\
 h \swarrow & \downarrow f & \\
 B & \xrightarrow{g} & C
 \end{array}$$

Definitsioon 1.27 Kategooria $\mathcal{C}$ objekti A nimetatakse objekti P **retraktiks**, kui leiduvad morfismid $r : P \rightarrow A$ ja $i : A \rightarrow P$ nii, et $r \circ i = \text{id}_A$.

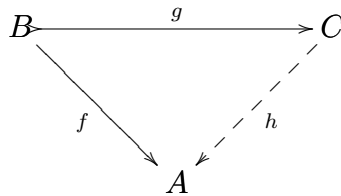
Lause 1.28 Projektiivse objekti retrakt on projektiivne.

TÕESTUS. Järgmises diagrammis olgu P projektiivne ja olgu A tema reakt, s.t. $ri = \text{id}_A$ mingite $r : P \rightarrow A$ ja $i : A \rightarrow P$ korral.



Kui $f : A \rightarrow C$, siis P projektiivsuse tõttu leidub selline $h : P \rightarrow B$, et $g \circ h = f \circ r$. Seega $g \circ h \circ i = f \circ r \circ i = f \circ \text{id}_A = f$. $\square$

Definitsioon 1.29 Kategooria $\mathcal{C}$ objekti A nimetatakse **injektiivseks**, kui iga monomorfismi $g : B \rightarrow C$ ja iga morfismi $f : B \rightarrow A$ korral leidub selline morfism $h : C \rightarrow A$, et $h \circ g = f$.



Näide 1.30 Kategooria **Set** iga objekt on projektiivne. Kasutades fakti, et iga epimorfism on paremalt pööratav kategoorias **Set** ja definitsiooni 1.26 tähistusi saame leida sellise $p : C \rightarrow B$, et $g \circ p = \text{id}_C$. Võttes $h := p \circ f$ saame, et $g \circ h = g \circ p \circ f = f$.

Näide 1.31 Saab näidata, et Abeli rühm A on injektiivne parajasti siis, kui ta on jaguv, s.t. iga elemendi $a \in A$ ja iga naturaalarvu n korral leidub selline $b \in A$, et $nb = a$.

Näide 1.32 Projektiivsed ja injektiivsed objektid mängivad tähtsat rolli moodulite teoorias (üle ringi). Saab näidata, et moodul projektiivne parajasti siis, kui ta on vaba mooduli otseliidetav (vt. teoreemi 6.33).

1.4 Funktorid

Funktoritest võib mõelda kui morfismidest kategooriate vahel.

Definitsioon 1.33 Kovariantne funktor F kategooriast $\mathcal{A}$ kategooriasse $\mathcal{B}$ koosneb

1. kujutusest $F_0 : \mathcal{A}_0 \rightarrow \mathcal{B}_0$ kategooriate $\mathcal{A}$ ja $\mathcal{B}$ objektide klasside vahel; objekti $A \in \mathcal{A}_0$ kujutist tähistatakse $F(A)$;
2. $\mathcal{A}$ iga objektipaari (A, A') jaoks kujutusest $F_1^{A, A'} : \mathcal{A}(A, A') \rightarrow \mathcal{B}(F(A), F(A'))$; morfismi $f \in \mathcal{A}(A, A')$ kujutist tähistatakse $F(f)$;

nii et on täidetud järgmised tingimused:

1. mistahes morfismide $f \in \mathcal{A}(A, A')$ ja $g \in \mathcal{A}(A', A'')$ korral

$$F(g \circ f) = F(g) \circ F(f);$$

2. iga objekti $A \in \mathcal{A}_0$ korral

$$F(\text{id}_A) = \text{id}_{F(A)}.$$

$$\begin{array}{ccc} A & \xrightarrow{\quad} & F(A) \\ f \downarrow & & \downarrow F(f) \\ A' & \xrightarrow{\quad} & F(A') \end{array}$$

Definitsioon 1.34 Kontravariantne funktor F kategooriast $\mathcal{A}$ kategooriasse $\mathcal{B}$ koosneb

1. kujutustest $F_0 : \mathcal{A}_0 \rightarrow \mathcal{B}_0$ kategooriate $\mathcal{A}$ ja $\mathcal{B}$ objektide klasside vahel; objekti $A \in \mathcal{A}_0$ kujutist tähistatakse $F(A)$;
2. $\mathcal{A}$ iga objektipaari (A, A') jaoks kujutustest $F_1^{A, A'} : \mathcal{A}(A, A') \rightarrow \mathcal{B}(F(A'), F(A))$; morfismi $f \in \mathcal{A}(A, A')$ kujutist tähistatakse $F(f)$;

nii et on täidetud järgmised tingimused:

1. mistahes morfismide $f \in \mathcal{A}(A, A')$ ja $g \in \mathcal{A}(A', A'')$ korral

$$F(g \circ f) = F(f) \circ F(g);$$

2. iga objekti $A \in \mathcal{A}_0$ korral

$$F(\text{id}_A) = \text{id}_{F(A)}.$$

$$\begin{array}{ccc} A & \xrightarrow{\quad} & F(A) \\ f \downarrow & & \uparrow F(f) \\ A' & \xrightarrow{\quad} & F(A') \end{array}$$

Näited 1.35 Toome mõned kovariantsete funktorite näited.

1. Iga kategooria $\mathcal{A}$ korral leidub **ühikfunktor** $\text{id}_{\mathcal{A}} : \mathcal{A} \rightarrow \mathcal{A}$, mis on objektidel defineeritud võrdusega $\text{id}_{\mathcal{A}}(A) = A$ ja morfismidel võrdusega $\text{id}_{\mathcal{A}}(f) = f$.
2. Kategooria $\mathcal{A}$ mistahes alamkategooria $\mathcal{B}$ tekitab loomulikul viisil **sisestusfunktori** $\mathcal{B} \rightarrow \mathcal{A}$, mis on lihtsalt ühikfunktori $\text{id}_{\mathcal{A}}$ ahend kategooriale $\mathcal{B}$.

3. Kui $\mathcal{A}$ ja $\mathcal{B}$ on kategooriad ja $B \in \mathcal{B}_0$ on fikseeritud objekt, siis leidub **konstantne funktor** objektile B , $\Delta_B^A : \mathcal{A} \rightarrow \mathcal{B}$ ehk lihtsalt Δ_B , mis on iga $A \in \mathcal{A}_0$ ja kategooria $\mathcal{A}$ iga morfismi f korral defineeritud võrdustega

$$\Delta_B(A) := B, \quad \Delta_B(f) := \text{id}_B.$$

4. **Unustav funktor** $U : \text{Gr} \rightarrow \text{Set}$ kujutab rühma $(A, \cdot)$ tema põhihulgaks A ja rühmade homomorfismid vastavateks kujutusteks. Samamoodi võib veel vaadelda unustavaid funktoreid $\text{Rng} \rightarrow \text{Ab}$ (“unustab ära” korrutamise) või $\text{Rng} \rightarrow \text{Mon}$ (“unustab ära” liitmise).
5. Olgu $(P, \leq)$ ja $(Q, \leq)$ järjestatud hulgad, mida vaatleme kategooriatena nii nagu näites 1.6. Selliste kategooriate vahelised funktorid on kujutused $f : P \rightarrow Q$, mis säilitavad järjestust.

Näide 1.36 Toome näite kontravariantsest funktorist. Vaatleme funktorit $\mathcal{P} : \text{Set} \rightarrow \text{Set}$, mis seab igale hulgale A vastavusse tema kõigi alamhulkade hulga $\mathcal{P}(A)$ ja kujutusele $f : A \rightarrow B$ kujutuse $f^{-1} : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$, mis kujutab B alamhulga C hulgaks $f^{-1}(C) \subseteq A$.

Järgmisena toome sisse funktorid, mis on kategooriateoorias väga suure tähtsusega.

Näide 1.37 Kategooria $\mathcal{C}$ fikseeritud objekti C korral defineerib reegel

$$\begin{array}{ccccc} A & \longrightarrow & \mathcal{C}(C, A) & \ni & g \\ f \downarrow & & \downarrow f \circ - & & \downarrow \\ B & \longrightarrow & \mathcal{C}(C, B) & \ni & f \circ g \end{array}$$

kovariantse funktori $\mathcal{C}(C, -) : \mathcal{C} \rightarrow \text{Set}$, mida nimetatakse **kovariantseks hom-funktoriks**. (Märgime, et tihti kirjutatakse $f \circ -$ asemel $\mathcal{C}(C, f)$.)

Näide 1.38 Kategooria $\mathcal{C}$ fikseeritud objekti C korral defineerib reegel

$$\begin{array}{ccccc} A & \longrightarrow & \mathcal{C}(A, C) & \ni & g \circ f \\ f \downarrow & & \uparrow - \circ f & & \uparrow \\ B & \longrightarrow & \mathcal{C}(B, C) & \ni & g \end{array}$$

kontravariantse funktori $\mathcal{C}(-, C) : \mathcal{C} \rightarrow \text{Set}$, mida nimetatakse **kontravariantseks hom-funktoriks**.

Funktorite $F : \mathcal{A} \rightarrow \mathcal{B}$ ja $G : \mathcal{B} \rightarrow \mathcal{C}$ korral on võimalik moodustada nende kompositsioon ehk korrutis $G \circ F : \mathcal{A} \rightarrow \mathcal{C}$ (mis osutub samuti funktoriks), kui defineerida

$$(G \circ F)(A) := G(F(A)), \quad (G \circ F)(f) := G(F(f))$$

$\mathcal{A}$ iga objekti $A \in \mathcal{A}_0$ ja iga morfismi f korral. Korrutise $G \circ F$ variantsus on määratud järgmise reegli:

F	G	$G \circ F$
kovariantne	kovariantne	kovariantne
kovariantne	kontravariantne	kontravariantne
kontravariantne	kovariantne	kontravariantne
kontravariantne	kontravariantne	kovariantne.

Lause 1.39 Iga funktor säilitab isomorfisme.

TÕESTUS. Olgu $f : A \rightarrow B$ isomorfism kategoorias $\mathcal{C}$. Siis leidub morfism $g : B \rightarrow A$ nii, et $g \circ f = \text{id}_A$ ja $f \circ g = \text{id}_B$. Rakendades kovariantset funktoori $F : \mathcal{C} \rightarrow \mathcal{D}$ näeme, et kategoorias $\mathcal{D}$ kehtib

$$\text{id}_{F(A)} = F(\text{id}_A) = F(g \circ f) = F(g) \circ F(f) \quad \text{ja} \quad \text{id}_{F(B)} = F(\text{id}_B) = F(f \circ g) = F(f) \circ F(g).$$

Seega $F(f)$ on isomorfism kategoorias $\mathcal{D}$. Kontravariantsete funktoore jaoks on tõestus analoogiline. $\square$

Samas funktoori üldiselt ei pruugi säilitada monomorfisme või epimorfisme.

1.5 Loomulikud teisendused

Loomulikke teisendusi võib vaadelda kui funktoorevahelisi morfisme.

Definitsioon 1.40 Olgu $F, G : \mathcal{A} \rightarrow \mathcal{B}$ kaks kovariantset funktoori kategooriast $\mathcal{A}$ kategooriasse $\mathcal{B}$. **Loomulik teisendus** $\alpha : F \Rightarrow G$ funktoori F funktooris G on kategooria $\mathcal{B}$ morfismide süsteem $(\alpha_A : F(A) \rightarrow G(A))_{A \in \mathcal{A}_0}$, mis on indekseeritud $\mathcal{A}$ objektide järgi, mille korral $\alpha_{A'} \circ F(f) = G(f) \circ \alpha_A$ kategooria $\mathcal{A}$ iga morfolmi $f : A \rightarrow A'$ korral, s.t. järgmine ruut on kommutatiivne:

$$\begin{array}{ccccc} A & & F(A) & \xrightarrow{\alpha_A} & G(A) \\ f \downarrow & & F(f) \downarrow & & \downarrow G(f) \\ A' & & F(A') & \xrightarrow{\alpha_{A'}} & G(A') \end{array} .$$

Morfismi α_A , kus $A \in \mathcal{A}_0$, nimetatakse loomuliku teisenduse $\alpha = (\alpha_A)_{A \in \mathcal{A}_0}$ **komponentiks** kohal A .

Loomulikud teisendused kontravariantsete funktoore vahel defineeritakse duaalselt. Funktoore $F, G : \mathcal{A} \rightarrow \mathcal{B}$ korral tähistame kõigi nende vaheliste loomulike teisenduste kogumit tähisega $\text{Nat}(F, G)$.

Definitsioon 1.41 Loomulikku teisendust $\alpha : F \Rightarrow G$, kus $F, G : \mathcal{A} \rightarrow \mathcal{B}$, nimetatakse **loomulikuks isomorfismiks**, kui $\alpha_A : F(A) \rightarrow G(A)$ on isomorfism kategoorias $\mathcal{B}$ iga $A \in \mathcal{A}_0$ korral. Funktooreid F ja G nimetatakse **loomulikult isomorfseteks** (tähistus: $F \cong G$), kui leidub loomulik isomorfism $F \Rightarrow G$.

Definitsioon 1.42 Öeldakse, et kategooriad $\mathcal{A}$ ja $\mathcal{B}$ on **ekvivalentsed**, kui leiduvad funktorid $F : \mathcal{A} \rightarrow \mathcal{B}$ ja $G : \mathcal{B} \rightarrow \mathcal{A}$ nii, et $G \circ F \cong \text{id}_{\mathcal{A}}$ ja $F \circ G \cong \text{id}_{\mathcal{B}}$.

Näide 1.43 Iga funktori $F : \mathcal{A} \rightarrow \mathcal{B}$ jaoks leidub selle funktori **samasusteisendus** $\text{id}_F : F \Rightarrow F$, mis on defineeritud võrdusega

$$(\text{id}_F)_A := \text{id}_{F(A)}$$

iga $A \in \mathcal{A}_0$ korral.

Näide 1.44 Olgu $f : B \rightarrow A$ fikseeritud morfism kategoorias $\mathcal{A}$. Definitsioon

$$\mathcal{A}(f, -)_C(g) := g \circ f,$$

$g : A \rightarrow C$, annab loomuliku teisenduse $\mathcal{A}(f, -) : \mathcal{A}(A, -) \Rightarrow \mathcal{A}(B, -)$ objektide A ja B poolt tekitatud hom-funktorite vahel, sest kategooria $\mathcal{A}$ iga morfismi $h : C \rightarrow C'$ korral $(h \circ g) \circ f = h \circ (g \circ f)$, s.t. järgmine ruut on kommutatiivne:

$$\begin{array}{ccccc} C & & \mathcal{A}(A, C) & \xrightarrow{\mathcal{A}(f, -)_C} & \mathcal{A}(B, C) \\ \downarrow h & & \downarrow \mathcal{A}(A, h) = h \circ - & & \downarrow \mathcal{A}(B, h) = h \circ - \\ C' & & \mathcal{A}(A, C') & \xrightarrow{\mathcal{A}(f, -)_{C'}} & \mathcal{A}(B, C'). \end{array}$$

Järgnevad kaks loomulike teisenduste näidet (või pigem näidete seeriat) tekivad loomulikult viisil lineaaralgebras.

Näide 1.45 Iga korpuse K korral on võimalik vaadelda kontravariantset hom-funktorit $\text{Vec}_K(-, K) : \text{Vec}_K \rightarrow \text{Set}$. On hästi teada, et vektorruumi V korral üle K saab lineaarkujutuste $V \rightarrow K$ (ehk lineaarsete funktsionaalide) hulka

$$V^* := \text{Vec}_K(V, K) = \{g : V \rightarrow K \mid g \text{ on lineaarkujutus}\}$$

vaadelda vektorruumina üle K punktiivisiliste tehete

$$\begin{aligned} (g + h)(v) &= g(v) + h(v), \\ (kg)(v) &= kg(v) \end{aligned}$$

suhtes. Veelgi enam, kui $f : V \rightarrow U$ on lineaarkujutus, siis on lihtne näha, et ka kujutus $\text{Vec}_K(-, K)(f) = - \circ f : U^* \rightarrow V^*$ on lineaarkujutus. Seega võib vaadelda ka kontravariantset funktorit

$$(-)^* := \text{Vec}_K(-, K) : \text{Vec}_K \rightarrow \text{Vec}_K.$$

Funktori $(-)^*$ kompositsioon iseendaga on kovariantne funktor $\text{Vec}_K \rightarrow \text{Vec}_K$. Me tähistame seda $(-)^{**}$ ja nimetame **teise kaasruumi funktoriks**.

Iga vektorruumi V korral defineerime kujutuse $\Phi_V : V \rightarrow V^{**} = \text{Vec}_K(\text{Vec}_K(V, K), K)$ võrdusega

$$(\Phi_V(a))(g) := g(a),$$

$a \in V$, $g \in \text{Hom}(V, K)$. Saab näidata, et Φ_V on lineaarkujutus. Iga $f \in \text{Vec}_K(V, U)$, iga $a \in V$ ja iga $g \in \text{Vec}_K(U, K) = U^*$ korral

$$\begin{aligned} (f^{**} \circ \Phi_V)(a)(g) &= (\Phi_V(a)(-\circ f))(g) = \Phi_V(a)(g \circ f) = (g \circ f)(a) \\ &= g(f(a)) = \Phi_U(f(a))(g) = (\Phi_U \circ f)(a)(g), \end{aligned}$$

mis tõestab, et $\Phi = (\Phi_V)_{V \in (\text{Vec}_K)_0} : 1_{\text{Vec}_K} \Rightarrow (-)^{**}$ on loomulik teisendus.

$$\begin{array}{ccc} V & \xrightarrow{\Phi_V} & V^{**} \\ f \downarrow & & \downarrow -\circ(-\circ f)=f^{**} \\ U & \xrightarrow{\Phi_U} & U^{**} \end{array} \quad \begin{array}{ccccc} & & \Phi_U(f(a)) & & \\ U^* & \xrightarrow{-\circ f} & V^* & \xrightarrow{\Phi_V(a)} & K \end{array}$$

Lineaaralgebrast on teada (vt. [1, teoreem 10.1.7]), et kui V on lõplikumõõtmeline vektorruum, siis Φ_V on vektorruumide isomorfism. Seega teise kaasruumi funktor $(-)^{**}$ on loomulikult isomorfne kategooria Vec_K^f ühikfunktoriga, kus Vec_K^f on Vec_K täielik alamkategooria, mille objektideks on lõplikumõõtmelised vektorruumid üle K .

Näide 1.46 Kui $K^\cdot$ on korpuse K multiplikatiivne monoid ja $\text{Mat}_n(K)$ on kõigi n -ndat järku ruutmaatriksite hulk üle K , mida vaatleme multiplikatiivse monoidina, siis kujutus

$$\det_K : \text{Mat}_n(K) \rightarrow K^\cdot, \quad A \mapsto \det(A)$$

on monoidide homomorfism. Veelgi enam, ruut

$$\begin{array}{ccc} \text{Mat}_n(K) & \xrightarrow{\det_K} & K^\cdot \\ \text{Mat}_n(f) \downarrow & & \downarrow f \\ \text{Mat}_n(L) & \xrightarrow{\det_L} & L^\cdot \end{array}$$

kommuteerub iga korpuste homomorfismi $f : K \rightarrow L$ korral (siin $\text{Mat}_n(f)$ rakendab kujutust f maatriksi kõigile elementidele). Sellega oleme konstrueerinud loomuliku teisenduse $\det : \text{Mat}_n \Rightarrow (-)^\cdot$ funktoore $\text{Mat}_n, (-)^\cdot : \text{Field} \rightarrow \text{Mon}$ vahel (siin $(-)^\cdot$ on unustav funktor, mis “unustab ära” korpuse aditiivse struktuuri).

1.6 Korrutised ja kokorrutised

Selles paragrahvis uurime kategooria objektide korrutisi ja kokorrutisi. Korrutised kategooriates üldistavad hulkade otsekorrutise mõistet.

Definitsioon 1.47 Kategooria $\mathcal{C}$ objektide A, B **korrutis** on kolmik (P, p_A, p_B) , kus $P \in \mathcal{C}_0$ ja $p_A : P \rightarrow A$, $p_B : P \rightarrow B$ on morfismid kategoorias $\mathcal{C}$ (mida nimetatakse

projektsioonideks), mis rahuldavad tingimust, et kui $Q \in \mathcal{C}_0$ on objekt ja $f : Q \rightarrow A$, $g : Q \rightarrow B$ on morfismid, siis leidub üheselt määratud morfism $m : Q \rightarrow P$ nii, et järgmine diagramm kommuteerub:

$$\begin{array}{ccccc}
 & & Q & & \\
 & \swarrow f & \downarrow m & \searrow g & \\
 A & \xleftarrow{p_A} & P & \xrightarrow{p_B} & B.
 \end{array}$$

Harilikult kirjutatakse P asemel $A \times B$. Üheselt määratud m leidumise omadust kutsutakse tihti korrutise **universaalomaduseks**.

Korrutise definitsiooni dualiseerimisel (s.t. noolte ringikeeramisel) saadakse kokorrutise mõiste, mis üldistab hulkade lõikumatu ühendi konstruktsiooni.

Definitsioon 1.48 Kategooria $\mathcal{C}$ objektide A ja B **kokorrutis** (ehk **summa**) on järjestatud kolmik (P, u_A, u_B) , kus $P \in \mathcal{C}_0$ ja $u_A : A \rightarrow P$, $u_B : B \rightarrow P$ on kategooria $\mathcal{C}$ morfismid (mida nimetatakse **sisestusteks**), mis rahuldavad tingimust, et kui $Q \in \mathcal{C}_0$ on mistahes objekt ja $f : A \rightarrow Q$, $g : B \rightarrow Q$ on morfismid, siis leidub üheselt määratud morfism $m : P \rightarrow Q$ nii, et järgmine diagramm kommuteerub:

$$\begin{array}{ccccc}
 & & Q & & \\
 & \nearrow f & \uparrow m & \nwarrow g & \\
 A & \xrightarrow{u_A} & P & \xleftarrow{u_B} & B
 \end{array}$$

Harilikult kirjutatakse P asemel $A \amalg B$.

Korrutiste ja kokorrutiste definitsiooni saab üldistada mistahes arvu objektide jaoks.

Definitsioon 1.49 Olgu I hulk ja $(C_i)_{i \in I}$ kategooria $\mathcal{C}$ objektide süsteem. Selle süsteemi **korrutis** on paar $(P, (p_i)_{i \in I})$, mis rahuldab tingimusi:

1. P on $\mathcal{C}$ objekt;
2. iga $i \in I$ korral $p_i : P \rightarrow C_i$ on $\mathcal{C}$ morfism, mida nimetatakse P **projektsiooniks** objektile C_i ;
3. (**universaalomadus**) iga paari $(Q, (q_i)_{i \in I})$ jaoks, kus $Q \in \mathcal{C}_0$ ja $q_i : Q \rightarrow C_i$ iga $i \in I$ korral, leidub üheselt määratud morfism $m : Q \rightarrow P$ nii, et kolmnurk

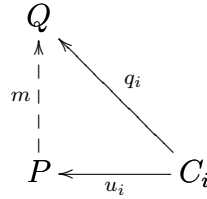
$$\begin{array}{ccc}
 Q & & \\
 \downarrow m & \searrow q_i & \\
 P & \xrightarrow{p_i} & C_i
 \end{array}$$

kommuteerub iga $i \in I$ korral.

Harilikult kirjutatakse P asemel $\prod_{i \in I} C_i$.

Definitsioon 1.50 Olgu I hulk ja $(C_i)_{i \in I}$ kategooria $\mathcal{C}$ objektide süsteem. Selle süsteemi **kokorrutis** on paar $(P, (u_i)_{i \in I})$, mis rahuldab tingimusi:

1. P on $\mathcal{C}$ objekt;
2. iga $i \in I$ korral $u_i : C_i \rightarrow P$ on $\mathcal{C}$ morfism, mida nimetatakse C_i **sisestuseks** objekti P ;
3. (**universaalomadus**) iga paari $(Q, (q_i)_{i \in I})$ jaoks, kus $Q \in \mathcal{C}_0$ ja $q_i : C_i \rightarrow Q$ iga $i \in I$ korral, leidub üheselt määratud morfism $m : P \rightarrow Q$ nii, et kolmnurk



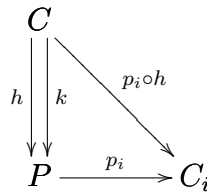
kommuteerub iga $i \in I$ korral.

Harilikult kirjutatakse P asemel $\prod_{i \in I} C_i$.

Tõestame korrutiste mõned omadused.

Lause 1.51 Kui $(P, (p_i)_{i \in I})$ on kategooria $\mathcal{C}$ objektide süsteemi $(C_i)_{i \in I}$ korrutis ja $h, k : C \rightarrow P$ on sellised morfismid, et iga $i \in I$ korral $p_i \circ h = p_i \circ k$, siis $h = k$.

TÕESTUS. Nii h kui ka k muudavad kõik kolmnurgad



kommutatiivseks, seega peavad nad korrutise universaalomaduse põhjal võrdsed olema. $\square$

Lauset 1.51 võib sõnastada ka nii, et korrutise projektsioonid on korruga vasakult taandatavad.

Lause 1.52 Kui $(P, (p_i)_{i \in I})$ ja $(P', (p'_i)_{i \in I})$ on kategooria $\mathcal{C}$ objektide süsteemi $(C_i)_{i \in I}$ korrutised, siis P ja P' on isomorfsed.

TÕESTUS. Kuna P ja P' on objektide C_i , $i \in I$, korrutised siis leiduvad morfismid φ ja ψ , mis muudavad nii ülemise kui alumise kolmnurga diagrammis

$$\begin{array}{ccc}
 P' & & \\
 \downarrow \varphi & \searrow p'_i & \\
 P & \xrightarrow{p_i} & C_i \\
 \downarrow \psi & \nearrow p'_i & \\
 P' & &
 \end{array}$$

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

$$\begin{aligned}
 p'_i \circ \text{id}_{P'} &= p'_i = p_i \circ \varphi = p'_i \circ \psi \circ \varphi, \\
 p_i \circ \text{id}_P &= p_i = p'_i \circ \psi = p_i \circ \varphi \circ \psi,
 \end{aligned}$$

järeldub lause 1.51 põhjal, et $\psi \circ \varphi = \text{id}_{P'}$ ja $\varphi \circ \psi = \text{id}_P$. Seega $P \cong P'$. $\square$

Öeldakse, et kategoorias $\mathcal{C}$ **leiduvad (ko)korrutised**, kui igal $\mathcal{C}$ objektide süsteemil $(C_i)_{i \in I}$ on olemas (ko)korrutis. Kategoorias $\mathcal{C}$ **leiduvad lõplikud (ko)korrutised**, kui igal lõplikul objektide süsteemil on olemas (ko)korrutis.

On lihtne näha, et tühja objektide süsteemi korrutis on lõppobjekt ja (A, id_A) on ühestainsast objektist A koosneva süsteemi korrutis. Kehtib ka järgmine lause.

Lause 1.53 Kategoorias leiduvad lõplikud korrutised parajasti siis, kui temas leidub lõppobjekt ja mistahes kahe objekti korrutis.

Näide 1.54 Kategoorias **Set** on hulkade 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 $p_k((x_i)_{i \in I}) = x_k$, $k \in I$.

Näide 1.55 Kui me vaatleme järjestatud hulka $(P, \leq)$ kategooriana (vt. näidet 1.6), siis korrutised (kui nad leiduvad) on täpselt alumised rajad.

Näide 1.56 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 $u_i : C_i \rightarrow \bigsqcup_{i \in I} C_i$ on defineeritud võrdusega $u_i(x) := (x, i)$, $x \in C_i$.

Näide 1.57 (Ko)korrutised kategoorias **Vec_K** on kirjeldatud lausetes 2.55 ja 2.56.

Näide 1.58 Kui vaatleme järjestatud hulka $(P, \leq)$ kategooriana (vt. näidet 1.6), siis kokorrutised (kui nad leiduvad) on ülemised rajad.

Korrutise konstruktsioon on erijuhuks üldisemast kategoorsest konstruktsioonist, mida kutsutakse piiri leidmiseks. On ka teisi loomulikke piiride näiteid, nagu võrdsustajad, tagasitõmbajad ja muud, aga neid me siin ei käsitle. Piiridega duaalsed on kopiirid.

Peatükk 2

Vektorruum

Algebraalne struktuur on hulk, millel on defineeritud mingid tehted, mis rahuldavad teatud tingimusi. Algebraaliste struktuuridega käivad kaasas sellised mõisted nagu alamstruktuur, homomorfism, isomorfism, faktorstruktuur. Selles peatükis vaatleme esialgu kõiki neid mõisteid üldisest universaalalgebra vaatepunktist ja siis uurime, mida need tähendavad konkreetsel juhul vektorruumide jaoks. Loodetavasti on lugeja vektorruumi mõistega kokku puutunud mõnes varasemas kursuses. Märkime veel, et selles peatükis tähistab K kõikjal korpust ning 0 ja 1 tähistavad vastavalt selle korpuse nullelementi ja ühikelementi. Selles kursuses eeldame, et korpuse korrutamine on kommutatiivne.

2.1 Algebraalne tehe

Abstraktse algebra kõige põhilisem mõiste on algebraalse tehte mõiste. Tehetel võib olla mistahes lõplik arv argumente.

Definitsioon 2.1 Olgu n mittenegatiivne täisarv. n -kohaline (ehk n -aarne) algebraalne tehe hulgal A on kujutus hulgast A^n hulka A .

Märkus 2.2 Sõna “algebraalne” selles definitsioonis rõhutab seda, et tehte tulemus kuulub ka hulka A . Põhimõtteliselt võib vaadelda ka tehteid $A^n \rightarrow B$, kus $B \neq A$. Näiteks kolmemõõtmelise ruumi vabavektorite liitmine on kahekohaline algebraalne tehe $\mathbb{E}_3 \times \mathbb{E}_3 \rightarrow \mathbb{E}_3$, aga skalaarkorrutamine on tehe $\mathbb{E}_3 \times \mathbb{E}_3 \rightarrow \mathbb{R}$, mis ei ole algebraalne.

Niisiis n -kohaline algebraalne tehe hulgal A seab igale hulga A elementide järjendile $(a_1, \dots, a_n)$ vastavusse hulga A mingi elemendi.

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

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

Definitsioon 2.3 Hulka Ω koos tükeldusega

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

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

Definitsioon 2.4 Olgu Ω tüüp ja A hulk. Kui iga arvu $n \in \mathbb{N} \cup \{0\}$ korral vastab igale tehtemärgile $\omega \in \Omega_n$ üks konkreetne n -kohaline algebraline tehe $\omega^A : A^n \rightarrow A$, siis ütleme, et paar $(A, \{\omega^A \mid \omega \in \Omega\})$ on **Ω -algebra**.

Näide 2.5 Olgu meil fikseeritud signatuur $\Omega = \Omega_2 = \{+, \cdot\}$, mis koosneb kahest kahekohalisest tehtemärgist (siin $\Omega_n = \emptyset$ iga $n \in \mathbb{N} \cup \{0\}$, $n \neq 2$ korral). Siis võime hulka $\mathbb{Z}$ vaadelda Ω -algebrana täisarvude hariliku liitmise ja korrutamise suhtes. Aga võime ka näiteks hulka $\mathbb{N}$ vaadelda Ω -algebrana, kus tehtemärgile $+$ vastab maksimumi võtmise tehe $\max$ ja tehtemärgile $\cdot$ vastab miinimumi võtmise tehe $\min$.

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

Üheks oluliseks algebraliseks struktuuriks on vektorruum. Tuletame meelde, kuidas harilikult defineeritakse vektorruum üle korpuse K .

Definitsioon 2.6 Hulka V nimetatakse **vektorruumiks** ehk **lineaarseks ruumiks** üle korpuse K , kui on defineeritud kujutused

$$\begin{aligned} V \times V &\rightarrow V, & (a, b) &\mapsto a + b, \\ K \times V &\rightarrow V, & (k, a) &\mapsto ka \end{aligned}$$

nii, et

- VR1.** $(a + b) + c = a + (b + c)$ iga $a, b, c \in V$ korral;
- VR2.** leidub element $0_V \in V$ nii, et iga $a \in V$ korral $a + 0_V = a = 0_V + a$;
- VR3.** iga elemendi $a \in V$ korral leidub element $-a \in V$ nii, et $a + (-a) = 0_V = (-a) + a$;
- 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 $0_V \in V$ tingimuses VR2 nimetatakse **nullvektoriks** ja elementi $-a \in V$ tingimuses VR3 nimetatakse vektori a **vastandvektori**. Tihti tähistatakse nullvektorit sümboliga 0 . Sellisel juhul peab kontekstist olema selge, kas mõeldakse täisarvu 0 , nullvektorit või korpuse nullelementi.

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 nullvektori 0_V ,
- ühekohaline tehe vastandvektori võtmine, $a \mapsto -a$,
- iga skalaari $k \in K$ jaoks on olemas ühekohaline tehe $a \mapsto ka$ (selle skalaariga korrumine).

Seega võime vektorruumi vaadelda Ω -algebrana, kus

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

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

Lisaks definitsioonis sisalduvatele tehetele (neid kutsutakse algebralise struktuuri põhitehete) 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 2.7 *Olgu V vektorruum üle korpuse K . Siis kehtivad järgmised väited.*

1. $k(a_1 + \dots + a_n) = ka_1 + \dots + ka_n$ iga $n \in \mathbb{N}$, $k \in K$ ja $a_1, \dots, a_n \in V$ korral.
2. $(k_1 + \dots + k_n)a = k_1a + \dots + k_na$ iga $n \in \mathbb{N}$, $k_1, \dots, k_n \in K$ ja $a \in V$ korral.
3. Iga $a, b, c \in V$ korral, kui $a + b = c$, siis $a = c - b$.
4. $0a = 0_V$ iga $a \in V$ korral.
5. $k0_V = 0_V$ iga $k \in K$ korral.

6. $(-1)a = -a$ iga $a \in V$ korral.
7. $(-k)a = k(-a) = -(ka)$ iga $k \in K$ ja $a \in V$ korral.
8. $k(a - b) = ka - kb$ iga $k \in K$ ja $a, b \in V$ korral.
9. $(k - l)a = ka - la$ iga $k, l \in K$ ja $a \in V$ korral.

Märkus 2.8 Kuigi enamasti uuritakse algebras struktuure, mille aarsus on 0, 1 või 2, on olemas siiski ka loomulikke näiteid struktuuridest, millel leidub suurema aarsusega tehteid.

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

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

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

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

2.2 Alamstruktuurid

Definitsioon 2.9 Ω -algebra A alamhulka A' nimetatakse **alamalgebraks**, kui A' on kinnine kõigi tehete $\omega^A, \omega \in \Omega$, suhtes. See tähendab, et

1. $\omega^A(a_1, a_2, \dots, a_n) \in A'$ iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, a_2, \dots, a_n \in A'$ korral (siin ja edaspidi kirjutame $\omega^A((a_1, a_2, \dots, a_n))$ asemel $\omega^A(a_1, a_2, \dots, a_n)$),
2. $0_\omega^A \in A'$ iga $\omega \in \Omega_0$ korral.

Vektorruumide alamalgebraid kutsutakse **alamruumideks**.

Lause 2.10 Vektorruumi V mittetühi alamhulk V' on alamruum parajasti siis, kui

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

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

TÕESTUS. **TARVILIKKUS.** See on ilmne.

PIISAVUS. Eeldame, et kehtivad AR1 ja AR2. Vastavalt definitsioonile 2.9 peame veel näitama, et V' sisaldab vektorruumi V nullelementi ja on kinnine vastandelemendi võtmise suhtes.

Kuna V' on mittetühi, siis leidub mingi $a \in V'$. Tingimuse AR2 ja lause 2.7(4) tõttu $0_V = 0a \in V'$. Kui $a \in V'$, siis lause 2.7(6) 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. $\square$

Lause 2.11 Vektorruumi V iga alamruum on ise ka vektorruum tehete suhtes, mis on defineeritud samamoodi nagu vektorruumi V tehted.

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

2.3 Homomorfismid

Homomorfismid on tehteid säilitavad kujutuse sama tüüpi algebrate vahel.

Definitsioon 2.12 Olgu A ja B Ω -algebrad. Kujutust $f : A \rightarrow B$ nimetatakse **homomorfismiks**, kui f säilitab kõiki nendel struktuuridel defineeritud tehteid. See tähendab, et

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

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

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

Ühekohalise tehte ω säilitamine tähendab seda, et

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

iga $a \in A$ korral.

Definitsioon 2.13 Homomorfismi Ω -algebrast A iseendasse nimetatakse Ω -algebra A **endomorfismiks**.

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

Lause 2.14 Olgu V ja U vektorruumid üle korpuse K . Kujutus $f : V \rightarrow U$ on vektorruumide homomorfism parajasti siis, kui

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

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

TÕESTUS. **TARVILIKKUS.** See on ilmne.

PIISAVUS. Kehtigu LK1 ja LK2. Peame näitama, et f säilitab nullelemendi ja vastandelemendi võtmise.

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

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

Definitsioon 2.15 Vektorruumide homomorfisme nimetatakse **lineaarkujutusteks** ja vektorruumide endomorfisme nimetatakse **lineaarteisendusteks**.

Meenutame nüüd hulgateooriast kujutise mõistet.

Definitsioon 2.16 Kui $f : A \rightarrow B$ on kujutus hulgast A hulka B , siis f **kujutiseks** nimetatakse hulka

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

Lause 2.17 Kui $f : A \rightarrow B$ on Ω -algebrate homomorfism, siis $\text{Im}(f)$ on Ω -algebra B alamalgebra.

TÕESTUS. Kontrollime alamstruktuuri definitsiooni tingimusi.

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

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

kust näeme, et $\omega^B(b_1, \dots, b_n) \in \text{Im}(f)$.

2. Kui $\omega \in \Omega_0$, siis $0_\omega^B = f(0_\omega^A)$ ja seega $0_\omega^B \in \text{Im}(f)$. $\square$

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

$$(g \circ f)(a) := g(f(a)).$$

Lause 2.18 Ω -algebrate homomorfismide korrutis on Ω -algebrate homomorfism.

TÕESTUS. Olgu A, B ja C Ω -algebrad ning olgu $f : A \rightarrow B$ ja $g : B \rightarrow C$ homomorfismid. Näitame, et $g \circ f : A \rightarrow C$ on homomorfism.

1. Olgu $\omega \in \Omega_n$ ($n \in \mathbb{N}$) ja $a_1, \dots, a_n \in A$. Siis

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

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

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

$\square$

Sellest lausest tuleb välja, et fikseeritud tüübi Ω korral moodustavad kõik Ω -algebrad kategooria, kus morfismideks on homomorfismid.

Lause 2.19 Ω -algebra A endomorfismide hulk $\text{End}(A)$ on monoid kujutuste korrutamise suhtes.

TÕESTUS. Lause 2.18 tõttu on kujutuste korrutamine algebraline tehe hulgal $\text{End}(A)$. Hulgateooriast on teada, et see tehe on alati assotsiatiivne, ja samasusteisendus id_A on ilmselt homomorfism, kusjuures $\text{id}_A \circ f = f = f \circ \text{id}_A$ iga $f \in \text{End}(A)$ korral. $\square$

2.4 Isomorfismid

Definitsioon 2.20 Bijektiivseid Ω -algebrate homomorfisme nimetatakse **isomorfismideks**. Ω -algebrad A ja B nimetatakse **isomorfseteks**, kui leidub isomorfism $f : A \rightarrow B$. Sellisel juhul kirjutatakse $A \cong B$.

Definitsioon 2.21 Isomorfismi Ω -algebrast iseendasse nimetatakse **automorfismiks**. Ω -algebra A kõigi automorfismide hulka tähistatakse sümboliga $\text{Aut}(A)$.

Näide 2.22 Vektorruumid $\text{Mat}_2(\mathbb{R})$ ja $\mathbb{R}^4$ (üle korpuse $\mathbb{R}$) on isomorfised. Isomorfismiks sobib näiteks kujutus $f : \text{Mat}_2(\mathbb{R}) \rightarrow \mathbb{R}^4$, mis on defineeritud võrdusega

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

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

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

Tõestame mõned lihtsamad isomorfismide omadused.

Lause 2.23 *Isomorfismide korrutis on isomorfism.*

TÕESTUS. Hulgateooriast teame, et bijektiivsete kujutuste korrutis on bijektiivne. Lause 2.18 põhjal on ka homomorfismide korrutis homomorfism. $\square$

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

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

Lause 2.24 *Isomorfismi pöördkujutus on isomorfism.*

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

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

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

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

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

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

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

□

Järeldus 2.25 Iga Ω -algebra A korral on $\text{Aut}(A)$ rühm kujutuste korrumise suhtes.

Lauses 2.24 tuleb välja, et ω -algebrate isomorfismid on parajasti isomorfismid Ω -algebrate kategoorias. Sellest järeldub tänu lausele 1.16, et Ω -algebrate isomorfisuse seos on ekvivalentsiseos.

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 isomorfisuse järgi ja võimaluse korral leida igast klassist üks võimalikult lihtne esindaja. Näiteks võib küsida: kui palju on (isomorfismi täpsuseni) neljaelemendilisi rühmi?

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

2.5 Faktorstruktuurid

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

Definitsioon 2.26 Ω -algebra A **kongruents** on selline ekvivalentsiseos ρ hulgal A , mis on kooskõlas tehete. See tähendab, et

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

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

Kooskõla kahekohalise tehete $*$ tähendab seda, et

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

Näide 2.27 Vaatleme poolrühma $(\mathbb{N}, \cdot)$ (siin $\Omega = \Omega_2 = \{\cdot\}$). Lihtne on veenduda, et seos ρ , mis on defineeritud eeskirjaga

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

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

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

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

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

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

Tuleb välja, et vektorruumi kongruentse saab kirjeldada alamruumide abil.

Lause 2.28 *Olgu V vektorruum üle korpusse 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*

$$a \rho b \iff a - b \in V'. \quad (2.1)$$

TÕESTUS. TARVILIKKUS. Olgu ρ vektorruumi V kongruents. Tähistame nullelemendi ekvivalentsiklassi sümboliga V' , s.t.

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

Näitame, et V' on vektorruumi V alamruum.

Kuna refleksiivsuse tõttu $0_V \rho 0_V$, siis $0_V \in V'$ ja V' on mittetühi. Olgu nüüd $a, b \in V'$. Siis $a \rho 0_V$ ja $b \rho 0_V$. Et ρ on kongruents, siis $(a + b) \rho (0_V + 0_V)$ ehk $(a + b) \rho 0_V$. Seega $a + b \in V'$. Kui veel $k \in K$, siis $ka \rho k0_V$ ehk $ka \rho 0_V$, mis tähendab, et $ka \in V'$. Kuna V' rahuldab tingimusi AR1 ja AR2, siis lause 2.10 põhjal on V' alamruum.

Tõestame samaväärsuse (2.1). Oletame, et $a \rho b$. Kuna ka $(-b) \rho (-b)$, siis kasutades ρ kooskõla liitmisega saame, et $(a - b) \rho (b - b)$ ehk $(a - b) \rho 0_V$. Järelikult $a - b \in V'$. Vastupidi, kui $a - b \in V'$, siis $(a - b) \rho 0_V$. Kuna $b \rho b$, siis saame, et $(a - b + b) \rho (0_V + b)$, kust $a \rho b$.

PIISAVUS. Oletame, et leidub V mingi alamruum V' nii, et kehtib (2.1). Näitame, et ρ on kongruents. Kõigepealt veendume, et ρ on ekvivalentsiseos.

Kuna $a - a = 0_V \in V'$ 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. Transitiiivsuse 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 transitiiivne ning me oleme näidanud, et ta on ekvivalentsiseos.

Veendume nüüd, et ρ on kooskõlas teheteaga. 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 (2.1) võime öelda, et $ka \rho kb$. Võttes $k = -1$ saame, et $(-a) \rho (-b)$. Seega on ρ kooskõlas ka kõigi ühekojaliste teheteaga. $\square$

Olgu ρ mingi kongruents Ω -algebral A . Vaatleme faktorhulka

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

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

$$\omega^{A/\rho}(\overline{a_1}, \overline{a_2}, \dots, \overline{a_n}) := \overline{\omega^A(a_1, a_2, \dots, a_n)}. \quad (2.2)$$

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

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

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

Vaatleme vektorruumi V (üle korpuse K) kongruentsi ρ , mille korral $\overline{0_V} = V'$. 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 2.28 ütleb muuhulgas, et iga alamruum V' tekitab ühe kongruentsi vektorruumil V , kusjuures ekvivalentsiklassid selle kongruentsi järgi on hulgad $a + V'$, $a \in V$. Hulka $a + V'$ nimetatakse **kõrvalklassiks alamruumi V' järgi esindajaga a** . On selge, et

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

Faktorhulka sellise kongruentsi järgi tähistatakse

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

Vastavalt eespoolöeldule defineeritakse faktorhulgal V/V' tehted järgmiselt:

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

Lause 2.29 Kui V' on vektorruumi V (üle korpuse K) alamruum, siis faktorhulk V/V' on ka vektorruum üle korpuse K eelpool defineeritud tehete suhtes.

TÕESTUS. Nagu juba nägime, tehete definitsioonid on korrektsed.

VR1. Olgu $a, b, c \in V$. Siis

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

VR2. Mistahes $a \in V$ korral

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

Ülejäänud tingimuste kontroll on analoogiline. □

Lause 2.30 Olgu V' vektorruumi V (üle korpuse K) alamruum. Kujutus

$$\pi : V \rightarrow V/V', \quad a \mapsto \bar{a}$$

on sürjektiivne lineaarkujutus.

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

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

□

Lauses 2.30 defineeritud kujutust π nimetatakse vektorruumi V **loomulikuks projektsiooniks** faktorruumile V/V' .

Näide 2.31 Vaatleme vektorruumi $V := \mathbb{R}^2$ üle korpuse $\mathbb{R}$ ja selle alamruumi $V' := \{(z, 0) \mid z \in \mathbb{R}\}$. Siis kõrvalklassid V' järgi on kujul

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

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

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

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

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

Tehted faktorruumil on defineeritud kõrvalklasside esindajate abil:

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

2.6 Homomorfismiteoreem

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

Definitsioon 2.32 Olgu V ja U vektorruumid üle korpuse K . Lineaarkujutuse $f : V \rightarrow U$ **tuum** $\text{Ker } f$ defineeritakse järgmiselt:

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

Lihtne on veenduda, et kehtivad järgmised tulemused tuumade kohta.

Lause 2.33 ([1], lemma 4.1.8) Kui $f : V \rightarrow U$ on lineaarkujutus, siis $\text{Ker}(f)$ on vektorruumi V alamruum.

Lause 2.34 ([1], lause 4.1.10) Lineaarkujutus $f : V \rightarrow U$ on üksühene parajasti siis, kui $\text{Ker } f = \{0_V\}$.

Teoreem 2.35 (Homomorfismiteoreem) Olgu $f : V \rightarrow U$ lineaarkujutus. Siis leidub üksühene lineaarkujutus $g : V/\text{Ker } f \rightarrow U$ nii, et $f = g \circ \pi$, kus $\pi : V \rightarrow V/\text{Ker } f$ on loomulik projektsioon.

$$\begin{array}{ccc} V & \xrightarrow{f} & U \\ & \searrow \pi & \nearrow g \\ & V/\text{Ker } f & \end{array}$$

TÕESTUS. Defineerime kujutuse $g : V/\text{Ker } f \rightarrow U$ võrdusega

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

$a \in V$. 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

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

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

$$\begin{aligned} g(\bar{a} + \bar{b}) &= g(\overline{a+b}) = f(a+b) = f(a) + f(b) = g(\bar{a}) + g(\bar{b}), \\ g(k\bar{a}) &= g(\overline{ka}) = f(ka) = kf(a) = kg(\bar{a}) \end{aligned}$$

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

$$(g \circ \pi)(a) = g(\pi(a)) = g(\bar{a}) = f(a)$$

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

Järeldus 2.36 Kui lineaarkujutus $f : V \rightarrow U$ on sürjektiivne, siis $V/\text{Ker}(f) \cong U$.

TÕESTUS. Näitame, et lineaarkujutus $g : V/\text{Ker}(f) \rightarrow U$ 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 $g(\bar{a}) = u$. $\square$

Näide 2.37 Vaatleme jälle faktorruumi V/V' näitest 2.31. Vaatleme ka hulka $\mathbb{R}$ vektorruumina üle iseenda ja defineerime kujutuse $f : V \rightarrow \mathbb{R}$ võrdusega

$$f(a, b) := b.$$

Lihtne on näha, et f on sürjektiivne lineaarkujutus ja $\text{Ker}(f) = V'$. Järelduse 2.36 põhjal võime öelda, et $V/V' = V/\text{Ker}(f) \cong \mathbb{R}$.

2.7 Baasi olemasolu

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

Teoreem 2.38 ([1], teoreem 3.2.3) Kui mittetriviaalses vektorruumis on olemas lõplik moodustajate süsteem, siis selles vektorruumis leidub baas.

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

Definitsioon 2.39 Osaliselt järjestatud hulk on hulk, millel on antud osalise järjestuse seos, s.t. binaarne seos, mis on refleksiivne, antisümmeetriline ja transitiivne.

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

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

Definitsioon 2.40 Ahel ehk lineaarselt järjestatud hulk on selline osaliselt järjestatud hulk $(P, \leq)$, kus iga $a, b \in P$ korral $a \leq b$ või $b \leq a$ (s.t. mistahes kaks elementi on võrreldavad).

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

Näide 2.41 Hulk $\mathbb{Q}$ on ahel osaliselt järjestatud hulgas $(\mathbb{R}, \leq)$. Samuti hulk, mis koosneb elementidest $-5 \leq -1 \leq 2 \leq 13$.

Definitsioon 2.42 Olgu A osaliselt järjestatud järjestatud hulga $(P, \leq)$ alamhulk. Elementi $u \in P$ nimetatakse hulga A **ülemiseks tõkkeks**, kui $a \leq u$ iga $a \in A$ korral.

Definitsioon 2.43 Öeldakse, et element $m \in P$ on osaliselt järjestatud järjestatud hulga $(P, \leq)$ **maksimaalne element**, kui ei leidu sellist elementi $p \in P$, et $m < p$.

Lemma 2.44 (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 2.45 Olgu V vektorruum üle korpuse K ja $a_1, \dots, a_s \in V$, kus $s \in \mathbb{N}$. Mistahes avaldist

$$k_1 a_1 + k_2 a_2 + \dots + k_s a_s, \quad (2.3)$$

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

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

Definitsioon 2.46 Vektorruumi V (mis on antud üle korpuse K) lõplikku vektorite hulka $\{a_1, a_2, \dots, a_s\}$, $s \in \mathbb{N}$, nimetatakse **lineaarselt sõltumatuks**, kui mistahes skalaaride $k_1, k_2, \dots, k_s \in K$ korral võrdusest

$$k_1 a_1 + k_2 a_2 + \dots + k_s a_s = 0_V$$

järeldub, et

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

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

Definitsioon 2.47 Vektorite hulka nimetatakse **lineaarselt sõltuvaks**, kui ta ei ole lineaarselt sõltumatu

Järgmised kolm lauset on tuttavad kursusest Algebra I.

Lause 2.48 ([1], lause 3.1.3) *Ühestainsast vektorist a koosnev hulk on lineaarselt sõltumatu parajasti siis, kui $a \neq 0_V$.*

Lause 2.49 ([1], lause 3.1.4) *Lineaarselt sõltumatu vektorite hulga iga alamhulk on ka lineaarselt sõltumatu.*

Lause 2.50 ([1], lause 3.1.6) *Nullist erinevate vektorite lõplik hulk, mis sisaldab vähemalt kahte vektorit, on lineaarselt sõltuv parajasti siis, kui selle hulga vektorite mistahes järjestuse korral leidub vektor, mis avaldub eelnevate vektorite lineaarkombinatsioonina.*

Definitsioon 2.51 Vektorruumi V vektorite hulka B nimetatakse **baasiks**, kui

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

Näide 2.52 Vaatleme reaalarvuliste kordajatega polünoomide vektorruumi $\mathbb{R}[X]$. Selles vektorruumis on üheks baasiks hulk

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

Selles vektorruumis ei leidu lõplikku baasi.

Tõestame nüüd selle paragrahvi põhitulemuse.

Teoreem 2.53 *Igas mittetriviaalses vektorruumis leidub baas.*

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

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

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

Vaatleme hulka P osaliselt järjestatud hulkana sisalduvusseose $\subseteq$ suhtes ja näitame, et ta rahuldab Zorni lemma eeldusi. Olgu $a \in V \setminus \{0_V\}$. Siis lause 2.48 tõttu on hulk $\{a\}$ lineaarselt sõltumatu. Seega $\{a\} \in P$ ja $P \neq \emptyset$.

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

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

ja näitame, et see hulk on lineaarselt sõltumatu. Olgu $\{a_1, \dots, a_s\}$ hulga A suvaline lõplik alamhulk. Siis leiduvad indeksid $\alpha_1, \dots, \alpha_s \in I$ nii, et $a_i \in A_{\alpha_i}$ iga $i \in \{1, \dots, s\}$ korral. Kuna hulgal A_{α_i} moodustavad lõpliku ahela, siis sisaldab üks neist hulkadest, olgu see näiteks A_{α_k} , kõiki ülejäänud hulki ning seega $a_1, \dots, a_s \in A_{\alpha_k}$. Kuna $A_{\alpha_k} \in P$, siis on ta lineaarselt sõltumatu ja seega ka tema alamhulk $\{a_1, \dots, a_s\}$ on lineaarselt sõltumatu tänu lausele 2.49. Sellega on näidatud, et A on lineaarselt sõltumatu, millest järeldub, et $A \in P$. Et $A_\alpha \subseteq A$ iga $\alpha \in I$ korral, siis A on ahela $\{A_\alpha \mid \alpha \in I\}$ ülemine tõke osaliselt järjestatud hulgas P . Sellega oleme näidanud, et Zorni lemma eeldused on täidetud. Lemmat rakendades saame järeldada, et hulgas P leidub maksimaalne element.

Olgu üheks hulga P maksimaalseks elementiks B . Näitame, et B on vektorruumi V baas. Kuna $B \in P$, siis B on lineaarselt sõltumatu. Näitame, et V iga nullist erinev vektor avaldub B elementide lineaarkombinatsioonina. Olgu $a \in V \setminus \{0_V\}$. Kui $a \in B$, siis a avaldub B elementide lineaarkombinatsioonina: $a = \mathbf{1}a$. Eeldame edasises, et $a \notin B$. Kuna $B \subset B \cup \{a\}$ ja B on maksimaalne lineaarselt sõltumatu vektorite hulk, siis hulk $B \cup \{a\}$ peab olema lineaarselt sõltuv. Seega hulgal $B \cup \{a\}$ peab leiduma lõplik lineaarselt sõltuv alamhulk S . Kuna B on lineaarselt sõltumatu, siis ei ole võimalik, et $S \subseteq B$. Seega S peab sisaldama vektori a . Järjestame hulga S vektorid nii, et a on viimane. Siis lause 2.50 põhjal avaldub mingi hulga S vektor eelnevate lineaarkombinatsioonina. Kuna B on lineaarselt sõltumatu, siis saab see olla vaid vektor a . Seega vektor a avaldub hulka B kuuluvate vektorite lineaarkombinatsioonina, mida oligi tarvis tõestada. $\square$

Märkus 2.54 Kuna me lugesime tühja vektorite hulga lineaarselt sõltumatuks, siis vastavalt definitsioonile 2.51 on $\emptyset$ triviaalse vektorruumi $V = \{0_V\}$ baas.

2.8 Otsekorrutised ja välised otsesummad

Tuletame meelde hulkade otsekorrutisega seotud mõisted.

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

$$\prod_{i \in I} X_i = \left\{ x : I \rightarrow \bigcup_{i \in I} X_i \mid (\forall i \in I) x(i) \in X_i \right\}.$$

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

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

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

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

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

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

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

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

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

Lause 2.55 Üle korpuse K vaadeldavate vektorruumide otsekorrutis on korrutis kategoorias Vec_K .

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

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

Ülejäänud vektorruumi definitsiooni tingimuste kontroll on analoogiline. Seega vektorruumide otsekorutus on vektorruum.

Veendume nüüd, et see on korutus kategoorias $\mathbf{Vec}_K$. Otsekorutise projektsioonid

$$p_i : V \longrightarrow V_i, \quad (x_j)_{j \in I} \mapsto x_i,$$

$i \in I$, on lineaarkujutused, sest

$$\begin{aligned} p_i((x_j)_{j \in I} + (x'_j)_{j \in I}) &= p_i((x_j + x'_j)_{j \in I}) = x_i + x'_i = p_i((x_j)_{j \in I}) + p_i((x'_j)_{j \in I}), \\ p_i(k(x_j)_{j \in I}) &= p_i((kx_j)_{j \in I}) = kx_i = kp_i((x_j)_{j \in I}). \end{aligned}$$

Oletame nüüd, et meil on antud veel mingi vektorruum Q koos lineaarkujutustega $q_i : Q \longrightarrow V_i$, $i \in I$. Defineerime kujutuse $m : Q \longrightarrow V$ võrdusega

$$m(a) := (q_j(a))_{j \in I}.$$

Kuna q_i -d on lineaarkujutused, siis tuleb kergesti välja, et ka m on lineaarkujutus. Ta muudab kolmnurga

$$\begin{array}{ccc} Q & & \\ \downarrow m & \searrow q_i & \\ V & \xrightarrow{p_i} & V_i \end{array}$$

kommutatiivseks, sest iga $a \in Q$ korral

$$(p_i \circ m)(a) = p_i((q_j(a))_{j \in I}) = q_i(a).$$

Tõestuse lõpetamiseks jääb veel näidata, et m on üheselt määratud. Olgu ka veel $n : Q \longrightarrow V$ lineaarkujutus, mille puhul $p_i \circ n = q_i$ iga $i \in I$ korral. Olgu $a \in Q$ ja $n(a) = (y_j)_{j \in I}$. Siis $q_i(a) = p_i(n(a)) = y_i$ ja

$$m(a) = (q_i(a))_{i \in I} = (y_i)_{i \in I} = n(a).$$

Järelikult $m = n$. □

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

$$\bigoplus_{i \in I} V_i := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} V_i \mid \text{peres } (x_i)_{i \in I} \text{ on lõplik arv nullist erinevaid komponente} \right\}.$$

Lihtne on veenduda, et see hulk on otsekorutise $\prod_{i \in I} V_i$ alamruum. Seega lause 2.11 põhjal on $\bigoplus_{i \in I} V_i$ ise ka vektorruum komponenthaaval defineeritud tehete suhtes. Seda vektorruumi nimetatakse **vektorruumide** $V_i, i \in I$ **väliseks otsesummaks**.

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

$$V_1 \oplus V_2 \oplus \dots \oplus V_n = V_1 \times V_2 \times \dots \times V_n. \quad (2.4)$$

Näitame, et väline otsesumma on kokorutus.

Lause 2.56 Üle korpuse K vaadeldavate vektorruumide väline otsesumma on kokorrutis kategoorias Vec_K .

TÕESTUS. Kokorrutise sisestused $u_i : V_i \rightarrow \bigoplus_{k \in I} V_k$ defineerime võrdusega

$$u_i(x) := (x_k)_{k \in I},$$

kus $x_i = x$ ja kõik teised komponendid on nullid. Lihtne on veenduda, et kujutused u_i , $i \in I$, on lineaarkujutused.

Kui Q on mingi vektorruum ja $q_i : V_i \rightarrow Q$, $i \in I$, on lineaarkujutuste süsteem, siis defineerime kujutuse $m : \bigoplus_{k \in I} V_k \rightarrow Q$ võrdusega

$$m((x_i)_{i \in I}) := \sum_{i \in I} q_i(x_i),$$

kus viimases summas on lõpliku arv nullist erinevaid liidetavaid ja me summeerime neid. Kujutuste q_i , $i \in I$, lineaarsusest järeldub kergesti, et m on lineaarkujutus. Ta muudab diagrammi

$$\begin{array}{ccc} & Q & \\ & \uparrow & \nwarrow q_i \\ m \downarrow & & \\ \bigoplus_{k \in I} V_k & \xleftarrow{u_i} & V_i \end{array}$$

kommutatiivseks, sest kui $a \in V_i$ ja $u_i(a) = (x_k)_{k \in I}$, siis

$$(m \circ u_i)(a) = m((x_k)_{k \in I}) = \sum_{k \in I} q_k(x_k) = q_i(a).$$

Oletame nüüd, et ka $n : \bigoplus_{k \in I} V_k \rightarrow Q$ on selline lineaarkujutus, et $n \circ u_i = q_i$ iga $i \in I$ korral. Siis iga $(x_k)_{k \in I} \in \bigoplus_{k \in I} V_k$ korral

$$\begin{aligned} m((x_k)_{k \in I}) &= m\left(\sum_{k \in I} u_k(x_k)\right) = \sum_{k \in I} m(u_k(x_k)) = \sum_{k \in I} q_k(x_k) = \sum_{k \in I} n(u_k(x_k)) \\ &= n\left(\sum_{k \in I} u_k(x_k)\right) = n((x_k)_{k \in I}). \end{aligned}$$

Järelikult $m = n$. □

Märkus 2.57 Täpselt samamoodi saab näidata, et Abeli rühmade kategoorias $\mathbf{Ab}$ ja R -moodulite kategoorias Mod_R on korrutisteks otsekorrutised ja kokorrutisteks välised otsesummad.

2.9 Vektorruumide kirjeldus

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

Teoreem 2.58 *Iga mittetriviaalse vektorruumi V korral (üle korpuse K) leidub selline hulk I , et*

$$V \cong \bigoplus_{i \in I} V_i,$$

kus $V_i = K$ iga $i \in I$ korral.

TÕESTUS. Teoreemi 2.53 põhjal leidub vektorruumis V baas. Indekseerime selle baasi vektorid ära mingi hulga I elementidega, s.t. olgu see baas $\{e_i \mid i \in I\}$. Võtame iga $i \in I$ korral $V_i := K$. Defineerime kujutuse $f : \bigoplus_{i \in I} V_i \rightarrow V$ võrdusega

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

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

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

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

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

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

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

Kujutuse f üksühesuse kontrollimiseks kasutame lauset 2.34. Oletame, et

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

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

Järeldus 2.59 *Kui n on naturaalarv ja V on n -mõõtmeline vektorruum üle korpuse K , siis $V \cong K^n$.*

TÕESTUS. See järeldub teoreemist 2.58 ja võrdusest (2.4).

□

Peatükk 3

Rühm

3.1 Rühm, alamrühm

Definitsioon 3.1 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 iga $a \in G$ korral $a * e = a = e * a$;

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

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

Niisiis rühm on Ω -algebra, millel on kolm tehet:

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

Näide 3.2 1. Iga $n \geq 2$ korral on $\mathbb{Z}_n$ rühm liitmise suhtes.

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

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

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

rühmad maatriksite korrumtamise suhtes.

Lihtne on veenduda, et kehtib järgmine tulemus.

Lause 3.3 Rühma G mittetühi alamhulk H on alamrühm parajasti siis, kui H on kinnine korrutamise ja pöördlemendi võtmise suhtes.

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

Definitsioon 3.4 Olgu H rühma G alamrühm ja $a \in G$. Hulka

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

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

Lause 3.5 Olgu G rühm, $H \leq G$ ja $a, b \in G$. Siis järgmised väited on samaväärsed.

1. $aH = bH$.

2. $a^{-1}b \in H$.

3. $b^{-1}a \in H$.

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

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

Väidete 1 ja 3 samaväärsuse saab tõestada analoogiliselt. $\square$

Järeldus 3.6 Kui H on rühma G alamrühm ja $b \in G$, siis $H = bH$ parajasti siis, kui $b \in H$.

Lause 3.7 Olgu H rühma G alamrühm. Siis vasakpoolsed kõrvalklassid aH , $a \in G$ tekitavad hulga G tükelduse.

TÕESTUS. Kuna $a \in aH$ iga $a \in G$ korral, siis hulgad aH on mittetühjad. Samuti on selge, et

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

Veendume, et kui hulgad aH ja bH lõikuvad, siis on nad sama hulk. Selleks oletame, et leidub element $g = ah_1 = bh_2 \in aH \cap bH$. Siis $h_1 = a^{-1}bh_2$ ja $a^{-1}b = h_1h_2^{-1} \in H$. Lause 3.5 põhjal $aH = bH$. Sellega oleme näidanud, et tegemist on tükeldusega. $\square$

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

Lause 3.8 Olgu G rühm ja $H \leq G$. Siis iga $a \in G$ korral $|aH| = |H|$.

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

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

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

Definitsioon 3.9 Lõpliku rühma **järguks** nimetatakse tema elementide arvu.

Teoreem 3.10 (Lagrange'i teoreem) Lõpliku rühma iga alamrühma järk jagab rühma järku.

TÕESTUS. Lause 3.8 põhjal teame, et kõik vasakpoolsed kõrvalklassid on sama võimsusega (võimsusega $|H|$). Samuti teame, et kõrvalklassid tekitavad hulga G tükelduse. Seega kui neid kõrvalklasse on m tükki, siis $|G| = m \cdot |H|$ ehk $|H|$ jagab arvu $|G|$. $\square$

3.2 Normaalgajaja, faktorrühm

Definitsioon 3.11 Rühma G alamrühma H nimetatakse **normaalseks alamrühmaks** ehk **normaalgajajaks**, kui iga $g \in G$ korral $gH = Hg$.

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

Lause 3.12 Rühma G alamrühm H on normaalgajaja 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. $\square$

Näide 3.13 1. Iga rühma G korral on alamrühmad G ja $\{1_G\}$ normaalsed. Neid normaalgajajaid nimetatakse **triviaalseteks**.

2. Kommutatiivse rühma kõik alamrühmad on normaalgajajad.

3. Rühma $GL_n(\mathbb{R})$ alamrühm $SL_n(\mathbb{R})$ on normaalgajaja.

Märkus 3.14 Üldiselt ei pruugi gH ja Hg võrdsed olla. Selle kohta võib näite leida raamatust [1] (näide 6.1.8).

Analoogiliselt lausega 2.14 saab tõestada järgmise tulemuse.

Lause 3.15 Olgu G ja G' rühmad. Kujutus $f : G \rightarrow G'$ on rühmade homomorfism parajasti siis, kui

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

iga $a, b \in G$ korral.

Definitsioon 3.16 Olgu $f : G \rightarrow G'$ rühmade homomorfism. Hulka

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

nimetatakse homomorfismi f **tuumaks**.

Lause 3.17 Rühmade homomorfismi tuum on normaaljagaja.

TÕESTUS. Olgu $f : G \rightarrow G'$ rühmade homomorfism, $a \in \text{Ker}(f)$ ja $g \in G$. Siis

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

s.t. $g^{-1}ag \in \text{Ker}(f)$. Järelikult $\text{Ker}(f) \trianglelefteq G$ lause 3.12 põhjal. $\square$

Teoreem 3.18 Iga rühma G korral leidub üksühene vastavus kongruentside hulga $\text{Con}(G)$ ja normaaljagajate hulga $\mathcal{N}(G)$ vahel.

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

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

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

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

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

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

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

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

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

Defineerime kujutuse

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

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

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

s.t. $\rho_H = \rho$. Järelikult

$$(\kappa \circ \nu)(\rho) = \kappa(\bar{1}) = \kappa(H) = \rho_H = \rho.$$

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

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

$$(\nu \circ \kappa)(H) = \nu(\rho_H) = \bar{1}_{\rho_H} = H,$$

sest $y \in \bar{1}_{\rho_H}$ parajasti siis, kui $1\rho_H y$ ehk $y \in H$. □

Olgu H rühma G normaalne alamrühm. Teoreemi 3.18 tõestuses nägime, et ν bijektiivsuse tõttu leidub täpselt üks G kongruents ρ , mille korral $\bar{1}_\rho = H$. Täpsemalt öeldes $\rho = \rho_H$. Paneme tähele, et mistahes $a \in G$ korral

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

Viimase võrduse puhul on sisalduvus $\{b \in G \mid aH = bH\} \subseteq aH$ ilmne. Vastupidi, kui $ah \in aH$, siis $a^{-1}ah = h \in H$ ja lauset 3.5 kasutades saame võrduse $aH = ahH$. Seega $ah \in \{b \in G \mid aH = bH\}$. Niisiis ρ -klassid on täpselt H (vasakpoolsed) kõrvalklassid rühmas G : iga $a \in G$ korral

$$\bar{a} = aH.$$

Seega faktorrühma G/ρ elementideks on kõrvalklassid $aH, a \in G$, ja faktorrühma korrutamistehte definitsiooni (vt. definitsiooni 2.2)

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

võib esitada kujul

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

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

Definitsioon 3.19 Rühma G **faktorrühmaks** normaalse alamrühma H järgi nimetatakse rühma G/H , mille elementideks on kõrvalklassid $aH, a \in G$, ja mille korrutamine toimub eeskirja

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

kohaselt. Selle rühma ühikelement on $H = 1_G H$ ja elemendi aH pöördement on $a^{-1}H$.

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

Analoogiliselt teoreemiga 2.35 saab näidata, et kehtib järgmine teoreem.

Teoreem 3.20 (Homomorfismiteoreem) Olgu $f : G \rightarrow G'$ rühmade homomorfism. Siis leidub üksühene homomorfism $g : G/\text{Ker}(f) \rightarrow G'$ nii, et $f = g \circ \pi$, kus $\pi : G \rightarrow G/\text{Ker}(f)$ on loomulik projektsioon.

Järeldus 3.21 Kui $f : G \rightarrow G'$ on surjektiivne rühmade homomorfism, siis $G' \cong G/\text{Ker}(f)$.

Näide 3.22 Kujutus

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

on multiplikatiivsete rühmade homomorfism (Miks?), kusjuures $\text{Ker}(\det) = \text{SL}_n(\mathbb{R})$. See homomorfism on surjektiivne, sest iga reaalarvu $r \in \mathbb{R} \setminus \{0\}$ jaoks leidub n -ndat järku ruutmaatriksi (Milline?), mille determinant on r . Järelduse 3.21 põhjal võime öelda, et

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

3.3 Tsüklilised rühmad

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

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

Lihtne on veenduda, et selliselt defineeritud rühma elemendi astmete jaoks kehtivad harilikud astendamise reeglid: mistahes $k, l \in \mathbb{Z}$ korral $g^{k+l} = g^k \cdot g^l$, $(g^k)^l = g^{kl}$ jne.

Kui tegemist on aditiivse rühmaga $(A, +)$, siis defineeritakse analoogiliselt elemendi $a \in A$ kordsed ka , kus $k \in \mathbb{Z}$.

Multiplikatiivse rühma $(G, \cdot)$ elemendi g korral tähistame sümboliga $\langle g \rangle$ hulga G alamhulka, mis koosneb elemendi g kõigist astmetest:

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

On lihtne näha, et hulk $\langle g \rangle$ on rühma G alamrühm. Seda alamrühma nimetatakse elemendi g poolt **tekitatud** (või **moodustatud**) **alamrühmaks**.

Definitsioon 3.23 Rühma $(G, \cdot)$ nimetatakse **tsükliliseks**, kui leidub selline element $g \in G$, et $G = \langle g \rangle$. Seda elementi g nimetatakse tsüklilise rühma **tekitajaks** (või **moodustajaks**).

Teisisõnu rühm $(G, \cdot)$ on tsükliline, kui temas leidub selline element g , mille astmetena esituvad kõik selle rühma elemendid: $G = \{g^k \mid k \in \mathbb{Z}\}$.

Aditiivne rühm $(A, +)$ on tsükliline, kui leidub selline $a \in A$, et $A = \{ka \mid k \in \mathbb{Z}\}$.

Näide 3.24 1. Rühm $(\{1, -1\}, \cdot)$ on tsükliline rühm moodustajaga -1 .

2. Rühm $(\mathbb{Z}, +)$ on tsükliline rühm moodustajaga 1 või -1 .

3. Rühm $(\mathbb{Z}_n, +)$ on tsükliline rühm moodustajaga $\bar{1}$ (aga sellel rühmal võib olla teisi moodustajaid).

Meil läheb vaja järgmisi arvuteoreetilisi tulemusi.

Lause 3.25 Kui $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$, siis leiduvad $q, r \in \mathbb{Z}$ nii, et $a = bq + r$ ja $0 \leq r < b$.

Lause 3.26 Mistahes $a, b \in \mathbb{Z}$ korral $\text{SÜT}(a, b) = 1$ parajasti siis, kui leiduvad $u, v \in \mathbb{Z}$ nii, et $au + bv = 1$.

Järgmine teoreem tõestatakse kursuses Algebra II.

Teoreem 3.27 Sama järku tsüklilised rühmad on isomorfsed, kusjuures iga lõpmatu tsükliline rühm on isomorfne rühmaga $(\mathbb{Z}, +)$ ja iga n -elemendiline tsükliline rühm on isomorfne rühmaga $(\mathbb{Z}_n, +)$.

3.4 Rühma elemendi järk

Definitsioon 3.28 Olgu g rühma $(G, \cdot)$ element. Kui $|\langle g \rangle| = n \in \mathbb{N}$, siis öeldakse, et elemendi g **järk on n** ja kirjutatakse $\text{ord}_G(g) = n$ või lihtsalt $\text{ord}(g) = n$. Kui $\langle g \rangle$ on lõpmatu rühm, siis öeldakse, et g on **lõpmatu järku element**.

Definitsioonist tuleb välja, et igas rühmas on täpselt üks esimest järku element — see on ühikelement.

Näide 3.29 1. Vaatleme rühmade $(\mathbb{Z}_3, +)$ ja $(\mathbb{Z}, +)$ otsekorrutist $G = \mathbb{Z}_3 \times \mathbb{Z}$. Siis $\text{ord}_G((\bar{2}, 0)) = 3$ ja $\text{ord}_G((\bar{0}, 5)) = \infty$.

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

Lagrange'i teoreemist järeldub vahetult järgmine väide.

Lause 3.30 Lõpliku rühma iga elemendi järk jagab rühma järku.

Teoreemi 3.27 tõestuse põhjal võime öelda, et kehtib järgmine tulemus.

Lause 3.31 Kui rühma $(G, \cdot)$ elemendi g järk on lõplik, siis on see vähim selline naturaalarv n , mille korral $g^n = 1_G$.

Lause 3.32 Olgu $(G, \cdot)$ rühm, $g \in G$ ja $k \in \mathbb{N}$. Siis

$$g^k = 1_G \iff \text{ord}(g) \mid k.$$

TÕESTUS. TARVILIKKUS. Kui $g^k = 1_G$, siis g on kindlasti lõplikku järku element, olgu $\text{ord}(g) = n$. Jagades arvu k jäägiga arvuga n saame leida $q, r \in \mathbb{Z}$ nii, et $k = nq + r$ ja $0 \leq r < n$. Järelikult

$$1_G = g^k = g^{nq+r} = g^{nq} \cdot g^r = (g^n)^q \cdot g^r = 1_G \cdot g^r = g^r.$$

Kuna n on vähim naturaalarv, mille korral $g^n = 1_G$, siis $r = 0$, s.t. $k = nq$. Seega n jagab arvu k .

PIISAVUS. Kui $\text{ord}(g) \mid k$, siis leidub $q \in \mathbb{N}$ nii, et $\text{ord}(g) \cdot q = k$, ning järelikult

$$g^k = g^{\text{ord}(g) \cdot q} = (g^{\text{ord}(g)})^q = 1_G^q = 1_G.$$

□

Lause 3.33 Olgu G n -ndat järku tsükliline rühm, $G = \langle g \rangle = \{1, g, \dots, g^{n-1}\}$ ja olgu $k \in \{1, \dots, n-1\}$. Element g^k on rühma G tekitaja parajasti siis, kui $\text{SÜT}(k, n) = 1$.

TÕESTUS. TARVILIKKUS. Olgu $G = \langle g^k \rangle$. Siis leidub selline $u \in \mathbb{Z}$, et $(g^k)^u = g$. Järelikult $g^{ku} = g$ ja $g^{ku-1} = 1$. Lause 3.32 põhjal $n \mid ku - 1$. Seega leidub $q \in \mathbb{Z}$ nii, et $ku - 1 = nq$ ehk $ku - nq = 1$. Lause 3.26 põhjal $\text{SÜT}(k, n) = 1$.

PIISAVUS. Olgu $\text{SÜT}(k, n) = 1$. Siis lause 3.26 põhjal leiduvad sellised $u, v \in \mathbb{Z}$, et $ku + nv = 1$. Järelikult

$$g = g^{ku+nv} = g^{ku} \cdot g^{nv} = (g^k)^u \cdot (g^n)^v = (g^k)^u \cdot 1^v = (g^k)^u$$

ja $g^l = (g^k)^{ul}$ iga $l \in \{1, \dots, n\}$ korral. Viimane tähendab, et $G = \langle g^k \rangle$. □

Lihtne on veenduda, et kehtib järgmine omadus.

Lemma 3.34 Kui $(G, \cdot)$ on rühm ja $g \in G$, siis $\text{ord}(g) = \text{ord}(g^{-1})$.

Lemma 3.35 Olgu $(G, \cdot)$ rühm, $g \in G$, $m, n \in \mathbb{N}$. Kui $\text{ord}(g) = mn$, siis $\text{ord}(g^m) = n$.

TÕESTUS. Tõestamiseks kasutame lauset 3.31. Olgu $\text{ord}(g) = mn$. Siis $(g^m)^n = g^{mn} = 1_G$. Kui oletada, et leidub $n' < n$, mille korral $(g^m)^{n'} = 1_G$, siis ka $g^{mn'} = 1$ ja $mn' < mn$, mis on vastuolus eeldusega. Seega n on vähim astendaja, mille korral $(g^m)^n = 1_G$; teiste sõnadega: $\text{ord}(g^m) = n$. □

Meenutame, et **triviaalseks rühmaks** loetakse üheelemendilist rühma.

Lause 3.36 Olgu G mittetriviaalne lõplik rühm. Rühmal G ei ole mittetriviaalseid pärisalamrühmi parajasti siis kui G on algarvulise järguga tsükliline rühm.

TÕESTUS. TARVILIKKUS. Eeldame, et rühmal $G \neq \{1_G\}$ ei ole mittetriviaalseid pärisalamrühmi. Võtame mingi elemendi $g \in G \setminus \{1_G\}$. Siis $\langle g \rangle = G$ (seega G on tsükliline) ja $\text{ord}(g) = |G|$. Oletame vastuväiteliselt, et $|G|$ ei ole algarv. Siis $|G| = mn$, kus $m, n \in \mathbb{N}$, $m, n \neq 1$. Lemma 3.35 põhjal

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

Kuna $n < |G|$, siis $\langle g^m \rangle$ on mittetriviaalne pärisalamrühm rühmas G , vastuolu. Järelikult $|G|$ peab olema algarv.

PIISAVUS. Olgu $G = \{1_G, g, g^2, \dots, g^{p-1}\}$ tsükliline rühm algarvulise järguga p ja $\{1\} \neq H \leq G$. Siis leidub $k \in \{1, \dots, p-1\}$ nii, et $g^k \in H$. Kuna $\text{SÜT}(k, p) = 1$, siis lause 3.33 põhjal

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

kust $H = G$. Seega rühmal G puuduvad mittetriviaalsed pärisalamrühmad. □

3.5 Lihtsad rühmad

Definitsioon 3.37 Rühma nimetatakse **lihtsaks**, kui tal ei ole mittetriviaalseid normaaljagajaid.

Ülesanne 3.38 Näidake, et kui p on algarv, siis rühm $(\mathbb{Z}_p, +)$ on lihtne.

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

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

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

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

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

nimetatakse **ühiksubstitutsiooniks**.

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

Definitsioon 3.39 Substitutsiooni nimetatakse **tsüklik**, kui ta paigutab mingeid elemente tsüklikiliselt ümber ning jätab ülejäänud elemendid paigale. Tsükli σ , mis paigutab ümber elemente $i_1, i_2, \dots, i_k$ nii, et

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

tähistame lühidalt

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

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

Definitsioon 3.40 Tsükleid $(i_1, i_2, \dots, i_k)$ ja $(j_1, j_2, \dots, j_l)$ nimetatakse **sõltumatuteks**, kui $\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_l\} = \emptyset$.

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

Lihtne on aru saada, et kehtib järgmine lause.

Lause 3.41 Iga substitutsiooni saab esitada sõltumatute tsüklite korrutisena.

Näide 3.42 Rühmas S_9 saame esitada

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

Definitsioon 3.43 **Transpositsioon** on tsükel pikkusega 2.

Algebra põhikursuses tõestatakse harilikult järgmine tulemus.

Lause 3.44 ([1], lause 4.3.15) *Transpositsioon on paaritu substitutsioon.*

Lause 3.45 *Olgu $n \geq 2$. Iga paarissubstitutsioon n elemendist on esitatav paarisarvu transpositsioonide korrutisena. Iga paaritu substitutsioon n elemendist on esitatav paaritu arvu transpositsioonide korrutisena.*

TÕESTUS. Paneme tähele, et

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

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

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

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

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

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

Järeldus 3.46 *Olgu $n \geq 2$. Siis on paaris- ja paarituid substitutsioone n elemendist ühepalju.*

Lause 3.47 *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 3.44 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. $\square$

Järeldus 3.48 *Substitutsioonid σ ja σ^{-1} on sama paarsusega.*

TÕESTUS. Lause 3.45 tõestuses nägime, et iga substitutsiooni saab esitada transpositsioonide korrutisena. Olgu σ esitatud k transpositsiooni korrutisena ja σ^{-1} l transpositsiooni korrutisena. Kuna $\varepsilon = \sigma \sigma^{-1}$ on paarissubstitutsioon, siis lause 3.47 põhjal on $k + l$ paarisarv. Järelikult on k ja l sama paarsusega, millest järeldub, et σ ja σ^{-1} on sama paarsusega. $\square$

Lause 3.49 *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 3.47 põhjal on tsükkel $(i_1, i_2, \dots, i_k)$ ja arv $k - 1$ sama paarsusega. $\square$

Lause 3.50 *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 3.45 põhjal saab σ ja τ esitada paarisarvu transpositsioonide korrutisena. Siis ka $\sigma\tau$ on paarisarvu transpositsioonide korrutis. Tänu lausele 3.47 on $\sigma\tau$ paarissubstitutsioon. Kuna pöördsubstitutsiooni paarsus on sama, mis esialgse oma, siis on A_n kinnine ka pöördlemendi 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 $\sigma^{-1}\tau\sigma \in A_n$. $\square$

Järeldus 3.51 *Kui $n \geq 3$, siis S_n ei ole lihtne.*

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

Ülesanne 3.52 Millise hästituntud rühmaga on isomorfne faktorühm S_n/A_n ?

Teoreem 3.53 *Kui $n \geq 5$, siis A_n on lihtne rühm.*

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

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

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

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

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

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

kus $s \geq 4$. Võtame $\psi := (i_1, i_2, i_3) \in S_n$. Tänu lausele 3.49 on 3-elemendilised tsüklid paarissubstitutsioonid, seega $\psi \in A_n$. Järelikult $\psi\varphi^{-1}\psi^{-1}\varphi \in N$. Arvutame välja korrutise $\psi\varphi^{-1}\psi^{-1}\varphi$. Selleks peame arvudele $1, 2, \dots, n$ rakendama järjest teisendusi $\varphi, \psi^{-1}, \varphi^{-1}$ ja ψ (just selles järjekorras). Paneme tähele, et kõik need teisendused jätavad arvud $j \in \{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_s\}$ paigale, s.t. $(\psi\varphi^{-1}\psi^{-1}\varphi)(j) = j$. Vaatame, kuidas need teisendused teisendavad arve $i_1, i_2, \dots, i_s$. Selleks koostame tabeli, kus iga rida näitab, kuidas vastav teisendus teisendab eelmises reas olevaid elemente:

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

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

2) Lahutuses leidub vähemalt kaks 3-elemendilist tsükli:

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

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

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

Sellega oleme vaadeldava olukorra taandanud juhule 1).

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

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

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:

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

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

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

Sellega on olukord taandatud juhule 2).

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

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

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

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

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

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

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

Seega N sisaldab kõiki 3-elementilisi tsükleid.

Tõestuse lõpetamiseks näitame, et $A_n \subseteq N$. Olgu $\psi \in A_n$ suvaline paarissubstitutsioon. Lause 3.45 põhjal on ψ esitatav paarisarvu transpositsioonide korrutisena:

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

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

Märkus 3.54 Saab näidata, et A_2 ja A_3 on lihtsad rühmad, aga A_4 ei ole.

Peatükk 4

Abeli rühm

4.1 Põhimõisted

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

Definitsioon 4.1 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 $0_A \in A$ nii, et iga $a \in A$ korral $a + 0_A = a = 0_A + a$;

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

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

Elementi 0_A tingimuses AG2 nimetatakse selle Abeli rühma **nullelemendiks** ja elementi $-a$ tingimuses AG3 nimetatakse elemendi a **vastandelemendiks**. Väga tihti kirjutatakse 0_A asemel lihtsalt 0 .

Näide 4.2 1. Iga vektorruum on muuhulgas Abeli rühm.

2. Iga $n \geq 2$ korral on jäägiklasside hulk $\mathbb{Z}_n$ Abeli rühm liitmise suhtes.

3. Iga $n \geq 3$ korral on substitutsioonide hulk S_n rühm, mis ei ole Abeli rühm.

Abeli rühmades räägitakse elementide a ja b korral summa kõrval ka nende **vahest**, mis defineeritakse võrdusega

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

Tingimuse AG3 põhjal on selge, et iga a korral

$$a - a = 0_A.$$

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

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

kus liidetavaid on n tükki. Lisaks sellele loetakse, et

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

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

$$\begin{aligned}(zw)a &= z(wa), \\ (z+w)a &= za + wa, \\ z(a+b) &= za + zb,\end{aligned}$$

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

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

Igas rühmas saab rääkida elementide järkudest. Siin paneme selle definitsiooni kirja kasutades Abeli rühmade aditiivset sümbolikat.

Definitsioon 4.3 Olgu a Abeli rühma A element ja $n \in \mathbb{N}$. Öeldakse, et elemendi a **järk** on n , kui $na = 0_A$ ja n on vähim naturaalarv, mille korral selline võrdus kehtib. Kui $na \neq 0_A$ ühegi naturaalarvu n korral, siis öeldakse, et element a on **lõpmatut järku**. Elemendi a järku tähistatakse sümboliga $\text{ord}(a)$.

On selge, et

$$\text{ord}(a) = 1 \iff a = 0_A.$$

Sõnastame lemma 3.35 ja lause 3.32 ümber Abeli rühmade keeles, sest neid läheb meil korduvalt vaja.

Lemma 4.4 Olgu $(A, +)$ Abeli rühm, $a \in A$ ja $m, n \in \mathbb{N}$. Kui $\text{ord}(a) = mn$, siis $\text{ord}(ma) = n$.

Lause 4.5 Kui A on Abeli rühm, $a \in A$ ja $m \in \mathbb{N}$, siis

$$ma = 0_A \iff \text{ord}(a) \mid m.$$

4.2 Sisemised otsesummad

Alustuseks defineerime Abeli rühma alamrühmade summa.

Definitsioon 4.6 Abeli rühma A alamrühmade $A_i, i \in I$, **summaks** nimetatakse A kõigi nende elementide hulka, mis esituvad alamrühmadesse A_i kuuluvate elementide lõpliku summana.

Abeli rühma A alamrühmade $A_i, i \in I$, summat tähistatakse $\sum_{i \in I} A_i$. Lõpliku arvu alamrühmade $A_1, \dots, A_n$ summat tähistatakse $A_1 + \dots + A_n$. Sellisel juhul

$$A_1 + \dots + A_n = \{a_1 + \dots + a_n \mid a_1 \in A_1, \dots, a_n \in A_n\}.$$

Lause 4.7 Abeli rühma A alamrühmade A_i , $i \in I$, summa on A vähim alamrühm, mis sisaldab kõiki neid alamrühmi.

TÕESTUS. Lihtne on näha, et hulk $\sum_{i \in I} A_i$ on A alamrühm. Samuti iga j korral $A_j \subseteq \sum_{i \in I} A_i$, sest iga elementi $a \in A_j$ saab vaadelda ühest liidetavast koosneva summana.

Kui B on rühma A alamrühm, mis sisaldab alamrühmi A_i , $i \in I$, siis peab B sisaldama kõiki summasid

$$a_1 + \dots + a_n, \quad \text{kus } n \in \mathbb{N}, a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}, i_1, \dots, i_n \in I.$$

Seega $\sum_{i \in I} A_i \subseteq B$. □

Definitsioon 4.8 Abeli rühma A alamrühmade A_i , $i \in I$, summat nimetatakse (**sisemiseks**) **otsesummaks** ja tähistatakse $\sum_{i \in I} A_i$, kui iga lõpliku arvu erinevate indeksite $i_1, \dots, i_n \in I$ korral summa $A_{i_1} + \dots + A_{i_n}$ iga element x avaldub üheselt kujul

$$x = a_1 + \dots + a_n, \quad \text{kus } a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}.$$

Teoreem 4.9 Olgu A_i , $i \in I$, Abeli rühma A alamrühmad. Siis järgmised tingimused on samaväärsed:

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

$$A_i \cap \left(\sum_{j \in I \setminus \{i\}} A_j \right) = \{0_A\}; \tag{4.1}$$

3. kui $a_1 + \dots + a_n = 0_A$, kus $a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}$ ning $i_1, \dots, i_n \in I$ on erinevad indeksid, siis $a_1 = \dots = a_n = 0_A$.

TÕESTUS. 1. $\Rightarrow$ 2. Eeldame, et $\sum_{i \in I} A_i = \sum_{i \in I} A_i$. Olgu

$$a \in A_i \cap \left(\sum_{j \in I \setminus \{i\}} A_j \right).$$

Siis $a \in A_i$ ning lisaks leiduvad veel erinevad indeksid $i_1, \dots, i_n \in I \setminus \{i\}$ ja elemendid $a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}$ nii, et

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

Tänu elemendi a esituse ühesusele alamrühmade summas $A_{i_1} + \dots + A_{i_n} + A_i$ (paneme tähele, et $a_1 + \dots + a_n + 0_A = a = 0_A + \dots + 0_A + a$) peab kehtima võrdus $a = 0_A$. Sellega oleme näidanud, et kehtib võrdus (4.1).

2. $\Rightarrow$ 3. Eeldame, et iga $i \in I$ korral kehtib võrdus (4.1) ning et $a_1 + \dots + a_n = 0_A$, kus $a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}$ ja $i_1, \dots, i_n \in I$ on erinevad indeksid. Siis iga $k \in \{1, \dots, n\}$ korral

$$-a_k = a_1 + \dots + a_{k-1} + a_{k+1} + \dots + a_n \in A_k \cap \left(\sum_{j \in I \setminus \{k\}} A_j \right) = \{0_A\}$$

ning seega $-a_k = 0$, kust $a_k = 0$.

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

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

kus $i_1, \dots, i_n \in I$ on erinevad indeksid ja $a_k, b_k \in A_{i_k}$ iga $k \in \{1, \dots, n\}$ korral. Siis

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

kus $a_k - b_k \in A_{i_k}$ iga $k \in \{1, \dots, n\}$ korral. Eelduse põhjal

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

ehk $a_1 = b_1, \dots, a_n = b_n$. □

Näide 4.10 Vaatleme Abeli rühma $A = \mathbb{Z}^3$ koos komponenthaaval defineeritud tehetege. Siis

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

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

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

See on otsesumma, sest kui $(x, y, z) \in A_1 \cap A_2$, siis $y = 0$ ja $x = y = z$, kust ka $x = z = 0$. Seega $A_1 \cap A_2 = \{(0, 0, 0)\}$.

Teoreem 4.11 Olgu A_i , $i \in I$, Abeli rühma A alamrühmad. Siis

$$A = \sum_{i \in I} A_i \implies A \cong \bigoplus_{i \in I} A_i.$$

TÕESTUS. Eeldame, et $A = \sum_{i \in I} A_i$. Defineerima kujutuse $\varphi : \bigoplus_{i \in I} A_i \rightarrow A$ võrdusega

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

Siin $\sum_{i \in I} a_i$ on pere $(a_i)_{i \in I}$ nullist erinevate komponentide (neid on lõplik arv!) summa rühmas A , kui selliseid komponente leidub, ja 0_A , kui neid ei leidu. Siis φ on rühmade homomorfism, sest mistahes $(a_i)_{i \in I}, (b_i)_{i \in I} \in \bigoplus_{i \in I} A_i$ korral

$$\begin{aligned} \varphi((a_i)_{i \in I} + (b_i)_{i \in I}) &= \varphi((a_i + b_i)_{i \in I}) && (\text{otsekorrutise} + \text{def.}) \\ &= \sum_{i \in I} (a_i + b_i) && (\varphi \text{ def.}) \\ &= \sum_{i \in I} a_i + \sum_{i \in I} b_i && (\text{AG1, AG4}) \\ &= \varphi((a_i)_{i \in I}) + \varphi((b_i)_{i \in I}), && (\varphi \text{ def.}) \end{aligned}$$

Kuna $A = \sum_{i \in I} A_i$, siis φ on sürjektiivne. Analoogiliselt lausega 2.34 saab näidata, et Abeli rühmade homomorfism on injektiivne parajasti siis, kui tema tuum koosneb ainult nullelemendist. Oletame, et $(a_i)_{i \in I} \in \text{Ker } \varphi$, s.t. $0_A = \varphi((a_i)_{i \in I}) = \sum_{i \in I} a_i$. Kuna A on alamruumide $A_i, i \in I$, sisemine otsesumma, siis teoreemi 4.9 põhjal peavad pere $(a_i)_{i \in I}$ kõik komponendid olema võrdsed 0_A -ga. Seega $(a_i)_{i \in I}$ on rühma $\bigoplus_{i \in I} A_i$ nullelement ja φ on injektiivne. Kokkuvõttes φ on rühmade isomorfism. $\square$

4.3 Perioodilised Abeli rühmad

Definitsioon 4.12 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.

Iga lõplik rühm on perioodiline, kuid leidub ka lõpmatuid perioodilisi rühmi.

Näide 4.13 Jäägiklassirühma $(\mathbb{Z}_2, +)$ loenduv otseaste

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots$$

on lõpmatu, kuid samas perioodiline, sest kõik nullist erinevad elemendid on teist järku.

Lemma 4.14 Olgu $(A, +)$ Abeli rühm ja p algarv. Siis hulk

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

on rühma A alamrühm.

TÕESTUS. Kuna $\text{ord}(0_A) = 1 = p^0$, siis $0_A \in A_p$ ja $A_p \neq \emptyset$.

Olgu $a, b \in A_p$, s.t. $\text{ord}(a) = p^k$ ja $\text{ord}(b) = p^l$, kus $k, l \in \mathbb{N} \cup \{0\}$. Siis $p^{\max(k, l)}(a+b) = 0_A$ ning järelikult $a+b$ järk peab jagama arvu $p^{\max(k, l)}$. Seega on see järk p aste ja $a+b \in A_p$.

Kui $a \in A_p$ ja $\text{ord}(a) = p^k$, siis lemma 3.34 põhjal $\text{ord}(-a) = \text{ord}(a) = p^k$ ja seega $-a \in A_p$. $\square$

Definitsioon 4.15 Alamrühma A_p nimetatakse Abeli rühma $(A, +)$ **p -komponendiks**. Kui $A = A_p$, siis öeldakse, et A on **p -rühm**. Seega A on p -rühm, kui tema iga elemendi järk on p aste.

Näide 4.16 Näiteks $(\mathbb{Z}_{p^n}, +)$ on p -rühm, sest iga elemendi järk peab olema rühma järgu p^n jagaja, seega arvu p mingi aste.

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

Lemma 4.17 Iga mittetriviaalne Abeli p -rühm sisaldab elementi, mille järk on p .

TÕESTUS. Olgu A mittetriviaalne Abeli p -rühm. Siis leidub nullist erinev element $a \in A$. Olgu $\text{ord}(a) = p^k$, kus $k \in \mathbb{N}$. Siis $p(p^{k-1}a) = 0_A$. Olgu $n = \text{ord}(p^{k-1}a)$. Siis lemma 4.5 põhjal $n \mid p$. Kuna p on algarv, siis on kaks võimalust. Kui oletaksime, et $n = 1$, siis $p^{k-1}a = 0_A$, mis on vastuolus sellega, et $\text{ord}(a) = p^k$. Järelikult $n = p$, mis tähendab, et otsitavaks p -ndat järku elemendiks sobib $p^{k-1}a$. $\square$

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

Teoreem 4.18 Perioodiline Abeli rühm on oma p -komponentide sisemine otsesumma.

TÕESTUS. Olgu A perioodiline Abeli rühm. Näitame, et A on oma p -komponentide summa:

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

Selleks tõestame, et $A \subseteq \sum_{p \in \mathbb{P}} A_p$ (vastupidine sisalduvus on ilmne). Olgu $a \in A$ suvaline element ja olgu tema järk n . Kui $n = 1$, siis $a = 0$ ja $a \in \sum_{p \in \mathbb{P}} A_p$. Kui $n \neq 1$, siis aritmeetika põhiteoreemi põhjal $n = p_1^{k_1} \dots p_s^{k_s}$, kus $p_1, \dots, p_s$ on paarikaupa erinevad algarvud ja $k_1, \dots, k_s$ on naturaalarvud. Tähistame

$$n_i := \frac{n}{p_i^{k_i}}.$$

Siis $\text{SÜT}(n_1, \dots, n_s) = 1$ ja lause 3.26 üldistuse tõttu leiduvad $u_1, \dots, u_n \in \mathbb{Z}$ nii, et $u_1 n_1 + \dots + u_s n_s = 1$. Järelikult

$$a = 1 \cdot a = (u_1 n_1 + \dots + u_s n_s) a = u_1 n_1 a + \dots + u_s n_s a.$$

Kuna iga $i \in \{1, \dots, s\}$ korral

$$p_i^{k_i}(u_i n_i a) = (p_i^{k_i} u_i n_i) a = (u_i p_i^{k_i} n_i) a = (u_i n) a = u_i(na) = u_i 0 = 0,$$

siis lause 3.32 põhjal elemendi $u_i n_i a$ järk on $p_i^{k_i}$ jagaja, seega p_i aste. Järelikult iga i korral $u_i n_i a \in A_{p_i}$ ja $a \in \sum_{p \in \mathbb{P}} A_p$.

Veel tuleb näidata, et rühma A alamrühmade A_p , $p \in \mathbb{P}$, summa on otsesumma. Kasutame selleks teoreemi 4.9 tingimust 2. Olgu q mingi algarv ja oletame, et $a \in A_q \cap \sum_{p \in \mathbb{P} \setminus \{q\}} A_p$. Et $a \in A_q$, siis $\text{ord}(a) = q^k$ mingi $k \in \mathbb{N} \cup \{0\}$ korral. Teisest küljest

$a \in \sum_{p \in \mathbb{P} \setminus \{q\}} A_p$ ja seega leiduvad $p_1, \dots, p_s \in \mathbb{P} \setminus \{q\}$, elemendid $a_{p_1}, \dots, a_{p_s} \in A$ ja arvud $k_1, \dots, k_s \in \mathbb{N} \cup \{0\}$ nii, et

$$a = a_{p_1} + \dots + a_{p_s}$$

ja iga $i \in \{1, \dots, s\}$ korral $\text{ord}(a_{p_i}) = p_i^{k_i}$. Olgu $n = p_1^{k_1} \dots p_s^{k_s}$. Siis $na = na_{p_1} + \dots + na_{p_s} = 0$, millest järeldub, et $q^k = \text{ord}(a) \mid n$. Kui $k \geq 1$, siis arvul n oleks algtegur $q \notin \{p_1, \dots, p_s\}$, mis aritmeetika põhiteoreemi tõttu on välistatud. Järelikult $k = 0$ ja $\text{ord}(a) = q^0 = 1$ ehk $a = 0$. Sellega oleme näidanud, et

$$A_q \cap \sum_{p \in \mathbb{P} \setminus \{q\}} A_p = \{0\}.$$

See tähendab, et A on alamrühmade A_p , $p \in \mathbb{P}$, otsesumma. $\square$

Näide 4.19 Vaatleme jäägiklassirühma $A = (\mathbb{Z}_{12}, +)$. Kuna $12 = 2^2 \cdot 3$ ja selle rühma elementide järgud peavad jagama arvu 12, siis on selles rühmas olemas ainult mittetriviaalne 2-komponent ja 3-komponent. Seega $A = A_2 \dot{+} A_3$, kus

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

4.3.1 Lõplikud Abeli p -rühmad

Lõpliku Abeli rühma p -komponendid on definitsiooni järgi p -rühmad ja me teame, et lõplik Abeli rühm esitub oma p -komponentide otsesummana. Seega lõplike Abeli rühmade kirjeldamiseks piisab, kui me oskame kirjeldada lõplikke Abeli p -rühmi. See ongi selle paragrahvi põhieesmärk. Alustuseks tõestame ühe kasuliku teoreemi.

Teoreem 4.20 (Cauchy) *Olgu p algarv. Kui $(A, +)$ on lõplik Abeli rühm ja $p \mid |A|$, siis rühmas A leidub element, mille järk on p .*

TÕESTUS. Tõestame väite induktsiooniga rühma A järgu $|A|$ järgi.

Alus. Kui $|A| = p$, siis selles rühmas peab leiduma element $a \neq 0$. Kuna $\text{ord}(a) \neq 1$ ja $\text{ord}(a)$ jagab rühma järku p , siis $\text{ord}(a) = p$. See tähendab, et A on tsükliline rühm tekitaajaga a .

Samm. Eeldame, et $|A| > p$ ja $p \mid |A|$ ning et väide kehtib väiksema elementide arvuga rühmade korral. Siis A järk ei saa olla algarv. Seega lause 3.36 põhjal A sisaldab mittetriviaalset pärisalamrühma B . Lagrange'i teoreemi (teoreem 3.10) põhjal

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

kusjuures $|B| < |A|$. Et B on mittetriviaalne, siis $|B| > 1$ ja seega $|A/B| < |A|$. Kuna $p \mid |A|$ ja p on algarv, siis on 2 võimalust.

1) $p \mid |B|$. Siis induktsiooni eelduse põhjal rühm B sisaldab p -ndat järku elementi ning selle elemendi järk on p ka rühmas A .

2) $p \mid |A/B|$. Sel juhul faktorrühm A/B rahuldab ka induktsiooni eeldust ja peab sisaldama mingit p -ndat järku elementi $a + B$. Olgu $n := \text{ord}_A(a)$. Kuna $na = 0$, siis ka

$$n(a + B) = (na) + B = 0_A + B = B$$

faktorrühmas A/B . Lause 3.32 tõttu $p \mid n$, järelikult $pk = n$ mingi $k \in \mathbb{N}$ korral. Kuna $\text{ord}_A(a) = pk$, siis lemmast 4.4 saame, et $\text{ord}_A(ka) = p$. $\square$

Järeldus 4.21 *Lõplik Abeli rühm on p -rühm parajasti siis, kui tema järk on p aste.*

TÕESTUS. TARVILIKKUS. Olgu A lõplik Abeli p -rühm. Oletame vastuväiteliselt, et $|A|$ ei ole p aste, siis ta jagub mingi teise algarvuga q . Teoreemi 4.20 põhjal leidub rühmas A q -ndat järku element, mis on vastuolus sellega, et A on p -rühm.

PIISAVUS. Olgu $|A| = p^n$. Siis lause 3.30 põhjal iga A elemendi järk on p^n jagaja, seega p aste. $\square$

Järgnev teoreem annab lõplike Abeli p -rühmade kirjelduse.

Teoreem 4.22 *Lõplik Abeli p -rühm on oma mingite tsükliliste alamrühmade otsesumma.*

TÕESTUS. Järelduse 4.21 põhjal on lõpliku Abeli p -rühma järk algarvu p aste. Tõestame teoreemi induktsiooniga rühma järgu järgi.

Alus. Kui Abeli p -rühma järk on p , siis teoreemi 4.20 põhjal sisaldab ta p -ndat järku elementi, seega on ta tsükliline rühm ja meil on triviaalne otsesumma ühe otseliidetavaga. Samm. Olgu A Abeli p -rühm ja $|A| = p^n$, kus $n \geq 2$. Lihtne on näha, et hulk

$$pA = \{pa \mid a \in A\} \subseteq A$$

on rühma A alamrühm. Kui $\text{ord}(a) = p^k$, siis lemma 4.4 põhjal $\text{ord}(pa) = p^{k-1}$, seega pA on samuti p -rühm. Kui oletada, et $pA = A$, siis

$$A = pA = p^2A = \dots = p^nA = \{0_A\},$$

sest lause 3.30 põhjal on A iga elemendi järk p^n jagaja. Vastuoluline võrdus $A = \{0_A\}$ näitab, et $pA \subset A$ ja seega saame rühmale pA rakendada induktsiooni eeldust. Selle põhjal leiduvad nullist erinevad elemendid $pa_1, \dots, pa_r$ rühmas pA nii, et

$$pA = \langle pa_1 \rangle + \dots + \langle pa_r \rangle. \quad (4.2)$$

Vaatleme tsükliliste alamrühmade summat

$$B := \langle a_1 \rangle + \dots + \langle a_r \rangle \leq A$$

ja näitame, et see summa on otsesumma. Selleks kontrollime teoreemi 4.9 tingimust 3. Oletame, et

$$k_1a_1 + \dots + k_ra_r = 0, \quad (4.3)$$

kus $k_1, \dots, k_r \in \mathbb{Z}$. On 2 võimalust.

1) Iga $i \in \{1, \dots, r\}$ korral $p \mid k_i$, s.t. $k_i = pm_i$ mingi $m_i \in \mathbb{Z}$ korral. Siis

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

kust võrduse (4.2) tõttu $0 = m_i pa_i = k_i a_i$ iga $i \in \{1, \dots, r\}$ korral.

2) Leidub $j \in \{1, \dots, r\}$ nii, et $p \nmid k_j$. Võrdusest (4.3) saame, et

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

kust võrduse (4.2) tõttu järeldub, et $pk_i a_i = 0_A$ iga $i \in \{1, \dots, r\}$ korral, muuhulgas $pk_j a_j = 0_A$. Olgu $\text{ord}(a_j) = p^e$, $e \in \mathbb{N} \cup \{0\}$. Lause 3.32 põhjal $p^e \mid pk_j$. Kuna $p \nmid k_j$, siis $p^e \mid p$ ehk $e \leq 1$. Järelikult $pa_j = 0_A$, mis on vastuolus sellega, et element pa_j pidi olema nullist erinev.

Kuna võrdusest (4.3) järeldus, et $k_1 a_1 = \dots = k_r a_r = 0_A$, siis oleme tõestanud, et

$$B = \langle a_1 \rangle + \dots + \langle a_r \rangle \leq A.$$

Tähistame

$$C := \{a \in A \mid pa = 0_A\} \leq A$$

(s.t. C koosneb rühma A p -ndat järku elementidest ja 0_A -st) ning näitame, et

$$A = B + C.$$

Selleks võtame suvalise $a \in A$. Siis $pa \in pA$ ja seega leiduvad $k_1, \dots, k_r \in \mathbb{Z}$ nii, et

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

Järelikult $p(a - k_1 a_1 - \dots - k_r a_r) = 0_A$ ehk

$$c := a - k_1 a_1 - \dots - k_r a_r \in C.$$

See tähendab, et

$$a = (k_1 a_1 + \dots + k_r a_r) + c \in B + C.$$

Kui nüüd $B = A$, siis on tõestus lõppenud. Kui $B \neq A$, siis $C \not\subseteq B$ ja leidub mingi element $c_1 \in C \setminus B$. Siis $c_1 \neq 0_A$ ja summa

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

on otsesumma, sest $\langle c_1 \rangle$ on tsükliline rühm algarvulise järguga p , seega lause 3.36 põhjal tema alamrühm $B \cap \langle c_1 \rangle$ peab olema triviaalne, $B \cap \langle c_1 \rangle = \{0_A\}$. Niisiis

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

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

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

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

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

□

Teoreemidest 4.18 ja 4.22 saame nüüd järgmise tulemuse.

Teoreem 4.23 *Lõplik Abeli rühm on oma mingite tsükliliste alamrühmade otsesumma.*

Järeldus 4.24 *Rühm A on lõplik Abeli rühm parajasti siis kui leiduvad $n_1, \dots, n_s \in \mathbb{N}$ nii, et $A \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$.*

Lõplike Abeli rühmade kirjelduse andis 1870. aastal saksa matemaatik Leopold Kronecker (1823–1891). On võimalik täpsustada, millisel kujul peavad arvud $n_1, \dots, n_s$ olema.

Näide 4.25 Vaatleme lõplikku Abeli rühma $A = (\mathbb{Z}_{12}, +)$. Selle rühma p -komponendid on

$$\begin{aligned} A_2 &= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \cong \mathbb{Z}_4, \\ A_3 &= \{\bar{0}, \bar{4}, \bar{8}\} \cong \mathbb{Z}_3, \\ A_p &= \{\bar{0}\}, \text{ kui } p \in \mathbb{P} \setminus \{2, 3\}. \end{aligned}$$

Seega $A = A_2 \dot{+} A_3$. Teoreemi 4.11 põhjal on A isomorfne oma alamrühmade A_2 ja A_3 välise otsesummaga, $A \cong A_2 \oplus A_3$. Et lõpliku arvu rühmade väline otsesumma on isomorfne nende otsekorrutisega, siis võime öelda, et

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

Peatükk 5

Ringid

5.1 Põhimõisted

Ringi all mõeldakse erinevates olukordades mõnevõrra erinevaid struktuure. Selles kursuses lähtume järgmisest definitsioonist.

Definitsioon 5.1 Hulka R koos kahe kahekohalise algebralise tehaga $+$ ja $\cdot$ nimetatakse (assotsiatiivseks) **ringiks**, kui

- R1.** $(a + b) + c = a + (b + c)$ iga $a, b, c \in R$ korral;
- R2.** leidub element $0_R \in R$ nii, et iga $a \in R$ korral $a + 0_R = a = 0_R + a$;
- R3.** iga $a \in R$ korral leidub element $-a \in R$ nii, et $a + (-a) = 0_R = (-a) + a$;
- R4.** $a + b = b + a$ iga $a, b \in R$ korral;
- R5.** $a \cdot (b + c) = a \cdot b + a \cdot c$ iga $a, b, c \in R$ korral;
- R6.** $(a + b) \cdot c = a \cdot c + b \cdot c$ iga $a, b, c \in R$ korral.
- R7.** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ iga $a, b, c \in R$ korral;

Niisiis ringidel on kaks kahekohalist tehet ($+$ ja $\cdot$), üks ühekohaline tehe (vastandelemendi võtmise) ja üks nullkohaline tehe (mis fikseerib nullelemendi 0_R).

Harilikult kirjutatakse ringi puhul $a \cdot b$ asemel lühemalt ab . Definitsiooni tingimustest R1–R4 näeme, et $(R, +)$ on Abeli rühm ja $(R, \cdot)$ on poolrühm. Tingimusi R5 ja R6 kutsutakse **distributiivsuse seadusteks**.

Definitsioon 5.2 Ühikelemendiga ring on ring R , mis rahuldab veel tingimust

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

Nagu näha, on ühikelemendiga ringidel kaks nullkohalist tehet. See tähendab, et assotsiatiivsed ringid ja ühikelemendiga ringid on eri tüüpi algebrad. Seda tuleb arvestada muuhulgas homomorfismidest ja alamringidest rääkimisel.

Definitsioon 5.3 Ringi $(R, +, \cdot)$ nimetatakse

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

Näide 5.4 1. Hulk $\mathbb{Z}$ on ühikelemendiga ring täisarvude liitmise ja korrutamise suhtes.

2. Paarisarvude hulk $2\mathbb{Z}$ on ring, milles ei ole ühikelementi.

3. Iga $n \in \mathbb{N}$ korral on hulk $\mathbb{Z}_n$ ühikelemendiga ring jäägiklasside liitmise ja korrutamise suhtes.

4. Iga ühikelemendiga ringi R korral on hulk $R[X]$ ühikelemendiga ring polünoomide liitmise ja korrutamise suhtes.

5. Iga ringi R ja naturaalarvu n korral on hulk $\text{Mat}_n(R)$ ring maatriksite liitmise ja korrutamise suhtes. Kui R on ühikelemendiga ring, siis ka maatriksringis $\text{Mat}_n(R)$ leidub ühikelement.

Lihtne on kontrollida, et kehtib järgmine lause.

Lause 5.5 *Mistahes ringis R kehtivad järgmised arvutusreeglid:*

1. *iga $a, b, c \in R$ korral kui $a + b = c$, siis $a = c - b$;*
2. *$0_R a = 0_R = a 0_R$ 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 5.6 Ringi puhul on võimalik, et $1_R = 0_R$. Sellisel juhul see ring koosnebki ainult ühest elemendist, sest mistahes elemendi a korral $a = a1_R = a0_R = 0_R$. Järelikult, kui ringis on vähemalt kaks elementi, siis selles ringis $1_R \neq 0_R$. Muuhulgas korpuses on ühikelement erinev nullelemendist.

Käesolevas kursuses vaatleme edaspidi ainult selliseid ringe, milles on vähemalt kaks elementi.

Lause 5.7 *Olgu R ja S ringid. Kujutus $f : R \rightarrow S$ on ringide homomorfism parajasti siis, kui*

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

TÕESTUS. Nii nagu lause 2.14 tõestuses saab ka siin näidata, et liitmise säilitamisest järeldub nullelemendi ja vastandelemendi säilitamine. $\square$

Ühikelemendiga ringide homomorfism $f : R \rightarrow S$ peab säilitama ka ühikelementi: $f(1_R) = 1_S$.

Definitsioon 5.8 Ringide homomorfismi $f : R \rightarrow S$ **tuumaks** nimetatakse hulka

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

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

Lause 5.9 *Ringide homomorfism $f : R \rightarrow S$ on üksühene parajasti siis, kui $\text{Ker}(f) = \{0_R\}$.*

5.2 Ideaalid

Definitsioon 5.10 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 $\{0_R\}$ ideaalid. Neid ideaale nimetatakse **triviaalseteks**. Ringi R ideaali I nimetatakse **pärisideaaliks**, kui $I \neq R$.

Näide 5.11 Vaatame ringis $R = \text{Mat}_n(S)$, kus S on mingi ring, alamhulka I , mis koosneb sellistest ruutmaatriksitest, kus nullist erinevad elemendid võivad esineda ainult esimeses reas. Seega

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

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

Järgmise kahe lause tõestused jätame läbimõtlemiseks lugejale.

Lause 5.12 Ringide homomorfismi tuum on ideaal.

Lause 5.13 Ringi parempoolsete ideaalide (vasakpoolsete ideaalide, ideaalide) ühisosa on samuti parempoolne ideaal (vasakpoolne ideaal, ideaal).

Lemma 5.14 Olgu R ühikelemendiga ring ja $a \in R$. Siis

1. hulk

$$aR = \{ar \mid r \in R\}$$

on ringi R parempoolne ideaal,

2. hulk

$$Ra = \{ra \mid r \in R\}$$

on ringi R vasakpoolne ideaal,

3. hulk

$$RaR = \left\{ \sum_{i=1}^n x_i a y_i \mid n \in \mathbb{N}, x_i, y_i \in R \right\}$$

on ringi R ideaal.

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

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

Seega rahuldab RaR ka definitsiooni 5.10 teist tingimust ja on ideaal. $\square$

Definitsioon 5.15 Ideaale aR , Ra ja RaR nimetatakse vastavalt ringi R elemendi a poolt tekitatud **parempoolseks peaideaaliks**, **vasakpoolseks peaideaaliks** ja (**kahepoolseks**) **peaideaaliks**.

Lause 5.16 Ühikelemendiga ringis ei ole mittetriviaalseid parempoolseid ideaale parajasti siis, kui see ring on jagamisega ring.

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

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

$$x = x1_R = x(yz) = (xy)z = 1_R z = z$$

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

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

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

Definitsioon 5.17 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. Seda näitab järgmine lause.

Lause 5.18 Olgu D jagamisega ring ja $n \in \mathbb{N}$. Siis ring $\text{Mat}_n(D)$ on lihtne.

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

Kuna $I \neq \{0_R\}$, siis leidub maatriks $A = (a_{ij}) \in I$, mis ei ole nullmaatriks. Järelikult leiduvad sellised indeksid k ja l , et $a_{kl} \neq 0_R$. Tähistame sümboliga E_{ij} n -ndat järku

ruutmaatriksi, kus kohal (i, j) on ringi D ühikelement 1_D ja ülejäänud elemendid on nullid. Siis $E_{ik}A \in I$, kus nullist erinevad elemendid on vaid i -ndas reas, ja

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

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

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

□

Definitsioon 5.19 Ringi R ideaali I nimetatakse **maksimaalseks ideaaliks**, kui I on maksimaalne element ringi R pärisideaalide järjestatud hulgas (sisalduvusseose suhtes).

Lause 5.20 Ühikelemendiga ringi iga pärisideaal sisaldub mingis maksimaalses ideaalis.

TÕESTUS. Olgu J ühikelemendiga ringi R pärisideaal ja vaatleme hulka

$$P = \{I \in \text{Id}(R) \mid J \subseteq I, I \neq R\}$$

järjestatud hulkana sisalduvusseose suhtes. Kuna $J \in P$, siis hulk P on mittetühi.

Näitame, et Zorni lemma eeldus on täidetud. Zorni lemmast järeldub siis, et järjestatud hulgas P leidub maksimaalne element I' , mis ongi ideaali J sisaldav maksimaalne ideaal ringis R .

Olgu $X \subseteq P$ mittetühi ahel. Vaatleme hulka

$$A := \bigcup_{I \in X} I \subseteq R.$$

Me tõestame, et $A \in P$.

- Esiteks näitame, et A on ringi R ideaal. Olgu $a, b \in A$. Siis leiduvad $I_a, I_b \in X$ nii, et $a \in I_a$ ja $b \in I_b$. Kuna X on ahel, siis kas $I_a \subseteq I_b$ või $I_b \subseteq I_a$. Vaatleme esimest juhtumit, teine on analoogne. Siis $a, b \in I_b$ ning järelikult $a + b \in I_b \subseteq A$, sest I_b on ideaal. Samuti $-b \in I_b \subseteq A$ ja $rb \in I_b \subseteq A$ iga $r \in R$ korral.
- Veendume, et $J \subseteq A$. Kuna ahel X on mittetühi, siis leidub mingi $I_0 \in X$. Seega $J \subseteq I_0 \subseteq A$, millest järeldub, et $J \subseteq A$.
- Kontrollime, et $A \neq R$. Oletame vastuväiteliselt, et $A = R$. Siis $1_R \in A$, seega $1_R \in I$ mingi $I \in X$ korral. Järelikult $r = 1_R r \in I$ iga $r \in R$ korral, mis tähendab, et $R = I$. Saimme vastuolu, mis näitab, et $A \neq R$.

Kuna $I \subseteq A$ iga $I \in X$ korral, siis ideaal A on ahela X ülemine tõke järjestatud hulgas P . Seega Zorni lemma eeldus on täidetud P jaoks. □

Ülesanne 5.21 Näidata, et ringi $\mathbb{Z}$ maksimaalsed ideaalid on kujul $p\mathbb{Z}$, kus p on algarv.

5.3 Lihtsad minimaalse parempoolse ideaaliga ringid

Definitsioon 5.22 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

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

Analoogiliselt defineeritakse minimaalsed vasakpoolsed ja minimaalsed kahepoolsed ideaalid.

Lõplikus ringis $R \neq \{0\}$ on maksimaalsed ja minimaalsed (ühepoolsed) ideaalid muidugi olemas. Lõplikus ringis ei pruugi leiduda minimaalset (ühepoolset) ideaali.

Ülesanne 5.23 Näidata, et ringis $\mathbb{Z}$ ei ole ühtegi minimaalset ideaali.

Lause 5.24 Olgu D jagamisega ring ja $n \in \mathbb{N}$. Siis ring $\text{Mat}_n(D)$ sisaldab minimaalset parempoolset ideaali.

TÕESTUS. Olgu I selliste maatriksite hulk, milles nullist erinevad elemendid esinevad ainult esimeses reas. Nagu mainisime näites 5.11 on I ringi $\text{Mat}_n(D)$ parempoolne ideaal.

Näitame, et I on minimaalne. Selleks vaatleme parempoolset ideaali $\{0_R\} \neq J \subseteq I$. Tähistame sümboliga E_{ij} maatriksit ringist $\text{Mat}_n(D)$, kus kohal (i, j) on 1_D ja kõik ülejäänud elemendid on nullid. Kuna $J \neq \{0_R\}$, 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

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

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

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

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

Ülesanne 5.25 Kas ringis $\text{Mat}_n(D)$ võib olla mitu erinevat minimaalset parempoolset ideaali? Kui jah, siis tooge näide mõnest sellisest minimaalsest parempoolsest ideaalist, mis erineb lause 5.24 tõestuses antust.

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

Teoreem 5.26 Ühikelemendiga ring R on lihtne minimaalset parempoolset ideaali sisaldav ring parajasti siis, kui leidub jagamisega ring D ja naturaalarv n nii, et

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

TÕESTUS. PIISAVUS. See järeldeb lausest 5.18 ja lausest 5.24.

TARVILIKKUS. Olgu R lihtne ring, mis sisaldab minimaalset parempoolset ideaali M . Siis $M \neq \{0_R\}$ ja seega leidub mingi element $x \in M \setminus \{0_R\}$. Et $0_R \neq 1_R x 1_R \in RxR$ ja RxR on ideaal, siis lihtsuse tõttu $RxR = R$. Muuhulgas $1_R \in RxR$ ja seega

$$1_R = \sum_{i=1}^t x_i x y_i \quad (5.1)$$

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

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

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

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

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

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

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

Näitame, et

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

Oletame vastuväiteliselt, et $M \cap I \neq \{0_R\}$. Tänu lemmale 5.13 on $M \cap I$ ringi R parempoolne ideaal. Kuna $\{0_R\} \subset M \cap I \subseteq M$ ja M on minimaalne, siis $M \cap I = M$ ehk $M \subseteq I$. Siis aga $am = 0_R$ iga $m \in M$ korral, mis on vastuolus sellega, et $ab \neq 0_R$, kus $b \in M$. Seega $M \cap I = \{0_R\}$.

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

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

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

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

$$M = eR.$$

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

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

Olgu

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

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

$$\begin{aligned} ex_1e + ex_2e &= e(x_1e + x_2e) = e(x_1 + x_2)e \in D, \\ (ex_1e)(ex_2e) &= e(x_1ex_2)e \in D, \\ -ex_1e &= e(-x_1)e \in D, \\ 0_R &= e0_Re \in D, \\ e &= eee \in D. \end{aligned}$$

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

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

$$e = e^2 = (exey)e = ex(ee)y = (exe)(eye).$$

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

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

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

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

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

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

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

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

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

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

mistahes $\varphi, \psi \in \text{End}_D(M)$ 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 teisendustena

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

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

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

$$g : R \rightarrow \text{End}_D(M)$$

võrdusega

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

kus

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

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

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

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

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

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

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

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

3) Kuna

$$mg(1_R) = m\rho_{1_R} = m1_R = m = m \text{id}_M$$

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

4) Näitame, et g on üksühene. Selleks oletame vastuväiteliselt, et $\text{Ker}(g) \neq \{0_R\}$. Kuna $\text{Ker}(g)$ on ringi R ideaal ja R on lihtne, siis peab $\text{Ker}(g) = R$. Sel juhul $g(r) = 0$ ($g(r)$ on

vektorruumi M nullteisendus) iga $r \in R$ korral. Muuhulgas $e = e\rho_{1_R} = eg(1_R) = e0 = 0_R$, mis on vastuolu.

5) Veendume, et g on pealekujutus. Võtame suvalise $\varphi \in \text{End}_D(M)$. Võrduses (5.1) võime elemendi x asendada korrutisega ex , sest $x \in M$. Seega

$$1_R = \sum_{i=1}^t x_i exy_i. \quad (5.2)$$

Olgu

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

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

$$\begin{aligned} m\rho_r &= mr && (\rho_r \text{ def.}) \\ &= m \left(\sum_{i=1}^t (x_i e)((exy_i)\varphi) \right) && (r \text{ def.}) \\ &= \sum_{i=1}^t (mx_i e)((exy_i)\varphi) && (R \text{ distributiivsus ja assotsiatiivsus}) \\ &= \sum_{i=1}^t (emx_i e)((exy_i)\varphi) && (m = em) \\ &= \sum_{i=1}^t ((emx_i e)(exy_i))\varphi && (\varphi \text{ on lineaarteisendus, LK2}) \\ &= \left(\sum_{i=1}^t (emx_i e)(exy_i) \right) \varphi && (\varphi \text{ on lineaarteisendus, LK1}) \\ &= \left(\sum_{i=1}^t mx_i exy_i \right) \varphi && (m = em, e^2 = e, R \text{ assotsiatiivsus}) \\ &= \left(m \left(\sum_{i=1}^t x_i exy_i \right) \right) \varphi && (R \text{ distributiivsus}) \\ &= (m1)\varphi && (\text{võrdus (5.2)}) \\ &= m\varphi. && (1 \text{ on ühikelement}) \end{aligned}$$

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

Sõltuvalt vektorruumi M mõõtmest on meil kaks võimalust. Osutub, et esimene neist viib vastuoluni ja teine annab soovitud isomorfismi $R \cong \text{Mat}_n(D)$.

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

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

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

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

$$m = d_1 e_{k_1} + \dots + d_v e_{k_v},$$

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

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

(Sisuliselt φ on vektorruumi M projektsioon 1-mõõtmelisele alamruumile De_l .) Saab näidata, et φ on lineaarteisendus, kusjuures $\text{Im}(\varphi) = De_l = \{de_l \mid d \in D\}$ ja seega $\dim(\text{Im}(\varphi)) = 1$. Järelikult $\varphi \in I$. Kuna φ ei ole nullkujutus, siis $I \neq \{0_R\}$.

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

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

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

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

$$m = (d_1 e'_1 + \dots + d_u e'_u)\psi = d_1(e'_1\psi) + \dots + d_u(e'_u\psi).$$

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

b) M on lõplikumõõtmeline vektorruum üle D . Siis on temas olemas mingi lõplik baas $B = \{e_1, \dots, e_n\}$. Iga lineaarteisenduse $\varphi \in \text{End}_D(M)$ korral võib vaadelda selle teisenduse maatriksit A_φ^B 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

$$f : \text{End}_D(M) \rightarrow \text{Mat}_n(D)$$

võrdusega

$$f(\varphi) := (A_\varphi^B)^T.$$

Lineaaralgebrast teame, et

$$A_\varphi^B + A_\psi^B = A_{\varphi+\psi}^B, \quad A_{\varphi \circ \psi}^B = A_\varphi^B A_\psi^B, \quad A_{1_M}^B = E,$$

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

$$\begin{aligned} f(\varphi + \psi) &= (A_{\varphi+\psi}^B)^T = (A_\varphi^B + A_\psi^B)^T = (A_\varphi^B)^T + (A_\psi^B)^T = f(\varphi) + f(\psi), \\ f(\varphi \bullet \psi) &= (A_{\varphi \bullet \psi}^B)^T = (A_{\psi \circ \varphi}^B)^T = (A_\psi^B A_\varphi^B)^T = (A_\varphi^B)^T (A_\psi^B)^T = f(\varphi)f(\psi), \\ f(\text{id}_M) &= (A_{1_M}^B)^T = E^T = E, \end{aligned}$$

s.t. f on ühikelemendiga ringide homomorfism.

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

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

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

Sellega oleme tõestanud, et f on ühikelemendiga ringide isomorfism ja

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

□

5.4 Algebra üle korpuse

Definitsioon 5.27 Algebra üle korpuse K (ehk **K -algebra**) on ring $(A, +, \cdot)$, mille korral on Abeli rühmal $(A, +)$ antud ka vektorruumi struktuur üle K nii, et iga $k \in K$ ja $a, b \in A$ korral

$$k(ab) = (ka)b = a(kb).$$

Alamalgebra on alamruum, mis on samal ajal ka alamring. **Algebrate homomorfism** on lineaarkujutus, mis on samal ajal ka ringide homomorfism.

On mitmeid loomulikke algebrate tüüpe, millega oleme tegelikult juba algebra põhikursuses kokku puutunud.

Näide 5.28 1. Iga korpuse K ja naturaalarvu n korral on ruutmaatriksite hulk $\text{Mat}_n(K)$ algebra üle korpuse K . Skalaari k ja maatriksite $A, B \in \text{Mat}_n(K)$ korral kehtivad muuhulgas ka võrdused $k(AB) = (kA)B = A(kB)$.

2. Iga korpuse K korral on polünoomide ring $K[X]$ ka K -algebra, kui defineerida skalaari k ja polünoomi $a_n X^n + \dots + a_1 X + a_0$ korrutis loomulikult viisil:

$$k(a_n X^n + \dots + a_1 X + a_0) := ka_n X^n + \dots + ka_1 X + ka_0.$$

3. Kompleksarvude korpus $\mathbb{C}$ on loomulikult viisl $\mathbb{R}$ -algebra. See algebra on muuhulgas kahemõõtmeline vektorruum üle $\mathbb{R}$ baasiga $\{1, i\}$.

Kirjeldame nüüd ühte konstruktsiooni, mille abil on võimalik saada korpusest ja mingist hulgast koos sobiva kujutusega uus algebra. Me teeme selle läbi juhul kui poolrühm on lõplik, aga sarnane konstruktsioon töötab ka siis, kui poolrühm on lõpmatu.

Olgu K korpus ja olgu $B = \{e_1, \dots, e_n\}$ mingi lõplik hulk. Algebra $K[B]$ konstrueeritakse järgmiselt. Vaatleme K -vektorruumi, mille baasiks on B . Täpsemalt öeldes võtame

$$K[B] = \{k_1e_1 + \dots + k_ne_n \mid k_1, \dots, k_n \in K\},$$

kus hulga elementideks on formaalsed avaldised $k_1e_1 + \dots + k_ne_n$, mida me nimetame **lineaarkombinatsioonideks** (baasi $\{e_1, \dots, e_n\}$ elementidest). Me loeme, et

$$k_1e_1 + \dots + k_ne_n = l_1e_1 + \dots + l_ne_n \iff k_1 = l_1 \wedge \dots \wedge k_n = l_n$$

ja tähistame $0 := 0e_1 + \dots + 0e_n$. Hulgal $K[B]$ defineerime liitmise ja skalaariga $k \in K$ korrutamise võrdustega

$$(k_1e_1 + \dots + k_ne_n) + (l_1e_1 + \dots + l_ne_n) = (k_1 + l_1)e_1 + \dots + (k_n + l_n)e_n, \quad (5.3)$$

$$k(k_1e_1 + \dots + k_ne_n) = kk_1e_1 + \dots + kk_ne_n. \quad (5.4)$$

Lihtne on veenduda, et niimoodi saame vektorruumi üle K . Muudame selle vektorruumi K -algebraks. Selleks anname ette baasidelementide korrutised mingi kujutusega

$$S \times S \longrightarrow K[B], \quad (e_i, e_j) \mapsto e_i * e_j,$$

mis rahuldab assotsiatiivsuse samasust $(e_i * e_j) * e_h = e_i * (e_j * e_h)$. (Märgime, et $*$ on mingi kahekohaline tehe hulgal S , mis ei pruugi olla algebraline.) Me laiendame selle korrutamise kogu hulga $K[S]$ defineerides lineaarkombinatsioonide korrutamise võrdusega

$$(k_1e_1 + \dots + k_ne_n) \cdot (l_1e_1 + \dots + l_ne_n) = \sum_{i,j=1}^n (k_il_j)(e_i * e_j). \quad (5.5)$$

Näide 5.29 Näiteks vaatleme korpust $\mathbb{R}$ ja hulka $B = \{e, i\}$, kus tehe $*$ on antud tabeli

$*$	e	i
e	e	i
i	i	$-e$

abil. Siis hulga $\mathbb{R}[B]$ elemente reegli (5.5) järgi korrutades saame, et

$$\begin{aligned} (ae + bi) \cdot (ce + di) &= (ac)(e * e) + (ad)(e * i) + (bc)(i * e) + (bd)(i * i) \\ &= (ac)e + (ad)i + (bc)i + (bd)(-e) \end{aligned}$$

$$= (ac)e + (ad)i + (bc)i + (-bd)e \quad (\text{VR7})$$

$$= (ac)e + (-bd)e + (ad)i + (bc)i \quad (\text{VR4})$$

$$= (ac - bd)e + (ad + bc)i \quad (\text{VR6})$$

Saadud algebras tunneme ära kompleksaruvde algebra üle $\mathbb{R}$.

Lause 5.30 *Hulk $K[B]$ on K -algebra tehete suhtes, mis on defineeritud võrdustega (5.3), (5.4) ja (5.5).*

TÕESTUS. Selles tõestuses muutuvad kõik summeerimisindeksid vahemikus $1, \dots, n$, seetõttu ei hakka me neid välja kirjutama. Tõestame kahest distributiivsuse seadusest ühe (teine on analoogiline):

$$\begin{aligned}
\left(\sum_i k_i e_i + \sum_i l_i e_i \right) \cdot \sum_h m_h e_h &= \sum_i (k_i + l_i) e_i \cdot \sum_h m_h e_h && \text{(def. (5.3))} \\
&= \sum_{i,h} ((k_i + l_i) m_h) (e_i * e_h) && \text{(def. (5.5))} \\
&= \sum_{i,h} (k_i m_h + l_i m_h) (e_i * e_h) && \text{(distributiivsus } K\text{-s)} \\
&= \sum_{i,h} (k_i m_h) (e_i * e_h) + \sum_{i,h} (l_i m_h) (e_i * e_h) && \text{(def. (5.3))} \\
&= \sum_i k_i e_i \cdot \sum_h m_h e_h + \sum_i l_i e_i \cdot \sum_h m_h e_h. && \text{(def. (5.5))}
\end{aligned}$$

Korrutamine on assotsiatiivne, sest

$$\begin{aligned}
\left(\sum_i k_i e_i \cdot \sum_j l_j e_j \right) \cdot \sum_h m_h e_h &= \sum_{i,j} (k_i l_j) (e_i * e_j) \cdot \sum_h m_h e_h && \text{(def. (5.5))} \\
&= \sum_{i,j,h} ((k_i l_j) m_h) ((e_i * e_j) * e_h) && \text{(def. (5.5))} \\
&= \sum_{i,j,h} ((k_i l_j) m_h) ((e_i * e_j) * e_h) && (* \text{ on assotsiatiivne}) \\
&= \sum_i k_i e_i \cdot \sum_{j,h} (l_j m_h) (e_j * e_h) && \text{(def. (5.5))} \\
&= \sum_i k_i e_i \cdot \left(\sum_j l_j e_j \cdot \sum_h m_h e_h \right). && \text{(def. (5.5))}
\end{aligned}$$

Lõpuks mistahes $k \in K$ korral

$$k \left(\sum_i k_i e_i \cdot \sum_j l_j e_j \right) = k \sum_{i,j} (k_i l_j) (e_i * e_j) \quad (\text{def. (5.5)})$$

$$= \sum_{i,j} (k(k_i l_j)) (e_i * e_j) \quad (\text{def. (5.4)})$$

$$= \sum_{i,j} ((k k_i) l_j) (e_i * e_j) \quad (K \text{ korrutamise assotsiatiivsus})$$

$$= \sum_i (k k_i) e_i \cdot \sum_j l_j e_j \quad (\text{def. (5.5)})$$

$$= k \sum_i k_i e_i \cdot \sum_j l_j e_j \quad (\text{def. (5.4)})$$

ning analoogiliselt

$$k \left(\sum_i k_i e_i \cdot \sum_j l_j e_j \right) = \sum_i k_i e_i \cdot k \sum_j l_j e_j.$$

Seega on tegemist algebraga. □

5.5 Kvaternioonide algebra

Rakendame nüüd eelmise paragrahvi konstruktsiooni selleks, et konstrueerida kvaternioonide algebra. Vaatleme neljamõõtmelist R -algebrat $\mathbb{R}[B]$, kus $B = \{e, i, j, k\}$ (elemente i, j, k nimetatakse **kvaternioonühikuteks**) ja kujutus $*$: $B \times B \longrightarrow \mathbb{R}[B]$ on antud tabeliga

$*$	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	$-j$
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

Algebrat

$$\mathbb{H} := \mathbb{R}[B] = \{ae + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

nimetatakse **kvaternioonide algebraks**.

Tabeli ülemisest vasakpoolsest nurgast on näha, et see algebra sisaldab kompleksarvude algebraga $\mathbb{C}$ isomorfset alamalgebrat $\{ae + bi \mid a, b \in \mathbb{R}\}$. Tabelist on näha ka see, et algebra $\mathbb{H}$ ei ole kommutatiivne, sest

$$i * j = k \neq -k = j * i.$$

Kaldkorpuse all peetakse tihti silmas jagamisega ringi, mille korrumine ei ole kommutatiivne.

Lause 5.31 *Kvaternioonide algebra $\mathbb{H}$ on kaldkorpuse.*

TÕESTUS. Iga kvaterniooni $\alpha = ae + bi + cj + dk$ korral võib vaadelda tema **kaaskvaterniooni**

$$\bar{\alpha} = ae - bi - cj - dk$$

(sarnaselt kompleksarvu kaaskompleksarvuga). Paneme tähele, et

$$\begin{aligned}\alpha \cdot \bar{\alpha} &= (ae + bi + cj + dk) \cdot (ae - bi - cj - dk) \\ &= a^2e - abi - acj - adk \\ &\quad + bai + b^2e - bck + bdj \\ &\quad + caj + cbk + c^2e - cdi \\ &\quad + dak + dbj + dci + d^2e \\ &= (a^2 + b^2 + c^2 + d^2)e = N(\alpha)e,\end{aligned}$$

kus

$$N(\alpha) = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}.$$

Kui $\alpha \neq 0$, siis vähemalt üks arvudest a, b, c, d on nullist erinev ja seega $N(\alpha) \neq 0$. Korrutades võrduse $\alpha \cdot \bar{\alpha} = N(\alpha)e$ mõlemaid pooli reaalarvuga $\frac{1}{N(\alpha)}$ saame, et

$$e = \frac{1}{N(\alpha)}(\alpha \cdot \bar{\alpha}) = \alpha \cdot \frac{1}{N(\alpha)}\bar{\alpha}.$$

Analoogiliselt $\frac{1}{N(\alpha)}\bar{\alpha} \cdot \alpha = e$ ja seega element $\frac{1}{N(\alpha)}\bar{\alpha} \in \mathbb{H}$ on elemendi α pöördelement. $\square$

Peatükk 6

Moodulid

6.1 Mooduli definitsioon

Mooduli definitsioon näeb välja väga sarnane vektorruumi definitsioonile, ainult et korpuse K asemel on ring R .

Definitsioon 6.1 Hulka A nimetatakse **vasakpoolseks mooduliks üle ringi R** ehk **vasakpoolseks R -mooduliks** (ja kirjutatakse ${}_RA$), kui on defineeritud kujutused

$$\begin{aligned} A \times A &\rightarrow A, & (a, b) &\mapsto a + b, \\ R \times A &\rightarrow A, & (k, a) &\mapsto ka \end{aligned}$$

nii, et

- M1.** $(a + b) + c = a + (b + c)$ iga $a, b, c \in A$ korral;
- M2.** leidub element $0_A \in A$ nii, et iga $a \in A$ korral $a + 0_A = a = 0_A + a$;
- M3.** iga elemendi $a \in A$ korral leidub element $-a \in A$ nii, et $a + (-a) = 0_A = (-a) + a$;
- 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.

Kui ring R sisaldab ühikelementi 1_R ja kehtib veel

- M8.** $1_R a = a$ iga $a \in A$ korral,

siis öeldakse, et moodul ${}_RA$ on **unitaarne**.

Analoogiliselt saab defineerida parempoolsed R -moodulid B_R .

Alammoodul, moodulite homomorfism, selle tuum ja kujutis, faktormoodul, moodulite väline otsesumma jm. mõisted defineeritakse sarnaselt vastavate mõistetega vektorruumide korral. Homomorfismiteoreem moodulite jaoks tõestatakse täpselt samamoodi nagu vektorruumide jaoks. Mooduli A alammoodulite B_i , $i \in I$, summa ja sisemine otsesumma langevad kokku Abeli rühma A alamrühmade B_i , $i \in I$, summa ja sisemise otsesummaga.

Näide 6.2 1. Iga vektorruum üle korpuse on unitaarne vasakpoolne moodul üle selle korpuse.

2. Otsekorutus $\mathbb{Z}^n$ ($n \in \mathbb{N}$) on unitaarne vasakpoolne $\mathbb{Z}$ -moodul, kui tehted defineerida komponenthaaval. Kuna $\mathbb{Z}$ ei ole korpus, siis see moodul ei ole vektorruum.

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

4. Ringi R iga vasakpoolne ideaal I on moodul üle ringi R . Muuhulgas ka R on vasakpoolne moodul üle R . Need moodulid ei pruugi olla unitaarsed.

5. Olgu $R = \text{Mat}_m(S)$, kus S on suvaline ring. Siis hulk $A = \text{Mat}_{m,n}(S)$ on vasakpoolne moodul moodul üle R , kui liitmiseks on matriksite liitmine ja kujutus $R \times A \rightarrow A$ on defineeritud matriksite korrutamise abil.

6.2 Morfismid ja välised otsesummad

Alustuseks tõestame moodulite jaoks homomorfismiteoreemi järgmisel kujul.

Teoreem 6.3 (Homomorfismiteoreem) *Olgu $\varphi : A \rightarrow B$ vasakpoolsete R -moodulite homomorfism ja $H \leq A$ selline alammodul, et $H \subseteq \text{Ker}(\varphi)$. Siis leidub üheselt määratud homomorfism $\psi : A/H \rightarrow B$ nii, et kolmnurk*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ & \searrow \pi & \nearrow \psi \\ & A/H & \end{array}$$

kommuteerub.

Kui $H = \text{Ker}(\varphi)$, siis ψ on isomorfism.

Kui $H = \text{Ker}(\varphi)$ ja φ on surjektiivne, siis ψ on isomorfism.

TÕESTUS. Defineerime kujutuse $\psi : A/H \rightarrow B$ võrdusega

$$\psi(a + H) := \varphi(a).$$

See definitsioon on korrektne, sest

$$a + H = a' + H \iff a - a' \in H \implies a - a' \in \text{Ker}(\varphi) \iff \varphi(a) = \varphi(a').$$

Kui $H = \text{Ker}(\varphi)$, siis keskmine implikatsioon on pööratav ja seega ψ on injektiivne. Vahetu kontroll näitab, et φ on moodulite homomorfism. Kuna $\varphi(a) = \psi(a + H) = (\psi \circ \pi)(a)$ iga $a \in A$ korral, siis kolmnurk kommuteerub.

Kui ka homomorfism $\chi : A/H \rightarrow B$ on selline, et $\chi \circ \pi = \varphi$, siis iga $a \in A$ korral

$$\chi(a + H) = (\chi \circ \pi)(a) = \varphi(a) = (\psi \circ \pi)(a) = \psi(a + H),$$

seega $\chi = \psi$ ja ψ on üheselt määratud.

Kui $H = \text{Ker}(\varphi)$ ja φ on surjektiivne, siis ka ψ on surjektiivne, seega ψ on isomorfism ja

$$A / \text{Ker}(\varphi) \cong B.$$

□

Kui R on ring, siis kõik vasakpoolsed (parempoolsed) R -moodulid koos vastavate homomorfismidega moodustavad loomulikul viisil kategooria, mida me tähistame ${}_R\mathbf{Mod}$ ($\mathbf{Mod}_R$). Uurime, millised on selles kategoorias monomorfismid ja epimorfismid.

Lause 6.4 *Olgu R ring. Monomorfismid kategoorias ${}_R\mathbf{Mod}$ on parajasti injektiivsed homomorfismid ja epimorfismid kategoorias ${}_R\mathbf{Mod}$ on parajasti sürjektiivsed homomorfismid.*

TÕESTUS. Kuna ${}_R\mathbf{Mod}$ on konkreetne kategooria, siis lause 1.13 tõttu on iga injektiivne homomorfism monomorfism ja iga sürjektiivne homomorfism epimorfism. Peame näitama, et kehtivad ka vastupidised implikatsioonid.

Olgu $f : {}_RA \rightarrow {}_RB$ monomorfism. Siis $\text{Ker}(f)$ on mooduli ${}_RA$ alammodul. Vaatleme sisestust $\iota : \text{Ker}(f) \rightarrow A$ ja nullkujutust $c_0 : \text{Ker}(f) \rightarrow A$, mis mõlemad on vasakpoolsete R -moodulite homomorfismid. Siis iga $a \in \text{Ker}(f)$ korral

$$(f \circ \iota)(a) = f(\iota(a)) = f(a) = 0_B = f(0_A) = (f \circ c_0)(a).$$

Kuna f on monomorfism, siis võrdusest $f \circ \iota = f \circ c_0$ järeldub võrdus $\iota = c_0$. Seega $\text{Ker}(f) = \{0_A\}$, mis tähendab, et f on injektiivne, sest moodulite jaoks kehtib lause 2.34 analoog.

Olgu $f : {}_RA \rightarrow {}_RB$ epimorfism. Siis $\text{Im}(f)$ on mooduli ${}_RB$ alammodul ja võime vaadelda faktormoodulit $B/\text{Im}(f)$. Olgu $\pi : B \rightarrow B/\text{Im}(f)$, $b \mapsto b + \text{Im}(f)$, loomulik projektsioon faktormoodulile ja vaatleme ka nullkujutust $c_0 : B \rightarrow B/\text{Im}(f)$, $b \mapsto \text{Im}(f)$. Iga $a \in A$ korral

$$(\pi \circ f)(a) = \pi(f(a)) = f(a) + \text{Im}(f) = \text{Im}(f) = c_0(f(a)) = (c_0 \circ f)(a).$$

Seega $\pi \circ f = c_0 \circ f$, millest epimorfismuse tõttu järeldub võrdus $\pi = c_0$. See tähendab, et iga $a \in A$ korral $a + \text{Im}(f) = \text{Im}(f)$, kust järelduse 3.6 annab, et $a \in \text{Im}(f)$. Järelikult $B = \text{Im}(f)$ ehk f on sürjektiivne. □

Olgu I mittetühi hulk ja M_i , $i \in I$, vasakpoolsed R -moodulid. Täpselt samamoodi nagu vektorruumide korral (vt. paragrahvi 2.8) saab moodustada nende välise otsesumma

$$\bigoplus_{i \in I} M_i := \left\{ (m_i)_{i \in I} \in \prod_{i \in I} M_i \mid \text{peres } (m_i)_{i \in I} \text{ on lõplik arv nullist erinevaid komponente} \right\}.$$

kusjuures sarnaselt lausega 2.55 saab näidata, et see väline otsesumma on kokorutis kategoorias ${}_R\mathbf{Mod}$. Kui kõik need moodulid on omavahel võrdsed, $M_i = {}_RM$ iga $i \in I$ korral, siis saame vasakpoolse R -mooduli

$${}_RM^{(I)} := \bigoplus_{i \in I} {}_RM = \{ (m_i)_{i \in I} \in M^I \mid \text{peres } (m_i)_{i \in I} \text{ on lõplik arv nullist erinevaid kompon.} \}.$$

Lause 6.5 *Iga hulga $I \neq \emptyset$ korral leidub funktor $(-)^{(I)} : {}_R\mathbf{Mod} \rightarrow {}_R\mathbf{Mod}$, mis viib mooduli ${}_RM$ mooduliks ${}_RM^{(I)}$.*

TÕESTUS. Meil on vaja näidata, kuidas funktor $(-)^{(I)}$ tegutseb morfismidel. Vaatleme morfismi $f : {}_R M \longrightarrow {}_R N$ kategoorias ${}_R \mathbf{Mod}$. Defineerime kujutuse $f^{(I)} : {}_R M^{(I)} \longrightarrow {}_R N^{(I)}$ võrdusega

$$f^{(I)}((m_i)_{i \in I}) := (f(m_i))_{i \in I}.$$

Nii saame vasakpoolsete R -moodulite homomorfismi, sest

$$\begin{aligned} f^{(I)}((m_i)_{i \in I} + (m'_i)_{i \in I}) &= f^{(I)}((m_i + m'_i)_{i \in I}) = (f(m_i + m'_i))_{i \in I} = (f(m_i) + f(m'_i))_{i \in I} \\ &= (f(m_i))_{i \in I} + (f(m'_i))_{i \in I} = f^{(I)}((m_i)_{i \in I}) + f^{(I)}((m'_i)_{i \in I}) \end{aligned}$$

ja analoogiliselt $f^{(I)}(r(m_i)_{i \in I}) = r f^{(I)}((m_i)_{i \in I})$ iga $r \in R$ ja $(m_i)_{i \in I}, (m'_i)_{i \in I} \in M^{(I)}$ korral.

Kui on antud veel homomorfism $g : {}_R N \longrightarrow {}_R P$, siis

$$\begin{aligned} (g \circ f)^{(I)}((m_i)_{i \in I}) &= ((g \circ f)(m_i))_{i \in I} = (g(f(m_i)))_{i \in I} = g^{(I)}((f(m_i))_{i \in I}) \\ &= (g^{(I)} \circ f^{(I)})((m_i)_{i \in I}). \end{aligned}$$

Lisaks sellele

$$(\text{id}_M)^{(I)}((m_i)_{i \in I}) = (\text{id}_M(m_i))_{i \in I} = (m_i)_{i \in I},$$

s.t. $(\text{id}_M)^{(I)} = \text{id}_{M^{(I)}}$. Kokkuvõttes saame öelda, et $(-)^{(I)}$ on funktor. $\square$

Märkus 6.6 Kui $R = \mathbb{Z}$, siis moodul ${}_Z M$ on sisuliselt Abeli rühm ja ka ${}_Z M^{(I)}$ on Abeli rühm. Seega võime iga hulga I korral vaadelda ka funktorit $(-)^{(I)} : \mathbf{Ab} \longrightarrow \mathbf{Ab}$.

6.3 Täpsed jada

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

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

$$\dots \xrightarrow{f_{\alpha-1}} A_\alpha \xrightarrow{f_\alpha} A_{\alpha+1} \xrightarrow{f_{\alpha+1}} \dots \quad (6.1)$$

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

Definitsioon 6.7 Moodulite jada kujul (6.1) nimetatakse **täpsaks kohal** α , kui

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

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

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

Näide 6.8 Vaatleme Abeli rühmi $\mathbb{Z}$ ja $\mathbb{Z}_2$ moodulitena üle ringi $\mathbb{Z}$. Siis leidub täpne jada

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

kus homomorfismid f ja g on defineeritud võrdustega

$$f(a) := 2a,$$

$$g(a) := \bar{a}.$$

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

Lemma 6.9 *Moodulite jada*

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

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

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

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

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

3. See järeldub vahetult osadest 1 ja 2. □

Definitsioon 6.10 Täpset jada kujul

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

nimetatakse **lühikeseks täpseks jadaks**.

Suvalise lühikese täpse jada kohta saab teha järgmised tähelepanekud:

1. f on injektiivne;
2. g on sürjektiivne;
3. $C \cong B / \operatorname{Ker}(g) = B / \operatorname{Im}(f)$ tänu järelduse 2.36 analoogile moodulite jaoks;

4. kui samastada A ja sellega isomorfne B alammodul $\text{Im}(f)$, siis võiks tinglikult kirjutada $C \cong B/A$.

Teoreem 6.11 *Olgu*

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

lühike täpne jada. Siis järgmised väited on samaväärsed.

- (i) *Leidub mooduli B alammodul H nii, et $B = \text{Im}(\iota) \dot{+} H$.*
- (ii) *Leidub homomorfism $\psi : C \rightarrow B$ nii, et $\pi \circ \psi = \text{id}_C$.*

TÕESTUS. (i) $\Rightarrow$ (ii). Eeldame, et $B = \text{Im}(\iota) \dot{+} H$, kus $H \leq B$. Peame defineerima kujutuse $\psi : C \rightarrow B$. Olgu $c \in C$. Kuna π on surjektiivne, siis leidub $b \in B$ nii, et $\pi(b) = c$. Et $B = \text{Im}(\iota) \dot{+} H$, siis leiduvad üheselt määratud $a \in A$ ja $h \in H$ nii, et $b = \iota(a) + h$. Defineerime

$$\psi(c) := h.$$

Tuleb näidata, et see definitsioon on korrektne. Oletame, et ka $\pi(b_1) = c$, kus $b_1 = \iota(a_1) + h_1$, $a_1 \in A$, $h_1 \in H$. Siis $b - b_1 \in \text{Ker}(\pi) = \text{Im}(\iota)$, seega leidub $a_2 \in A$ nii, et $b - b_1 = \iota(a_2)$. Järelikult $\iota(a_2) = \iota(a) - \iota(a_1) + h - h_1$ ja

$$h - h_1 = \iota(a_2) - \iota(a) - \iota(a_1) = \iota(a_2 - a - a_1) \in \text{Im}(\iota) \cap H = \{0_B\}.$$

Seega $h = h_1$, mis tähendab, et ψ definitsioon on korrektne.

Olgu nüüd veel $c' = \pi(b')$, kus $b' = \iota(a') + h'$, $a' \in A$ ja $h' \in H$. Siis $c + c' = \pi(b + b')$ ning

$$b + b' = \iota(a) + h + \iota(a') + h' = \iota(a) + \iota(a') + h + h' = \iota(a + a') + (h + h'),$$

kus $a + a' \in A$ ja $h + h' \in H$. Seega

$$\psi(c + c') = h + h' = \psi(c) + \psi(c').$$

Lisaks sellele, iga $r \in R$ korral $rc = r\pi(b) = \pi(rb)$ ja $rb = r\iota(a) + rh = \iota(ra) + rh$, mis tähendab, et

$$\psi(rc) = rh = r\psi(c).$$

Sellega oleme näidanud, et ψ on R -moodulite homomorfism. Kuna

$$c = \pi(b) = \pi(\iota(a)) + \pi(h) = 0_C + \pi(h) = \pi(h),$$

siis $\pi(\psi(c)) = \pi(h) = c$ iga $c \in C$ korral. Seega $\pi \circ \psi = \text{id}_C$.

(ii) $\Rightarrow$ (i). Leidugu homomorfism $\psi : C \rightarrow B$ nii, et $\pi \circ \psi = \text{id}_C$. Olgu $H := \text{Im}(\psi) \leq B$. Näitame, et

$$B = \text{Im}(\iota) \dot{+} H.$$

Selleks tõestame esmalt, et $B = \text{Im}(\iota) + H$. Mistahes $b \in B$ korral ka $b - (\psi \circ \pi)(b) \in B$. Kuna

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

siis $b - (\psi \circ \pi)(b) \in \text{Ker}(\pi) = \text{Im}(\iota)$. Järelikult leidub $a \in A$ nii, et $b - (\psi \circ \pi)(b) = \iota(a)$, kust saame, et

$$b = \iota(a) + \psi(\pi(b)) \in \text{Im}(\iota) + \text{Im}(\psi) = \text{Im}(\iota) + H.$$

Sellega on näidatud, et $B = \text{Im}(\iota) + H$.

Oletame nüüd, et $b \in \text{Im}(\iota) \cap H$. Siis leiduvad $a \in A$ ja $c \in C$ nii, et $b = \iota(a)$ ja $b = \psi(c)$. Siis

$$c = \text{id}_C(c) = (\pi \circ \psi)(c) = \pi(b) = (\pi \circ \iota)(a) = 0(a) = 0_C,$$

kust $b = \psi(0_C) = 0_B$. Seega $\text{Im}(\iota) \cap H = \{0_B\}$. □

Näide 6.12 Vaatleme vasakpoolsete $\mathbb{Z}$ -moodulite homomorfisme $\iota : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, $a \mapsto (a, 0)$, ja $\pi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(a, b) \mapsto b$. Siis

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

on lühike täpne jada, sest ι on injektiivne, π on surjektiivne ja lisaks sellele $\text{Im}(\iota) = \{(a, 0) \mid a \in \mathbb{Z}\} = \text{ker}(\pi)$. See jada rahuldab ka teoreemi 6.11 tingimusi, sest võime võtta $\psi : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, $b \mapsto (0, b)$.

6.4 Vabad moodulid

Selles ja järgmises paragrahvis vaatleme unitaarseid mooduleid üle ühikelemendiga ringi.

Definitsioon 6.13 Mooduli ${}_R A$ elementide süsteemi $a_1, \dots, a_n$ nimetatakse

- **lineaarselt sõltumatuks**, kui

$$(\forall r_1, \dots, r_n \in R)(r_1 a_1 + \dots + r_n a_n = 0_A \implies r_1 = \dots = r_n = 0_R),$$

- **lineaarselt sõltuvaks**, kui ta ei ole lineaarselt sõltumatu.

Lõpmatut elementide süsteemi nimetatakse **lineaarselt sõltumatuks**, kui selle iga lõplik alamsüsteem on lineaarselt sõltumatu. Avaldise $r_1 a_1 + \dots + r_n a_n$ nimetatakse elementide $a_1, \dots, a_n$ **lineaarkombinatsioonideks**.

Definitsioon 6.14 Mooduli ${}_R A$ elementide süsteemi nimetatakse **moodustajate süsteemiks**, kui A iga element avaldub selle süsteemi elementide lineaarkombinatsioonina.

Definitsioon 6.15 Unitaarset moodulit üle ühikelemendiga ringi nimetatakse **vabaks** kui temas leidub baas, s.t. lineaarselt sõltumatu moodustajate süsteem.

Näide 6.16 Näiteks $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ on vaba $\mathbb{Z}$ -moodul, kusjuures üheks tema baasiks on $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. Näiteks element $(5, -2, 3)$ esitub lineaarkombinatsioonina

$$(5, -2, 3) = 5(1, 0, 0) - 2(0, 1, 0) + 3(0, 0, 1).$$

Näide 6.17 Arvestades teoreemi 2.53 võime öelda, et iga mittetriviaalne unitaarne moodul üle korpuse (s.t. iga vektorruum) on vaba.

Mooduli ${}_R M$ iga baas on minimaalne moodustajate süsteem. Tõestame selle. Kui X on baas, siis ta kindlasti on moodustajate süsteem. Tõestame tema minimaalsuse. Oletame vastuväiteliselt, et ka $Y \subset X$ on moodustajate süsteem. Valime elemendi $x \in X \setminus Y$. Siis $x = r_1 y_1 + \dots + r_n y_n$, kus $r_1, \dots, r_n \in R$ ja $y_1, \dots, y_n \in Y$. Me näeme, et

$$1_R x - r_1 y_1 - \dots - r_n y_n$$

on X elementide mittetriviaalne lineaarkombinatsioon, mis võrdub 0-ga. Oleme saanud vastuolu.

Teisest küljest: mooduli minimaalne moodustajate süsteem ei pruugi olla baas (see on oluline erinevus vektorruumide juhuga, kus baasid on parajasti minimaalsed moodustajate süsteemid).

Näide 6.18 Vaatleme Abeli rühma $(\mathbb{Z}_3, +)$ moodulina üle $\mathbb{Z}$ standardsel viisil. Siis $\{\bar{1}\}$ on minimaalne moodustajate süsteem ($\bar{0} = 0 \cdot \bar{1}$, $\bar{1} = 1 \cdot \bar{1}$, $\bar{2} = 2 \cdot \bar{1}$). Samas ta on lineaarselt sõltuv, sest $3 \cdot \bar{1} = \bar{0}$, kuid $3 \neq 0$ ringis $\mathbb{Z}$. Järelikult ta ei ole baas.

Lause 6.19 Olgu R ühikelemendiga ring ja olgu ${}_R F$ unitaarne vaba moodul baasiga $B = \{e_x \mid x \in X\}$. Siis iga element $a \in F \setminus \{0_F\}$ avaldub üheselt kujul

$$a = r_1 e_{x_1} + \dots + r_n e_{x_n},$$

kus $n \in \mathbb{N}$, $e_{x_1}, \dots, e_{x_n} \in B$ on erinevad elemendid ja $r_1, \dots, r_n \in R \setminus \{0_R\}$.

TÕESTUS. Kuna B on moodustajate süsteem, siis iga element $a \in F \setminus \{0_F\}$ saab sellisel kujul esitada. Oletame, et elemendil a on kaks esitust:

$$\begin{aligned} a &= r_1 e_{x_1} + \dots + r_k e_{x_k} + r_{k+1} e_{x_{k+1}} + \dots + r_n e_{x_n}, \\ a &= r'_1 e_{x_1} + \dots + r'_k e_{x_k} + r'_{k+1} e_{y_{k+1}} + \dots + r'_m e_{y_m}, \end{aligned}$$

kus $m, n \in \mathbb{N}$, $r_i, r'_i \in R \setminus \{0_R\}$, $e_{x_1}, \dots, e_{x_n} \in B$ on erinevad elemendid, $e_{x_1}, \dots, e_{x_k}, e_{y_{k+1}}, \dots, e_{y_m} \in B$ on erinevad elemendid ja $\{e_{x_{k+1}}, \dots, e_{x_n}\} \cap \{e_{y_{k+1}}, \dots, e_{y_m}\} = \emptyset$. Siis

$$0_F = (r_1 - r'_1) e_{x_1} + \dots + (r_k - r'_k) e_{x_k} + r_{k+1} e_{x_{k+1}} + \dots + r_n e_{x_n} - r'_{k+1} e_{y_{k+1}} - \dots - r'_m e_{y_m},$$

kus viimases lineaarkombinatsioonis on kõik baasielemendid erinevad. Lineaarse sõltumatause tõttu peavad kõik selle lineaarkombinatsiooni kordajad olema nullid. Kui oletaksime, et $\{e_{x_{k+1}}, \dots, e_{x_n}\} \neq \emptyset$ või $\{e_{y_{k+1}}, \dots, e_{y_m}\} \neq \emptyset$, siis saaksime vastavalt

$$r_{k+1} = \dots = r_n = 0_R \quad \text{või} \quad r'_{k+1} = \dots = r'_m = 0_R,$$

mis on vastuolus eeldustega. Seega need hulgad peavad olema tühjad ja

$$r_1 e_{x_1} + \dots + r_k e_{x_k} = a = r'_1 e_{x_1} + \dots + r'_k e_{x_k}.$$

Seega

$$0_F = (r_1 - r'_1)e_{x_1} + \dots + (r_k - r'_k)e_{x_k},$$

millest lineaarse sõltumatuse tõttu

$$r_1 - r'_1 = \dots = r_k - r'_k = 0_R \quad \text{ehk} \quad r_1 = r'_1, \dots, r_k = r'_k.$$

See tähendab, et esitus on ühene. $\square$

Järgmine lause näitab, kuidas saab konstrueerida suvalise baasi võimsusega vabu mooduleid.

Lause 6.20 Iga ühikelemendiga ringi R ja mittetühja hulga X korral leidub unitaarne vaba vasakpoolne R -moodul $R^{(X)}$ ja injektiivne kujutus $\iota : X \longrightarrow R^{(X)}$ nii, et $\iota(X)$ on mooduli $R^{(X)}$ baas.

TÕESTUS. Vaatleme vasakpoolset R -moodulit

$$R^{(X)} = \bigoplus_{x \in X} R = \{(r_x)_{x \in X} \in R^X \mid \text{peres } (r_x)_{x \in X} \text{ on lõplik arv nullist erinevaid komp.}\}$$

(vt. lauset 6.5). Kuna $1_R(r_x)_{x \in X} = (1_R r_x)_{x \in X} = (r_x)_{x \in X}$, siis on see moodul unitaarne. Iga $x \in X$ korral olgu $\delta_x = (\delta_{x,y})_{y \in X}$ selline pere, kus

$$\delta_{x,y} = \begin{cases} 1_R, & \text{kui } x = y \\ 0_R, & \text{kui } x \neq y \end{cases} \quad (6.2)$$

(see on sarnane Kroneckeri deltale). Siis $R^{(X)}$ iga nullist erineva elemendi saab esitada lõpliku summana

$$a = \sum_{x \in X} a_x \delta_x$$

liidetavaist, kus $a_x \in R \setminus \{0_R\}$. Kaks sellist summat on võrdsed, kui iga $x \in X$ korral on δ_x kordajad mõlemas summas võrdsed. Lihtne on veenduda, et $\{\delta_x \mid x \in X\}$ on mooduli $R^{(X)}$ baas ja kujutus

$$\iota : X \longrightarrow R^{(X)}, \quad x \mapsto \delta_x$$

on injektiivne. Seega $R^{(X)}$ on vaba vasakpoolne R -moodul. $\square$

Järgmine lause ütleb, et homomorfismi defineerimiseks vabast moodulist piisab kui näidata ära, kuidas see homomorfism tegutseb baasi elementidel.

Lause 6.21 (Universaalomadus) Olgu R ühikelemendiga ring. Kui ${}_R F$ on unitaarne vaba moodul baasiga $B = \{e_x \mid x \in X\}$, siis iga unitaarse mooduli ${}_R M$ ja kujutuse $\bar{g} : B \longrightarrow M$ korral leidub üheselt määratud moodulite homomorfism $g : {}_R F \longrightarrow {}_R M$ nii, et $g|_B = \bar{g}$.

$$\begin{array}{ccc}
 B & \subseteq & {}_R F \\
 & \searrow \bar{g} & \downarrow g \\
 & & {}_R M
 \end{array}$$

TÕESTUS. Kuna B on baas, siis lause 6.19 tõttu avaldub iga element $a \in F \setminus \{0_F\}$ üheselt lineaarkombinatsioonina

$$a = r_1 e_{x_1} + \dots + r_n e_{x_n},$$

kus $n \in \mathbb{N}$, $e_{x_1}, \dots, e_{x_n} \in B$ on erinevad elemendid ja $r_1, \dots, r_n \in R \setminus \{0_R\}$. Defineerime $g(a) \in M$ võrdusega

$$g(a) := r_1 \bar{g}(e_{x_1}) + \dots + r_n \bar{g}(e_{x_n}).$$

Lisaks sellele loeme, et $g(0_F) := 0_M$. Nii oleme defineerinud kujutuse $g : F \longrightarrow M$. Peame veenduma, et g on vasakpoolsete R -moodulite homomorfism.

Selleks näitame kõigepealt, et $g(a+b) = g(a) + g(b)$ iga $a, b \in F$ korral. Kui vähemalt üks elementidest a ja b on 0_F , siis on see võrdus ilmne. Eeldame nüüd, et $a, b \neq 0_F$. Siis need elemendid avalduvad B elementide lineaarkombinatsioonidena. Lisades lineaarkombinatsioonidesse 0_F -ga võrduvaid liidetavaid võime eeldada, et

$$a = r_1 e_{x_1} + \dots + r_n e_{x_n} \quad \text{ja} \quad b = r'_1 e_{x_1} + \dots + r'_n e_{x_n},$$

kus $n \in \mathbb{N}$, $x_1, \dots, x_n \in X$ ja $r_1, \dots, r_n, r'_1, \dots, r'_n \in R$ (s.t. a ja b on lineaarkombinatsioonid samadest baasidelementidest). Järelikult

$$\begin{aligned}
 g(a+b) &= g((r_1 + r'_1)e_{x_1} + \dots + (r_n + r'_n)e_{x_n}) && ({}_R F \text{ on moodul}) \\
 &= (r_1 + r'_1)\bar{g}(e_{x_1}) + \dots + (r_n + r'_n)\bar{g}(e_{x_n}) && (g \text{ def.}) \\
 &= r_1 \bar{g}(e_{x_1}) + r'_1 \bar{g}(e_{x_1}) + \dots + r_n \bar{g}(e_{x_1}) + r'_n \bar{g}(e_{x_1}) && (\text{M6}) \\
 &= r_1 \bar{g}(e_{x_1}) + \dots + r_n \bar{g}(e_{x_n}) + r'_1 \bar{g}(e_{x_1}) + \dots + r'_n \bar{g}(e_{x_n}) && (\text{M1, M4}) \\
 &= g(a) + g(b) && (g \text{ def.})
 \end{aligned}$$

ja analoogiliselt $g(ra) = rg(a)$ iga $r \in R$ korral. Seega g on moodulite homomorfism.

Võrdus $g|_B = \bar{g}$ kehtib tänu sellele, et iga $x \in X$ korral

$$g(e_x) = g(1_r \cdot e_x) = 1_R \cdot \bar{g}(e_x) = \bar{g}(e_x).$$

Kui $h : {}_R F \longrightarrow {}_R M$ on ka mingi moodulite homomorfism, mille korral $h|_B = \bar{g}$, siis iga $a = r_1 e_{x_1} + \dots + r_n e_{x_n} \in F \setminus \{0_F\}$ korral

$$\begin{aligned}
 h(a) &= r_1 h(e_{x_1}) + \dots + r_n h(e_{x_n}) && (h \text{ on homomorfism}) \\
 &= r_1 \bar{g}(e_{x_1}) + \dots + r_n \bar{g}(e_{x_n}) && (h|_B = \bar{g}) \\
 &= r_1 g(e_{x_1}) + \dots + r_n g(e_{x_n}) && (g|_B = \bar{g}) \\
 &= g(a). && (g \text{ def.})
 \end{aligned}$$

Kuna ka $h(0_F) = 0_M = g(0_F)$, siis $h = g$ ning me oleme tõestanud g ühesuse. $\square$

Järgmine teoreem kirjeldab isomorfismi täpsuseni ära vabad moodulid.

Teoreem 6.22 *Olgu R ühikelemendiga ring. Unitaarne vasakpoolne R -moodul ${}_R F$ on vaba parajasti siis, kui leidub hulk $X \neq \emptyset$ nii, et ${}_R F \cong R^{(X)}$.*

TÕESTUS. TARVILIKKUS. Eeldame, et ${}_R F$ on unitaarne vaba moodul, mille baas on $B = \{e_x \mid x \in X\}$, kus $X \neq \emptyset$ on mingi indeksite hulk. Siis F iga nullist erinev element on üheselt esitatav lineaarkombinatsioonina

$$r_1 e_{x_1} + \dots + r_n e_{x_n},$$

kus $n \in \mathbb{N}$, $x_1, \dots, x_n \in X$ ja $r_1, \dots, r_n \in R \setminus \{0_R\}$. Vaatleme kujutust

$$\bar{g} : B \longrightarrow R^{(X)}, \quad e_x \mapsto \delta_x,$$

kus δ_x on defineeritud võrdusega (6.2).

$$\begin{array}{ccc} B & \subseteq & {}_R F \\ & \searrow \bar{g} & \downarrow g \\ & & R^{(X)} \end{array}$$

Tänu universaalomadusele (s.t. lausele 6.21) leidub moodulite homomorfism $g : {}_R F \longrightarrow R^{(X)}$ nii, et

$$g(e_x) = \bar{g}(e_x) = \delta_x$$

iga $x \in X$ korral. Järelikult

$$g(r_1 e_{x_1} + \dots + r_n e_{x_n}) = r_1 g(e_{x_1}) + \dots + r_n g(e_{x_n}) = r_1 \delta_{x_1} + \dots + r_n \delta_{x_n},$$

mis näitab, et g on surjektiivne, sest $\{\delta_x \mid x \in X\}$ on $R^{(X)}$ baas. Tõestuse lõpetamiseks peame veel näitama, et g on injektiiivne. Kui $f = r_1 e_{x_1} + \dots + r_n e_{x_n} \in \text{Ker}(g)$, siis $g(f) = r_1 \delta_{x_1} + \dots + r_n \delta_{x_n}$ on nullidest koosnev pere, seega $r_1 = \dots = r_n = 0_R$ ja $f = 0_F$. Oleme näidanud, et $\text{Ker}(g) = \{0_F\}$, mis tähendab, et g on injektiiivne. Järelikult g on isomorfism.

PIISAVUS. Lauses 6.20 on tõestatud, et moodul $R^{(X)}$ on vaba. Vaba mooduliga isomorfne moodul on samuti vaba. $\square$

Meenutame, et epimorfismid moodulite kategooriates on parajasti surjektiivsed homomorfismid (lause 6.4). Öeldakse, et moodul A on mooduli B **epimorfne kujutis**, kui leidub surjektiivne homomorfism $B \longrightarrow A$. Sellisel juhul on B tänu homomorfismiteoreemile isomorfne mooduli B faktormooduliga.

Lause 6.23 *Iga unitaarne moodul üle ühikelemendiga ringi on vaba mooduli epimorfne kujutis.*

TÕESTUS. Olgu ${}_R A$ unitaarne vasakpoolne R -moodul. Vaatleme hulka A indeksite hulgana. Lause 6.20 põhjal on $F := R^{(A)}$ vaba moodul baasiga $\{\delta_a \mid a \in A\}$. Vaatleme kujutust

$$\bar{g} : \{\delta_a \mid a \in A\} \longrightarrow {}_R A, \quad \delta_a \mapsto a.$$

Tänu vaba mooduli universaalomadusele leidub üheselt määratud moodulite homomorfism $g : R^{(A)} \rightarrow {}_R A$, mis jätkab kujutust $\bar{g}$, s.t. $g(\delta_a) = \bar{g}(\delta_a) = a$ iga $a \in A$ korral. Järelikult g on sürjektiivne homomorfism. $\square$

Vaba R -mooduli konstruktsioon on funktoriaalne.

Lause 6.24 Iga ühikelemendiga ringi R korral leidub funktor $F : \mathbf{Set} \rightarrow \mathbf{Mod}_R$, mis viib hulga X vabaks mooduliks $R^{(X)}$.

TÕESTUS. Niisiis loeme, et $F(X) = R^{(X)}$ iga hulga X korral. Peame defineerima funktori F morfismidel. Olgugi $f : X \rightarrow Y$ suvaline kujutus hulgast X hulka Y . Vaatleme kujutusi $\iota_X : X \rightarrow R^{(X)}$ ja $\iota_Y : Y \rightarrow R^{(Y)}$, mis on defineeritud nii nagu lause 6.20 tõestuses. Vaba mooduli $R^{(X)}$ universaalomaduse tõttu leidub üheselt määratud rühmade homomorfism $F(f) : R^{(X)} \rightarrow R^{(Y)}$ nii, et diagramm

$$\begin{array}{ccc} X & \xrightarrow{\iota_X} & R^{(X)} \\ f \downarrow & & \downarrow F(f) \\ Y & \xrightarrow{\iota_Y} & R^{(Y)} \end{array}$$

kommuteerub. Sellega on funktor F defineeritud morfismil f . Kui on antud kujutused $f : X \rightarrow Y$ ja $g : Y \rightarrow Z$, siis leiduvad homomorfismid $F(f) : R^{(X)} \rightarrow R^{(Y)}$ ja $F(g) : R^{(Y)} \rightarrow R^{(Z)}$ nii, et ülemine ja alumine ruut diagrammis

$$\begin{array}{ccc} X & \xrightarrow{\iota_X} & R^{(X)} \\ f \downarrow & & \downarrow F(f) \\ Y & \xrightarrow{\iota_Y} & R^{(Y)} \\ g \downarrow & & \downarrow F(g) \\ Z & \xrightarrow{\iota_Z} & R^{(Z)} \end{array}$$

kommuteeruvad. Seega ka suur ristkülik kommuteerub. Samas kujutuse $g \circ f : X \rightarrow Z$ jaoks leidub samuti üheselt määratud homomorfism $F(g \circ f) : R^{(X)} \rightarrow R^{(Z)}$ nii, et välimine ristkülik kommuteerub. Ühesuse tõttu peab $F(g \circ f) = F(g) \circ F(f)$. Seega F säilitab morfismide kompositsioone.

Diagrammi

$$\begin{array}{ccc} X & \xrightarrow{\iota_X} & R^{(X)} \\ \text{id}_X \downarrow & & \downarrow F(\text{id}_X) \\ X & \xrightarrow{\iota_X} & R^{(X)} \end{array}$$

kommutatiivsus tähendab seda, et $F(\text{id}_X) \circ \iota_X = \iota_X$. See tähendab, et kujutus $F(\text{id}_X)$ jätab vaba Abeli rühma $R^{(X)}$ baasi $\iota_X(X)$ kõik elemendid paigale. See tähendab, et ta jätab ka rühma $R^{(X)}$ kõik elemendid paigale, s.t. $F(\text{id}_X) = \text{id}_{R^{(X)}} = \text{id}_{F(X)}$. Oleme näidanud, et F on funktor. $\square$

Nagu eespool mainitud, iga Abeli rühma saab loomulikul viisil vaadelda $\mathbb{Z}$ -moodulina. Öeldakse, et Abeli rühm on **vaba**, kui ta on vaba $\mathbb{Z}$ -moodulina. Seega moodulite jaoks tõestatud tulemustest saame erijuhtudena kätte tulemused Abeli rühmade vabaduse kohta. Sõnastame neist mõned siin.

Lause 6.25 Iga mittetühja hulga X korral leidub vaba Abeli rühm $\mathbb{Z}^{(X)}$ ja injektiivne kujutus $\iota : X \rightarrow \mathbb{Z}^{(X)}$ nii, et $\iota(X)$ on Abeli rühma $\mathbb{Z}^{(X)}$ baas.

Lause 6.26 (Universaalomadus) Kui F on vaba Abeli rühm baasiga $B = \{e_x \mid x \in X\}$, siis iga Abeli rühma A ja kujutuse $g : B \rightarrow A$ korral leidub üheselt määratud rühmade homomorfism $\bar{g} : F \rightarrow A$ nii, et $\bar{g}|_B = g$.

$$\begin{array}{ccc} B & \subseteq & F \\ & \searrow g & \downarrow \bar{g} \\ & & A \end{array}$$

Teoreem 6.27 Abeli rühm F on vaba parajasti siis, kui leidub hulk $X \neq \emptyset$ nii, et $F \cong \mathbb{Z}^{(X)}$.

Lause 6.28 Iga Abeli rühm on vaba Abeli rühma epimorfne kujutis.

Lause 6.29 Leidub funktor $F : \text{Set} \rightarrow \text{Ab}$, mis viib hulga X vabaks Abeli rühmaks $\mathbb{Z}^{(X)}$.

6.5 Projektiivsed moodulid

Vabade moodulitega on üsna lähedalt seotud projektiivsed moodulid.

Definitsioon 6.30 Unitaarne vasakpoolne moodul üle ringi R on **projektiivne**, kui ta on projektiivne objekt kategoorias unitaarsete vasakpoolsete R -moodulite kategoorias ${}_R\text{UMod}$. See tähendab, et iga epimorfismi $\pi : {}_R A \rightarrow {}_R B$ ja iga morfismi $f : {}_R P \rightarrow {}_R B$ korral leidub morfism $g : {}_R P \rightarrow {}_R A$ nii, et $f = \pi \circ g$.

$$\begin{array}{ccc} & P & \\ g \swarrow & \downarrow f & \\ A & \xrightarrow{\pi} & B \end{array}$$

Lause 6.31 Iga unitaarne vaba moodul üle ühikelemendiga ringi on projektiivne.

TÕESTUS. Olgu ${}_R F$ vaba vasakpoolne R -moodul baasiga $\{e_x \mid x \in X\}$. Näitame, et F on projektiivne. Olgu A, B unitaarsed vasakpoolsed R -moodulid, $f : F \rightarrow B$ homomorfism ja $\pi : A \rightarrow B$ sürjektiivne homomorfism. Tähistame $b_x := f(e_x)$ iga $x \in X$ korral. Et π on sürjektiivne, siis iga $x \in X$ jaoks saame valida mingi elemendi $a_x \in A$ nii, et $\pi(a_x) = b_x$. Vaatleme kujutust

$$\bar{g} : \{e_x \mid x \in X\} \rightarrow A, \quad e_x \mapsto a_x.$$

$$\begin{array}{ccc} \{e_x \mid x \in X\} & \subseteq & F \\ \bar{g} \downarrow & \nearrow g & \downarrow f \\ A & \xrightarrow{\pi} & B \end{array}$$

Tänu F universaalomadusele leidub vasakpoolsed moodulite homomorfism $g : F \rightarrow A$ nii, et $g(e_x) = \bar{g}(e_x) = a_x$ iga $x \in X$ korral. Siis

$$(\pi \circ g)(e_x) = \pi(a_x) = b_x = f(e_x)$$

iga $x \in X$ korral. On selge, et kui kaks homomorfismi tegutsevad samamoodi vaba mooduli baasi elementidel, siis nad tegutsevad samamoodi kõigil elementidel. Seega $\pi \circ g = f$. $\square$

Projektiivsuse omadus kandub moodulite otsesummalt üle otseliidetavatele.

Lause 6.32 Olgu R ühikelemendiga ring. Kui P ja Q on unitaarsed vasakpoolsed R -moodulid ja moodul $P \oplus Q$ on projektiivne, siis ka P ja Q on projektiivsed.

TÕESTUS. Tõestame, et P on projektiivne (Q jaoks on tõestus analoogiline). Vaatleme diagrammi

$$\begin{array}{ccc} & P & \\ & \downarrow f & \\ A & \xrightarrow{\pi} & B \end{array}$$

kus f ja π on homomorfismid ja π on sürjektiivne. Meenutame, et $P \oplus Q = P \times Q$, sest tegemist on lõpliku arvu moodulite välise otsesummaga. Lihtne on näha, et ka kujutus

$$f' : P \times Q \rightarrow B, \quad (p, q) \mapsto f(p)$$

on homomorfism. Kuna $P \times Q$ on projektiivne, siis leidub homomorfism $g' : P \times Q \rightarrow A$ nii, et $\pi \circ g' = f'$.

$$\begin{array}{ccc} P \times Q & \xleftarrow{\iota_P} & P \\ \downarrow g' & \searrow f' & \downarrow f \\ A & \xrightarrow{\pi} & B \end{array}$$

Vaatleme veel moodulite homomorfismi

$$\iota_P : P \longrightarrow P \times Q, \quad p \mapsto (p, 0)$$

ja defineerime homomorfismi $g : P \longrightarrow A$ korrutisena $g := g' \circ \iota_P$. Siis

$$(\pi \circ g)(p) = (\pi \circ g' \circ \iota_P)(p) = (f' \circ \iota_P)(p) = f'(p, 0) = f(p)$$

iga $p \in P$ korral. Järelikult $\pi \circ g = f$. □

Järgmine teoreem annab projektiivsuse kirjelduse täpsete jadade keeles ja ütleb, et moodul on projektiivne parajasti siis kui ta on (isomorfismi täpsuseni) vaba mooduli otseliidetav.

Teoreem 6.33 *Olgu R ühikelemendiga ring. Järgmised väited unitaarse vasakpoolse R -mooduli P kohta on samaväärsed.*

(i) *Moodul P on projektiivne.*

(ii) *Iga lühikese täpse jada*

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

korral leidub homomorfism $\psi : P \rightarrow B$ nii, et $\pi \circ \psi = \text{id}_P$.

(iii) *Leidub vaba moodul F nii, et $F = A \dot{+} B$, kusjuures üks otseliidetavatest on isomorfne mooduliga P .*

TÕESTUS. (i) $\Rightarrow$ (ii) Rakendame P projektiivsust epimorfismidele $\pi : B \rightarrow P$ ja $\text{id}_P : P \rightarrow P$. Siis leidub selline homomorfism $\psi : P \rightarrow B$, et $\pi \circ \psi = \text{id}_P$, mida oligi tarvis tõestada.

$$\begin{array}{ccc} & & P \\ & \swarrow \psi & \downarrow \text{id}_P \\ B & \xrightarrow{\pi} & P \end{array}$$

(ii) $\Rightarrow$ (iii) Lause 6.23 tõttu leidub meil lühike täpne jada

$$0 \longrightarrow \text{Ker}(\pi) \xrightarrow{\iota} F \xrightarrow{\pi} P \longrightarrow 0,$$

kus F on vaba moodul, π on epimorfism ja ι on sisestus. Eelduse (ii) kohaselt leidub homomorfism $\psi : P \rightarrow F$ nii, et $\pi \circ \psi = \text{id}_P$, mis teoreemist 6.11 tulenevalt annab meile, et $F = \text{Im}(\iota) \dot{+} B$ mingi F alammoduli B korral. Kujutus

$$f : F \longrightarrow B, \quad \iota(a) + b \mapsto b$$

on sürjektiivne homomorfism, mille tuum on $\text{Im}(\iota)$. Seega

$$\begin{aligned} B &\cong F / \text{Im}(\iota) && \text{(teoreem 6.3)} \\ &= F / \text{Ker}(\pi) && \text{(jada täpsus)} \\ &\cong P. && \text{(teoreem 6.3)} \end{aligned}$$

(iii) $\Rightarrow$ (i) Vaba moodul $F = A \dot{+} P \cong A \oplus P = A \times P$ on projektiivne lause 6.31 tõttu. Lause 6.32 annabki nüüd, et nii A kui P on projektiivsed. □

6.6 Tensorkorrutise definitsioon ja konstruktsioon

Selles ja kahes järgnevas paragrahvis tutvustame moodulite tensorkorrutist ja selle omadusi. Tensorkorrutised mängivad tähtsat rolli näiteks homoloogilises algebras ja algebralises geomeetrias. Siinne materjal tugineb suures osas Kristo Väljako raamatule [4]. Me ei eelda ringilt ühikelemendi olemasolu ega moodulitelt unitaarsust.

Definitsioon 6.34 Olgu R ring, M_R parempoolne R -moodul, ${}_R N$ vasakpoolne R -moodul ja A Abeli rühm. Kujutus $\beta: M \times N \longrightarrow A$ on **R -tasakaalustatud**, kui iga $m, m' \in M$, $n, n' \in N$ ja $r \in R$ korral

1. $\beta(m + m', n) = \beta(m, n) + \beta(m', n)$;
2. $\beta(m, n + n') = \beta(m, n) + \beta(m, n')$;
3. $\beta(mr, n) = \beta(m, rn)$.

Tasakaalustatud kujutuste abil saab defineerida tensorkorrutise.

Definitsioon 6.35 Paari (T, τ) , kus T on Abeli rühm ja $\tau: M \times N \longrightarrow T$ on R -tasakaalustatud kujutus, nimetatakse moodulite M_R ja ${}_R N$ **tensorkorrutiseks**, kui iga Abeli rühma A ja iga R -tasakaalustatud kujutuse $\beta: M \times N \longrightarrow A$ korral leidub täpselt üks Abeli rühmade homomorfism $f: T \longrightarrow A$ nii, et $\beta = f \circ \tau$.

$$\begin{array}{ccc}
 & M \times N & \\
 \tau \swarrow & & \searrow \beta \\
 T & \xrightarrow{\quad f \quad} & A
 \end{array}$$

Tuleb välja, et moodulite tensorkorrutis on isomorfismi täpsuseni üheselt määratud.

Lause 6.36 Kui (T, τ) ja (T', τ') on moodulite M_R ja ${}_R N$ tensorkorrutised, siis leidub Abeli rühmade isomorfism $f: T \longrightarrow T'$ nii, et $\tau' = f \circ \tau$.

TÕESTUS. Olgu (T, τ) ja (T', τ') kaks moodulite M_R ja ${}_R N$ tensorkorrutist. Siis leiduvad ühesed Abeli rühmade homomorfismid f ja g nii, et kolmnurgad diagrammil

$$\begin{array}{ccccc}
 & & M \times N & & \\
 & \tau \swarrow & \downarrow \tau' & \searrow \tau & \\
 T & \xrightarrow{\quad f \quad} & T' & \xrightarrow{\quad g \quad} & T
 \end{array}$$

kommuteeruvad. Järelikult $(g \circ f) \circ \tau = g \circ (f \circ \tau) = g \circ \tau' = \tau$. Samas ka $\text{id}_T \circ \tau = \tau$. Ühesuse nõude tõttu $g \circ f = \text{id}_T$ ning analoogiliselt ka $f \circ g = \text{id}_{T'}$. Järelikult on kujutus $f: T \longrightarrow T'$ Abeli rühmade isomorfism. $\square$

Nüüd tutvustame kanoonilist viisi moodulite tensorkorrutise konstrueerimiseks.

Konstruksioon 6.37 (Moodulite tensorkorrutis) Olgu R ring, M_R parempoolne R -moodul ja ${}_R N$ vasakpoolne R -moodul. Vaatleme vaba Abeli rühma hulgal $M \times N$ (vt. lauset 6.25), s.t. hulka

$$\mathbb{Z}^{(M \times N)} := \{f: M \times N \longrightarrow \mathbb{Z} \mid f(m, n) \neq 0 \text{ lõpliku arvu paaride } (m, n) \text{ korral}\}$$

punktiviisilise liitmise

$$(f + g)(m, n) := f(m, n) + g(m, n), \quad (m, n) \in M \times N,$$

suhtes. Selle Abeli rühma nullelement on nullkujutus

$$c_0: M \times N \longrightarrow \mathbb{Z}, \quad (m, n) \mapsto 0.$$

Iga paari $(m, n) \in M \times N$ korral olgu kujutus $x_{(m, n)}: M \times N \longrightarrow \mathbb{Z}$ defineeritud võrdusega

$$x_{(m, n)}(m', n') := \begin{cases} 1, & (m', n') = (m, n), \\ 0, & (m', n') \neq (m, n). \end{cases}$$

On selge, et $x_{(m, n)} \in \mathbb{Z}^{(M \times N)}$. Nendest elementidest koosnev hulk

$$\mathcal{B} := \{x_{(m, n)} \mid (m, n) \in M \times N\}$$

on baas Abeli rühmas $\mathbb{Z}^{(M \times N)}$ (vaata lause 6.20 tõestust; meil $x_{(m, n)} = \delta_{(m, n)}$). Seega rühma $\mathbb{Z}^{(M \times N)}$ elementideks on baasielementide lineaarkombinatsioonid

$$z_1 x_{(m_1, n_1)} + \dots + z_s x_{(m_s, n_s)},$$

kus $s \in \mathbb{N}$, $z_1, \dots, z_s \in \mathbb{Z}$ ja $(m_1, n_1), \dots, (m_s, n_s) \in M \times N$.

Olgu H rühma $\mathbb{Z}^{(M \times N)}$ alamrühm, mis on tekitatud järgnevate elementide poolt (s.t. H on vähim alamrühm, mis sisaldab neid elemente):

$$\begin{aligned} x_{(m+m', n)} - x_{(m, n)} - x_{(m', n)}, \\ x_{(m, n+n')} - x_{(m, n)} - x_{(m, n')}, \\ x_{(mr, n)} - x_{(m, rn)}, \end{aligned} \tag{6.3}$$

kus $m, m' \in M$, $n, n' \in N$ ja $r \in R$. Iga $f \in \mathbb{Z}^{(M \times N)}$ korral tähistame f kõrvalklassi alamrühma H järgi

$$[f] := f + H = \{f + h \mid h \in H\}.$$

Vaatleme faktorrühma

$$M \otimes_R N := \mathbb{Z}^{(M \times N)} / H = \{[f] \mid f \in \mathbb{Z}^{(M \times N)}\},$$

millel liitmistehe on defineeritud võrdusega

$$[f] + [f'] = [f + f'],$$

kus $f, f' \in \mathbb{Z}^{(M \times N)}$, ning mille nullelement on $[c_0] = c_0 + H = H$. Kuna elemendid (6.3) kuuluvad alamrühma H , siis nende kõrvalklassid on võrdsed nullelemendi kõrvalklassiga:

$$\begin{aligned} [x_{(m+m',n)} - x_{(m,n)} - x_{(m',n)}] &= [c_0], \\ [x_{(m,n+n')} - x_{(m,n)} - x_{(m,n')}] &= [c_0], \\ [x_{(mr,n)} - x_{(m,rn)}] &= [c_0]. \end{aligned}$$

Arvestades tehete definitsioone faktorrühmal saame võrdsed

$$\begin{aligned} [x_{(m+m',n)}] &= [x_{(m,n)}] + [x_{(m',n)}], \\ [x_{(m,n+n')}] &= [x_{(m,n)}] + [x_{(m,n')}], \\ [x_{(mr,n)}] &= [x_{(m,rn)}]. \end{aligned} \tag{6.4}$$

Tähistame

$$m \otimes n := [x_{(m,n)}] = x_{(m,n)} + H.$$

Vaatleme veel kujutust

$$\otimes: M \times N \longrightarrow M \otimes_R N, \quad (m, n) \mapsto m \otimes n.$$

Lause 6.38 Paar $(M \otimes_R N, \otimes)$ on moodulite M_R ja ${}_R N$ tensorkorrutis.

TÕESTUS. Kujutus $\otimes$ on R -tasakaalustatud, sest iga $m, m' \in M$, $n, n' \in N$ ja $r \in R$ korral

$$\begin{aligned} \otimes(m + m', n) &= (m + m') \otimes n = m \otimes n + m' \otimes n = \otimes(m, n) + \otimes(m', n), \\ \otimes(m, n + n') &= m \otimes (n + n') = m \otimes n + m \otimes n' = \otimes(m, n) + \otimes(m, n') \\ \otimes(mr, n) &= mr \otimes n = m \otimes rn = \otimes(m, rn). \end{aligned}$$

Olgu A Abeli rühm ja olgu $\bar{\beta}: M \times N \longrightarrow A$ mingi R -tasakaalustatud kujutus. Vaatleme injektivset kujutust

$$\iota: M \times N \longrightarrow \mathbb{Z}^{(M \times N)}, \quad (m, n) \mapsto x_{(m,n)}$$

ning kujutust

$$\bar{\varphi}: \mathcal{B} \longrightarrow A, \quad x_{(m,n)} \mapsto \bar{\beta}(m, n).$$

Abeli rühmade universaalomaduse põhjal (lause 6.26) põhjal leidub rühmade homomorfism $\varphi: \mathbb{Z}^{(M \times N)} \longrightarrow A$ nii, et $\varphi|_{\mathcal{B}} = \bar{\varphi}$. Tähistagu $\pi: \mathbb{Z}^{(M \times N)} \longrightarrow M \otimes_R N$, $f \mapsto [f]$, loomulikku projektsiooni faktorrühmale. Paneme tähele, et ülemine kolmnurk joonisel

$$\begin{array}{ccc} M \times N & & \\ \downarrow \otimes & \searrow \iota & \searrow \bar{\beta} \\ & \mathbb{Z}^{(M \times N)} & \xrightarrow{\varphi} A \\ & \swarrow \pi & \nearrow \beta \\ & M \otimes_R N & \end{array}$$

kommuteerub, sest iga $(m, n) \in M \times N$ korral

$$(\varphi \circ \iota)(m, n) = \varphi(\iota(m, n)) = \varphi(x_{(m, n)}) = \overline{\varphi}(x_{(m, n)}) = \overline{\beta}(m, n).$$

Ka selle joonise vasakpoolne kolmnurk kommuteerub, sest iga $(m, n) \in M \times N$ korral

$$(\pi \circ \iota)(m, n) = \pi(x_{(m, n)}) = [x_{(m, n)}] = m \otimes n = \otimes(m, n).$$

Kujutus φ viib alamrühma H tekitajad (6.3) nulliks:

$$\begin{aligned} \varphi(x_{(m_1+m_2, n)} - x_{(m_1, n)} - x_{(m_2, n)}) &= \varphi(x_{(m_1+m_2, n)}) - \varphi(x_{(m_1, n)}) - \varphi(x_{(m_2, n)}) \\ &= \beta(m_1 + m_2, n) - (\beta(m_1, n) + \beta(m_2, n)) \\ &= \beta(m_1 + m_2, n) - \beta(m_1 + m_2, n) = 0_A, \\ \varphi(x_{(m, n_1+n_2)} - x_{(m, n_1)} - x_{(m, n_2)}) &= 0_A, \\ \varphi(x_{(mr, n)} - x_{(m, rn)}) &= \beta(mr, n) - \beta(m, rn) = 0_A. \end{aligned}$$

Seega $H \subseteq \text{Ker}(\varphi)$. Teoreemi 6.3 kasutades saame, et leidub rühmade homomorfism $\beta: M \otimes_R N \rightarrow A$ nii, et alumine kolmnurk joonisel kommuteerub. Seega kommuteerub kogu diagramm, mistõttu kehtib võrdus $\beta \circ \otimes = \overline{\beta}$.

Lõpetuseks tuleb veel vaja näidata, et homomorfism β on ühene. Olgu ka $\beta': M \otimes_R N \rightarrow A$ selline Abeli rühmade homomorfism, et $\overline{\beta} = \beta' \circ \otimes$. Iga $(m, n) \in M \times N$ korral

$$\beta'(m \otimes n) = (\beta' \circ \otimes)(m, n) = \overline{\beta}(m, n) = (\beta \circ \otimes)(m, n) = \beta(m \otimes n).$$

Kuna baasi $\mathcal{B}$ elemendid tekitavad vaba Abeli rühma $\mathbb{Z}^{(M \times N)}$, siis nende kõrvalklassid $m \otimes n$ tekitavad faktorrühma $M \otimes_R N$. Et β' ja β langevad kokku $M \otimes_R N$ tekitajatel, siis nad langevad kokku kõigil elementidel. Seega $\beta' = \beta$, mis tähendab, et β on üheselt määratud. Sellega on tõestatud, et $(M \otimes_R N, \otimes)$ on R -moodulite M_R ja ${}_R N$ tensorkorrutis. $\square$

Sõnastame veelkord iniversaalomaduse kanoonilise tensorkorrutise $M \otimes_R N$ jaoks.

Tensorkorrutise universaalomadus. Iga Abeli rühma A ja R -tasakaalustatud kujutuse $\overline{\beta}: M \times N \rightarrow A$ korral leidub üheselt määratud Abeli rühmade homomorfism $\beta: M \otimes_R N \rightarrow A$ nii, et järgmine diagramm on kommutatiivne:

$$\begin{array}{ccc} & M \times N & \\ \otimes \swarrow & & \searrow \overline{\beta} \\ M \otimes_R N & \xrightarrow{\beta} & A. \end{array}$$

Märkus 6.39 Kahe vektorruumi tensorkorrutis defineeritakse üsna sarnaselt moodulite tensorkorrutisega. Erinevus tuleb sellest, et vektorruumide tensorkorrutis on samuti vektorruum ja et vektorruumide puhul ei pea vaatlema eraldi vasakpoolseid ja parempoolseid vektorruume. Vektorruumide tensorkorrutisi kasutatakse palju füüsikas ja geomeetrias.

Olgu V ja W vektorruumid üle korpuse K . Vaatleme vektorruumi $K^{(V \times W)}$, kus tehted on defineeritud punktiivisiliselt. Sarnaselt moodulite juhuga vaatleme selle vektorruumi baasi

$$\mathcal{B} = \{x_{(v,w)} \mid (v,w) \in V \times W\}.$$

Olgu $H \subseteq K^{(V \times W)}$ elementide

$$\begin{aligned} x_{(v+v',w)} - x_{(v,w)} - x_{(v',w)}, \\ x_{(v,w+w')} - x_{(v,w)} - x_{(v,w')}, \\ kx_{(v,w)} - x_{(kv,w)}, \\ kx_{(v,w)} - x_{(v,kw)} \end{aligned} \tag{6.5}$$

lineaarne kate (s.t. vähim alamruum, mis neid elemente sisaldab). Kanooniline tensorkorrutis $V \otimes W$ defineeritakse kui faktorruum

$$V \otimes W = K^{(V \times W)} / H.$$

Tähistades jällegi elemendi $x_{(v,w)}$ kõrvalklassi $v \otimes w := x_{(v,w)} + H$ näeme, et

$$V \otimes W = \left\{ \sum_{i=1}^s k_i(v_i \otimes w_i) \mid s \in \mathbb{N}, k_i \in K, v_i \in V, w_i \in W \right\},$$

kusjuures tensorkorrutises arvutamisel saab kasutada arvutusreegleid

$$(v + v') \otimes w = v \otimes w + v' \otimes w, \tag{6.6}$$

$$v \otimes (w + w') = v \otimes w + v \otimes w', \tag{6.7}$$

$$k(v \otimes w) = kv \otimes w = v \otimes kw. \tag{6.8}$$

Märgime veel, et vektorruumide tensorkorrutise moodustamisel ei pea piirduma kahe vektorruumiga, võib vaadelda suvalise lõpliku arvu vektorruumide tensorkorrutist.

6.7 Tensorkorrutise omadused

Tutvume nüüd tensorkorrutise lihtsamate omadustega. Muuhulgas näitame, kuidas tensorkorrutise elemente saab esitada teatud lõplike summadena.

Lause 6.40 *Olgu R ring, M_R parempoolne R -moodul ja ${}_R N$ vasakpoolne R -moodul. Tensorkorrutise $M \otimes_R N$ suvaline element ν on esitatav lõpliku summana moodustajatest:*

$$\nu = \sum_{k=1}^s m_k \otimes n_k, \quad s \in \mathbb{N}, m_k \in M, n_k \in N. \tag{6.9}$$

Lisaks kehtivad iga $m, m' \in M$, $n, n' \in N$ ja $r \in R$ korral järgnevad võrdused:

TENS1. $(m + m') \otimes n = (m \otimes n) + (m' \otimes n);$

TENS2. $m \otimes (n + n') = (m \otimes n) + (m \otimes n');$

TENS3. $mr \otimes n = m \otimes rn$;

TENS4. $0_M \otimes 0_N = m \otimes 0_N = 0_M \otimes n$ on Abeli rühma $M \otimes_R N$ nullelement;

TENS5. $-(m \otimes n) = (-m) \otimes n = m \otimes (-n)$.

TÕESTUS. Tensorkorrutis $M \otimes_R N$ on faktorrühm $\mathbb{Z}^{(M \times N)}/H$ eelmises paragrahvis kirjelatud alamrühma H järgi. Järelikult selle iga element ν avaldub kujul

$$\nu = \left[\sum_{k=1}^s z_k x_{(m_k, n_k)} \right] = \sum_{k=1}^s z_k [x_{(m_k, n_k)}] = \sum_{k=1}^s z_k (m_k \otimes n_k),$$

kus $s \in \mathbb{N}$, $z_k \in \mathbb{Z}$ ja $(m_k, n_k) \in M \times N$. Lisaks sellele, kui mingi $k \in \{1, \dots, s\}$ korral $z_k \neq 1$, siis võime liidetavat $m_k \otimes n_k$ lisada summasse $|z_k|$ korda ning vajadusel saab miinusmärgi viia liidetava $m_k \otimes n_k$ sisse (vastavalt omadusele TENS5).

Omadused TENS1–TENS3 kehtivad tänu võrdustele (6.4). Tõestame omaduse TENS4. Kui $m \in M$ ja $n \in N$, siis

$$\begin{aligned} m \otimes n + 0_M \otimes 0_N &= m \otimes n + 0_M \otimes (0_R n) = m \otimes n + (0_M \cdot 0_R) \otimes n = m \otimes n + 0_M \otimes n \\ &= (m + 0_M) \otimes n = m \otimes n. \end{aligned}$$

Seega $0_M \otimes 0_N$ on Abeli rühma $M \otimes_R N$ nullelement. Lisaks kehtib

$$m \otimes 0_N = m \otimes 0_R \cdot 0 : N = m 0_R \otimes 0_N = 0_M \otimes 0_N$$

ja analoogiliselt $0_M \otimes n = 0_M \otimes 0_N$.

Tõestame omaduse TENS5. Kui $m \in M$ ja $n \in N$, siis

$$m \otimes n + (-m) \otimes n = (m + (-m)) \otimes n = 0_M \otimes n = 0_M \otimes 0_N.$$

Seega $-(m \otimes n) = (-m) \otimes n$ Abeli rühmas $M \otimes_R N$. □

Kuigi iga tensorkorrutise $M \otimes_R N$ element avaldub summana kujul (6.9), see esitus ei ole üldiselt ühene. Tensorkorrutise $M \otimes_R N$ elemente nimetatakse **tensoriteks**. Esitusest (6.9) on selge, et hulk

$$\{m \otimes n \mid m \in M, n \in N\} \subseteq M \otimes_R N$$

on Abeli rühma $M \otimes_R N$ moodustajate süsteem. Selle hulga elemente $m \otimes n$ nimetatakse tensorkorrutise $M \otimes_R N$ **elementaartensoriteks**. Seega võib öelda, et *tensorkorrutise iga element on elementaartensorite lõplik summa*.

Nüüd saame täpsustada universaalomaduses oleva homomorfismi β kuju.

Lemma 6.41 Olgu R ring, M_R ja ${}_R N$ R -moodulid, A Abeli rühm ning $\bar{\beta} : M \times N \longrightarrow A$ R -tasakaalustatud kujutus. Siis defineerib eeskiri

$$\beta : M \otimes_R N \longrightarrow A, \quad \sum_{k=1}^s m_k \otimes n_k \mapsto \sum_{k=1}^s \bar{\beta}(m_k, n_k) \quad (6.10)$$

Abeli rühmade homomorfismi.

TÕESTUS. Tensorkorrutise universaalomaduse tõttu leidub üheselt määratud Abeli rühmade homomorfism $\beta: M \otimes_R N \longrightarrow A$ nii, et $\bar{\beta} = \beta \circ \otimes$. Kuna β on homomorfism, siis iga elemendi $\sum_{k=1}^s m_k \otimes n_k \in M \otimes_R N$ korral kehtib

$$\beta \left(\sum_{k=1}^s m_k \otimes n_k \right) = \sum_{k=1}^s \beta(m_k \otimes n_k) = \sum_{k=1}^s (\beta \circ \otimes)(m_k, n_k) = \sum_{k=1}^s \bar{\beta}(m_k, n_k).$$

□

6.8 Tensorfunktorid

Selles paragrahvis näitame, et tensorkorrutamine fikseeritud mooduliga tekitab loomulikult viisil funktori.

Olgu R ring ning olgu $f: M_R \longrightarrow M'_R$ ja $g: {}_R N \longrightarrow {}_R N'$ R -moodulite homomorfismid. Defineerime kujutuse $(f; g): M \times N \longrightarrow M' \otimes_R N'$ võrdusega

$$(f; g)(m, n) := f(m) \otimes g(n).$$

See kujutus $(f; g)$ on R -tasakaalustatud, sest iga $m, m' \in M$, $n, n' \in N$ ja $r \in R$ korral

$$\begin{aligned} (f; g)(m + m', n) &= f(m + m') \otimes g(n) = (f(m) + f(m')) \otimes g(n) \\ &= f(m) \otimes g(n) + f(m') \otimes g(n) = (f; g)(m, n) + (f; g)(m', n), \\ (f; g)(m, n + n') &= (f; g)(m, n) + (f; g)(m, n'), \\ (f; g)(mr, n) &= f(mr) \otimes g(n) = f(m)r \otimes g(n) = f(m) \otimes rg(n) \\ &= f(m) \otimes g(rn) = (f; g)(m, rn). \end{aligned}$$

Tensorkorrutise universaalomadust kasutades saame leida Abeli rühmade homomorfismi $f \otimes g: M \otimes_R N \longrightarrow M' \otimes_R N'$ nii, et $(f \otimes g) \circ \otimes = (f; g)$. Järelikult

$$(f \otimes g)(m \otimes n) = ((f \otimes g) \circ \otimes)(m, n) = (f; g)(m, n) = f(m) \otimes g(n).$$

Homomorfismi $f \otimes g$ nimetatakse **moodulite homomorfismide f ja g tensorkorrutiseks**. Nagu nägime,

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

iga $m \in M$ ja $n \in N$ korral. Kuna $f \otimes g$ Abeli rühmade homomorfism, siis $M \otimes_R N$ iga elemendi $\sum_{k=1}^s m_k \otimes n_k$ puhul

$$(f \otimes g) \left(\sum_{k=1}^s m_k \otimes n_k \right) = \sum_{k=1}^s (f \otimes g)(m_k \otimes n_k) = \sum_{k=1}^s f(m_k) \otimes g(n_k).$$

Lause 6.42 Olgu R ring ning olgu $f: M_R \longrightarrow M'_R$, $f': M'_R \longrightarrow M''_R$, $g: {}_R N \longrightarrow {}_R N'$ ja $g': {}_R N' \longrightarrow {}_R N''$ R -moodulite homomorfismid. Siis kehtib võrdus

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g).$$

TÕESTUS. Iga elementaartensori $m \otimes n \in M \otimes_R N$ korral

$$\begin{aligned} ((f' \otimes g') \circ (f \otimes g))(m \otimes n) &= (f' \otimes g')(f(m) \otimes g(n)) = f'(f(m)) \otimes g'(g(n)) \\ &= (f' \circ f)(m) \otimes (g' \circ g)(n) = ((f' \circ f) \otimes (g' \circ g))(m \otimes n). \end{aligned}$$

□

Nüüd saame konstrueerida fikseeritud mooduliga tensorkorrutamise funktori.

Lause 6.43 Olgu R ring ja ${}_R N$ moodul. Siis eeskiri

$$\begin{array}{ccc} M_R & \xrightarrow{\quad} & M \otimes_R N \\ f \downarrow & & \downarrow f \otimes \text{id}_N \\ M'_R & \xrightarrow{\quad} & M' \otimes_R N \end{array}$$

defineerib funktori $- \otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$.

TÕESTUS. Niisiis eeskiri $- \otimes_R N$ viib parempoolse R -mooduli M_R Abeli rühmaks $M \otimes_R N$ ja parempoolsete R -moodulite homomorfismi $f : M_R \longrightarrow M'_R$ Abeli rühmade homomorfismiks $f \otimes \text{id}_N$. See eeskiri on funktor, sest iga $M_R \in \mathbf{Mod}_R$ korral

$$(- \otimes_R N)(\text{id}_M) = \text{id}_M \otimes \text{id}_N = \text{id}_{M \otimes_R N}$$

kuna iga $m \in M$ ja $n \in N$ puhul

$$(\text{id}_M \otimes \text{id}_N)(m \otimes n) = \text{id}_M(m) \otimes \text{id}_N(n) = m \otimes n = \text{id}_{M \otimes_R N}(m \otimes n),$$

ning mistahes homomorfismide $f : M_R \longrightarrow M'_R$ ja $g : M'_R \longrightarrow M''_R$ korral tänu lausele 6.42 kehtib

$$\begin{aligned} (- \otimes_R N)(g \circ f) &= (g \circ f) \otimes \text{id}_N = (g \circ f) \otimes (\text{id}_N \circ \text{id}_N) = (g \otimes \text{id}_N) \circ (f \otimes \text{id}_N) \\ &= (- \otimes_R N)(g) \circ (- \otimes_R N)(f). \end{aligned}$$

□

Duaalselt tekitab iga parempoolne moodul M_R funktori $M \otimes_R - : {}_R \mathbf{Mod} \longrightarrow \mathbf{Ab}$.

Lause 6.44 Olgu R ring. Iga mooduli ${}_R N$ korral säilitab funktor $- \otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$ epimorfisme.

TÕESTUS. Meenutame et lause 6.4 tõttu on kategooriates $\mathbf{Mod}_R$ ja $\mathbf{Ab}$ epimorfismid parajasti sürjektiivsed homomorfismid.

Niisiis olgu $f : M_R \longrightarrow M'_R$ sürjektiivne homomorfism. Peame näitama, et Abeli rühmade homomorfism $f \otimes \text{id}_N : M \otimes_R N \longrightarrow M' \otimes_R N$ on sürjektiivne. Olgu $\sum_{k=1}^s m'_k \otimes n_k \in M' \otimes_R N$ suvaline element. Tänu f sürjektiivsusele leidub iga $k \in \{1, \dots, s\}$ korral $m_k \in M$ nii, et $m'_k = f(m_k)$. Järelikult

$$\sum_{k=1}^s m'_k \otimes n_k = \sum_{k=1}^s f(m_k) \otimes n_k = (f \otimes \text{id}_N) \left(\sum_{k=1}^s m_k \otimes n_k \right).$$

□

Samas funktor $- \otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$ ei pruugi säilitada monomorfisme. See annab põhjuse defineerida mooduli lameduse mõiste, mida uurime järgmises paragrahvis.

6.9 Lamedad moodulid

Definitsioon 6.45 Moodul M_R on **lame**, kui funktor $M \otimes_R - : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ säilitab monomorfisme, s.t. viib iga monomorfismi monomorfismiks.

Meenutame, et lause 6.4 põhjal on moodulite ja Abeli rühmade monomorfismid parajasti injektiivsed homomorfismid.

Selles paragrahvis tahame tõestada, et iga unitaarne vaba moodul üle ühikelemendiga ringi on lame. Tõestus tugineb järgmisele tensorskorrutise omadusele. Selle lause tõestuse juhul $I = \{1, 2\}$ võib leida raamatust [4] (lause 3.16).

Teoreem 6.46 Kui R on ring, $M_i, i \in I$, on parempoolsed R -moodulid ja ${}_R N$ on vasakpoolne R -moodul, siis kehtib Abeli rühmade isomorfism

$$\left(\bigoplus_{i \in I} M_i \right) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N).$$

Lühidalt öelduna: tensorskorrutamise funktor $- \otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$ säilitab moodulite väliseid otsesummasid. Täpselt nagu vektorruumide korralgi (vt. lauset 2.55) saab näidata, et parempoolsete R -moodulite (Abeli rühmade) välised otsesummad on kokorrutised kategoorias $\mathbf{Mod}_R$ (kategoorias $\mathbf{Ab}$). Seega võib ka öelda: tensorskorrutamise funktor $- \otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$ säilitab kokorrutisi.

TÕESTUS. Vaatleme kujutust

$$\hat{\varphi} : \left(\bigoplus_{i \in I} M_i \right) \times N \longrightarrow \bigoplus_{i \in I} (M_i \otimes_R N), \quad ((m_i)_{i \in I}, n) \mapsto (m_i \otimes n)_{i \in I}.$$

See kujutus on R -tasakaalustatud, sest

$$\begin{aligned} \hat{\varphi}((m_i)_{i \in I} + (m'_i)_{i \in I}, n) &= \hat{\varphi}((m_i + m'_i)_{i \in I}, n) && \text{(liitmine otsesummas)} \\ &= ((m_i + m'_i) \otimes n)_{i \in I} && (\hat{\varphi} \text{ def.}) \\ &= (m_i \otimes n + m'_i \otimes n)_{i \in I} && \text{(TENS1)} \\ &= (m_i \otimes n)_{i \in I} + (m'_i \otimes n)_{i \in I} && \text{(liitmine otsesummas)} \\ &= \hat{\varphi}((m_i)_{i \in I}) + \hat{\varphi}((m'_i)_{i \in I}), && (\hat{\varphi} \text{ def.}) \\ \hat{\varphi}((m_i)_{i \in I}, n + n') &= (m_i \otimes (n + n'))_{i \in I} && (\hat{\varphi} \text{ def.}) \\ &= (m_i \otimes n + m_i \otimes n')_{i \in I} && \text{(TENS2)} \\ &= (m_i \otimes n)_{i \in I} + (m_i \otimes n')_{i \in I} && \text{(liitmine otsesummas)} \\ &= \hat{\varphi}((m_i)_{i \in I}, n) + \hat{\varphi}((m_i)_{i \in I}, n'), && (\hat{\varphi} \text{ def.}) \\ \hat{\varphi}((m_i)_{i \in I} r, n) &= \hat{\varphi}((m_i r)_{i \in I}, n) && \text{(} R \text{-toime otsesummal)} \\ &= (m_i r \otimes n)_{i \in I} && (\hat{\varphi} \text{ def.}) \\ &= (m_i \otimes rn)_{i \in I} && \text{(TENS3)} \\ &= \hat{\varphi}((m_i)_{i \in I}, rn). && (\hat{\varphi} \text{ def.}) \end{aligned}$$

Seega leidub Abeli rühmade homomorfism $\varphi : \left(\bigoplus_{i \in I} M_i\right) \otimes_R N \longrightarrow \bigoplus_{i \in I} (M_i \otimes_R N)$ nii, et

$$\varphi((m_i)_{i \in I} \otimes n) = (m_i \otimes n)_{i \in I} \quad (6.11)$$

iga $(m_i)_{i \in I} \in \bigoplus_{i \in I} M_i$ ja $n \in N$ korral. Konstrueerime kujutusele φ pöördkujutuse ψ . Selleks vaatleme iga $j \in I$ korral kujutust

$$\hat{\psi}_j : M_i \times N \longrightarrow i \left(\bigoplus_{i \in I} M_i \right) \otimes_R N, \quad (m, n) \mapsto \iota_j(m) \otimes n,$$

kus $\iota_j(m) \in \bigoplus_{i \in I} M_i$ on selline pere, mille i -komponent on

$$(\iota_j(m))_i = \begin{cases} m, & \text{kui } i = j, \\ 0_{M_i}, & \text{kui } i \neq j. \end{cases}$$

Kujutus $\hat{\psi}_j$ on R -tasakaalustatud, sest

$$\begin{aligned} \hat{\psi}_j(m + m', n) &= \iota_j(m + m') \otimes n = (\iota_j(m) + \iota_j(m')) \otimes n = \iota_j(m) \otimes n + \iota_j(m') \otimes n \\ &= \hat{\psi}_j(m, n) + \hat{\psi}_j(m', n), \\ \hat{\psi}_j(m, n + n') &= \iota_j(m) \otimes (n + n') = \iota_j(m) \otimes n + \iota_j(m) \otimes n' = \hat{\psi}_j(m, n) + \hat{\psi}_j(m, n'), \\ \hat{\psi}_j(mr, n) &= \iota_j(mr) \otimes n = \iota_j(m)r \otimes n = \iota_j(m) \otimes rn = \hat{\psi}_j(m, rn). \end{aligned}$$

õ Tensorkorrutise $M_j \otimes_R N$ universaalomaduse põhjal leidub Abeli rühmade homomorfism $\psi_j : M_j \otimes_R N \longrightarrow \left(\bigoplus_{i \in I} M_i\right) \otimes_R N$ nii, et

$$\psi_j(m_j \otimes n) = \iota_j(m_j) \otimes n$$

iga $m_j \in M_j$ ja $n \in N$ korral.

Vaatleme ka kujutusi

$$u_j : M_j \otimes_R N \longrightarrow \bigoplus_{i \in I} (M_i \otimes_R N), \quad m \otimes n \mapsto u_j(m \otimes n),$$

kus

$$(u_j(m \otimes n))_i = \begin{cases} m \otimes n, & \text{kui } i = j, \\ 0, & \text{kui } i \neq j \end{cases}$$

iga $i, j \in I$ korral. Välise otsesumma universaalomaduse tõttu (vt. definitsiooni 1.50 ja lauset 2.55) leidub üheselt määratud Abeli rühmade homomorfism

$$\psi : \bigoplus_{i \in I} (M_i \otimes_R N) \longrightarrow \left(\bigoplus_{i \in I} M_i \right) \otimes_R N$$

nii, et $\psi \circ u_j = \psi_j$ iga $j \in I$ korral, s.t. diagramm

$$\begin{array}{ccc}
 & (\bigoplus_{i \in I} M_i) \otimes_R N & \\
 \psi_j \nearrow & \uparrow \psi & \\
 M_j \otimes_R N & \xrightarrow{u_j} & \bigoplus_{i \in I} (M_i \otimes_R N)
 \end{array}$$

kommuteerub. Siis

$$\begin{aligned}
 \psi((m_i \otimes n_i)_{i \in I}) &= \psi\left(\sum_{i \in I} u_i(m_i \otimes n_i)\right) && (u_i \text{ definitsioon}) \\
 &= \sum_{i \in I} (\psi \circ u_i)(m_i \otimes n_i) && (\psi \text{ on homomorfism}) \\
 &= \sum_{i \in I} \psi_i(m_i \otimes n_i) && (\psi \circ u_i = \psi_i) \\
 &= \sum_{i \in I} (\iota_i(m_i) \otimes n_i). && (\psi_i \text{ definitsioon})
 \end{aligned}$$

Kujutused φ ja ψ on teineteise pöördkujutused, sest

$$\begin{aligned}
 (\varphi \circ \psi)((m_i \otimes n_i)_{i \in I}) &= \varphi\left(\sum_{i \in I} (\iota_i(m_i) \otimes n_i)\right) && (\psi \text{ def.}) \\
 &= \sum_{i \in I} \varphi(\iota_i(m_i) \otimes n_i) && (\varphi \text{ on homomorfism}) \\
 &= \sum_{i \in I} \varphi((\dots, 0, m_i, 0 \dots) \otimes n_i) && (\iota_i \text{ def.}) \\
 &= \sum_{i \in I} (\dots, 0, m_i \otimes n_i, 0 \dots) && (\varphi \text{ def.}) \\
 &= (m_i \otimes n_i)_{i \in I} && (\text{liitmine otseummas})
 \end{aligned}$$

rühma $\bigoplus_{i \in I} (M_i \otimes_R N)$ iga tekitaja $(m_i \otimes n_i)_{i \in I}$ korral ja

$$\begin{aligned}
 (\psi \circ \varphi)((m_i)_{i \in I} \otimes n) &= \psi((m_i \otimes n)_{i \in I}) && (\varphi \text{ def.}) \\
 &= \sum_{i \in I} (\iota_i(m_i) \otimes n) && (\psi \text{ def.}) \\
 &= \left(\sum_{i \in I} \iota_i(m_i)\right) \otimes n && (\text{TENS1}) \\
 &= (m_i)_{i \in I} \otimes n && (\iota_i \text{ def.})
 \end{aligned}$$

rühma $(\bigoplus_{i \in I} M_i) \otimes_R N$ iga tekitaja $(m_i)_{i \in I} \otimes n$ korral. $\square$

Lause 6.47 Iga unitaarse vasakpoolse mooduli ${}_R M$ korral üle ühikelemendiga ringi R leidub Abeli rühmade isomorfism $\gamma_M : R \otimes_R M \longrightarrow M$.

TÕESTUS. Lihtne on veenduda, et kujutus

$$\widehat{\gamma}_M : R \times M \longrightarrow M, \quad (r, m) \mapsto rm,$$

on R -tasakaalustatud. Seega leidub Abeli rühmade homomorfism $\gamma_M : R \otimes_R M \longrightarrow M$ nii, et

$$\gamma_M(r \otimes m) = rm$$

iga $r \in R$ ja $m \in M$ korral. Võime vaadelda ka kujutust

$$\delta_M : M \longrightarrow R \otimes_R M, \quad m \mapsto 1_R \otimes m.$$

Siis

$$\begin{aligned} (\gamma_M \circ \delta_M)(m) &= \gamma_M(1_R \otimes m) = 1_R m = m, \\ (\delta_M \circ \gamma_M)(r \otimes m) &= \delta_M(rm) = 1_R \otimes rm = r \otimes m, \end{aligned}$$

seega γ_M ja δ_M on teineteise pöördkujutused. $\square$

Märkus 6.48 Tegelikult on võimalik veel näidata, et definitsioon $r'(r \otimes m) := r'r \otimes m$ muudab Abeli rühma $R \otimes_R M$ vasakpoolseks R -mooduliks ja γ_M on vasakpoolsete R -moodulite homomorfism.

Teoreem 6.49 *Unitaarne vaba moodul üle ühikelemendiga ringi on lame.*

TÕESTUS. Olgu R ühikelemendiga ring ja F_R unitaarne vaba moodul. Teoreemiga 6.22 duaalse tulemuse tõttu võime eeldada, et F_R on kujul $F_R = R^{(I)}$, kus I on mingi hulk. Olgu $f : {}_R M \longrightarrow {}_R N$ suvaline injektiivne vasakpoolsete unitaarsete moodulite homomorfism. Me peame näitama, et Abeli rühmade homomorfism

$$\text{id}_F \otimes f : R^{(I)} \otimes_R M \longrightarrow R^{(I)} \otimes_R N, \quad (r_i)_{i \in I} \otimes m \mapsto (r_i)_{i \in I} \otimes f(m),$$

on injektiivne. Kõigepealt paneme tähele, et ruut

$$\begin{array}{ccc} R \otimes_R M & \xrightarrow{\text{id}_R \otimes f} & R \otimes_R N \\ \gamma_M \downarrow & & \downarrow \gamma_N \\ {}_R M & \xrightarrow{f} & {}_R N \end{array}$$

kommuteerub, sest

$$(\gamma_N \circ (\text{id}_R \otimes f))(r \otimes m) = \gamma_N(r \otimes f(m)) = rf(m) = f(rm) = (f \circ \gamma_M)(r \otimes m)$$

Abeli rühma $R \otimes_R M$ iga tekitaja $r \otimes m$ korral. Rakendades sellele ruudule funktoorit $(-)^{(I)} : \mathbf{Ab} \longrightarrow \mathbf{Ab}$ (vt. märkust 6.6) saame alumise kommutatiivse ruudu diagrammis

$$\begin{array}{ccc}
R^{(I)} \otimes_R M & \xrightarrow{\text{id}_F \otimes f} & R^{(I)} \otimes_R N \\
\varphi_M \downarrow & & \downarrow \varphi_N \\
(R \otimes_R M)^{(I)} & \xrightarrow{(\text{id}_R \otimes f)^{(I)}} & (R \otimes_R N)^{(I)} \\
\gamma_M^{(I)} \downarrow & & \downarrow \gamma_N^{(I)} \\
{}_R M^{(I)} & \xrightarrow{f^{(I)}} & {}_R N^{(I)}.
\end{array}$$

Siin φ_M ja φ_N on defineeritud sarnaselt φ -ga eelmise teoreemi tõestuses (vt. võrdust (6.11)). Kõik vertikaalsed nooled on eelneva põhjal isomorfismid. Ka ülemine ruut kommuteerub:

$$\begin{aligned}
((\text{id}_R \otimes f)^{(I)} \circ \varphi_M)((r_i)_{i \in I} \otimes m) &= (\text{id}_R \otimes f)^{(I)}((r_i \otimes m)_{i \in I}) && (\varphi_M \text{ def.}) \\
&= ((\text{id}_R \otimes f)(r_i \otimes m))_{i \in I} && ((\text{id}_R \otimes f)^{(I)} \text{ def.}) \\
&= (r_i \otimes f(m))_{i \in I} && (\text{id}_R \otimes f \text{ def.}) \\
&= \varphi_N((r_i)_{i \in I} \otimes f(m)) && (\varphi_N \text{ def.}) \\
&= (\varphi_N \circ (\text{id}_F \otimes f))((r_i)_{i \in I} \otimes m). && (\text{id}_F \otimes f \text{ def.})
\end{aligned}$$

Seega on kogu diagramm kommutatiivne. Nüüd

$$\begin{aligned}
f \text{ injektiivne} &\implies f^{(I)} \text{ injektiivne} && (\text{funktor } (-)^I \text{ säilitab monomorfisme}) \\
&\implies (\text{id}_R \otimes f)^{(I)} \text{ injektiivne} && (\text{hulgateooria}) \\
&\implies \text{id}_F \otimes f \text{ injektiivne.} && (\text{hulgateooria})
\end{aligned}$$

□

Märkus 6.50 Kasutades seda teoreemi ja teoreemi 6.33 (projektiivne moodul on vaba mooduli otseliidetav) saab näidata, et ka iga unitaarne projektiivne moodul üle ühikelemendiga ringi on lame.

Peatükk 7

Poolrühmad

7.1 Põhimõisted

Definitsioon 7.1 Poolrühmaks nimetatakse hulka S koos sellel defineeritud kahekohalise algebralise tehtega $\cdot$, mis on assotsiatiivne, see tähendab, et mistahes $a, b, c \in S$ korral $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Harilikult kirjutatakse $a \cdot b$ asemel lihtsalt ab .

Definitsioon 7.2 Poolrühma S nimetatakse **monoidiks**, kui temas leidub ühikelement, s.t. selline element e , et iga $a \in S$ korral $ea = a = ae$.

Poolrühma S ühikelement (kui ta leidub) on üheselt määratud ja siin kursuses tähistatame seda harilikult sümboliga 1_S .

Näide 7.3 1. $(\mathbb{N}, +)$ on poolrühm, mis ei ole monoid.

2. $(\mathbb{N}, \cdot)$ on monoid ühikelemendiga 1.

3. Kordarvude hulk on poolrühm korrutamise suhtes.

4. Mittetühja hulga X kõigi teisenduste hulk $\mathcal{T}(X)$ on monoid teisenduste järjestamiseks suhtes. Selle monoidi ühikelement on hulga X samasusteisendus id_X .

5. Olgu X suvaline mittetühi hulk. Defineerides

$$xy := x$$

iga $x, y \in X$ korral saame poolrühma, mida nimetatakse **vasakpoolsete nullide poolrühmaks**.

Definitsioon 7.4 Poolrühma S elementi e nimetatakse **idempotendiks**, kui $e^2 = e$. Poolrühma S kõigi idempotentide hulka tähistatakse $E(S)$.

Lemma 7.5 Kui S on rühm, siis temas on täpselt üks idempotent.

TÕESTUS. Korrutades võrduse $ee = e$ pooli elemendiga e^{-1} saame võrduse $e = 1_S$. $\square$

Näide 7.6 Poolrühmas $(\mathbb{Z}, \cdot)$ on kaks idempotenti: 0 ja 1. Vasakpoolsete nullide poolrühmas (vt. näidet 7.3) on kõik elemendid idempotendid.

Definitsioon 7.7 Olgu S ja T poolrühmad. Kujutust $f: S \rightarrow T$ nimetatakse **poolrühmade homomorfismiks**, kui iga $x, y \in S$ korral

$$f(xy) = f(x)f(y).$$

Definitsioon 7.8 Poolrühmade **isomorfism** on bijektiivne homomorfism.

Definitsioon 7.9 Poolrühma S alamhulka U nimetatakse **alampoolrühmaks**, kui ta on kinnine korrutamise suhtes.

Definitsioon 7.10 Monoidi S alamhulka U nimetatakse **alammonoidiks**, kui ta on kinnine korrutamise suhtes ja sisaldab monoidi S ühikelementi.

Näide 7.11 Paarisarvude hulk $2\mathbb{N}$ on poolrühma $(\mathbb{N}, \cdot)$ alampoolrühm, aga ta ei ole monoidi $(\mathbb{N}, \cdot)$ alammonoid, sest ei sisalda selle ühikelementi 1.

Nii nagu ringiteoorias, on ka poolrühmateoorias oluline roll ideaalidel.

Definitsioon 7.12 Alamhulka I poolrühmas S nimetatakse poolrühma S **parempoolseks (vasakpoolseks) ideaaliks**, kui

$$as \in I \quad (sa \in I)$$

mistahes $a \in I$, $s \in S$ korral. Poolrühma S **ideaaliks** nimetatakse parempoolset ideaali I , mis on samal ajal ka vasakpoolne ideaal.

Definitsiooni järgi loeme ka poolrühma tühja alamhulga ideaaliks.

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

Näide 7.13 Vaatleme poolrühma $S = (\mathbb{N}, \cdot)$. Siis paaritute naturaalarvude hulk U on selle poolrühma alampoolrühm, kuid ei ole ideaal, sest näiteks $3 \in U$, $2 \in S$ ja $3 \cdot 2 \notin U$.

Poolrühma S kõigi ideaalide hulka $\text{Id}(S)$ võib vaadelda järjestatud hulga sisalduvussuhte suhtes. Selle järjestatud hulga vähim element on $\emptyset$ ja suurim element on S .

Definitsioon 7.14 Poolrühma S ideaali I nimetatakse **minimaalseks ideaaliks**, kui

1. $I \neq \emptyset$
2. iga ideaali J korral

$$J \neq \emptyset \quad \text{ja} \quad J \subseteq I \Rightarrow J = I.$$

Analoogiliselt saab defineerida minimaalsed vasak- ja parempoolsed ideaalid.

Definitsioon 7.15 Olgu S poolrühm, olgu 1 mingi element, mis ei kuulu hulka S ja

$$S^1 = S \cup \{1\}.$$

Defineerime hulgal S^1 korrutamise nii, et poolrühma S elementide omavahelisi korrutisi ei muudeta, $1 \cdot 1 = 1$ ja

$$1s = s1 = s$$

iga $s \in S$ korral. Ilmselt on S^1 monoid ühikelemendiga 1. Öeldakse, et monoid S^1 on saadud poolrühmast S **ühikelemendi välisel lisamisel**.

Näide 7.16 Lõpliku poolrühma korrutamistehe antakse sageli tabeli abil, mida kutsutakse Cayley tabeliks. Sellises tabelis on elemendiga a märgistatud rea ja elemendiga b märgistatud veeru lõikekohas korrutis ab . Näiteks võib vaadelda poolrühma

$$S = \{e, a, f, b\},$$

mille Cayley tabel on

	e	a	f	b
e	e	e	e	b
a	e	e	a	b
f	e	e	f	b
b	b	b	b	e

Välise ühikelemendi lisamisel saame poolrühma $S^1 = \{e, a, f, b, 1\}$, mille Cayley tabel on

	e	a	f	b	1
e	e	e	e	b	e
a	e	e	a	b	a
f	e	e	f	b	f
b	b	b	b	e	b
1	e	a	f	b	1

Mistahes poolrühma S ja elemendi $a \in S$ korral tähistame

$$\begin{aligned} Sa &= \{sa \mid s \in S\}, \\ aS &= \{as \mid s \in S\}, \\ SaS &= \{sat \mid s, t \in S\}. \end{aligned}$$

Siis

$$\begin{aligned} S^1a &= Sa \cup \{a\}, \\ aS^1 &= aS \cup \{a\}, \\ S^1aS^1 &= SaS \cup Sa \cup aS \cup \{a\}. \end{aligned}$$

Lihtne on veenduda, et kehtib järgmine lemma.

Lemma 7.17 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 7.18 Öeldakse, et S^1a (aS^1 , S^1aS^1) on poolrühma S elemendi a poolt tekitatud **vasakpoolne peaideaal** (vastavalt **parempoolne peaideaal**, **peaideaal**).

7.2 Lihtsad poolrühmad

Definitsioon 7.19 Poolrühma S ideaali I nimetatakse **pärisideaaliks**, kui $I \neq S$.

Definitsioon 7.20 Poolrühma S nimetatakse **lihtsaks**, kui ta ei sisalda mittetühje pärisideaale.

Seega poolrühm on lihtne parajasti siis, kui tema ainsad ideaalid on $\emptyset$ ja S .

Lause 7.21 Poolrühm S on lihtne parajasti siis, kui $SaS = S$ iga $a \in S$ korral.

TÕESTUS. TARVILIKKUS. Oletame, et S on lihtne poolrühm ja olgu $a \in S$ suvaline. Kui $sat \in SaS$ ja $u \in S$ siis

$$u(sat) = (us)at \in SaS, \quad (sat)u = sa(tu) \in SaS.$$

Seega SaS on ideaal. See ideaal on mittetühi, sest $aaa \in SaS$. Kuna S on lihtne, siis $SaS = S$.

PIISAVUS. Oletame, et $SaS = S$ iga $a \in S$ korral ja olgu I poolrühma S mittetühi ideaal. On vaja näidata, et $S \subseteq I$. Võtame $s \in S$. Kuna $I \neq \emptyset$ siis leidub mingi element $a \in I$. Eelduse põhjal $SaS = S$. Järelikult leiduvad $x, y \in S$ nii, et $s = xay$. Kuna I on vasakpoolne ideaal poolrühmas S , siis $xa \in I$. Et ta on ka parempoolne ideaal, siis $s = xay \in I$. Seega $I = S$ ning S on lihtne poolrühm. $\square$

Ülesanne 7.22 Näidake, et iga rühm on lihtne poolrühm.

Kui A ja B on poolrühma S alamhulga, siis kasutatakse tähistust

$$AB = \{ab \mid a \in A, b \in B\}.$$

Muuhulgas $A = B = S$ korral kirjutatakse $SS = S^2$.

Definitsioon 7.23 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 $(\{2, 3, 4, 5, \dots\}, \cdot)$ aga ei ole faktoriseeruv, sest näiteks elementi 2 ei saa esitada kahe elemendi korrutisena.

Lause 7.24 Lihtne poolrühm on faktoriseeruv.

TÕESTUS. Tühja poolrühma korral võrdus $S^2 = S$ ilmselt kehtib. Olgu S lihtne mittetühi poolrühm. Kerge on näha, et S^2 on poolrühma S mittetühi ideaal. Järelikult $S^2 = S$. $\square$

Lause 7.25 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 mittetühi 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 7.21 põhjal on M lihtne poolrühm. $\square$

7.3 Greeni seosed

Poolrühmade struktuuri uurimisel on suureks abiks teatud ideaalide abil defineeritud seosed, mida kutsutakse nende kasutusele võtja järgi Greeni¹ seosteks.

Definitsioon 7.26 Olgu $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ ja $\mathcal{D}$ seosed poolrühmal S , mis on defineeritud järgmiselt:

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

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

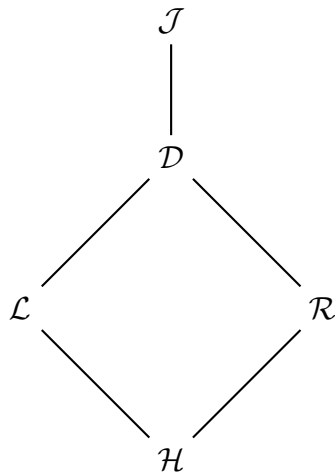
$$a\mathcal{L}b \iff S^1a = S^1b$$

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

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

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

Märkus 7.27 Lihtne on aru saada, et $\mathcal{R}$, $\mathcal{L}$ ja $\mathcal{J}$ on ekvivalentsiseosed hulgal S . Saab näidata, et $\mathcal{H} = \mathcal{L} \wedge \mathcal{R}$ ja $\mathcal{D} = \mathcal{L} \vee \mathcal{R}$, kus alumine ja ülemine raja $\mathcal{R}$ ja $\mathcal{L}$ vahel leitakse hulga S kõigi ekvivalentsiseoste hulgas, mis on järjestatud hulk sisalduvusseose suhtes. Sümbol $\circ$ tähistab binaarsete seoste korrutamist. Saab näidata, et $\mathcal{D} \subseteq \mathcal{J}$. On selge, et $\mathcal{H} \subseteq \mathcal{L} \subseteq \mathcal{D}$ ja $\mathcal{H} \subseteq \mathcal{R} \subseteq \mathcal{D}$. Seega Greeni seoste vahelisi sisalduvusi võib kirjeldada järgmise diagrammi abil:



Elemendi $a \in S$ $\mathcal{L}$ -klassi ($\mathcal{R}$ -klassi, $\mathcal{H}$ -klassi, $\mathcal{D}$ -klassi ja $\mathcal{J}$ -klassi) tähistatakse L_a (vastavalt R_a , H_a , D_a ja J_a). Lihtne on veenduda, et kehtib järgmine lause.

Lause 7.28 Mistahes poolrühma S ja elementide $a, b \in S$ korral

$$a\mathcal{R}b \iff (\exists u, v \in S^1)(a = bu \wedge b = av);$$

$$a\mathcal{L}b \iff (\exists u, v \in S^1)(a = ub \wedge b = va);$$

$$a\mathcal{J}b \iff (\exists u, v, s, t \in S^1)(a = ubv \wedge b = sat).$$

¹James Alexander Green (1926–2014) — briti matemaatik

Näide 7.29 Mistahes hulkade A ja X korral on hulk $S = A \times X$ poolrühm korrutamise

$$(a, x)(a', x') := (a, x')$$

suhtes. Selliseid poolrühmi nimetatakse **ristkülikpoolrühmadeks** (inglise keeles *rectangular band*).

Vaatleme konkreetseuse mõttes olukorda, kus $A = \{a, b\}$ ja $X = \{x, y, z\}$. Otsekorrutise $A \times X$ elemendid võib kirjutada üles tabelina

(a, x)	(a, y)	(a, z)
(b, x)	(b, y)	(b, z)

On võimalik näidata, et selle tabeli read on poolrühma $A \times X$ $\mathcal{R}$ -klassid ja veerud on $\mathcal{L}$ -klassid. Seega $\mathcal{H}$ -klassid on üheelemendilised ja poolrühmal on üksainus $\mathcal{D}$ -klass, mis koosneb kõigist tema elementidest.

Vaatleme nüüd suvalist poolrühma S . Kuna $\mathcal{L} \subseteq \mathcal{D}$, siis on iga $\mathcal{D}$ -klass $\mathcal{L}$ -klasside lõikumatu ühend. Samuit on iga $\mathcal{D}$ -klass $\mathcal{R}$ -klasside lõikumatu ühend.

Lemma 7.30 *Olgu D poolrühma S mingi $\mathcal{D}$ -klass, olgu $L \subseteq D$ mingi $\mathcal{L}$ -klass ja $R \subseteq D$ mingi $\mathcal{R}$ -klass. Siis $R \cap L$ on $\mathcal{H}$ -klass.*

TÕESTUS. Kõigepealt näitame, et $R \cap L \neq \emptyset$. Võtame mingid $b \in L \subseteq D$ ja $a \in R \subseteq D$. Kuna $a\mathcal{D}b$ ehk $a(\mathcal{R} \circ \mathcal{L})b$, siis leidub $c \in S$ nii, et $a\mathcal{R}c$ ja $c\mathcal{L}b$. Siis $c \in R_a \cap L_b = R \cap L$ ja $R \cap L \neq \emptyset$.

Näitame veel, et $H_c = R \cap L$. Kui $x \in H_c$, siis $x\mathcal{R}c$ ja $x\mathcal{L}c$, seega $x \in R_c = R_a = R$ ja $x \in L_c = L_b = L$. Järelikult $x \in R \cap L$. Vastupidi, kui $x \in R \cap L$, siis $x\mathcal{R}a\mathcal{R}c$ ja $x\mathcal{L}b\mathcal{L}c$, seega $x\mathcal{H}c$ ja $x \in H_c$. $\square$

See lemma võimaldab lõpliku poolrühma $\mathcal{D}$ -klasse esitada nn. „munaresti diagrammi“ (ingl. k. *eggbox diagram*) abil. Kui näiteks poolrühma mingis $\mathcal{D}$ -klassis olevad $\mathcal{L}$ -klassid on L_1, L_2, L_3, L_4 ja $\mathcal{R}$ -klassid on R_1, R_2, R_3 ning tähistame $H_{ij} := R_i \cap L_j$, siis diagramm näeb välja nii:

	L_1	L_2	L_3	L_4
R_1	H_{11}	H_{12}	H_{13}	H_{14}
R_2	H_{21}	H_{22}	H_{23}	H_{24}
R_3	H_{31}	H_{32}	H_{33}	H_{34}

Lisaks kongruentsidele räägitakse poolrühmade puhul ka ühepoolsetest kongruentsidest.

Lause 7.31 *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*

$$\begin{aligned} a\mathcal{R}b &\implies ca\mathcal{R}cb, \\ a\mathcal{L}b &\implies ac\mathcal{L}bc. \end{aligned}$$

TÕESTUS. Olgu $a, b, c \in S$ ja olgu $a\mathcal{R}b$. Siis $aS^1 = bS^1$. Tänu lausele 7.28 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 7.28 põhjal võime öleda, et $ca\mathcal{R}cb$.

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

Lemma 7.32 (Greeni lemma) *Olgu $a, b \in S$, $a\mathcal{R}b$, $u, v \in S^1$, $au = b$ ja $bv = a$. Siis viib kujutus $\rho_u : x \mapsto xu$, klassi L_a üksüheselt terveks klassiks L_b ning kujutus $\rho_v : y \mapsto yv$, klassi L_b üksüheselt terveks klassiks L_a , kusjuures ρ_u ei vii välja $\mathcal{R}$ -klassist (seega $\mathcal{H}$ -klassid klassist L_a viiakse $\mathcal{H}$ -klassideks klassis L_b).*

TÕESTUS. Olgu $x \in L_a$. Siis $x\mathcal{L}a$, järelikult lause 7.31 põhjal $xu\mathcal{L}au = b$ ehk $xu = \rho_u(x) \in L_b$. Analoogiliselt, kui $y \in L_b$, siis $yv \in L_a$. Seega saab vaadelda kujutusi

$$\begin{aligned}\rho_u : L_a &\longrightarrow L_b, \quad x \mapsto xu, \\ \rho_v : L_b &\longrightarrow L_a, \quad y \mapsto yv.\end{aligned}$$

Näitame, et need on teineteise pöördkujutused. Kui $x \in L_a$, siis leidub $t \in S^1$ nii, et $x = ta$, ning järelikult

$$(\rho_v \circ \rho_u)(x) = \rho_v(\rho_u(x)) = (xu)v = ((ta)u)v = t(au)v = tbv = ta = x.$$

Analoogiliselt näeme, et $\rho_u \circ \rho_v = \text{id}_{L_b}$. Seega ρ_u ja ρ_v on bijektsioonid.

Vaja on veel näidata, et ρ_u ei vii välja $\mathcal{R}$ -klassist. Olgu $x, y \in L_a$ ja $x\mathcal{R}y$ (seega $x\mathcal{R}y$). Kuna $(xu)v = \rho_v(\rho_u(x)) = x$, siis $x\mathcal{R}(xu)$. Analoogiliselt $y\mathcal{R}(yu)$. Järelikult

$$\rho_u(x) = xu\mathcal{R}x\mathcal{R}y\mathcal{R}yu = \rho_u(y)$$

ja tänu seose $\mathcal{R}$ transitiiivsusele $\rho_u(x)\mathcal{R}\rho_u(y)$.

	L_a		L_b
R_a	a		b
	x, y		xu, yu

$\square$

7.4 Täiesti lihtsad poolrühmad

Ei ole võimalik kirjeldada ära kõiki lihtsaid poolrühmi. Küll aga on võimalik ära kirjeldada lihtsate poolrühmade klassi üks alamklass — täiesti lihtsate poolrühmade klass.

Definitsioon 7.33 Poolrühma S idempotenti e nimetatakse **primitiivseks**, kui iga $f \in E(S)$ korral:

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

Definitsioon 7.34 Lihtsat poolrühma S , mis sisaldab primitiivset idempotenti, nimetatakse **täiesti lihtsaks**.

Lemma 7.35 *Poolrühma iga minimaalne vasakpoolne (parempoolne) ideaal on selle poolrühma $\mathcal{L}$ -klass ($\mathcal{R}$ -klass).*

TÕESTUS. Teeme läbi tõestuse minimaalse vasakpoolse ideaali korral. Olgu L poolrühma S minimaalne vasakpoolne ideaal ja $x \in L$ suvaline element. Siis $S^1x \subseteq L$ ja tänu L minimaalsusele $S^1x = L$. Fikseerides mingi elemendi $a \in L$ näeme, et iga $x \in L$ korral $S^1x = L = S^1a$. Järelikult $x\mathcal{L}a$ ehk $x \in L_a$. Seega $L \subseteq L_a$.

Kui aga $c \in L_a$, siis $c \in S^1c = S^1a = L$. See tähendab, et $L_a \subseteq L$. Kokkuvõttes oleme näidanud, et $L = L_a$, s.t. L on elemendi a $\mathcal{L}$ -klass. $\square$

Järgmiseks tõestame ühe piisava tingimuse selleks, et poolrühm oleks oma minimaalsete vasakpoolsete (parempoolsete) ideaalide ühend.

Lause 7.36 *Kui S on lihtne poolrühm ja sisaldab minimaalset vasakpoolset ideaali L (minimaalset parempoolset ideaali R), siis S on oma minimaalsete vasakpoolsete (parempoolsete) ideaalide ühend.*

TÕESTUS. Olgu S lihtne poolrühm ja olgu L minimaalne vasakpoolne ideaal. Olgu $s \in S$, tähistame $Ls = \{as \mid a \in L\}$. Siis hulk Ls on vasakpoolne ideaal poolrühmas S . Näitame, et Ls on minimaalne vasakpoolne ideaal. Oletame, et $B \neq \emptyset$ on vasakpoolne ideaal poolrühmas S ja $B \subseteq Ls$. Siis hulk

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

on vasakpoolne ideaal poolrühmas S . Tänu L minimaalsusele kehtib võrdus $A = L$. Teiste sõnadega: iga $a \in L$ korral $as \in B$ ehk $Ls \subseteq B$. Seega $B = Ls$. Nüüd olgu

$$M = \bigcup_{s \in S} Ls.$$

Siis kindlasti M on vasakpoolne ideaal. See on tegelikult ideaal, sest kui $m \in Ls \subseteq M$, siis $mt \in L(st) \subseteq M$ iga $t \in S$ korral. Siit järeldub S lihtsuse tõttu, et $M = S$, ning oleme näidanud, et S on minimaalsete vasakpoolsete ideaalide Ls ühend.

Lause teise poole tõestus on analoogiline. $\square$

Lemma 7.37 *Mittetühi poolrühm S on rühm parajasti siis, kui $aS = S$ ja $Sa = S$ iga $a \in S$ korral.*

TÕESTUS. **TARVILIKKUS.** Seda on lihtne kontrollida.

PIISAVUS. Fikseerime mingi elemendi $a \in S$. Siis $aS = S$. Muuhulgas leidub selline element $e \in S$, et $a = ae$. Kui $s \in S = Sa$, siis $s = ua$ mingi $u \in S$ korral ja seega $se = uae = ua = s$. Niisiis $se = s$ iga $s \in S$ korral. Analoogiliselt saab leida elemendi $f \in S$ nii, et $fs = s$ iga $s \in S$ korral. Järelikult

$$f = fe = e$$

ja S on monoid ühikelemendiga e .

Kui $s \in S$, siis võrdustest $S = sS$ ja $S = Ss$ järeldub, et $e = su$ ja $e = vs$ mingite $u, v \in S$ korral. Siis aga

$$v = ve = v(su) = (vs)u = eu = u,$$

s.t. u on elemendi s pöördement. □

Üldiselt poolrühma $\mathcal{H}$ -klassid ($\mathcal{L}$ -klassid, $\mathcal{R}$ -klassid, $\mathcal{D}$ -klassid, $\mathcal{J}$ -klassid) ei pruugi olla alampoolrühmad. Vaatleme ühte olukorda, kus $\mathcal{H}$ -klassid on alampoolrühmad.

Lause 7.38 *Järgmised väited poolrühma S $\mathcal{H}$ -klassi H kohta on samaväärsed.*

1. *Leidub $e^2 = e \in H$.*
2. *Leiduvad $a, b \in H$ nii, et $ab \in H$.*
3. *H on poolrühma S alampoolrühm, mis on rühm.*

TÕESTUS. 1. $\Rightarrow$ 2. Võtame $a = b = e$.

2. $\Rightarrow$ 3. Olgu $a, b \in H$ sellised, et $ab \in H$. Lemma 7.32 põhjal on kujutus

$$\lambda_a : H \rightarrow H, \quad x \mapsto ax$$

bijektiivne. Kuna λ_a on kujutus, siis $ac \in H$ iga $c \in H$ korral ning kuna λ_a on sürjektiivne, siis $H = aH$. Nüüd iga $c \in H$ korral $a \mathcal{H} ac$ ja seega $H = H_a = H_{ac}$. Lemmaga 7.32 duaalne tulemus (mille tõestus on täiesti analoogiline) ütleb, et ka

$$\rho_c : H \rightarrow H, \quad x \mapsto xc$$

on bijektiivne kujutus. Seega $Hc = H$ iga $c \in H$ korral. Kuna $dc \in H$ mistahes $d, c \in H$ korral, siis H on kinnine korrutamise suhtes, s.t. alampoolrühm. Muuhulgas $cc \in H$ iga $c \in H$ korral. Võttes a ja b ossa c ja kasutades tõestuse alguse mõttekäiku näeme, et ka $H = cH$ iga $c \in H$ korral. Kokkuvõttes $cH = H = Hc$ iga $c \in H$ korral. Me oleme juba näidanud, et H on S alampoolrühm, järelikult ka ise poolrühm. Et $a \in H$, siis H on mittetühi. Lemma 7.37 kohaselt on H rühm.

3. $\Rightarrow$ 1. Idempotendiks e sobib rühma H ühikelement. □

Lause 7.39 *Täiesti lihtsa poolrühma kõik $\mathcal{H}$ -klassid on rühmad.*

TÕESTUS. Olgu S täiesti lihtne poolrühm ja e tema primitiivne idempotent. Näitame, et Se on minimaalne vasakpoolne ideaal. Selleks oletame, et $I \neq \emptyset$ on vasakpoolne ideaal ja $I \subseteq Se$. Võtame mingi elemendi $a \in I$. Kuna $a \in Se$, siis leidub selline $s \in S$, et $a = se$. Järelikult $ae = see = se = a$. Et S on lihtne, siis $S^1 a S^1 = S$ ning seega $e = uav$ mingite $u, v \in S^1$ korral. Tähistame $f := eveua$. Kasutades võrdusi $ae = a$ ja $uav = e$ saame, et

$$\begin{aligned} f^2 &= (eveua)(eveua) = (eveu)(ae)(veua) = (eveu)a(veua) = (eve)(uav)(eua) \\ &= eveeeua = eveua = f, \\ ef &= eeveua = eveua = f, \\ fe &= eveuae = eveua = f. \end{aligned}$$

Kuna e on primitiivne idempotent, siis $e = f$ ehk $e = eveua \in I$, sest $a \in I$ ja I on vasakpoolne ideaal. Seega iga $t \in S$ korral $te = teveua \in I$. Järelikult $Se \subseteq I$ ning kokkuvõttes oleme saanud, et $I = Se$. Sellega on näidatud, et Se on minimaalne vasakpoolne ideaal.

Lause 7.36 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 7.35 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 7.38 on H_a rühm. $\square$

7.5 Reesi maatrikspoolrühmad

Osutub, et täiesti lihtsad poolrühmad on võimalik saada suhteliselt lihtsa konstruktsiooni abil rühmadest. Seda konstruktsiooni kirjeldas esimesena David Rees².

Olgu G rühm ühikelemendiga 1_G ning olgu I, Λ mittetühjad hulgid. Võtame ühe $(\Lambda \times I)$ -maatriksi $P = (p_{\lambda i})$, mille elemendid kuuluvad rühma G . Sellist maatriksit võib vaadelda kujutusena $\Lambda \times I \longrightarrow G, (\lambda, i) \mapsto p_{\lambda i}$.

Olgu $S = I \times G \times \Lambda$ ja defineerime hulka S kuuluvate järjestatud kolmikute korrutamise järgmiselt:

$$(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda j}h, \mu),$$

$(i, g, \lambda), (j, h, \mu) \in S$. Märgime, et korrutis $gp_{\lambda j}h$ leitakse rühmas G .

Lemma 7.40 S on poolrühm.

TÕESTUS. Kontrollime kas hulgal S defineeritud korrutamine on assotsiatiivne. Tõepoolest:

$$\begin{aligned} ((i, g, \lambda)(i', g', \lambda'))(i'', g'', \lambda'') &= (i, gp_{\lambda, i'}g', \lambda')(i'', g'', \lambda'') \\ &= (i, (gp_{\lambda, i'}g')p_{\lambda', i''}g'', \lambda'') \\ &= (i, gp_{\lambda, i'}(g'p_{\lambda', i''}g''), \lambda'') \\ &= (i, g, \lambda)(i', g'p_{\lambda', i''}g'', \lambda'') \\ &= (i, g, \lambda)((i', g', \lambda')(i'', g'', \lambda'')). \end{aligned}$$

$\square$

Niimoodi konstrueeritud poolrühma tähistatakse $\mathcal{M}[G; I, \Lambda; P]$ ja nimetatakse $I \times \Lambda$ **Reesi maatrikspoolrühmaks** üle rühma G „sändvitšmaatriksiga“ P . Märgime, et selle konstruktsiooniga saaksime poolrühma ka siis, kui G oleks poolrühm, mitte rühm.

Ülesanne 7.41 Olgu $I = \{i, j\}$, $\Lambda = \{\lambda, \mu\}$ ja $G = (\mathbb{Z}_2, +)$. Anname kujutuse $P : \Lambda \times I \longrightarrow G$ maatriksiga

$$\begin{array}{c|cc} & i & j \\ \hline \lambda & \bar{1} & \bar{0} \\ \mu & \bar{1} & \bar{0} \end{array}.$$

Kirjutage välja Reesi maatrikspoolrühma $\mathcal{M}[G; I, \Lambda; P]$ korrutamistehte Cayley tabel.

²David Rees (1918–2013) — briti matemaatik

Lause 7.42 Poolrühm $\mathcal{M} = \mathcal{M}[G; I, \Lambda; P]$ on täiesti lihtne.

TÕESTUS. Kontrollimaks, et poolrühm $\mathcal{M}$ on lihtne, võib tähele panna, et poolrühma $\mathcal{M}$ iga kahe elemendi (i, a, λ) ja (j, b, μ) korral

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

Lause 7.21 põhjal on poolrühm $\mathcal{M}$ lihtne.

Näitame, et $\mathcal{M}$ on täiesti lihtne poolrühm, see tähendab, et temas leidub primitiivne idempotent. Selleks vaatame elementi $(i, a, \lambda) \in \mathcal{M}$. Paneme tähele, et

$$\begin{aligned} (i, a, \lambda) \in E(\mathcal{M}) &\iff (i, a, \lambda)(i, a, \lambda) = (i, a, \lambda) \\ &\iff (i, ap_{\lambda i}a, \lambda) = (i, a, \lambda) \\ &\iff ap_{\lambda, i}a = a \\ &\iff p_{\lambda, i}a = 1 \\ &\iff a = p_{\lambda, i}^{-1}. \end{aligned}$$

Seega poolrühma $\mathcal{M}$ idempotentide hulk

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

Võtame kaks idempotenti $e = (i, p_{\lambda i}^{-1}, \lambda)$ ja $f = (j, p_{\mu j}^{-1}, \mu)$ ning oletame, et $ef = fe = e$ ehk

$$(i, p_{\lambda i}^{-1}p_{\lambda j}p_{\mu j}^{-1}, \mu) = (j, p_{\mu j}^{-1}p_{\mu i}p_{\lambda i}^{-1}, \lambda) = (i, p_{\lambda i}^{-1}, \lambda),$$

Siis $j = i$ ja $\lambda = \mu$, kust järeldub, et $e = f$, sest ka $p_{\lambda i} = p_{\mu j}$ ja $p_{\lambda i}^{-1} = p_{\mu j}^{-1}$. Seega näeme, et kõik idempotendid on primitiivsed. Järelikult on poolrühm $\mathcal{M}$ täiesti lihtne. $\square$

7.6 Reesi teoreem

Lause 7.43 Olgu S täiesti lihtne poolrühm, mis sisaldab primitiivset idempotenti $e \in S$. Siis

1. $R_e = eS$;
2. iga $a \in S$ korral $R_a = aS^1$,
3. iga $a \in S$ korral $L_a = S^1a$.

TÕESTUS. Kui $a \in R_e$, siis $a\mathcal{R}e$ ja seega $a \in aS^1 = eS^1 = eS$. See tähendab, et $R_e \subseteq eS$.

Vastupidise sisalduvuse näitamiseks olgu $a = es$ hulga eS element. Siis $ea = ees = es = a$. Kuna S on lihtne poolrühm, siis lause 7.21 põhjal elementide e ja a jaoks leiduvad $z, t \in S$ nii, et $e = zat$. Siis

$$e = zat = zeat = ezeate.$$

Tähistame $x := eze$ ja $y := te$. Siis

$$e = xay, \quad ex = xe = x, \quad ye = y. \quad (7.1)$$

Nüüd vaatame elementi $f = ayx$. Siis

$$f^2 = ayxayx = ayeax = ayx = f,$$

ehk f on idempotent. Võrdustest $ea = a$ ja $xe = x$ tuleneb, et $ef = fe = f$. Kuna e on primitiivne idempotent, siis $e = f = ayx \in aS^1$. Kuna veel $a \in eS$, siis $aS^1 = eS^1 = eS$, mis tähendab, et $a \in R_e$. Seega $eS \subseteq R_e$ nagu nõutud.

2. Kui $b \in R_a$, siis $b \in bS^1 = aS^1$, seega $R_a \subseteq aS^1$.

Vastupidise sisalduvuse näitamiseks eeldame, et $b \in aS^1$. Tänu poolrühma S lihtsusele leiduvad elemendid $z, t \in S$ nii, et $a = zet$. Seetõttu $b = zeu$ mingi $u \in S$ korral. Teades, et $R_e = eS$ ja $\mathcal{R}$ on vasakpoolne kongruents, saame, et

$$eu, et \in eS \implies eu, et \in R_e \implies eu\mathcal{R}et \implies zeu\mathcal{R}zet \iff b\mathcal{R}a \iff b \in R_a,$$

Sellega oleme näidanud, et $aS^1 \subseteq R_a$.

3. Selle omaduse tõestamine on duaalne eelmisega. □

Teoreem 7.44 (Reesi teoreem) *Poolrühm on täiesti lihtne siis ja ainult siis, kui ta on isomorfne Reesi maatrikspoolrühmaga üle rühma.*

TÕESTUS. PIISAVUS. Järeldub lausest 7.42.

TARVILIKKUS. Olgu S täiesti lihtne poolrühm, mis sisaldab primitiivset idempotenti e . Näitame, et S on isomorfne Rees'i maatrikspoolrühmaga. Selleks tõestame esimese asjana, et S sisaldab ainult ühte $\mathcal{D}$ -klassi.

Olgu $a, b \in S$ ja $c := ab$. Lause 7.43 põhjal

$$c \in aS^1 \cap S^1b = R_a \cap L_b.$$

Kuna $b\mathcal{L}c\mathcal{R}a$, siis $b\mathcal{D}a$. See tähendab, et $\mathcal{D} = S \times S$ ja S sisaldab ainult ühte $\mathcal{D}$ -klassi $D = S$.

Meenutame, et poolrühma S kõik $\mathcal{H}$ -klassid on rühmad lause 7.39 põhjal.

Konstrueerime nüüd poolrühma S põhjal Reesi maatrikspoolrühma. Tähistagu I poolrühma S $\mathcal{R}$ -klasside hulka ja Λ tähistagu $\mathcal{L}$ -klasside hulka. Käsitleme hulki I ja Λ indekseid hulkadena ja kirjutame $\mathcal{R}$ -klasse kujul R_i , kus $i \in I$, ja $\mathcal{L}$ -klasse kujul L_λ , kus $\lambda \in \Lambda$. Lisaks sellele, $\mathcal{H}$ -klassi kujul $R_i \cap L_\lambda$ tähistame $H_{i\lambda}$.

Olgu L_{λ_1} elemendi e $\mathcal{L}$ -klass ja R_{i_1} selle elemendi $\mathcal{R}$ -klass. Siis $H_{i_1\lambda_1} = R_{i_1} \cap L_{\lambda_1}$ (nii nagu ka kõik teised $\mathcal{H}$ -klassid) on rühm tänu lausele 7.39. Me näitame, et S on isomorfne Reesi maatrikspoolrühmaga üle selle rühma. Lihtsuse mõttes kirjutame edaspidi i_1 ja λ_1 asemel lihtsalt 1, seega $H_{11} = R_1 \cap L_1$.

Iga $i \in I$ ja $\lambda \in \Lambda$ jaoks fikseerime mingi elemendi r_i rühmast $H_{i1} = R_i \cap L_1$ ja elemendi q_λ rühmast $H_{1\lambda} = R_1 \cap L_\lambda$. Kuna $r_i\mathcal{L}e$, siis $r_ie = r_i$, ja kuna $q_\lambda\mathcal{R}e$, siis $eq_\lambda = q_\lambda$. Greeni lemmast (lemma 7.32) ja sellega duaalsest tulemusest järeldub, et kujutused

$$\begin{aligned} \lambda_{r_i}: H_{11} &\longrightarrow H_{i1}, \quad x \mapsto r_ix \\ \rho_{q_\lambda}: H_{i1} &\longrightarrow H_{i\lambda}, \quad y \mapsto yq_\lambda \end{aligned}$$

on bijektiivsed. Seega saab iga $H_{i\lambda}$ elemendi kirjutada üheselt kujul $r_i a q_\lambda = (\rho_{q_\lambda} \circ \lambda_{r_i})(a)$, kus a on rühma H_{11} element. Kuna

$$S = \bigsqcup_{i \in I, \lambda \in \Lambda} H_{i\lambda},$$

siis kujutus

$$\varphi : I \times H_{11} \times \Lambda \rightarrow S, \quad (i, a, \lambda) \mapsto r_i a q_\lambda$$

on bijektsioon. Defineerime veel sändvitsmaatriksi $P = (p_{\lambda i})$ võrdusega

$$p_{\lambda i} := q_\lambda r_i$$

iga $i \in I$ ja $\lambda \in \Lambda$ korral. Et see definitsioon oleks korrektne, peab $q_\lambda r_i \in H_{11}$. Näitame seda. Olgu e' rühma $H_{i\lambda} = R_i \cap L_\lambda$ ühikelement. Kuna $e' \mathcal{R} r_i$, siis leidub $u \in S^1$ nii, et $r_i = e' u$, millest $e' r_i = r_i$. Kuna $e' \mathcal{L} q_\lambda$, siis leidub $v \in S^1$ nii, et $q_\lambda = v e'$, millest $q_\lambda e' = q_\lambda$. Järelikult

$$\begin{aligned} e' \mathcal{R} r_i &\implies (q_\lambda e') \mathcal{R} (q_\lambda r_i) \implies q_\lambda \mathcal{R} (q_\lambda r_i) \implies q_\lambda r_i \in R_{q_\lambda} = R_1, \\ e' \mathcal{L} q_\lambda &\implies (e' r_i) \mathcal{L} (q_\lambda r_i) \implies r_i \mathcal{L} (q_\lambda r_i) \implies q_\lambda r_i \in L_{r_i} = L_1 \end{aligned}$$

ehk $q_\lambda r_i \in R_1 \cap L_1 = H_{11}$.

	L_1		L_λ	
R_1	H_{11} $q_\lambda r_i$		$H_{1\lambda}$ q_λ	
R_i	H_{i1} r_i		$H_{i\lambda}$ e'	

Tõestuse lõpetamiseks paneme tähele, et mistahes $i, j \in I$, $a, b \in H_{11}$ ja $\lambda, \mu \in \Lambda$ korral

$$\begin{aligned} \varphi((i, a, \lambda)(j, b, \mu)) &= \varphi((i, a p_{\lambda j} b, \mu)) = r_i (a q_\lambda r_j b) q_\mu \\ &= (r_i a q_\lambda) (r_j b q_\mu) = \varphi((i, a, \lambda)) \varphi((j, b, \mu)), \end{aligned}$$

seega kujutus $\varphi : \mathcal{M}[H_{11}; I, \Lambda; P] \rightarrow S$ on poolrühmade isomorfism. $\square$

7.7 Regulaarsed ja inverssed poolrühmad

Definitsioon 7.45 Poolrühma S nimetatakse **regulaarseks**, kui

$$(\forall a \in S)(\exists x \in S) a = axa.$$

Kui a ja x on sellised elemendid, et $a = axa$, siis $ax = axax$ ja $xa = xaxa$, mis tähendab, et ax ja xa on idempotendid. Seega regulaarsetes poolrühmades on üldiselt “palju” idempotente.

Näide 7.46 1. Kui poolrühma S kõik elemendid on idempotendid, siis S on regulaarne.

2. Iga rühm on regulaarne poolrühm. Iga täiesti lihtne poolrühm on lause 7.39 tõttu rühmade ühend ja seega samuti regulaarne.

3. Kui X on mittetühi hulk, siis tema teisenduste poolrühm $\mathcal{T}(X)$ on regulaarne. Kui $f \in \mathcal{T}(X)$, siis defineerime teisenduse $g \in \mathcal{T}(X)$ nii, et ta viib iga elemendi hulgast $\text{Im}(f)$ mingiks selle elemendi originaaliks f suhtes, ja kõigil teistel X elementidel on g defineeritud suvaliselt. Siis $f = fgf$.

4. Poolrühm $(\text{Mat}_n(K), \cdot)$, kus K on korpus, on regulaarne. Ruutmaatriksi A Moore'i-Penrose'i pöördmaatriks A^+ rahuldab muuhulgas võrdust $AA^+A = A$.

Definitsioon 7.47 Poolrühma S elementi a' nimetatakse elemendi a **inversseks elemendiks**, kui $a = aa'a$ ja $a' = a'aa'$.

Lause 7.48 Regulaarse poolrühma iga elemendil leidub vähemalt üks inversne element.

TÕESTUS. Olgu S regulaarne poolrühm ja $a \in S$. Siis leidub $x \in S$ nii, et $a = axa$. Tähistame $a' := xax$. Siis

$$aa'a = a(xax)a = (axa)xa = axa = a$$

ja

$$a'aa' = (xax)a(xax) = x(axa)xax = x(axa)x = xax = a'.$$

□

Definitsioon 7.49 Poolrühma nimetatakse **inversseks**, kui tema iga elemendil leidub täpselt üks inversne element.

Edaspidi tähistame inversse poolrühma elemendi a üheselt määratud inversset elementi sümboliga a' . Definitsioonist järeldeb, et $(a')' = a$. Kuna iga idempotent e on iseenda inversne element, siis inversses poolrühmas $e' = e$.

Näide 7.50 Iga rühm on inversne poolrühm, kus $a' = a^{-1}$.

On selge, et iga inversne poolrühm on regulaarne. Järgmine tulemus ütleb, millised regulaarsed poolrühmad on inverssed. Selles kursuses me tõestust ei anna.

Teoreem 7.51 Regulaarne poolrühm on inversne parajasti siis, kui tema idempotendid commuteeruvad.

Peatükk 8

Polügonid

8.1 Põhimõisted

Polügon on mooduli mitteaditiivne analoog.

Definitsioon 8.1 Hulka A nimetatakse **parempoolseks polügoniks üle poolrühma S** ehk **parempoolseks S -polügoniks**, kui on antud kujutus $A \times S \rightarrow A, (a, s) \mapsto as$, nii, et

$$(as)t = a(st)$$

iga $a \in A$ ja $s, t \in S$ korral. Seda kujutust $A \times S \rightarrow A$ nimetatakse poolrühma S **toimeks** hulgal A . Mõnikord kirjutatakse as asemel $a \cdot s$. Parempoolset S -polügoni tähistatakse harilikult A_S . Analoogiliselt saab defineerida vasakpoolsed S -polügonid.

Definitsioon 8.2 Olgu S ja T poolrühmad. Hulka A koos vasakpoolse T -toime ja parempoolse S -toimega nimetatakse (S, T) -bipolügoniks, kui iga $t \in T$, $a \in A$ ja $s \in S$ korral

$$(ta)s = t(as).$$

Definitsioon 8.3 Olgu S poolrühm. Polügoni A_S nimetatakse **unitaarseks**, kui $AS = A$, kus $AS = \{as \mid a \in A, s \in S\}$. Teiste sõnadega: A_S on unitaarne, kui iga $a \in A$ jaoks leiduvad $a' \in A$ ja $s \in S$ nii, et $a = a's$.

Lemma 8.4 *Polügon A_S üle monoidi S on unitaarne parajasti siis, kui $a1_S = a$ iga $a \in A$ korral.*

TÕESTUS. **TARVILIKKUS.** Eeldame, et A_S on unitaarne ja võtame elemendi $a \in A$. Siis leiduvad $a' \in A$ ja $s \in S$ nii, et $a = a's$. Seega $a = a's = a'(s1_S) = (a's)1_S = a1_S$.

PIISAVUS. See on ilmne. $\square$

Näide 8.5 1. Olgu $(R, +, \cdot)$ ring. Siis iga parempoolne R -moodul on polügon üle selle ringi multiplikatiivse poolrühma $(R, \cdot)$.

2. Olgu S poolrühm. Siis S on polügon üle iseenda, kui toime $S \times S \rightarrow S$ defineerida poolrühma S korrutamise abil. Seda polügoni tähistatakse S_S .

3. Olgu A mittetühi hulk ja $\mathcal{T}$ selle hulga kõigi teisenduste monoid järjestrakendamise suhtes. Defineerides vasakpoolse toime $\mathcal{T} \times A \longrightarrow A$ võrdusega

$$fa := f(a)$$

$a \in A$, $f \in \mathcal{T}$, saame unitaarse vasakpoolse polügooni τA .

4. Automaatide teoorias vaadeldavad automaadid on polügonid. 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 poolrühmaks S tihti mõni vaba poolrühm.

5. Geomeetriast tuntud afinsed ruumid on unitaarsed polügonid. Afinne ruum on punktide hulk, millele saab liita mingist vektorruumist V pärit vektoreid nii, et tulemuseks on punkt. See polügon on üle vektorruumi aditiivse rühma $(V, +)$.

Definitsioon 8.6 Alalhulka B nimetatakse polügoni A_S **alampolügoniks**, kui iga $b \in B$ ja $s \in S$ korral $bs \in B$.

Näide 8.7 1. Mistahes S -polügonil A_S on olemas triviaalsed alampolügonid $\emptyset$ ja A .

2. Olgu S poolrühm. Siis S iga parempoolne ideaal on polügoni S_S alampolügon. Muuhulgas parempoolsed peaideaalid sS^1 , kus $s \in S$, on polügoni S_S alampolügonid.

3. Kui A_S on polügon, siis iga $a \in A$ korral $aS^1 = \{a\} \cup \{as \mid s \in S\}$ on alampolügon. Kui $A = aS^1$, siis öeldakse, et A_S on **tsükliline polügon** ja a on selle tekitaja.

Definitsioon 8.8 Olgu A_S polügon. Ekvivalentsiseos ρ hulgal A on polügoni A_S **kongruents**, kui iga $a, a' \in A$ ja $s \in S$ korral

$$a \rho a' \implies as \rho a's.$$

Faktorhulk $A/\rho = \{[a]_\rho \mid a \in A\}$ koos S -toimega

$$[a]_\rho s := [as]_\rho$$

on parempoolne S -polügon, mida nimetatakse polügoni A_S **faktorpolügoniks** kongruentsi ρ järgi.

Definitsioon 8.9 Kujutus $f : A_S \longrightarrow B_S$ on **parempoolsete S -polügonide homomorfism**, kui $f(as) = f(a)s$ iga $a \in A$ ja $s \in S$ korral.

Kõik parempoolsed S -polügonid koos nendevaheliste homomorfismidega moodustavad kategooria, mida tähistame Act_S . Selle täielikku alamkategooriat, mille tekitavad unitaarsed polügonid, tähistame UAct_S .

Lause 8.10 Iga poolrühma S korral on epimorfismid kategooriates Act_S ja UAct_S parajasti sürjektiivsed homomorfismid.

TÕESTUS. Sürjektiivne homomorfism on epimorfism tänu lausele 1.13. Tõestame kategoorias Act_S vastupidise implikatsiooni. Olgu $f : A_S \rightarrow B_S$ epimorfism kategoorias Act_S . Vaatleme lõikumatu ühendit $B_S \sqcup B_S = \{1, 2\} \times B$ parempoolse S -toimega

$$(i, b)s := (i, bs),$$

$i \in \{1, 2\}$, $b \in B$, $s \in S$. Defineerime binaarse seose σ hulgal $B_S \sqcup B_S$ järgmiselt:

$$(i, b)\sigma(i', b') \iff (i, b) = (i', b') \text{ või } i = i' \text{ ja } b = b' \in f(A).$$

Saab näidata, et σ on polügoni $B_S \sqcup B_S$ kongruents. Me tähistame paari (i, b) σ -klassi $[i, b]$. Vaatleme faktorpolügoni $C_S := (B_S \sqcup B_S)/\sigma$ ja defineerime parempoolsete S -polügonide homomorfismid $g, h : B_S \rightarrow C_S$ võrdustega

$$\begin{aligned} g(b) &:= [1, b], \\ h(b) &:= [2, b]. \end{aligned}$$

Siis $g \circ f = h \circ f$. Kuna f on epimorfism, siis $g = h$. Kui leidub element $b \in B \setminus f(A)$, siis $((1, b), (2, b)) \notin \sigma$ and $g(b) \neq h(b)$, vastuolu. Seega $f(A) = B$ ja f on sürjektiivne.

Sama tõestus läheb läbi ka kategoorias UAct_S , sest unitaarsete polügonide lõikumatu ühend on unitaarne ja unitaarse polügoni faktorpolügon on unitaarne. $\square$

Saab näidata, et monomorfismid kategoorias Act_S on parajasti injektiivsed homomorfismid.

8.2 Lahutumatud polügonid

Definitsioon 8.11 Polügoni nimetatakse **lahutumatuks**, kui teda ei saa esitada kahe mittetühja lõikumatu alampolügoni ühendina.

Näide 8.12 Olgu s poolrühma S suvaline element. Näitame, et parempoolne peaideaal $sS^1 = \{s\} \cup \{st \mid t \in S\}$ on lahutumatu S -polügon. Oletame vastuväiteliselt, et $sS^1 = C \sqcup D$, kus C ja D on mittetühjad alampolügoonid. Oletame, et $s \in C$. Siis $sS^1 \subseteq C$ ja seega $C \sqcup D = sS^1 \subseteq C$, kust $D \subseteq C$, mis on vastuolus C ja D lõikumatusesega. Analoogiliselt saaksime vastuolu siis, kui oletaksime, et $s \in D$. Rohkem võimalusi s jaoks ei ole.

Näide 8.13 Olgu S suvaline poolrühm ja $A = \{a_1, \dots, a_n\}$, kus $n \geq 2$, mingi hulk. Defineerime S -toime järgmiselt:

$$a_i s := a_i$$

iga $i \in \{1, \dots, n\}$ ja iga $s \in S$ korral. On selge, et nii saame parempoolse S -polügoni, kus iga alamhulk on alampolügon. Kuna näiteks

$$A_S = \{a_1\} \sqcup \{a_2, \dots, a_n\},$$

siis see polügon on lahutuv.

Lause 8.14 Iga mittetühi polügon on esitatav mittetühjade lahutumatute alampolügonide lõikumatu ühendina.

TÕESTUS. Vaatleme polügoni A_S . Defineerime hulgal A binaarse seose ρ järgmiselt: apb parajasti siis, kui leiduvad sellised $b_1, \dots, b_n \in A$ ja $s_1, \dots, s_n, t_1, \dots, t_n \in S^1$, et

$$\begin{aligned} a &= b_1 s_1 \\ b_1 t_1 &= b_2 s_2 \\ b_2 t_2 &= b_3 s_3 \\ &\dots \\ b_n t_n &= b. \end{aligned} \tag{8.1}$$

Ei ole raske näha, et ρ on ekvivalentsiseos. Seega A on ρ -klasside lõikumatu ühend. Paneme veel tähele, et kui $as = bt$, $a, b \in A$, $s, t \in S^1$, siis apb . Tõepoolest,

$$\begin{aligned} a &= a1 \\ as &= bt \\ b1 &= b. \end{aligned}$$

Muuhulgas, kuna $as \cdot 1 = a \cdot s$, siis $aspa$ iga $a \in A$ ja $s \in S$ korral. Oletame, et $b \in [a]_\rho$. Siis apb ja sobivate elementide korral kehtivad võrdused (8.1). Korrutades kõiki võrdusi paremalt S mistahes elemendiga s saame võrdused

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

kust näeme, et $aspbs$. Et $apas$, siis transitiivsuse tõttu $apbs$ ehk $bs \in [a]_\rho$. See tähendab, et iga ρ -klass $[a]_\rho$ on polügoni A_S alampolügon.

Tõestuse lõpetamiseks näitame, et ρ -klassid on lahutumatud. Oletame vastuväiteliselt, et

$$[a]_\rho = C \sqcup D,$$

kus C ja D on polügoni A_S mittetühjad alampolügonid. Valime mingid elemendid $c \in C$ ja $d \in D$. Siis $cpapd$ ja seega cpd . Järelikult leiduvad sellised $b_1, \dots, b_n \in A$ ja $s_1, \dots, s_n, t_1, \dots, t_n \in S^1$, et

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

Siit näeme, et

$$apcpb_1pb_2p \dots pb_npd.$$

Järelikult $b_1, \dots, b_n, d \in [a]_\rho = C \sqcup D$. Kui $b_1 \in D$, siis $c = b_1 s_1 \in C \cap D$, mis on vastuolus eeldusega, et $C \cap D = \emptyset$. Seega $b_1 \in C$. Analoogiliselt näeme, et ka $b_2, \dots, b_n, d \in C$. Viimane ($d \in C$) on aga samuti vastuolus sellega, et $C \cap D = \emptyset$. $\square$

8.3 Projektiivsed polügonid

Selles paragrahvis vaatleme polügonide projektiivsuse omadust kategoorias $\mathbf{UAct}_S$. Üldine kategoorne definitsioon (definitsioon 1.26) võtab järgmise kuju.

Definitsioon 8.15 Polügon $P_S \in \mathbf{UAct}_S$ on **projektiivne** kategoorias $\mathbf{UAct}_S$, kui selle kategooria iga sürjektiivse homomorfismi $\pi : A_S \rightarrow B_S$ ja iga homomorfismi $f : P_S \rightarrow B_S$ korral leidub homomorfism $g : P_S \rightarrow A_S$ nii, et $\pi \circ g = f$, s.t. järgmine diagramm on kommutatiivne:

$$\begin{array}{ccc} & P_S & \\ g \swarrow & & \searrow f \\ A_S & \xrightarrow{\pi} & B_S \end{array}$$

Näide 8.16 Tühi polügon $\emptyset_S$ on projektiivne, sest ainuke homomorfism $\emptyset_S \rightarrow B_S$ on tühi kujutus ja seega ka g ossa sobib tühi kujutus.

Eesmärk on anda mittetühjade projektiivsete polügonide kirjeldus kategoorias $\mathbf{UAct}_S$.

Lause 8.17 Olgu unitaarne polügon P_S oma mittetühjade alampolügonide P_i , $i \in I$, lõikumatu ühend, s.t. $P_S = \bigsqcup_{i \in I} P_i$. Polügon P_S on projektiivne kategoorias $\mathbf{UAct}_S$ parajasti siis, kui iga $i \in I$ korral polügon P_i on projektiivne kategoorias $\mathbf{UAct}_S$.

TÕESTUS. TARVILIKKUS. Olgu P_S projektiivne kategoorias $\mathbf{UAct}_S$ ning $j \in J$. Näitame, et P_j on projektiivne kategoorias $\mathbf{UAct}_S$. Olgu $f : P_j \rightarrow B_S$ morfism ja $\pi : A_S \rightarrow B_S$ sürjektiivne morfism kategoorias $\mathbf{UAct}_S$. Vaatleme diagrammi

$$\begin{array}{ccc} & P_S & \\ & \downarrow f' & \\ A_S \sqcup \Theta_S & \xrightarrow{\pi'} & B_S \sqcup \Theta_S \end{array},$$

kus $\Theta_S = \{\theta\}$ on ühe-elementiline polügon (s.t. $\theta s = \theta$ iga $s \in S$ korral) ja kujutused π', f' on defineeritud võrdustega

$$\pi'(x) = \begin{cases} \pi(x), & \text{kui } x \in A, \\ \theta, & \text{kui } x = \theta, \end{cases}$$

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

Lihtne on aru saada, et π' ja f' on homomorfismid ning π' on sürjektiivne. Kuna polügonid $A_S \sqcup \Theta_S$ ja $B_S \sqcup \Theta_S$ on unitaarsed ning P_S on projektiivne, siis leidub homomorfism

$g' : P_S \rightarrow A_S \sqcup \Theta_S$ nii, et $\pi' \circ g' = f'$.

$$\begin{array}{ccc} & P_S & \\ g' \swarrow & & \searrow f' \\ A_S \sqcup \Theta_S & \xrightarrow{\pi'} & B_S \sqcup \Theta_S \end{array}$$

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 $g : P_j \rightarrow A$ võrdusega

$$g(y) := g'(y).$$

Kuna g' on homomorfism, siis ka g on homomorfism. Kolmnurk

$$\begin{array}{ccc} & P_j & \\ g \swarrow & & \searrow f \\ A_S & \xrightarrow{\pi} & B_S \end{array}$$

kommuteerub, sest iga $y \in P_j$ korral

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

Järelikult $\pi g = f$, nagu vaja.

PIISAVUS. Eeldame, et kõik alampolügonid P_i , $i \in I$, on projektiivsed kategoorias $\mathbf{UAct}_S$. Vaatleme diagrammi

$$\begin{array}{ccc} & P_S & \\ & \downarrow f & \\ A_S & \xrightarrow{\pi} & B_S, \end{array}$$

kus π on sürjektiiivne homomorfism. Siis iga $i \in I$ korral leidub homomorfism $g_i : P_i \rightarrow A_S$ nii, et diagramm

$$\begin{array}{ccc} & P_i & \\ g_i \swarrow & & \searrow f|_{P_i} \\ A_S & \xrightarrow{\pi} & B_S \end{array}$$

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

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

kus $x \in P_i$ (iga $x \in P$ kuulub täpselt ühte alampolügooni P_i). Siis iga $i \in I$ ja iga $x \in P_i$ korral

$$\pi(g(x)) = \pi(g_i(x)) = f|_{P_i}(x) = f(x)$$

ehk diagramm

$$\begin{array}{ccc} & P_S & \\ g \swarrow & & \searrow f \\ A_S & \xrightarrow{\pi} & B_S \end{array}$$

on kommutatiivne. Kuna kujutused g_i , $i \in I$, on homomorfismid, siis ka g on homomorfism. $\square$

Märgime, et kui $e \in E(S)$ on idempotent, siis $eS = \{es \mid s \in S\}$ on polügoni S_S alampolügon (vt. näidet 8.7) ja seega ise ka parempoolne S -polügon. Tuleb välja, et mittetühjad projektiivsed S -polügonid unitaarsete polügonide kategoorias on parajasti seda tüüpi polügonide lõikumatud ühendid.

Järgnevad kaks teoreemi on pärit artiklist [5] (teoreem 1 ja teoreem 2).

Teoreem 8.18 *Olgu S faktoriseeruv poolrühm. Polügon P_S on lahutumatu ja projektiivne objekt kategoorias $\mathbf{UAct}_S$ parajasti siis, kui $P_S \cong eS$, kus $e \in E(S)$.*

TÕESTUS. TARVILIKKUS. Olgu P_S lahutumatu ja projektiivne objekt kategoorias $\mathbf{UAct}_S$. Unitarsuse tõttu saame iga elemendi $p \in P$ esitada kujul $p = q_p s_p$, kus $q_p \in P$ ja $s_p \in S$. Vaatleme polügoni $(P \times S)_S$ toimega

$$(p, s)s' := (p, ss').$$

See polügon on unitaarne, sest kui $(p, s) \in P \times S$, siis S faktoriseeruvuse tõttu leiduvad $s_1, s_2 \in S$ nii, et $s = s_1 s_2$ ja seega $(p, s) = (p, s_1 s_2) = (p, s_1)s_2$. (See polügon on tegelikult kokorutis $\coprod_{p \in P} S_S$ kategoorias $\mathbf{UAct}_S$.) Defineerime kujutuse $f : (P \times S)_S \rightarrow P_S$ võrdusega

$$f(p, s) := q_p s.$$

Lihtne on näha, et f on parempoolsete polügonide homomorfism. Kuna $p = q_p s_p = f(p, s_p)$, siis f on surjektiivne. Projektiivsuse tõttu leidub homomorfism $g : P_S \rightarrow (P \times S)_S$ nii, et diagramm

$$\begin{array}{ccc} & P_S & \\ g \swarrow & & \searrow \text{id}_P \\ (P \times S)_S & \xrightarrow{f} & P_S \end{array}$$

kommuteerub, s.t. $f \circ g = \text{id}_{P_S}$. Järelikult g on injektiivne ja seega $g(P_S) \cong P_S$ on lahutumatu. Kuna $(P \times S)_S = \bigsqcup_{p \in P} \{p\} \times S$, kus iga $\{p\} \times S$ on mittetühi alampolügon, siis leidub üheselt määratud $p_0 \in P$ nii, et $g(P_S) \subseteq \{p_0\} \times S$. Järelikult

$$P = \text{id}_P(P_S) = (f \circ g)(P_S) \subseteq f(\{p_0\} \times S) \subseteq P$$

ehk $P = f(\{p_0\} \times S) = q_{p_0}S$. Tähistades $q := q_{p_0}$ võime vaadelda sürjektiivset homomorfismi

$$h : S_S \longrightarrow P_S = qS, \quad s \mapsto qs,$$

kategoorias $\mathbf{UAct}_S$. Projektiivsuse tõttu leidub homomorfism $k : P_S \longrightarrow S_S$ nii, et diagramm

$$\begin{array}{ccc} & P_S & \\ \swarrow k & \downarrow \text{id}_P & \\ S_S & \xrightarrow{h} & P_S \end{array}$$

kommuteerub, s.t. $h \circ k = \text{id}_P$. Tähistame $e := k(q) \in S$. Kuna

$$q = \text{id}_P(q) = (h \circ k)(q) = h(e) = qe,$$

siis

$$e = k(q) = k(qe) = k(q)e = e^2.$$

Kuna k on injektiivne, siis

$$P_S \cong k(P_S) = k(qS) = k(q)S = eS.$$

PIISAVUS. Tänu näitele 8.12 on tsükliline polügoon $P_S = eS = eS^1$, kus $e \in S$ on idempotent, lahutumatu. Ta on ka unitaarne, sest $es = e(es)$ iga $s \in S$ korral. Näitame, et eS on projektiivne. Selleks vaatleme unitaarseid polügone A_S, B_S , homomorfismi $f : eS \rightarrow B_S$ ja sürjektiivset homomorfismi $\pi : A_S \rightarrow B_S$. Olgu $b := f(e) \in B$. Sürjektiivsuse tõttu saame valida $a \in A$ nii, et $\pi(a) = b$. Defineerime kujutuse $g : eS \rightarrow A$ võrdusega

$$g(es) := aes.$$

$$\begin{array}{ccc} & eS & \\ \swarrow g & \downarrow f & \\ A_S & \xrightarrow{\pi} & B_S \end{array}$$

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 $\pi \circ g = f$. □

Teoreem 8.19 *Olgu S faktoriseeruv poolrühm. Mittetühi polügon P_S on projektiivne objekt kategoorias $\mathbf{UAct}_S$ 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. Eeldame, et $P_S \in \mathbf{UAct}_S$ on projektiivne. Tänu lausele 8.14 saame P_S esitada kujul

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

kus iga P_i on mittetühi lahutumatu alampolügon. On lihtne aru saada, et siis ka iga P_i on unitaarne. Lause 8.17 tõttu on iga alampolügon P_i projektiivne kategoorias $\mathbf{UAct}_S$. Teoreemi 8.18 põhjal leidub iga $i \in I$ korral idempotent $e_i \in S$ nii, et $P_i \cong e_i S$.

PIISAVUS. Eeldame, et $P = \bigsqcup_{i \in I} P_i$, kus $P_i \cong e_i S$ ja $e_i \in S$ on idempotent iga $i \in I$ korral. Teoreemi 8.18 tõttu on iga P_i projektiivne ja lause 8.17 põhjal on P_S projektiivne. $\square$

8.4 Polügonide tensorkorrutis

Sarnaselt moodulite juhuga on võimalik moodustada polügonide tensorkorrutis. Juhul kui S on monoid vaatles unitaarsete polügonide tensorkorrutist esimesena Tartu Ülikooli emeriitprofessor Mati Kilp artiklis [7].

Konstruksioon 8.20 Parempoolse polügoni A_S ja vasakpoolse polügoni ${}_S B$ **tensor-korrutis** on faktorhulk

$$(A \times B) / \rho(H) =: A \otimes B,$$

kus $\rho(H)$ on vähim ekvivalentsiseos, mis sisaldab hulka

$$H = \{((as, b), (a, sb)) \mid a \in A, b \in B, s \in S\}.$$

Paari (a, b) $\rho(H)$ -klassi tähistatakse $a \otimes b$. Seega kehtib tensorkorrutises arvutusreegel

$$as \otimes b = a \otimes sb.$$

Kanoonilist kujutust

$$A \times B \longrightarrow A \otimes_S B, \quad (a, b) \mapsto a \otimes b,$$

tähistatakse $- \otimes -$.

Definitsioon 8.21 Olgu A_S ja ${}_S B$ polügonid. Öeldakse, et kujutus $f : A \times B \longrightarrow C$ on **S -tasakaalustatud**, kui

$$f(as, b) = f(a, sb)$$

iga $a \in A$, $b \in B$ ja $s \in S$ korral.

Tensorkorrutisel on järgmine universaalomadus.

Lause 8.22 (Tensorkorrutise universaalomadus) Olgu A_S ja ${}_S B$ polügonid üle poolrühma S ja olgu C hulk. Iga S -tasakaalustatud kujutuse $\hat{f} : A \times B \longrightarrow C$ korral leidub üheselt määratud kujutus $f : A \otimes_S B \longrightarrow C$ nii, et diagramm

$$\begin{array}{ccc}
 A \times B & \xrightarrow{- \otimes -} & A \otimes_S B \\
 & \searrow \hat{f} & \downarrow f \\
 & & C
 \end{array}$$

kommuteerub, s.t.

$$f(a \otimes b) = \hat{f}(a, b)$$

iga $a \in A$ ja $b \in B$ korral.

TÕESTUS. Kui $\hat{f}$ on S -tasakaalustatud, siis $H \subseteq \ker(\hat{f})$. Kuna $\ker \hat{f}$ on ekvivalentsiseos hulgal $A \times B$, siis $\rho(H) \subseteq \ker(f)$. Teiste sõnadega:

$$a \otimes b = a' \otimes b' \implies \hat{f}(a, b) = \hat{f}(a', b').$$

Seetõttu saame defineerides

$$f(a \otimes b) := \hat{f}(a, b)$$

kujutuse $f : A \otimes_S B \longrightarrow C$

□

See lause on väga kasulik selleks, et defineerida kujutusi tensorkorrutistel. Näiteks läheb seda vaja järgmise tulemuse tõestamisel.

Lause 8.23 Olgu R, S, T poolrühmad. Tensorkorrutis $A \otimes_S B$ on

1. parempoolne T -polügon toimega

$$(a \otimes b)t := a \otimes bt,$$

kui $A_S \in \text{Act}_S$ ja ${}_S B_T \in {}_S \text{Act}_T$;

2. vasakpoolne R -polügon toimega

$$r(a \otimes b) := ra \otimes b,$$

kui ${}_R A_S \in {}_R \text{Act}_S$ ja ${}_S B \in {}_S \text{Act}$;

3. (R, T) -bipolügon eespool defineeritud toimetega, kui ${}_R A_S \in {}_R \text{Act}_S$ ja ${}_S B_T \in {}_S \text{Act}_T$.

TÕESTUS. Tõestame ainult esimese väite, teised on analoogilised. Iga $t \in T$ korral on kujutus

$$\hat{f}_t : A \times B \longrightarrow A \otimes_S B, \quad (a, b) \mapsto a \otimes bt$$

S -tasakaalustatud, sest $\hat{f}_t(as, b) = as \otimes bt = a \otimes s(bt) = a \otimes (sb)t = \hat{f}_t(a, sb)$. Lause 8.22 põhjal leidub kujutus

$$f_t : A \otimes_S B \longrightarrow A \otimes_S B, \quad a \otimes b \mapsto a \otimes bt.$$

Järelikult on olemas ka selline kujutus

$$f : (A \otimes_S B) \times T \longrightarrow A \otimes_S B, \quad (a \otimes b, t) \mapsto f_t(a \otimes b) = a \otimes bt =: (a \otimes b)t,$$

et

$$((a \otimes b)t)t' = (a \otimes bt)t' = a \otimes (bt)t' = a \otimes b(tt') = (a \otimes b)(tt')$$

iga $t, t' \in T$ korral. Seega $A \otimes_S B$ on parempoolne T -polügon.

□

Teoreem 8.24 (Tensorkorrutise assotsiatiivsus) Kui S ja T on poolrühmad, $A_S \in \text{Act}_S$, ${}_S B_T \in {}_S \text{Act}_T$ ja ${}_T C \in {}_T \text{Act}$, siis leidub bijektsioon

$$\alpha_{A,B,C}: (A \otimes_S B) \otimes_T C \longrightarrow A \otimes_S (B \otimes_T C) \quad (a \otimes b) \otimes c \mapsto a \otimes (b \otimes c).$$

Kui ${}_R A_S \in {}_R \text{Act}_S$, siis α on vasakpoolsete R -polügonide isomorfism.

Kui ${}_T C_U \in {}_T \text{Act}_U$, siis α on parempoolsete U -polügonide isomorfism.

Näitame nüüd, kuidas konstrueerida tensorfunktoreid. Järgmises paragrahvis kasutame neid poolrühmade Morita ekvivalentsuse uurimisel.

Lemma 8.25 Iga bipolügoni ${}_S P_T$ ja mistahes parempoolsete S -polügonide homomorfismi $f: A_S \longrightarrow B_S$ korral leidub parempoolsete T -polügonide homomorfism

$$f \otimes \text{id}_P: (A \otimes_S P)_T \longrightarrow (B \otimes_S P)_T, \quad a \otimes p \mapsto f(a) \otimes p.$$

TÕESTUS. Kujutus

$$\beta: A \times P \longrightarrow B \otimes_S P, \quad (a, p) \mapsto f(a) \otimes p,$$

on S -tasakaalsutatud, sest

$$\beta(as, p) = f(as) \otimes p = f(a)s \otimes p = f(a) \otimes sp = \beta(a, sp)$$

iga $a \in A$, $s \in S$ ja $p \in P$ korral. Seega leidub kujutus $f \otimes \text{id}_P: A \otimes_S P \longrightarrow B \otimes_S P$ nii, et

$$(f \otimes \text{id}_P)(a \otimes p) = \beta(a, p) = f(a) \otimes p.$$

See kujutus on parempoolsete T -polügonide homomorfism, sest

$$(f \otimes \text{id}_P)((a \otimes p)t) = (f \otimes \text{id}_P)(a \otimes pt) = f(a) \otimes pt = (f(a) \otimes p)t = ((f \otimes \text{id}_P)(a \otimes p))t.$$

□

Lause 8.26 Iga bipolügoni ${}_S P_T$ korral defineerib eeskiri

$$\begin{array}{ccc} A_S & \xrightarrow{\quad} & (A \otimes_S P)_T \\ f \downarrow & & \downarrow f \otimes \text{id}_P \\ B_S & \xrightarrow{\quad} & (B \otimes_S P)_T \end{array}$$

funktori $- \otimes_S P_T: \text{Act}_S \longrightarrow \text{Act}_T$.

TÕESTUS. Olgu $f: A_S \longrightarrow B_S$ ja $g: B_S \longrightarrow C_S$ parempoolsete S -polügonide homomorfismid. Siis iga $a \in A$ ja $p \in P$ korral

$$\begin{aligned} ((g \circ f) \otimes \text{id}_P)(a \otimes p) &= g(f(a)) \otimes p = (g \otimes \text{id}_P)(f(a) \otimes p) \\ &= ((g \otimes \text{id}_P) \circ (f \otimes \text{id}_P))(a \otimes p) \end{aligned}$$

ning seega $(- \otimes_S P_T)(g \circ f) = (- \otimes_S P_T)(g) \circ (- \otimes_S P_T)(f)$. Kuna $(\text{id}_A \otimes \text{id}_P)(a \otimes p) = a \otimes p$ iga $a \in A$ ja $p \in P$ korral, siis $(- \otimes_S P_T)(\text{id}_A) = \text{id}_{(- \otimes_S P_T)(A)}$. Seega $- \otimes_S P_T$ on funktor.

□

8.5 Poolrühmade Morita teooria

Poolrühma Morita ekvivalentsuse seos defineeritakse püsivate polügonide kategooriate abil. Püsivuse defineerimiseks vajame järgmist tulemust.

Lause 8.27 Iga poolrühma S korral leidub funktor $- \otimes_S S : \text{Act}_S \longrightarrow \text{Act}_S$ ja loomulik teisendus $\mu = (\mu_A)_{A \in \text{Act}_S} : - \otimes_S S \Rightarrow \text{id}_{\text{Act}_S}$, kus

$$\mu_A : A \otimes_S S \longrightarrow A, \quad a \otimes s \mapsto as.$$

TÕESTUS. Olgu A_S parempoolne S -polügoon. Kujutus

$$\widehat{\mu}_A : A \times S \longrightarrow A, \quad (a, s) \mapsto as,$$

on S -tasakaalustatud, sest $\widehat{\mu}_A(as', s) = (as')s = a(s's) = \widehat{\mu}_A(a, s's)$ iga $a \in A$ ja $s, s' \in S$ korral. Lause 8.22 põhjal leidub kujutus $\mu_A : A \otimes_S S \longrightarrow A$ nii, et

$$\mu_A(a \otimes s) = as$$

iga $a \in A$ ja $s \in S$ korral. See kujutus on ka parempoolsete S -polügonide homomorfism, sest $\mu_A((a \otimes s)s') = \mu_A(a \otimes ss') = a(ss') = (as)s' = \mu_A(a \otimes s)s'$. Mistahes homomorfismi $f : A_S \longrightarrow B_S$ korral ruut

$$\begin{array}{ccc} A \otimes_S S & \xrightarrow{\mu_A} & A \\ f \otimes \text{id}_S \downarrow & & \downarrow f \\ B \otimes_S S & \xrightarrow{\mu_B} & B \end{array}$$

kommuteerub, sest kui $a \in A$ ja $s \in S$, siis

$$(\mu_B \circ (f \otimes \text{id}_S))(a \otimes s) = \mu_B(f(a) \otimes s) = f(a)s = f(as) = (f \circ \mu_A)(a \otimes s).$$

Järelikult μ on loomulik teisendus. □

Definitsioon 8.28 Polügoni A_S nimetatakse **püsivaks** (ingl. k. *firm*), kui kujutus $\mu_A : A \otimes S \longrightarrow A$ on bijektiivne.

Paneme tähele, et $AS = A$ parajasti siis, kui μ_A on sürjektiivne. Seega iga püsiv polügon on unitaarne. Vastupidine ei kehti. Kategooria Act_S täielikku alamkategooriat, mille tekitavad püsivad polügonid, tähistatakse $\mathbf{Fact}_S$. Seega iga poolrühma S korral

$$\mathbf{Fact}_S \subseteq \mathbf{UAct}_S \subseteq \text{Act}_S.$$

Lause 8.29 Iga unitaarne polügon üle monoidi on püsiv.

TÕESTUS. Olgu A_S unitaarne polügon üle monoidi S . Näitame, et kujutus

$$\mu_A : A \otimes_S S \longrightarrow A, \quad a \otimes s \mapsto as,$$

on injektiivne. Tõepoolest, kui $as = a's'$, siis tensorkorrutises $A \otimes_S S$ kehtib

$$a \otimes s = a \otimes s1_S = as \otimes 1_S = a's' \otimes 1_S = a' \otimes s'1_S = a' \otimes s'.$$

□

Tuleb välja, et püsiva polügoniga tensorkorrutamine annab püsiva polügoni.

Lemma 8.30 *Kui $A_S \in \text{Act}_S$ ja ${}_S P_T$ on bipolügon, kusjuures P_T on püsiv, siis ka polügon $(A \otimes_S P)_T$ on püsiv.*

TÕESTUS. Kolmnurk

$$\begin{array}{ccc} (A \otimes_S P) \otimes_T T & \xrightarrow{\alpha_{A,P,T}} & A \otimes_S (P \otimes_T T) \\ & \searrow \mu_{A \otimes P} & \downarrow \text{id}_A \otimes \mu_P \\ & & A \otimes_S P \end{array}$$

kommuteerub, sest iga $a \in A$, $p \in P$ ja $t \in T$ korral

$$\begin{aligned} ((\text{id}_A \otimes \mu_P) \circ \alpha_{A,P,T})((a \otimes p) \otimes t) &= (\text{id}_A \otimes \mu_P)(a \otimes (p \otimes t)) = a \otimes pt = (a \otimes p)t \\ &= \mu_{A \otimes P}((a \otimes p) \otimes t). \end{aligned}$$

Siin $\alpha_{A,P,T}$ on bijektiivne tänu teoreemile 8.24 ja $\text{id}_A \otimes \mu_P$ on bijektiivne tänu sellele, et ta on saadud isomorfismist $\mu_P : {}_S(P \otimes_T T)_T \longrightarrow {}_S P_T$ funktori $A \otimes_S - : {}_S \text{Act}_T \longrightarrow \text{Act}_T$ rakendamisel (vt. lauset 1.39). Järelikult ka $\mu_{A \otimes P}$ on bijektiivne, mis tähendab, et polügon $(A \otimes_S P)_T$ on püsiv. □

Definitsioon 8.31 Öeldakse, et poolrühmad S ja T on **Morita ekvivalentsed**, kui kategooriad FAct_S ja FAct_T on ekvivalentsed (vt. definitsiooni 1.42).

Kuna kategooriate ekvivalentsuse seos on refleksiivne, sümmeetriline ja transitiivne, siis on samad omadused ka Morita ekvivalentsuse seosel kõigi poolrühmade klassil. Isomorfseid poolrühmad on Morita ekvivalentsed, kuid vastupidine ei kehti.

Definitsioon 8.32 **Morita kontekst** on kuuk $(S, T, {}_S P_T, {}_T Q_S, \theta, \phi)$, kus

- S ja T on poolrühmad,
- ${}_S P_T$ ja ${}_T Q_S$ on bipolügonid,

- kujutused

$$\theta : {}_S(P \otimes_T Q)_S \longrightarrow {}_S S_S, \quad \phi : {}_T(Q \otimes_S P)_T \longrightarrow {}_T T_T$$

on sellised bipolügonide homomorfismid, mis rahuldavad kooskõla tingimusi: iga $p, p' \in P$ ja $q, q' \in Q$ korral

$$\theta(p \otimes q)p' = p\phi(q \otimes p'), \quad q\theta(p \otimes q') = \phi(q \otimes p)q'.$$

Järgnev teoreem näitab teataval määral, kuidas Morita kontekstid on seotud Morita ekvivalentsusega.

Teoreem 8.33 *Olgu $(S, T, {}_S P_T, {}_T Q_S, \theta, \phi)$ Morita kontekst, kus S ja T on poolrühmad, ${}_S P_T$ ja ${}_T Q_S$ on püsivad polügonid ning θ ja ϕ on bijektiivsed bipolügonide homomorfismid. Siis S ja T on Morita ekvivalentsed.*

TÕESTUS. Vaatleme funktoreid

$$- \otimes_S P_T : \mathbf{Act}_S \longrightarrow \mathbf{Act}_T, \quad - \otimes_T Q_S : \mathbf{Act}_T \longrightarrow \mathbf{Act}_S.$$

Lemma 8.30 tõttu viivad need funktorid püsivad polügonid püsivateks, seega võime neid ahendada kategooriatele $\mathbf{Fact}_S$ ja $\mathbf{Fact}_T$:

$$- \otimes_S P_T : \mathbf{Fact}_S \longrightarrow \mathbf{Fact}_T, \quad - \otimes_T Q_S : \mathbf{Fact}_T \longrightarrow \mathbf{Fact}_S.$$

Vaatleme funktorit $F := (- \otimes_T Q_S) \circ (- \otimes_S P_T) : \mathbf{Fact}_S \longrightarrow \mathbf{Fact}_S$, mis on antud eeskirjaga

$$\begin{array}{ccc} A_S & \longmapsto & (A \otimes_S P) \otimes_T Q \\ f \downarrow & & \downarrow (f \otimes \text{id}_P) \otimes \text{id}_Q \\ B_S & \longmapsto & (B \otimes_S P) \otimes_T Q. \end{array}$$

Näitame, et F on loomulikult isomorfne kategooria $\mathbf{Fact}_S$ ühikfunktoriga. Iga $A_S \in \mathbf{Fact}_S$ korral vaatleme kompositsiooni

$$\gamma_A : (A \otimes_S P) \otimes_T Q \xrightarrow{\alpha_{A,P,Q}} A \otimes_S (P \otimes_T Q) \xrightarrow{\text{id}_A \otimes \theta} A \otimes_S S \xrightarrow{\mu_A} A,$$

kus

$$\gamma_A((a \otimes p) \otimes q) = a\theta(p \otimes q).$$

Siin kõik kolm komponeeritavat kujutust on parempoolsed S -homomorfismid ja

- $\alpha_{A,P,Q}$ on bijektiivne tänu teoreemile 8.24,
- $\text{id}_A \otimes \theta$ on bijektiivne tänu sellele, et ta on saadud funktori $A \otimes_S - : {}_S \mathbf{Act}_S \longrightarrow \mathbf{Act}_S$ rakendamisel isomorfismile $\theta : {}_S(P \otimes_T Q)_S \longrightarrow {}_S S_S$,
- μ_A on bijektiivne selle tõttu, et A_S on püsiv,

seega γ_A on parempoolsete S -polügonide isomorfism. Kategooria $\mathbf{Fact}_S$ iga morfismi $f : A_S \longrightarrow B_S$ korral ruut

$$\begin{array}{ccc} (A \otimes_S P) \otimes_T Q & \xrightarrow{\gamma_A} & A_S \\ (f \otimes \text{id}_P) \otimes \text{id}_Q \downarrow & & \downarrow f \\ (B \otimes_S P) \otimes_T Q & \xrightarrow{\gamma_B} & B_S \end{array}$$

kommuteerub, sest

$$\begin{aligned} (\gamma_B \circ (f \otimes \text{id}_P) \otimes \text{id}_Q)((a \otimes p) \otimes q) &= \gamma_B((f(a) \otimes p) \otimes q) = f(a)\theta(p \otimes q) \\ &= f(a\theta(p \otimes q)) = (f \circ \gamma_A)((a \otimes p) \otimes q). \end{aligned}$$

Seega $\gamma : F \Rightarrow \text{id}_{\mathbf{Fact}_S}$ on loomulik isomorfism. Analooiliselt saab näidata, et funktor $G := (- \otimes_S P_T) \circ (- \otimes_T Q_S) : \mathbf{Fact}_T \longrightarrow \mathbf{Fact}_T$ on loomulikult isomorfne kategooria $\mathbf{Fact}_T$ ühikfunktoriga. $\square$

Saab tõestada järgmise teoreemi.

Teoreem 8.34 ([6, teoreem 4.11]) *Faktoriseeruvad poolrühmad S ja T on Morita ekvivalentsed parajasti siis, kui leidub Morita kontekst $(S, T, {}_S P_T, {}_T Q_S, \theta, \phi)$, kus ${}_S P_T$ ja ${}_T Q_S$ on püsivad polügonid ning θ ja ϕ on sürjektiivsed bipolügonide homomorfismid.*

Definitsioon 8.35 Öeldakse, et poolrühmas S leiduvad **nõrgad lokaalsed ühikelemendid**, kui iga $s \in S$ jaoks leiduvad $u, v \in S$ nii, et $s = us$ ja $s = sv$.

On selge, et igas monoidis leiduvad nõrgad lokaalsed ühikelemendid ja et kui poolrühmas on nõrgad lokaalsed ühikelemendid, siis on ta faktoriseeruv.

Tihti on Morita ekvivalentsetel poolrühmadel sarnased omadused. Morita kontekstid annavad mugava võimaluse seda tüüpi tulemuste tõestamiseks. Näitena vaatleme järgmist lauset.

Lause 8.36 *Olgu S ja T nõrkade lokaalsete ühikelementidega poolrühmad. Kui S ja T on Morita ekvivalentsed ja S on regulaarne, siis ka T on regulaarne. (Teiste sõnadega: regulaarsus on Morita invariant nõrkade lokaalsete ühikelementidega poolrühmade jaoks.)*

TÕESTUS. Teoreemi 8.34 tõttu leidub Morita kontekst $(S, T, {}_S P_T, {}_T Q_S, \theta, \phi)$, kus ${}_S P_T$ ja ${}_T Q_S$ on püsivad polügonid ning θ ja ϕ on sürjektiivsed bipolügonide homomorfismid. Vaatleme elementi $t \in T$. Siis leiduvad $u, v \in T$ nii, et $t = ut = tv$. Kuna ϕ on sürjektiivne, siis leiduvad $q_u, q_v \in Q$ ja $p_u, p_v \in P$ nii, et $u = \phi(q_u \otimes p_u)$ ja $v = \phi(q_v \otimes p_v)$. Et $\theta(p_u t \otimes q_v) \in S$ ja S on regulaarne, siis leidub $s \in S$ nii, et

$$\theta(p_u t \otimes q_v) = \theta(p_u t \otimes q_v) s \theta(p_u t \otimes q_v).$$

Nüüd

$$\begin{aligned}
t &= utv = \phi(q_u \otimes p_u) t \phi(q_v \otimes p_v) \\
&= \phi(q_u \otimes p_u t \phi(q_v \otimes p_v)) && (\phi \text{ on parempoolne } T\text{-homomorfism}) \\
&= \phi(q_u \otimes \theta(p_u t \otimes q_v) p_v) && (\theta \text{ ja } \phi \text{ kooskõla}) \\
&= \phi(q_u \otimes \theta(p_u t \otimes q_v) s \theta(p_u t \otimes q_v) p_v) && (S \text{ on regulaarne}) \\
&= \phi(q_u \otimes \theta(p_u \otimes t q_v s) \theta(p_u t \otimes q_v) p_v) && (\theta \text{ on parempoolne } S\text{-homomorfism}) \\
&= \phi(q_u \otimes p_u \phi(t q_v s \otimes p_u t) \phi(q_v \otimes p_v)) && (\theta \text{ ja } \phi \text{ kooskõla}) \\
&= \phi(q_u \otimes p_u) \phi(t q_v s \otimes p_u t) \phi(q_v \otimes p_v) && (\phi \text{ on parempoolne } T\text{-homomorfism}) \\
&= \phi(q_u \otimes p_u) t \phi(q_v s \otimes p_u) t \phi(q_v \otimes p_v) && (\phi \text{ on bipolügonide homomorfism}) \\
&= ut \phi(q_v s \otimes p_u) tv \\
&= t \phi(q_v s \otimes p_u) t.
\end{aligned}$$

Seega T on regulaarne. □

Definitsioon 8.37 Öeldakse, et poolrühm S on oma alampoolrühma T **laiend** (ingl. k. *enlargement*), kui $S = STS$ ja $T = TST$, kus $STS = \{sts' \mid s, s' \in S, t \in T\}$ ja $TST = \{tst' \mid t, t' \in T, s \in S\}$. Kui poolrühm U on isomorfne poolrühmaga T , siis öeldakse, et S on ka U laiend.

Poolrühmade laiendeid uuris esimesena briti matemaatik Mark Lawson artiklis [8]. Iga poolrühmade laiend tekitab loomulikult viisil Morita konteksti.

Lause 8.38 Olgu S oma alampoolrühma T laiend, kusjuures S ja T on faktoriseeruvad poolrühmad. Siis kuuik $(S, T, {}_S ST_T, {}_T TS_S, \theta, \phi)$, kus

$$\begin{aligned}
\theta : ST \otimes_T TS &\longrightarrow S, \quad st \otimes t's' \mapsto stt's' \in STTS = S, \\
\phi : TS \otimes_S ST &\longrightarrow T, \quad ts \otimes s't' \mapsto tss't' \in TSST = T,
\end{aligned}$$

on unitaarsete bipolügonide ja sürjetkiivsete kujutustega Morita kontekst.

TÕESTUS. Me vaatleme hulki $ST = \{st \mid s \in S, t \in T\}$ ja $TS = \{ts \mid t \in T, s \in S\}$ bipolügonidena loomulike toimete

$$s'(st) = (s's)t, \quad (st)t' = s(tt'), \quad t'(ts) = (t't)s, \quad (ts)s' = t(ss')$$

suhtes. Lause 8.22 abil saab veenduda, et θ ja ϕ on korrektselt defineeritud. Vahetu kontroll näitab, et nad on bipolügonide homomorfismid. Kooskõla tingimused θ ja ϕ jaoks järelduvad korrutamise assotsiatiivsusest poolrühmas S . Faktoriseeruvusest järeldub, et bipolügonid ST ja TS on unitaarsed. Kuna $S = STS = STTS$ ja $T = TST = TSST$, siis θ ja ϕ on sürjetkiivsed. □

Järgmine lause annab ühe võimaluse rühma laiendi konstrueerimiseks.

Lause 8.39 Reesi maatrikspoolrühm $\mathcal{M} = \mathcal{M}[G; I, \Lambda; P]$ on rühma G laiend.

TÕESTUS. Fikseerime mingid elemendid $j \in I$ ja $\mu \in \Lambda$. Hulk

$$T = \{(j, g, \mu) \mid g \in G\} \subseteq \mathcal{M}$$

on poolrühma $\mathcal{M}$ alampoolrühm. Kujutus

$$f : G \longrightarrow T, \quad g \mapsto (j, gp_{\mu,j}^{-1}, \mu),$$

on surjektiivne. Ta on injektiivne, sest

$$f(g) = f(g') \implies gp_{\mu,j}^{-1} = g'p_{\mu,j}^{-1} \implies g = g'.$$

Kujutus f on ka poolrühmade homomorfism, sest

$$f(g)f(g') = (j, gp_{\mu,j}^{-1}, \mu)(j, g'p_{\mu,j}^{-1}, \mu) = (j, gp_{\mu,j}^{-1}p_{\mu,j}g'p_{\mu,j}^{-1}, \mu) = (j, gg'p_{\mu,j}^{-1}, \mu) = f(gg').$$

Seega f on poolrühmade isomorfism ja $G \cong T$. Näitame, et $\mathcal{M}$ on T laiend.

Veendume, et $\mathcal{M} = \mathcal{MTM}$. Sisalduvus $\mathcal{MTM} \subseteq \mathcal{M}$ on ilmne. Olgu $(i, g, \lambda) \in \mathcal{M}$. Siis

$$(i, g, \lambda) = (i, p_{\lambda,j}^{-1}, \lambda)(j, g, \mu)(i, p_{\mu,i}^{-1}, \lambda) \in \mathcal{MTM}.$$

Seega $\mathcal{M} \subseteq \mathcal{MTM}$.

Kuna $T \cong G$ on rühm, siis $T = TTT \subseteq T\mathcal{MT}$. Ka sisalduvus $T\mathcal{MT} \subseteq T$ kehtib, sest

$$(j, g, \mu)(i, h, \lambda)(j, g', \mu) = (j, gp_{\mu,i}hp_{\lambda,j}g', \mu) \in T.$$

Järelikult $T = T\mathcal{MT}$. □

Teoreem 8.40 *Kui G on rühm, siis on ta Morita ekvivalentne iga Reesi maatrikspoolrühmaga $\mathcal{M} = \mathcal{M}[G; I, \Lambda; P]$.*

TÕESTUS. Olgu $\mathcal{M}$ alampoolrühm T konstrueeritud samamoodi nagu lause 8.39 tõestuses. Siis $\mathcal{M}$ on T laiend. Lause 8.38 põhjal leidub Morita kontekst $(\mathcal{M}, T, \mathcal{MT}, T\mathcal{M}, \theta, \phi)$, kus θ ja ϕ on surjektiivsed ja bipolügonid $\mathcal{MT}, T\mathcal{M}$ on unitaarsed. Teoreemi 8.34 tõttu piisab näidata, et need bipolügonid on püsivad. Sümmeetria tõttu teeme seda ainult $T\mathcal{M}$ jaoks. Kuna T on rühm, siis lausest 8.29 järeldub, et vasakpoolne polügon ${}_T T\mathcal{M}$ on püsiv. Jääb veel näidata, et kujutus

$$\mu_{T\mathcal{M}} : T\mathcal{M} \otimes_{\mathcal{M}} \mathcal{M} \longrightarrow T\mathcal{M}, \quad x \otimes m \mapsto xm,$$

on injektiivne. Paneme tähele, et

$$\begin{aligned} T\mathcal{M} &= \{(j, g, \mu)(i, g', \lambda) \mid g, g' \in G, i \in I, \lambda \in \Lambda\} \\ &= \{(j, gp_{\mu,i}g', \lambda) \mid g, g' \in G, i \in I, \lambda \in \Lambda\} \\ &= \{(j, h, \lambda) \mid h \in G, \lambda \in \Lambda\}. \end{aligned}$$

Olgu $x = (j, h, \lambda), x' = (j, h', \lambda') \in T\mathcal{M}$ ja $m = (i, g, \nu), m' = (i', g', \nu') \in \mathcal{M}$ sellised, et $xm = x'm'$, s.t.

$$(j, hp_{\lambda,i}g, \nu) = (j, h'p_{\lambda',i'}g', \nu') \quad \text{ehk} \quad hp_{\lambda,i}g = h'p_{\lambda',i'}g', \quad \nu = \nu'.$$

Nüüd

$$m = (i, g, \nu) = (i, g(g')^{-1}p_{\lambda' i'}^{-1}, \lambda') (i', g', \nu) = (i, g(g')^{-1}p_{\lambda' i'}^{-1}, \lambda') m',$$

seega tensorkorrutises $T\mathcal{M} \otimes_{\mathcal{M}} \mathcal{M}$ kehtib

$$\begin{aligned} x \otimes m &= (j, h, \lambda) (i, g(g')^{-1}p_{\lambda' i'}^{-1}, \lambda') \otimes m \\ &= (j, hp_{\lambda i}g(g')^{-1}p_{\lambda' i'}^{-1}, \lambda') \otimes m' \\ &= (j, h'p_{\lambda' i'}g'(g')^{-1}p_{\lambda' i'}^{-1}, \lambda') \otimes m' \\ &= (j, h', \lambda') \otimes m' \\ &= x' \otimes m'. \end{aligned}$$

Sellega ongi näidatud, et kujutus $\mu_{T\mathcal{M}}$ on injektiivne.

□

Peatükk 9

Korpused

Selles peatükis tuleb juttu korpuse karakteristikast, korpuste laienditest ja lihtsatest korpustest. Põhieesmärk on tutvuda lõplike korpuste teooria algetega. Kõige lihtsamaks näiteks lõplikest korpustest on jäägiklassikorpused $\mathbb{Z}_p$, kuid osutub, et on ka teisi lõplikke korpusi. Lõplikud korpused on väga olulised tööriistad teoreetilises informaatikas, eelkõige kodeerimisteoorias ja krüptograafias. Samuti on neil tihedad seosed arvuteooria ja lineaaralgebraga (muuhulgas polünoomidega).

9.1 Korpuse karakteristik

Definitsioon 9.1 Korpus on kommutatiivne ring, mille nullist erinevad elemendid moodustavad korrutamise suhtes rühma.

Korpuse K ühikelementi tähistame $\mathbf{1}$ ja nullelementi $\mathbf{0}$. Me tähistame ka $K^* := K \setminus \{\mathbf{0}\}$ ja ütleme, et $(K^*, \cdot)$ on korpuse K **multiplikatiivne rühm**.

Tuletame meelde, et iga Abeli rühma on võimalik vaadelda $\mathbb{Z}$ -moodulina (vt. paragrahvi 3.1). Muuhulgas ka korpuse aditiivne rühm $(K, +)$ on $\mathbb{Z}$ -moodul, kui defineerida mistahes naturaalarvu m ja elemendi $a \in K$ korral

$$ma = \underbrace{a + a + \dots + a}_m \text{ liidetavat}$$

$0a = \mathbf{0}$ ning $(-m)a = -(ma)$. Lihtne on kontrollida, et lisaks mooduli omadustele kehtivad

- $(\forall m \in \mathbb{Z})(\forall a, b \in K)(m(ab) = (ma)b)$;
- $(\forall m, k \in \mathbb{Z})(\forall a, b \in K)((ma)(kb) = (mk)(ab))$.

Korpuse K korral on kaks võimalust.

1. Ühikelement $\mathbf{1} \in K$ on lõpmatut järku aditiivses rühmas $(K, +)$. Siis öeldakse, et korpuse K **karakteristika on** 0. Sellised korpused on näiteks $\mathbb{Q}, \mathbb{R}$ ja $\mathbb{C}$.

2. Ühikelemendi $\mathbf{1} \in K$ järk aditiivses rühmas $(K, +)$ on lõplik, s.t. mingi naturaalarv p . Sellisel juhul öeldakse, et korpuse K **karakteristika on** p ja kirjutatakse $\text{char} K = p$.

Siis iga $a \in K$ korral $pa = \mathbf{0}$, sest

$$pa = p(\mathbf{1} \cdot a) = (p\mathbf{1})a = \mathbf{0}a = \mathbf{0}.$$

Näiteks jäägiklassikorpuse $\mathbb{Z}_p$ karakteristika on p .

Lause 9.2 *Lõpliku korpuse karakteristika on algarv.*

TÕESTUS. Olgu p elemendi $\mathbf{1} \in K$ järk rühmas $(K, +)$, s.t. et p on vähim naturaalarv, mille korral $p\mathbf{1} = \mathbf{0}$. Näitame, et p on algarv. Selleks oletame vastuväiteliselt, et $p = kl$, kus $1 < k, l < p$. Siis $k\mathbf{1} \neq \mathbf{0}$ ja $l\mathbf{1} \neq \mathbf{0}$, kuid

$$(k\mathbf{1}) \cdot (l\mathbf{1}) = (kl)(\mathbf{1} \cdot \mathbf{1}) = (kl)\mathbf{1} = p\mathbf{1} = \mathbf{0}.$$

Korrutades selle võrduse pooli elemendiga $(k\mathbf{1})^{-1}$ saame vastuolu $l\mathbf{1} = \mathbf{0}$. Seega p peab olema algarv. $\square$

Lemma 9.3 *Kui korpuse K karakteristika on algarv p , siis iga $a, b \in K$ ja $n \in \mathbb{N}$ korral*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

TÕESTUS. Tõestame väite induktsiooniga n järgi. Olgu $n = 1$. Kuna K korrutamise on kommutatiivne, siis

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i.$$

Olgu $i \in \{1, \dots, p-1\}$. Kuna

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-i+1)}{i!},$$

siis

$$p \cdot (p-1) \cdot \dots \cdot (p-i+1) = \binom{p}{i} \cdot i!.$$

Et p jagab viimase võrduse vasakut poolt, aga ei jaga arvu $i!$ (sest selle algtegurite hulgas ei esine p), siis $p \mid \binom{p}{i}$, s.t. leidub selline $k_i \in \mathbb{N}$, et $k_i p = \binom{p}{i}$. Järelikult iga $i \in \{1, \dots, p-1\}$ korral

$$\binom{p}{i} a^{p-i} b^i = (k_i p)(a^{p-i} b^i) = k_i (p(a^{p-i} b^i)) = k_i \mathbf{0} = \mathbf{0},$$

seega $(a + b)^p = a^p + b^p$ ning induktsiooni alus on tõestatud.

Oletame nüüd, et $(a + b)^{p^k} = a^{p^k} + b^{p^k}$. Kasutades äsjatõestatud saame

$$(a + b)^{p^{k+1}} = \left((a + b)^{p^k} \right)^p = \left(a^{p^k} + b^{p^k} \right)^p = \left(a^{p^k} \right)^p + \left(b^{p^k} \right)^p = a^{p^{k+1}} + b^{p^{k+1}}.$$

$\square$

Definitsioon 9.4 Korpuse L alamringi K nimetatakse **alamkorpuseks**, kui $a^{-1} \in K$ iga $a \in K \setminus \{\mathbf{0}\}$ korral.

Seega alamhulk $L \subseteq K$ on korpuse K alamkorpus parajasti siis, kui

- L on aditiivse rühma $(K, +)$ alamrühm ja
- L^* on multiplikatiivse rühma $(K^*, \cdot)$ alamrühm.

Definitsioon 9.5 Kui korpus K on korpuse L alamkorpus, siis öeldakse, et korpus L on korpuse K **laiend**.

Näiteks korpused $\mathbb{R}$ ja $\mathbb{C}$ on korpuse $\mathbb{Q}$ laiendid.

Lause 9.6 Korpuse iga laiendi karakteristika on võrdne selle korpuse karakteristikaga.

TÕESTUS. Olgu L korpuse K laiend ja $\text{char} K = p$. Siis K kui korpuse L alamkorpus peab sisaldama korpuse L ühikelementi $\mathbf{1}$, mis on seega ka K ühikelemendiks. Kuna elemendi $\mathbf{1}$ järk rühmas $(K, +)$ on p , siis tema järk rühmas $(L, +)$ on samuti p ja seega $\text{char} L = p$. $\square$

9.2 Lihtsad korpused

Igal korpusel on vähemalt üks alamkorpus – ta ise.

Definitsioon 9.7 Korpust nimetatakse **lihtsaks**, kui tal on täpselt üks alamkorpus.

Näiteks korpused $\mathbb{R}$ ja $\mathbb{C}$ ei ole lihtsad, sest sisaldavad alamkorpusena lisaks iseendale ka korpust $\mathbb{Q}$. Selles paragrahvis anname lihtsate korpuste kirjelduse isomorfismi täpsuseni.

Definitsioon 9.8 Kahte korpust nimetatakse **isomorfseteks**, kui nad on isomorfsed ringidena.

Teoreem 9.9 Iga korpus K sisaldab täpselt ühte lihtsat alamkorpust P . Kui $\text{char} K = 0$, siis $P \cong \mathbb{Q}$. Kui $\text{char} K = p$, siis $P \cong \mathbb{Z}_p$.

TÕESTUS. Vaatleme kõigepealt juhtu, kus $\text{char} K = 0$. Siis $n\mathbf{1} \neq \mathbf{0}$ kõigi naturaalarvude n korral. Iga ratsionaalarvu saab esitada kujul $\frac{a}{n}$, kus $a \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Defineerime ratsionaalarvu $\frac{a}{n}$ ja korpuse K ühikelemendi $\mathbf{1}$ kordsed järgmiselt:

$$\frac{a}{n}\mathbf{1} := (a\mathbf{1})(n\mathbf{1})^{-1} \in K.$$

See definitsioon on korrektne, s.t. ei sõltu ratsionaalarvu esitusest jagatisena, sest mistahes $a, b \in \mathbb{Z}$ ja $m, n \in \mathbb{N}$ korral

$$\begin{aligned} \frac{a}{n} = \frac{b}{m} &\implies am = bn \implies (am)\mathbf{1} = (bn)\mathbf{1} \implies (a\mathbf{1})(m\mathbf{1}) = (b\mathbf{1})(n\mathbf{1}) \\ &\implies (a\mathbf{1})(n\mathbf{1})^{-1} = (b\mathbf{1})(m\mathbf{1})^{-1} \implies \frac{a}{n}\mathbf{1} = \frac{b}{m}\mathbf{1}. \end{aligned}$$

Muuhulgas $\frac{ak}{nk}\mathbf{1} = \frac{a}{n}\mathbf{1}$ iga $k \in \mathbb{N}$ korral.

Vaatleme hulka

$$P = \left\{ \frac{a}{n}\mathbf{1} \mid a \in \mathbb{Z}, n \in \mathbb{N} \right\} \subseteq K.$$

See sisaldab muuhulgas elemente $\mathbf{1} = \frac{1}{1}\mathbf{1}$ ja $\mathbf{0} = \frac{0}{1}\mathbf{1}$. Veendume, et P on korpuse K alamkorpus.

- Hulk P on kinnine lahutamise suhtes, sest

$$\begin{aligned} \frac{a}{n}\mathbf{1} - \frac{b}{m}\mathbf{1} &= (a\mathbf{1})(n\mathbf{1})^{-1} - (b\mathbf{1})(m\mathbf{1})^{-1} \\ &= (a\mathbf{1})(m\mathbf{1})(n\mathbf{1})^{-1}(m\mathbf{1})^{-1} - (b\mathbf{1})(n\mathbf{1})(m\mathbf{1})^{-1}(m\mathbf{1})^{-1} \\ &= (am\mathbf{1} - bn\mathbf{1})(n\mathbf{1})^{-1}(m\mathbf{1})^{-1} \\ &= (am - bn)\mathbf{1}(nm\mathbf{1})^{-1} \\ &= \frac{am - bn}{nm}\mathbf{1} \in P. \end{aligned}$$

- Hulk P on kinnine korrutamise suhtes, sest

$$\begin{aligned} \frac{a}{n}\mathbf{1} \cdot \frac{b}{m}\mathbf{1} &= (a\mathbf{1})(n\mathbf{1})^{-1}(b\mathbf{1})(m\mathbf{1})^{-1} = (a\mathbf{1})(b\mathbf{1})(n\mathbf{1})^{-1}(m\mathbf{1})^{-1} \\ &= (ab\mathbf{1})(nm\mathbf{1})^{-1} = \frac{ab}{nm}\mathbf{1} \in P. \end{aligned}$$

- Näitame veel, et P sisaldab nullist erineva elemendi $\frac{a}{n}\mathbf{1}$, $a \neq 0$, pöördelementi. On kaks võimalust. Kui $a > 0$, siis

$$\frac{a}{n}\mathbf{1} \cdot \frac{n}{a}\mathbf{1} = \frac{an}{na}\mathbf{1} = \frac{1}{1}\mathbf{1} = \mathbf{1},$$

seega $\left(\frac{a}{n}\mathbf{1}\right)^{-1} = \frac{n}{a}\mathbf{1} \in P$. Kui $a < 0$, siis

$$\frac{a}{n}\mathbf{1} \cdot \frac{-n}{-a}\mathbf{1} = \frac{a(-n)}{n(-a)}\mathbf{1} = \frac{-an}{-na}\mathbf{1} = \frac{1}{1}\mathbf{1} = \mathbf{1},$$

seega $\left(\frac{a}{n}\mathbf{1}\right)^{-1} = \frac{-n}{-a}\mathbf{1} \in P$.

Näitame nüüd, et P on lihtne korpus. Oletame, et Q on P mingi alamkorpus. Siis Q peab sisaldama ühikelementi $\mathbf{1}$ ja nullelementi $\mathbf{0}$. Olles kinnine liitmise suhtes, peab ta sisaldama elemente $a\mathbf{1}$, kus $a \in \mathbb{N}$. Kuna Q on kinnine ka vastandelemendi võtmise suhtes, siis $a\mathbf{1} \in Q$ iga $a \in \mathbb{Z}$ korral. Alamkorpus Q peab sisaldama nullist erinevate elementide pöördelemente, seega $(n\mathbf{1})^{-1} \in Q$ iga $n \in \mathbb{N}$ korral. Kinnisusest korrutamise suhtes järeldeb, et $\frac{a}{n}\mathbf{1} \in Q$ iga $a \in \mathbb{Z}$ ja $n \in \mathbb{N}$ korral. Seega $P \subseteq Q \subseteq P$ ehk $P = Q$.

Defineerime kujutuse $f : \mathbb{Q} \rightarrow P$ võrdusega

$$f\left(\frac{a}{n}\right) := \frac{a}{n}\mathbf{1}.$$

Eespool toodud arutelu kohaselt on see definitsioon korrektne, s.t. ei sõltu ratsionaalarvu esitusest jagatisena. On selge, et f on sürjektiivne. Kui $\mathbf{0} = f\left(\frac{a}{n}\right) = \frac{a}{n}\mathbf{1} = (a\mathbf{1})(n\mathbf{1})^{-1}$, siis korrutades selle võrduse mõlemat poolt elemendiga $n\mathbf{1}$ saame, et $a\mathbf{1} = \mathbf{0}$. Kuna $\text{char} K = 0$, siis $a = 0$ ja seega $\frac{a}{n} = \frac{0}{n} = \frac{0}{1}$. Oleme näidanud, et $\text{Ker}(f) = \left\{\frac{0}{1}\right\}$, seega f on injektiivne.

Jääb veel näidata, et f on ringide homomorfism. Sarnaselt eespool tehtuga

$$\begin{aligned} f\left(\frac{a}{n} + \frac{b}{m}\right) &= f\left(\frac{am + bn}{nm}\right) = \frac{am + bn}{nm}\mathbf{1} = \frac{a}{n}\mathbf{1} + \frac{b}{m}\mathbf{1} = f\left(\frac{a}{n}\right) + f\left(\frac{b}{m}\right), \\ f\left(\frac{a}{n} \cdot \frac{b}{m}\right) &= f\left(\frac{ab}{nm}\right) = \frac{ab}{nm}\mathbf{1} = \frac{a}{n}\mathbf{1} \cdot \frac{b}{m}\mathbf{1} = f\left(\frac{a}{n}\right) \cdot f\left(\frac{b}{m}\right) \end{aligned}$$

mistahes $a, b \in \mathbb{Z}$ ja $n, m \in \mathbb{N}$ korral. Seega oleme näidanud, et f on korpuste isomorfism.

Uurime nüüd olukorda, kus korpuse K karakteristika on algarv p . Vaatleme hulka

$$P = \{\mathbf{1}, \mathbf{1} + \mathbf{1}, \mathbf{1} + \mathbf{1} + \mathbf{1}, \dots, (p-1)\mathbf{1}, p\mathbf{1} = \mathbf{0}\} \subseteq K.$$

Iga täisarvu m korral leiduvad $q, r \in \mathbb{Z}$ nii, et $m = pq + r$ ja $0 \leq r < p$. Seega

$$m\mathbf{1} = (pq)\mathbf{1} + r\mathbf{1} = q(p\mathbf{1}) + r\mathbf{1} = q\mathbf{0} + r\mathbf{1} = r\mathbf{1}$$

ja $P = \{m\mathbf{1} \mid m \in \mathbb{Z}\}$. Me näeme, et P on korpuse K alamkorpus, sest mistahes $k, l \in \{1, \dots, p\}$ korral

- $k\mathbf{1} - l\mathbf{1} = (k - l)\mathbf{1} \in P$,
- $(k\mathbf{1}) \cdot (l\mathbf{1}) = (kl)\mathbf{1} \in P$,
- kui $k \neq p$, siis $(k\mathbf{1})^{-1} = u\mathbf{1} \in P$, kus $ku \equiv 1 \pmod{p}$ (ehk $\bar{u} = \bar{k}^{-1}$ korpuses $\mathbb{Z}_p$).

Kui Q on P alamkorpus, siis $\mathbf{1} \in Q$, millest järeldub kohe (tänu kinnisusele liitmise suhtes), et $Q = P$. Seega P on lihtne korpus. Sarnaselt tõestuse esimese poolega saab näidata, et korpus P on isomorfne korpusega $\mathbb{Z}_p$, kusjuures isomorfismi realiseerib kujutus $f: P \rightarrow \mathbb{Z}_p$,

$$f(k\mathbf{1}) = \bar{k}.$$

□

Järeldus 9.10 Ainsad lihtsad korpused on $\mathbb{Q}$ ja $\mathbb{Z}_p$, kus p on algarv.

9.3 Lõplike korpuste ehitus

Uurime nüüd lähemalt lõplike korpuste ehitust.

Lause 9.11 Korpuse K iga laiendit L võib vaadelda vektorruumina üle korpuse K . Kui L on lõplik ja $|K| = q$, siis $|L| = q^m$, kus $m \in \mathbb{N}$.

TÕESTUS. Vaatleme hulka L vektorruumina, kus liitmine on korpuse L liitmine ning vektori $a \in L$ ja skalaari $\alpha \in K$ korrutis on lihtsalt nende elementide korrutis αa korpuses L . Vektorruumi aksioomide täidetud järeldub kohe korrutamise assotsiatiivsusest ja distributiivsuse seadustest korpuses L . Kui L on lõplik, siis on ta lõplikumõõtmeline vektorruum üle korpuse K , s.t. omab lõplikku baasi. Olgu $e_1, \dots, e_m$ baas vektorruumis L üle korpuse K . Siis iga $a \in L$ esitub üheselt lineaarkombinatsioonina $a = \alpha_1 e_1 + \dots + \alpha_m e_m$, kus $\alpha_1, \dots, \alpha_m \in K$. Et iga kordaja α_i valikuks on q võimalust, siis selliseid lineaarkombinatsioone on q^m tükki, s.t. $|L| = q^m$. $\square$

Teoreem 9.12 *Lõpliku korpuse elementide arv on algarvu aste.*

TÕESTUS. Olgu K lõplik korpus, mille karakteristika on p . Teoreemi 9.9 tõestuses nägime, et hulk

$$P = \{\mathbf{1}, \mathbf{1} + \mathbf{1}, \mathbf{1} + \mathbf{1} + \mathbf{1}, \dots, (p-1)\mathbf{1}, p\mathbf{1} = \mathbf{0}\} \subseteq K$$

on korpuse K lihtne alamkorpus, mis on isomorfne korpusega $\mathbb{Z}_p$. Lause 9.11 põhjal leidub selline naturaalarv n , et $|K| = |P|^n = |\mathbb{Z}_p|^n = p^n$. $\square$

Meil läheb vaja järgmist abitulemust, mille üheks erijuhuks on Fermat' väike teoreem.

Lemma 9.13 *Kui K on lõplik korpus ning $|K| = q$, siis*

1. iga $a \in K^*$ korral $a^{q-1} = \mathbf{1}$,
2. iga $a \in K$ korral $a^q = a$.

TÕESTUS. 1. Olgu m elemendi a järk korpuse K multiplikatiivses rühmas K^* . Lause 3.30 tõttu $m \mid q-1 = |K^*|$ ehk $mk = q-1$ mingi naturaalarvu k korral. Järelikult

$$a^{q-1} = a^{mk} = (a^m)^k = \mathbf{1}^k = \mathbf{1}.$$

2. Võrdus $a^q = a$ kehtib nii nullelemendi kui nullist erinevate elementide korral. $\square$

Lõplikud korpused konstrueeritakse enamasti polünoomide ringide faktoringidena. Ringe faktoriseeritakse ideaalide järgi (saab näidata, et need vastavad ringi kongruentsidele). Kui I on ringi R ideaal ja $a \in R$, siis hulka $a + I = \{a + b \mid b \in I\} =: [a]$ nimetatakse **kõrvalklassiks** ideaali I järgi esindajaga a . Muuhulgas $[0_R] = I$, s.t. I ise on ka üks kõrvalklassidest. Lause 3.5 põhjal

$$a + I = b + I \iff a - b \in I.$$

Vahetu kontroll näitab, et kõrvalklasside hulk

$$R/I = \{a + I \mid a \in R\}$$

on ring tehete

$$\begin{aligned} [a] + [b] &:= [a + b], \\ [a][b] &:= [ab] \end{aligned}$$

suhtes. Seda ringi nimetatakse ringi R **faktorringiks** ideaali I järgi.

Rakendame nüüd seda konstruktsiooni olukorras, kus K on korpus ja $R = K[x]$ on polünoomide ring muutuja x suhtes. See ring on kommutatiivne ja selle ühikelemendiks on konstantne polünoom $\mathbf{1}$. Kui $h \in K[x]$ on mingi polünoom üle korpuse K , siis selle polünoomi poolt tekitatud peaideaal

$$I = h \cdot K[x] = \{hg \mid g \in K[x]\}$$

koosneb kõigist polünoomidest ringis $K[x]$, mis jaguvad polünoomiga h . Kõrvalklass esindajaga $f \in K[x]$ ideaali $h \cdot K[x]$ järgi on hulk

$$[f] = f + h \cdot K[x] = \{f + hg \mid g \in K[x]\}.$$

Muuhulgas $[0] = h \cdot K[x]$ ja kehtib

$$[f] = [g] \iff f - g \in h \cdot K[x] \iff h \mid f - g. \quad (9.1)$$

Näiteks $[h] = [0]$, sest $h \mid h$. Faktorringis

$$K[x]/(h \cdot K[x]) = \{[f] \mid f \in K[x]\}$$

ideaali $h \cdot K[x]$ järgi on tehned defineeritud võrdustega

$$\begin{aligned} [f] + [g] &= [f + g], \\ [f] \cdot [g] &= [fg] \end{aligned}$$

ja selle nullelemendiks on $[0]$.

Definitsioon 9.14 Mittekonstantset polünoomi $h \in K[x]$ nimetatakse **taandumatuks**, kui teda ei saa esitada kahe mittekonstantse polünoomi korrutisena, s.t. kui võrdusest $h = fg$ järeldub, et kas polünoom f on konstantne või g on konstantne.

Lause 9.15 Olgu K korpus ja $h \in K[x]$ taandumatu polünoom, mille aste $d \geq 2$. Siis faktorring $L = K[x]/(h \cdot K[x])$ on korpus, mis sisaldab korpusega K isomorfset alamkorpust ning milles polünoomil h on olemas juur. Kui $|K| = p^m$, siis $|L| = p^{md}$.

TÕESTUS. Olgu

$$L = K[x]/(h \cdot K[x]) = \{[f] \mid f \in K[x]\}$$

ringi $K[x]$ faktorring ideaali $h \cdot K[x]$ järgi. Esimene väide on tõestatud raamatus [1] lausena 7.3.1. Meenutame, et elemendi $[0] \neq [f] \in L$ pööratavus järeldub sellest, et h ei jaga polünoomi f ja h on taandumatu (seega $\text{SÜT}(h, f) = \mathbf{1}$), korpusega K isomorfseks alamkorpuseks korpuses L on konstantsete polünoomide kõrvalklasside hulk $K' = \{[k] \mid k \in K\}$ ning polünoomi h üheks juureks korpuses L on lineaarpolünoomi x kõrvalklass $[x]$ (s.t. $h([x]) = [0]$).

Näitame veel, et korpuses L on p^{md} elementi. Selleks tõestame, et

$$K[x]/(h \cdot K[x]) = \{[f] \mid f \in K[x], \deg f < d\}.$$

Tuleb veenduda, et

$$\{[f] \mid f \in K[x]\} \subseteq \{[f] \mid f \in K[x], \deg f < d\}$$

(vastupidine sisalduvus on ilmne). Võttes $g \in K[x]$ võime selle polünoomi jagada jäägiga polünoomiga h , s.t. leida sellised $q, r \in K[x]$, et

$$g = hq + r \quad \text{ja} \quad \deg(r) < \deg(h) = d.$$

Järelikult

$$[g] = [h][q] + [r] = [\mathbf{0}][q] + [r] = [r] \in \{[f] \mid f \in K[x], \deg(f) < d\}.$$

Seega iga kõrvalklassi esindajaks saab valida polünoomi, mille aste on väiksem kui d :

$$L = \{[k_{d-1}x^{d-1} + \dots + k_1x + k_0] \mid k_0, \dots, k_{d-1} \in K\}. \quad (9.2)$$

Erinevaid selliseid polünoome on $|K|^d$ tükki ning erinevatele sellistele polünoomidele vastavad erinevad kõrvalklassid, sest kui $f, g \in K[x]$, $f \neq g$, $\deg(f) < d$ ja $\deg(g) < d$, siis $f - g \neq \mathbf{0}$ ja $\deg(f - g) < d$, mistõttu h ei jaga polünoomi $f - g$ ja seega (9.1) põhjal $[f] \neq [g]$. Sellega oleme tõestanud, et $|L| = |K|^d = p^{md}$. $\square$

Lauset 9.15 kasutades saab tõestada järgmise teoreemi.

Teoreem 9.16 ([1], teoreem 7.3.3) *Olgu $f \in K[x]$ polünoom kordajatega korpusest K ning olgu f aste $n \geq 1$. Siis leidub korpuse K selline laiend L , milles polünoomil f on n juurt.*

Kui need teoreemis 9.16 mainitud juured on $a_1, \dots, a_n \in L$, siis f lahutub lineaartegurite korrutiseks üle korpuse L : $f = b(x - a_1) \dots (x - a_n)$, kus $b \in K$ on x^n kordaja polünoomis f .

Definitsioon 9.17 Korpuse K laiendit L nimetatakse polünoomi $f \in K[x]$ **lahutuskorpuseks**, kui

1. f lahutub lineaartegurite korrutiseks üle L , s.t. leiduvad $a_1, \dots, a_n, b \in L$ nii, et

$$f = b(x - a_1) \dots (x - a_n),$$

2. korpuse L iga alamkorpuse M korral, mis sisaldab korpust K ja elemente $a_1, \dots, a_n$, kehtib võrdus $M = L$.

Kuna korpuse alamkorpuste ühisosa on samuti alamkorpus, siis teoreemist 9.16 järeldub, et igal mittekonstantsel polünoomil f üle korpuse K on lahutuskorpus olemas. Kui K on lõplik, siis ka f lahutuskorpus L on lõplik. Veelgi enam, kehtib järgmine teoreem, mida me siinkohal ei tõesta.

Teoreem 9.18 *Polünoomi lahutuskorpus on isomorfismi täpsuseni üheselt määratud.*

Selle paragrahvi põhitulemus on järgmine.

Teoreem 9.19 *Iga algarvu p ja naturaalarvu n korral leidub korpus, milles on p^n elementi. See korpus on isomorfismi täpsuseni üheselt määratud.*

TÕESTUS. Olgu $q = p^n$. Vaatleme polünoomi $x^q - x \in \mathbb{Z}_p[x]$. Olgu L polünoomi $x^q - x$ lahutuskorpus ning olgu

$$x^q - x = (x - a_1) \dots (x - a_q),$$

kus $a_1, \dots, a_q \in L$. Kuna $\mathbb{Z}_p \subseteq L$ on alamkorpus, siis lause 9.6 põhjal on korpuse L karakteristika p , s.t. $p\mathbf{1} = \mathbf{0}$ ja seega ka $q\mathbf{1} = \mathbf{0}$. Järelikult

$$(x^q - x)' = q\mathbf{1}x^{q-1} - \mathbf{1} = -\mathbf{1} \in L[x].$$

Näitame, et sellest järeldub, et polünoomil $x^q - x$ ei ole kordseid juuri. Oletame vastuväiteliselt, et $a \in L$ on polünoomi $x^q - x$ kordne juur, s.t.

$$x^q - x = (x - a)^k g,$$

kus $k \geq 2$ ja $g \in L[x]$. Siis korrutise tuletise leidmise reegli põhjal

$$(x^q - x)' = k\mathbf{1}(x - a)^{k-1}g + (x - a)^k g' = (x - a) (k\mathbf{1}(x - a)^{k-2}g + (x - a)^{k-1}g').$$

Siit näeme, et $(x - a) \mid (x^q - x)' = -\mathbf{1}$ ringis $L[x]$. Kuna aga lineaarpolünoom ei saa jagada konstantset polünoomi, siis oleme saanud vastuolu. Järelikult tõesti polünoomil $x^q - x$ pole kordseid juuri, s.t. elemendid $a_1, \dots, a_q$ on erinevad.

Vaatleme q -elemendilist alamhulka

$$K = \{a_1, \dots, a_q\} \subseteq L.$$

Paneme tähele, et

$$K = \{a \in L \mid a^q = a\}.$$

Tõepoolest, kuna $a_1, \dots, a_q$ on polünoomi $x^q - x$ juured, siis nad peavad kuuluma hulka $\{a \in L \mid a^q = a\}$. Kui aga $a^q = a$, siis a on polünoomi $x^q - x$ juur. Kuna q -nda astme polünoomil ei saa olla rohkem kui q juurt, siis $a \in \{a_1, \dots, a_q\}$.

Näitame, et K on korpuse L alamkorpus. Selleks näitame, et K on kinnine tehete suhtes. Olgu $a, b \in K$, s.t. $a^q = a$ ja $b^q = b$.

- Lemma 9.3 põhjal

$$(a + b)^q = (a + b)^{p^n} = a^{p^n} + b^{p^n} = a^q + b^q = a + b,$$

$$\text{s.t. } a + b \in K.$$

- Kui $p = 2$, siis $a + a = \mathbf{0}$ ehk $-a = a \in K$. Kui aga $p > 2$, siis q on paaritu ja

$$(-a)^q = ((-\mathbf{1})a)^q = (-\mathbf{1})^q a^q = (-\mathbf{1})a = -a,$$

$$\text{s.t. } -a \in K.$$

- Korrumise kommutatiivsuse tõttu ka $(ab)^q = a^q b^q = ab$, s.t. $ab \in K$.
- Kuna $1^q = 1$, siis korpuse L ühikelement 1 kuulub hulka K .
- Olgu $a \neq 0$. Siis $(a^{-1})^q = (a^q)^{-1} = a^{-1}$, s.t. $a^{-1} \in K$.

Seega K on alamkorpus. Lisaks sellele $\mathbb{Z}_p \subseteq K$, sest iga $\bar{c} \in \mathbb{Z}_p$ korral

$$\bar{c}^q = \bar{c}^{p^n} = (\bar{c}^p)^{p^{n-1}} = \bar{c}^{p^{n-1}} = \dots = \bar{c}.$$

Kuna L on korpuse L vähim alamkorpus, mis sisaldab korpust $\mathbb{Z}_p$ ja elemente $a_1, \dots, a_q$, siis $L = K$, järelikult $|L| = |K| = q$.

Ühesuse näitamiseks paneme tähele, et mistahes q -elemendilise korpuse L' korral on lemma 9.13 tõttu kõik tema elemendid polünoomi $x^q - x \in \mathbb{Z}_p[x]$ juured. Kuna sellel polünoomil ei saa olla üle q juure, siis on L' selle polünoomi lahutuskorpus. Kuna polünoomi mistahes kaks lahutuskorpus on isomorfseid, siis on ka korpus L' isomorfne korpusega L . $\square$

Korpust, milles on $q = p^n$ elementi, tähistatakse tihti kas $\mathbb{F}_q$ või $\text{GF}(q)$ ($\text{GF} = \text{Galois field}$). Sellise korpuse konstrueerimiseks on otstarbekas kasutada lauset 9.15. Võtame näiteks korpuse $\mathbb{Z}_p$, leiame mingi n -nda astme taandumatu polünoomi h üle $\mathbb{Z}_p$ ning moodustame faktoringi $\mathbb{Z}_p[x]/(h \cdot \mathbb{Z}_p[x])$. Tulemus on p^n -elemendiline korpus, mis tänu teoreemile 9.19 ongi $\mathbb{F}_q$.

Arvuteooria konspektist võib leida järgmise teoreemi tõestuse.

Teoreem 9.20 *Lõpliku korpuse multiplikatiivne rühm on tsükliline.*

Lõpliku korpuse multiplikatiivse rühma tekitajaid nimetatakse selle korpuse **primitiivseteks elementideks**. Korpuse $\mathbb{Z}_p$ (p on algarv) primitiivseid elemente nimetatakse **algjuurteks** mooduli p järgi.

9.4 Aritmeetika lõplikes korpustes

Lõpliku korpuse elementide esitamiseks on mitmeid võimalusi. Üks viis on kasutada faktoringi $\mathbb{Z}_p[x]/(h \cdot \mathbb{Z}_p[x])$, kus h on taandumatu polünoom üle $\mathbb{Z}_p$. Teine võimalus on kasutada fakti, et rühm $\mathbb{F}_q^*$ on tsükliline ja seega tema elemendid on esitatavad tekitaja (primitiivse elemendi) astmetena. On selge, et liita on lihtsam elemente, mis on esitatud polünoomidena ning korrumada on lihtsam rühma moodustaja astmeid. Osutub, et neid kahte viisi saab omavahel kombineerida, mis annab võimaluse aritmeetiliste tehete efektiivseks sooritamiseks lõplikus korpuses.

Näide 9.21 Vaatleme lõplikku korpust $\mathbb{F}_{16}$ kui korpuse $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ ($\bar{0}$ ja $\bar{1}$ asemel kirjutame 0 ja 1) laiendit.

Näitame, et polünoom $h = x^4 + x + 1$ on taandumatu üle $\mathbb{F}_2$. Selleks paneme tähele, et kui h oleks taanduv, siis ta peaks omama kas lineaar- või ruuttegurit. Kuna $p(0) \neq 0$

ja $p(1) \neq 0$, siis polünoomil h pole lineaartegureid. Veendumaks, et polünoom h ei jagu ühegi ruutpolünoomiga, märgime, et üle $\mathbb{F}_2$ on täpselt neli erinevat ruutpolünoomi

$$x^2, x^2 + 1, x^2 + x, x^2 + x + 1$$

ning vahetu kontroll näitab, et neid polünoome omavahel korrutades me ei saa polünoomi h .

Kuna polünoomi h aste on 4, siis lause 9.15 põhjal

$$\mathbb{F}_2[x]/(x^4 + x + 1)\mathbb{F}_2[x] = \mathbb{F}_{16}.$$

Tähistame $a = [x]$ ning samastame kõrvlaklassid $[0]$ ja $[1]$ esindajatega 0 ja 1. Kui vaatleme polünoomile h vastavat polünoomi $\tilde{h} = y^4 + y + 1 \in \mathbb{F}_{16}[y]$, siis a on polünoomi $\tilde{p}$ juur, sest

$$\tilde{p}(a) = a^4 + a + 1 = [x]^4 + [x] + [1] = [x^4 + x + 1] = [0].$$

Tänu võrdusele (9.2) võib korpuse $\mathbb{F}_{16}$ elemente esitada kui ülimalt kolmanda astme polünoome a suhtes:

konstantsed	$0, 1,$
lineaarsed	$a, a + 1,$
ruutpolünoomid	$a^2, a^2 + 1, a^2 + a, a^2 + a + 1$
kuuppolünoomid	$a^3, a^3 + 1, a^3 + a, a^3 + a^2, a^3 + a + 1,$ $a^3 + a^2 + 1, a^3 + a^2 + a, a^3 + a^2 + a + 1.$

Sellisel kujul elementide liitmine on lihtne, sest see on lihtsalt polünoomide liitmine. Korrutamine nõuab taandamist “mooduli $p(x)$ järgi”, s.o. jäägiga jagamist polünoomiga $x^4 + x + 1$, kuid võib kasutada ka seost $a^4 + a + 1 = 0$ ehk $a^4 = a + 1$. Näiteks

$$\begin{aligned} a^{14} &= (a^4)^3 a^2 = (a + 1)^3 a^2 = (a^3 + a^2 + a + 1)a^2 = a^5 + a^4 + a^3 + a^2 \\ &= (a + 1)a + a + 1 + a^3 + a^2 = a^2 + a + a + 1 + a^3 + a^2 = a^3 + 1. \end{aligned}$$

Kuna $a \neq 0$, siis $a \in \mathbb{F}_{16}^*$. Samuti $a \neq 1$. Elemendi a järk multiplikatiivses rühmas $\mathbb{F}_{16}^*$ peab olema rühma järgu (s.t. arvu 15 jagaja). Seega $\text{ord}(a) \in \{3, 5, 15\}$. Et $a^3 \neq 1$ ja $a^5 = a^2 + a \neq 1$, siis $\text{ord}(a) = 15$, s.t. element a on rühma $\mathbb{F}_{16}^*$ tekitaja. Seega

$$\mathbb{F}_{16} = \{0, 1, a, a^2, \dots, a^{14}\}.$$

Sellisel viisil esitatud elementide korrutamine on lihtne, kuid liitmine on tülikas.

Need kaks esitust saab omavahel siduda, kui arvutada välja tabel, mis näitab, kuidas element a^m esitub ülimalt kolmanda astme polünoomina a suhtes. Kasutades seost $a^4 = a + 1$ saame

$$\begin{aligned} a^4 &= a + 1, \\ a^5 &= a \cdot a^4 = a(a + 1) = a^2 + a, \\ a^6 &= a \cdot a^5 = a^3 + a^2, \\ a^7 &= a \cdot a^6 = a^4 + a^3 = a^3 + a + 1 \end{aligned}$$

ja nii edasi. Tulemused võtame kokku alljärgneva tabelina, kus elemendi a^m asemel kirjutame lihtsalt m ning polünoomi $k_3 a^3 + k_2 a^2 + k_1 a + k_0$ asemel kirjutame tema kordajate jada $k_3 k_2 k_1 k_0$.

0	0001
1	0010
2	0100
3	1000
4	0011
5	0110
6	1100
7	1011
8	0101
9	1010
10	0111
11	1110
12	1111
13	1101
14	1001

Selle tabeli ning seose $a^{15} = 1$ abil võime nüüd näiteks arvutada

$$\begin{aligned}(a^8 + a^4 + 1)(a^3 + a) &= (0101 + 0011 + 0001)(1000 + 0010) = (0111)(1010) \\ &= a^{10} \cdot a^9 = a^{19} = a^4 = a + 1.\end{aligned}$$

Seega arvutamiseks (liitmiseks ja korrutamiseks) lõplikus korpuses on kasulik teada tema multiplikatiivse rühma moodustajat koos mingi taandumatu polünoomiga, mille juureks ta on. Üldjuhul pole taandumatu polünoomi leidmine lihtne. Siiski on paljude konkreetsete korpuste jaoks leitud taandumatud polünoomid ja tabelid.

Peatükk 10

Võred

10.1 Kaks vaatenurka võredele

Võret on võimalik defineerida kahel erineval viisil, üks neist on järjestusteoreetiline ja teine puhtalt algebraline. Osutub, et need kaks definitsiooni on samaväärsed. Alustame järjestusteoreetilisest definitsioonist.

Definitsioon 10.1 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 $a \wedge b$.

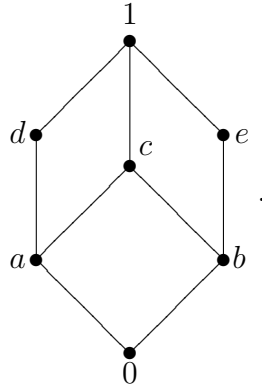
Definitsioon 10.2 Võre on järjestatud hulk, mille igal kahel elemendil leidub ülemine ja alumine raja.

Näide 10.3 1. Hulga A kõigi alamhulkade hulk $\mathcal{P}(A)$ koos sisalduvusseosega $\subseteq$ on võre. Selles võres on A alamhulkade X ja Y alumiseks rajaks ühisosa $X \cap Y$ ja ülemiseks rajaks ühend $X \cup Y$.

2. Öeldakse, et järjestatud hulk on **lineaarselt järjestatud**, kui mistahes kahe elemendi a ja b korral kas $a \leq b$ või $b \leq a$. Iga lineaarselt järjestatud hulk on võre, kus $a \wedge b = \min(a, b)$ ja $a \vee b = \max(a, b)$. Näiteks hulk $\mathbb{Z}$ on lineaarselt järjestatud.
3. Naturaalarvude hulk, mida vaatleme järjestatud hulgana jaguvusseose $|$ suhtes, on võre, kus alumine raja on SÜT ja ülemine raja on VÜK.
4. Vektorruumi V kõigi alamruumide hulk $\text{Sub}(V)$ on võre, kus alamruumide V_1 ja V_2 alumine raja on $V_1 \cap V_2$ ja ülemine raja on $V_1 + V_2$.

Näide 10.4 Lõplike järjestatud hulkade (muuhulgas lõplike võrede) kujutamiseks kasutatakse tihti teatud graafe, kus punktid (tipud) märgivad hulga elemente ja kaks punkti on ühendatud joonega (servaga) kui üks elementidest on teisest väiksem ja nende kahe vahel ei ole järjestusseose mõttes kolmandaid elemente (sellisel juhul öeldakse ka, et üks element

katab teist). Kokkuleppeliselt asuvad suuremas elemendid joonisel kõrgemal. Näiteks on võimalik vaadelda 7-elementilist võret



Selles võres näiteks $a < d$ ja $d < 1$, aga ka $a < 1$. Jooniselt on näha, et näiteks $a \vee b = c$, $a \vee e = 1$ ja $d \wedge c = a$.

Võret võib defineerida ka kui kahe kahekohalise algebralise tehtega struktuuri.

Definitsioon 10.5 Võre on mittetühi hulk L , millel on defineeritud kaks algebralist tehet $+$ ja $\cdot$ (liitmine ja korrutamine) nii, et mistahes $a, b, c \in L$ korral

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

On lihtne aru saada, et esimese tulba omadused on duaalsed teise tulba omadega selles mõttes, et kui liitmine asendada korrutamisega ja vastupidi, siis saame esimese tulba omadusest samas reas asuva teise tulba omaduse.

Lause 10.6 Olgu $(L, +, \cdot)$ võre definitsiooni 10.5 mõttes. Siis mistahes $a, b \in L$ korral

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

TÕESTUS. TARVILIKKUS. Kui $a = ab$, siis kommutatiivsuse ja neelduvuse tõttu $a + b = ab + b = ba + b = b$.

PIISAVUS. Kui $b = a + b$, siis $ab = a(a + b) = (a + b)a = a$. □

Teoreem 10.7 1. Kui $(L, \leq)$ on võre definitsiooni 10.2 mõttes ja defineerime kahekohalised tehted $+$ ja $\cdot$ võrdustega

$$\begin{aligned}
 a + b &:= a \vee b, \\
 ab &:= a \wedge b,
 \end{aligned}$$

siis $(L, +, \cdot)$ on võre definitsiooni 10.5 mõttes.

2. Kui $(L, +, \cdot)$ on võre definitsiooni 10.5 mõttes ja defineerime seose $\leq$ järgmiselt:

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

siis $(L, \leq)$ on võre definitsiooni 10.2 mõttes. Selles võres

$$a \leq b \implies ac \leq bc \quad \text{ja} \quad a + c \leq b + c \quad (10.1)$$

mistahes $a, b, c \in L$ korral, s.t. järjestusseos on kooskõlas liitmise ja korrutamisega.

TÕESTUS. 1. Näitame, et kehtivad definitsiooni 10.5 parempoolses tulbas toodud samasused. Vasakpoolse tulba omaduste kontroll on sarnane.

Assotsiatiivsus. Veendume, et $(ab)c = a(bc)$ ehk $(a \wedge b) \wedge c = a \wedge (b \wedge c)$. Tähistame $d := (a \wedge b) \wedge c$ ja $e := a \wedge (b \wedge c)$. Siis $d \leq a \wedge b$ ja $d \leq c$, järelikult ka $d \leq a$ ja $d \leq b$. Seega $d \leq b \wedge c$ ning koos võrratusega $d \leq a$ saame, et $d \leq a \wedge (b \wedge c) = e$. Võrratuse $e \leq d$ tõestus on analoogiline. Järjestusseose antisümmeetria tõttu $e = d$.

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 x elementide $a \wedge b$ ja a suvaline ülemine tõke. Siis $a \wedge b \leq x$ ja $a \leq x$. Seega a on definitsiooni põhjal elementide $a \wedge b$ ja a ülemine raja, $a = (a \wedge b) \vee a$.

2. Veendume, et $\leq$ on järjestusseos.

Refleksiivsus. Kuna $aa = a$, siis $a \leq a$.

Antisümmeetria. Olgu $a \leq b$ ja $b \leq a$. Siis $a = ab$ ja $b = ba$. Järelikult $a = ab = ba = b$.

Transitiivsus. Olgu $a \leq b$ ja $b \leq c$. Siis $a = ab$ ja $b = bc$. Järelikult $a = ab = a(bc) = (ab)c = ac$, kust $a \leq c$.

Tõestame nüüd, et $a \wedge b = ab$, s.t. et ab on elementide a ja b alumine raja. Kasutame selleks alumise raja definitsiooni.

1) Kuna $(ab)a = a(ba) = a(ab) = (aa)b = ab$, siis $ab \leq a$. Et $(ab)b = a(bb) = ab$, siis $ab \leq b$.

2) Oletame, et $x \leq a$ ja $x \leq b$. Siis $x = xa$ ja $x = xb$. Järelikult $x(ab) = (xa)b = xb = x$ ehk $x \leq ab$. Sellega on näidatud, et $a \wedge b = ab$.

Kasutades seda, et $a \leq b$ parajasti siis, kui $b = a + b$ (vt. lauset 10.6), saab tõestada, et $a \vee b = a + b$. Kuna mistahes kahel elemendil leidub nii alumine kui ülemine raja, siis $(L, \leq)$ on võre definitsiooni 10.2 mõttes.

Tõestuse lõpetamiseks näitame, et kehtib implikatsioon (10.1). 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 $a + c \leq b + c$. $\square$

Järgnevas tutvume põgusalt kolme olulise võrede klassiga, need on täielikud võred, modulaarsed võred ja distributiivsed võred.

10.2 Täielikud võred

Definitsioon 10.8 Osaliselt järjestatud hulka L nimetatakse **täielikuks võreks**, kui selle mistahes alamhulgal on olemas nii ülemine kui alumine raja.

Definitsiooni järgi peab leiduma ka tühja alamhulga alumine ja ülemine raja. Kui $a := \bigwedge \emptyset$, siis iga element $b \in L$ on tühja hulga alumine tõke ja seega $b \leq a$. See tähendab, et a on järjestatud hulga L suurim element. Analoogiliselt saab näidata, et $\bigvee \emptyset$ on järjestatud hulga L vähim element. Seega igas täielikus võres peab leiduma suurim element (seda tähistatakse sümboliga 1) ja vähim element (tähistatakse sümboliga 0). Muuhulgas $1 = \bigvee L$ ja $0 = \bigwedge L$.

Näide 10.9 1. Kõik lõplikud võred on täielikud.

2. Hulga X alamhulkade võre $(\mathcal{P}(X), \cup, \cap)$ on täielik.
3. Naturaalarvude hulk $\mathbb{N}$ ja $\mathbb{N}$ võtmise suhtes on võre, mis ei ole täielik, sest puudub suurim element.
4. Reaalarvude järjestatud hulk $[0, 1]$ on täielik võre.
5. Ratsionaalarvude hulk $\mathbb{Q}$ ei ole täielik võre. Näiteks hulgal $\{a \in \mathbb{Q}^+ \mid 2 < a^2\}$ on lõpmata palju alumisi tõkkeid, aga puudub suurim alumine tõke ehk alumine raja.
6. Abeli rühma A kõigi alamrühmade hulk on täielik võre alamrühmade summa (ülemine raja) ja ühisosa (alumine raja) suhtes.
7. Topoloogia (lahtiste hulkade hulk) on täielik võre $\bigcup$ ja $(\cap)^\circ$ suhtes, kus $^\circ$ tähistab sisepunktide hulga võtmist.
8. Poolrühma kõigi ideaalide hulk on täielik võre $\cap$ ja $\cup$ suhtes.
9. Ringi kõigi ideaalide hulk on täielik võre $\cap$ ja $+$ suhtes.

Lause 10.10 Järjestatud hulga L korral on järgmised väited samaväärsed.

1. L on täielik võre.
2. Hulga L igal alamhulgal on olemas alumine raja.
3. Hulga L igal mittetühjal alamhulgal on olemas alumine raja ning hulk L sisaldab suurimat elementi.

TÕESTUS. $1 \Rightarrow 2 \Rightarrow 3$. See on ilmne.

$3 \Rightarrow 1$. Peame näitama, et mistahes alamhulgal leidub ülemine raja. Olgu $A \subseteq L$ ja vaatleme selle hulga kõigi ülemiste tõkete hulka A^Δ . Kuna $1 \in L$, siis $A^\Delta \neq \emptyset$ ja sellel hulgal peab leiduma alumine raja. Olgu $x = \bigwedge A^\Delta \in L$. Näitame, et $x = \bigvee A$. Selleks kasutame ülemise raja definitsiooni.

Kui $a \in A$, siis iga $d \in A^\Delta$ korral $a \leq d$. Seega a on hulga A^Δ alumine tõke. Järelikult $a \leq x$, sest x on alumine raja hulgale A^Δ . Kuna see võrratus kehtib iga $a \in A$ korral, siis x on hulga A ülemine tõke ja $x \in A^\Delta$.

Tesiest küljest $x \leq d$ iga $d \in A^\Delta$ korral. Sellega oleme tõestanud, et $x = \vee A$. $\square$

Tõestatud lause on väga kasulik, sest tihti on tingimust 2 või 3 lihtsam kontrollida kui tingimust 1. Järgmised kaks tulemust illustreerivad seda.

Lause 10.11 *Mistahes Ω -algebra A kõigi kongruentside hulk $\mathbf{Con}(A)$ on täielik võre.*

TÕESTUS. Vaatleme hulka $\mathbf{Con}(A)$ järjestatud hulgana sisalduvusseose $\subseteq$ suhtes. Kontrollime lause 10.10 tingimust 2. Selleks vaatleme alamhulka $\{\rho_i \mid i \in I\} \subseteq \mathbf{Con}(A)$. Näitame, et

$$\rho := \bigcap_{i \in I} \rho_i$$

on selle alamhulga alumine raja. On hästi teada, et ekvivalentsiseoste ühisosa on ekvivalentsiseos, seega ρ on ekvivalentsiseos. Näitame, et ta on ka kongruents (vt. definitsiooni 2.26). Iga $n \in \mathbb{N}$, iga teitemärgi $\omega \in \Omega_n$ ja mistahes elementide $a_1, \dots, a_n, b_1, \dots, b_n \in A$ korral

$$\begin{aligned} a_1 \rho b_1, \dots, a_n \rho b_n, &\implies (\forall i \in I)(a_1 \rho_i b_1, \dots, a_n \rho_i b_n,) && (\text{ühisosa def.}) \\ &\implies (\forall i \in I)(\omega^A(a_1, \dots, a_n) \rho_i \omega^A(b_1, \dots, b_n)) && (\rho_i \in \mathbf{Con}(A)) \\ &\implies \omega^A(a_1, \dots, a_n) \rho \omega^A(b_1, \dots, b_n). && (\text{ühisosa def.}) \end{aligned}$$

Seega $\rho \in \mathbf{Con}(A)$. On selge, et $\rho \subseteq \rho_i$ iga $i \in I$ korral. Kui $\sigma \in \mathbf{Con}(A)$ on selline, et $\sigma \subseteq \rho_i$ iga $i \in I$ korral, siis ka $\sigma \subseteq \bigcap_{i \in I} \rho_i = \rho$. Seega ρ on alumine raja. $\square$

Kuigi kongruentside alumise raja (s.o. ühisosa) leidmine on väga lihtne, on ülemise raja konstruktsioon mõnevõrra keerulisem. Antud tõestus seda ilmutatult ei kirjelda. Siiski ütleb tõestatud lause vähemalt seda, et selline ülemine raja on alati olemas.

Lause 10.12 *Mistahes Ω -algebra A kõigi alamalgebraate hulk $\mathbf{Sub}(A)$ on täielik võre.*

TÕESTUS. Vaatleme hulka $\mathbf{Sub}(A)$ järjestatud hulgana sisalduvusseose suhtes. Kontrollime jällegi lause 10.10 tingimust 2. Selleks vaatleme alamhulka $\{B_i \mid i \in I\} \subseteq \mathbf{Sub}(A)$. Näitame, et

$$B := \bigcap_{i \in I} B_i$$

on selle alamhulga alumine raja. Selleks näitame, et B on alamalgebra (vt. definitsiooni 2.9). Iga $n \in \mathbb{N}$, iga teitemärgi $\omega \in \Omega_n$ ja mistahes elementide $b_1, \dots, b_n \in B$ korral

$$\begin{aligned} b_1, \dots, b_n \in B &\implies (\forall i \in I)(b_1, \dots, b_n \in B_i) && (\text{ühisosa def.}) \\ &\implies (\forall i \in I)(\omega^A(b_1, \dots, b_n) \in B_i) && (B_i \in \mathbf{Sub}(A)) \\ &\implies \omega^A(b_1, \dots, b_n) \in B. && (\text{ühisosa def.}) \end{aligned}$$

Lisaks sellele iga $\omega \in \Omega_0$ korral $0_\omega^A \in B_i$ iga $i \in I$ korral ning järelikult $0_\omega^A \in B$. Seega $B \in \mathbf{Sub}(A)$. Nii nagu eelmises tõestuses näeme, et B on alumine raja. $\square$

Märkus 10.13 Viimane lause kehtib tänu sellele, et me lubame tühjasid alamalgebraid. See vaatepunkt on mõnevõrra ebatraditsiooniline, sest paljud algebraistid nõuavad alamalgebralt, et see oleks mittetühi. Samas mittetühjade alamalgebrate ühisosa võib mingitel juhtudel (nt. poolrühmade korral) olla tühi, seega sellisel juhul ei pruugi alumist raja leiduda. Kui algebras on nullkohalisi tehteid (nii on see näiteks monoidides, rühmades, ringides jne), siis seda probleemi muidugi ei ole. Ka kongruentside ühisosa puhul seda probleemi ei ole, sest mistahes hulga kongruentside ühisosa peab kindlasti sisaldama vähemalt võrdusseost.

Selle teema lõpetuseks tõestame veel ühe tulemuse täieliku võre teisenduste kohta.

Teoreem 10.14 *Täieliku võre L ja mistahes järjestust säilitava teisenduse $f : L \rightarrow L$ korral leidub element $x_0 \in L$ nii, et $f(x_0) = x_0$.*

TÕESTUS. Vaatleme hulka

$$P = \{x \in L \mid x \leq f(x)\} \subseteq L.$$

Olgu $x_0 = \bigvee P$. Kuna f säilitab järjestust, siis iga $x \in P$ korral

$$x \leq x_0 \Rightarrow f(x) \leq f(x_0) \Rightarrow x \leq f(x_0).$$

See tähendab, et $f(x_0)$ on hulga P ülemine tõke. Ülemise raja definitsiooni kohaselt nüüd $x_0 \leq f(x_0)$ ja veelkord kujutust f rakendades ka $f(x_0) \leq f(f(x_0))$. Seega $f(x_0) \in P$ ja kokkuvõttes $f(x_0) \leq \bigvee P = x_0 \leq f(x_0)$, kust $f(x_0) = x_0$. $\square$

Elementi x_0 nimetatakse teisenduse f **püsipunktiks**.

10.3 Modulaarsed võred

Lause 10.15 *Mistahes võre $(L, +, \cdot)$ ja elementide $a, b, c \in L$ korral*

1. $a + bc \leq (a + b)(a + c)$;
2. kui $a \leq c$, siis $a + bc \leq (a + b)c$.

TÕESTUS. 1. Tähistame $u := (a + b)(a + c)$. Kuna $a \leq a + b$ ja $a \leq a + c$, siis $a \leq u$. Et $b \leq a + b$ ja $c \leq a + c$, siis $bc \leq (a + b)c \leq (a + b)(a + c) = u$. Seega u on elementide a ja bc ülemine tõke. Järelikult

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

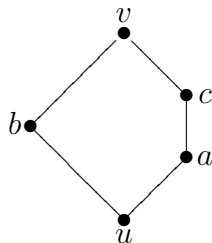
2. See järeldub eelmisest väitest, sest kui $a \leq c$, siis $a + c = c$. $\square$

Kui lause 10.15 viimase võrratuse asemel kehtib võrdus, siis kutsutakse võret modulaarseks.

Definitsioon 10.16 Võret $(L, +, \cdot)$ nimetatakse **modulaarseks**, kui mistahes $a, b, c \in L$ korral

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

Näide 10.17 Viieelemendiline võre



ei ole modulaarne. Tõepoolest, selles võres $a \leq c$, $(a+b)c = vc = c$ ja $a+bc = a+u = a$, seega $(a+b)c \neq a+bc$. Seda võret tähistatakse sümboliga N_5 .

Lause 10.18 Mooduli M_R (R on ring) alammodulite võre $(\text{Sub}(M), +, \cap)$ on modulaarne.

TÕESTUS. Olgu $A, B, C \in \text{Sub}(M)$ ja $A \subseteq C$. Tänu lause 10.15 teisele osale kehtib sisalduvus $A + B \cap C \subseteq (A + B) \cap C$. Seega peame veel näitama, et

$$(A + B) \cap C \subseteq A + B \cap C.$$

Võtame elemendi $c \in (A + B) \cap C$. Siis leiduvad $a \in A$ ja $b \in B$ nii, et $c = a + b$. Siis $a \in C$ ja $b = c - a \in C$. Seega $b \in B \cap C$ ja $c \in A + B \cap C$. $\square$

Eelmise lause erijuhtudena saame, et vektorruumi alamruumide võre ja Abeli rühma alamrühmade võre on modulaarsed.

Definitsioon 10.19 Võre $(L, +, \cdot)$ alamhulk K on **alamvõre**, kui ta on kinnine tehete $+$ ja $\cdot$ suhtes.

Teoreem 10.20 Võre L jaoks on järgmised väited samaväärsed.

1. L on modulaarne.
2. Kui $a, b, c \in L$, $a \geq b$, $a + c = b + c$ ja $ac = bc$, siis $a = b$.
3. L ei sisalda võrega N_5 isomorfset alamvõret.

TÕESTUS. 2. $\Rightarrow$ 1. Olgu $a, b, c \in L$ ja $a \leq c$. Siis

$$\begin{aligned}
 a + b &= (a + b)a + b && \text{(neelduvus)} \\
 &\leq (a + b)c + b && (a \leq c) \\
 &\leq (a + b)c + (a + b) && (b \leq a + b) \\
 &= a + b, && \text{(neelduvus)} \\
 bc &= (a + bc)bc && \text{(neelduvus)} \\
 &\leq (a + bc)b && (bc \leq b) \\
 &\leq (c + bc)b && (a \leq c) \\
 &= cb && \text{(neelduvus)} \\
 &= bc. && \text{(kommutatiivsus)}
 \end{aligned}$$

Tänu järjestusseose antisümmeetriaale 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

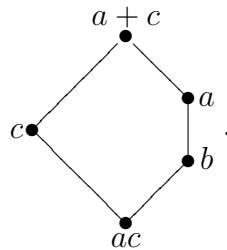
$$(a+b)c + b = (a+bc) + b, \quad (10.2)$$

$$(a+b)cb = (a+bc)b. \quad (10.3)$$

Lause 10.15(2) ütleb, et $a+bc \leq (a+b)c$. Rakendades nüüd tingimust 2 võrdustele (10.2) ja (10.3) saame järeldada, et $(a+b)c = a+bc$.

1. $\Rightarrow$ 3. Kui võre L sisaldaks võrega N_5 isomorfset alamvõret, siis ta ei saaks olla modulaarne.

3. $\Rightarrow$ 2. Oletame vastuväiteliselt, et leiduvad elemendid $a, b, c \in L$ nii, et $a > b$, $a+c = b+c$ ja $ac = bc$. Vaatleme elemente $a, b, c, a+c, ac \in L$. Kui nad oleksid paarikaupa erinevad, siis L sisaldaks võrega N_5 isomorfset alamvõret



Seega tõestuse lõpetamiseks piisab näidata, et tehtud eeldustel peavad need 5 elementi olema paarikaupa erinevad.

- Kuna $a > b$, siis $a \neq b$.
- Oletame, et $a = c$. Siis $c = cc = ac = bc$, kust $c \leq b$ ehk $a \leq b$, mis on vastuolus võrratusega $a > b$. Seega $a \neq c$.
- Oletame, et $a = a+c$. Siis

$$c \leq a \Rightarrow c = ac = bc \Rightarrow c \leq b \Rightarrow b = b+c = a+c = a,$$

mis on vastuolus võrratusega $a > b$.

- Oletame, et $a = ac$. Siis võrratustest $b < a$ ja $a \leq c$ järeldub, et $b \leq c$. Seega $b = bc = ac = a$, vastuolu.
- Oletame, et $b = c$. Siis $a+c = b+c = c+c = c$ ehk $a \leq c$. Järelikult $a = ac$ ja me saame vastuolu sarnaselt eelneva juhuga.
- Ka ülejäänud juhtudel tekib vastuolu. Jätame selle läbimõtlemiseks lugejale.

□

10.4 Distributiivsed võred

Definitsioon 10.21 Võret L nimetatakse **distributiivseks**, kui mistahes $a, b, c \in L$ korral

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

Lemma 10.22 Iga distributiivne võre on modulaarne.

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

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

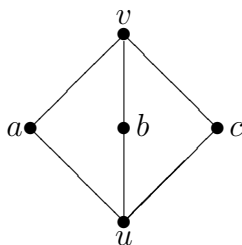
□

Näide 10.23 1. Hulga X alamhulkade võre $(\mathcal{P}(X), \cup, \cap)$ on distributiivne.

2. Naturaalarvude hulk suurima ühisteguri ja vähima ühiskordse võtmise suhtes on distributiivne võre.

3. Ahelad on distributiivsed võred.

4. Võre



ei ole distributiivne, sest

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

Seda võret tähistatakse lühidalt sümboliga M_3 .

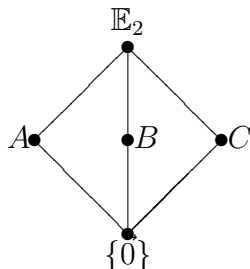
5. Vektorruumi V alamruumide võre $(\text{Sub}(V), +, \cap)$ ei ole üldjuhul distributiivne. Vaatleme näiteks tasandi vabavektorite vektorruumis $\mathbb{E}_2$ kolme mittekollineaarset vektorit $\vec{a}, \vec{b}, \vec{c}$ ja nende poolt tekitatud alamruume A, B, C . Siis

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

ja

$$A + B = A + C = B + C = \mathbb{E}_2.$$

Seega $\mathbb{E}_2$ alamruumide võre sisaldab võrega M_3 isomorfset alamvõret



ja ei saa olla distributiivne.

Järgmise kahe teoreemi tõestust me käesolevas kursuses anda ei jõua.

Teoreem 10.24 *Võre L on distributiivne parajasti siis, kui ta ei sisalda võredega N_5 ja M_3 isomorfseid alamvõresid.*

Teoreem 10.25 *Võre on distributiivne parajasti siis, kui ta on isomorfne mingi hulga X kõigi alamhulkade võre $(\mathcal{P}(X), \cup, \cap)$ mingi alamvõrega.*

Peatükk 11

Universaalalgebrad ja nende muutkonnad

11.1 Põhimõisted

Universaalalgebra on algebra valdkond, mis uurib algebralisi struktuure üldisest vaatepunktist, mitte keskendudes mingit konkreetset tüüpi struktuuridele (nt. rühmad, ringid). Peatükis 2 oleme juba mitmete universaalalgebra mõistetega tutvunud: Ω -algebrad, almalgebrad, homomorfismid, isomorfismid, kongruentsid, faktoralgebrad ja korrutised on defineeritud definitsioonides 2.4, 2.9, 2.12, 2.20, 2.26, lausele 2.28 järgnevas ja lausele 2.55 eelnevas lõigus, ning siin me neid definitsioone kordama ei hakka. Samuti oleme erinevate struktuuride puhul näinud, millist tüüpi Ω -algebratena (ehk universaalalgebratena) neid võib vaadelda.

Olgu $\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$ tüüp ehk signatuur (vt. definitsiooni 2.3). Meenutame, et **Ω -algebra** ehk **universaalalgebra** signatuuriga Ω on paar $(A, \{\omega^A \mid \omega \in \Omega\})$, kus

- A on hulk,
- igale tehtemärgile $\omega \in \Omega_n$, kus $n \in \mathbb{N} \cup \{0\}$, vastab üks n -kohaline algebraline tehe $\omega^A : A^n \longrightarrow A$.

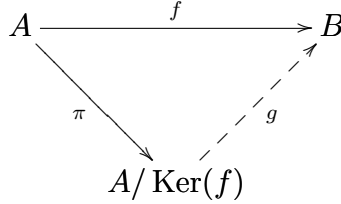
Hulka A nimetatakse universaalalgebra **kandjaks** ehk **põhihulgaks**. Universaalalgebrat ennast tähistatakse tavaliselt sümboliga **A**, et teda oma kandjast eristada. Seega **A** = $(A, \{\omega^A \mid \omega \in \Omega\})$.

Definitsioon 11.1 Olgu **A** ja **B** sama tüüpi algebrad. Homomorfismi $f : \mathbf{A} \rightarrow \mathbf{B}$ tuum $\text{Ker}(f)$ on binaarne seos

$$\text{Ker}(f) = \{(a, a') \in A \times A \mid f(a) = f(a')\}.$$

On lihtne veenduda, et homomorfismi f tuum on algebra **A** kongruents. Algebrate jaoks kehtivad järgmised teoreemi 2.35 ja järelduse 2.36 analoogid, mille tõestus on praktiliselt sama.

Teoreem 11.2 (Homomorfismiteoreem) Olgu $f : \mathbf{A} \rightarrow \mathbf{B}$ sama tüüpi algebrate homomorfism. Siis leidub üksühene homomorfism $g : \mathbf{A}/\text{Ker}(f) \rightarrow \mathbf{B}$ nii, et $f = g \circ \pi$, kus $\pi : \mathbf{A} \rightarrow \mathbf{A}/\text{Ker}(f)$ on loomulik projektsioon faktoralgebrale.



TÕESTUS. Defineerime kujutuse $g : A/\text{Ker } f \rightarrow U$ võrdusega

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

kus $\bar{a}$ on elemendi $a \in A$ ekvivalentsiklass seose $\text{Ker}(f)$ järgi. Kuna mistahes $a, b \in V$ korral

$$\bar{a} = \bar{b} \iff (a, b) \in \text{Ker } f \iff f(a) = f(b),$$

siis see definitsioon on korrektne ja g on üksühene. Sellest, et f on homomorfism tuleb kergesti välja, et ka g on homomorfism. Lisaks sellele $(g \circ \pi)(a) = g(\bar{a}) = f(a)$ iga $a \in A$ korral ja seega $g \circ \pi = f$. $\square$

Järeldus 11.3 Kui homomorfism $f : \mathbf{A} \rightarrow \mathbf{B}$ on sürjektiivne, siis $\mathbf{A}/\text{Ker}(f) \cong \mathbf{B}$.

Universaalalgebra on tihedalt seotud võreteooriaga. Peatükis 10 nägime, et algebra $\mathbf{A}$ kõigi alamalgebrate hulk $\text{Sub}(\mathbf{A})$ ja kõigi kongruentside hulk $\text{Con}(\mathbf{A})$ on täielikud võred. Nende kahe võre struktuurist saab tihti välja lugeda informatsiooni algebra $\mathbf{A}$ omaduste kohta.

11.2 Muutkonnad

Universaalalgebras uuritakse tihti mitte ühte konkreetset algebrat vaid sama tüüpi algebrate kogumeid, mis rahuldavad teatud samasusi. Selliseid kogumeid nimetatakse muutkondadeks. Range definitsiooni andmiseks on meil vaja termi mõistet.

Olgu $\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$ signatuur ja X mittetühi hulk. Me mõtleme X elementidest kui muutujatest (selles tähenduses nagu muutuja esineb polünoomi definitsioonis).

Definitsioon 11.4 (Ω, X) -termid defineeritakse järgmiste tingimuste abil.

1. Hulga $\Omega_0 \cup X$ elemendid on (Ω, X) -termid.
2. Kui $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $t_1, \dots, t_n$ on (Ω, X) -termid, siis “sõna” $\omega(t_1, \dots, t_n)$ on (Ω, X) -term.
3. Rohkem (Ω, X) -terme ei ole.

Termid on seega teatud reeglite abil tähestikus $\Omega \cup X \cup \{(\cup \})\} \cup \{,\}$ kirja pandud sõnad ehk sümbolite järjendid.

Märkus 11.5 Iga (Ω, X) -term definitsiooni 11.4 mõttes on term ka kursuse “Diskreetne matemaatika I” mõttes. Nimelt

- hulga Ω_0 elemente saame tõlgendada konstantsümbolitena,
- hulga $\bigsqcup_{n=1}^{\infty} \Omega_n$ elemendid loeme funktsionaalsümboliteks,
- predikaatsümbolid meil praegu signatuuris puuduvad.

Kõigi (Ω, X) -termide hulka tähistame sümboliga $F(X)$ (kasutusel on ka $T(X)$ ja $T(\Omega, X)$). Hulga $F(X)$ saab muuta Ω -algebraks, kui defineerida iga $\omega \in \Omega_0$ jaoks

$$\omega^{F(X)} := \omega \in F(X)$$

ning mistahes $n \in \mathbb{N}$, $\omega \in \Omega_n$ ja $t_1, \dots, t_n \in F(X)$ korral võtta

$$\omega^{F(X)}(t_1, \dots, t_n) := \omega(t_1, \dots, t_n) \in F(X). \quad (11.1)$$

Saadud algebrat $\mathbf{F}(X)$ nimetatakse **termide algebraks** või **absoluutselt vabaks algebraks** baasiga X ja signatuuriga Ω .

Näide 11.6 Olgu Ω ühikuga ringi signatuur, s.t. $\Omega = \{0, 1\} \cup \{-\} \cup \{+, \cdot\}$, ja $X = \{x, y\}$. Siis $F(X)$ elemendid on näiteks termid

$$((x + y) \cdot (x + 1)) + (-(y + x)), \quad x + y, \quad y + x.$$

Isegi kui me vaatleksime ainult kommutatiivseid ringe, on kaks viimast $F(X)$ elementi erinevad. Formaalselt peaksime definitsiooni 11.4 järgides $x+y$ asemel kirjutama $+(x, y)$, aga üldlevinud kokkuleppe kohaselt kirjutatakse kahekohaline tehtemärk argumentide vahele.

Algebras $\mathbf{F}(X)$ on näiteks elementide $x + y$ ja $y + x$ korrutiseks term $(x + y) \cdot (y + x)$.

Konkreetses termi $t \in F(X)$ korral on tihti otstarbekas välja tuua need muutujad, mis selles termis esineda võivad. Edaspidi kirjutame $t = t(x_1, \dots, x_n)$, kui muutujad hulgast $X \setminus \{x_1, \dots, x_n\}$ termis t kindlasti ei esine. Muutujad $x_1, \dots, x_n$ võivad, aga ei pea seal esinema. Näiteks saame ühikelemendiga ringi signatuuris kirjutada, et

$$t(x, y, z) = ((x + y) \cdot (x + 1)) + (-(y + x)).$$

Kui termis t on ülimalt n muutujat, siis seda termi nimetatakse **n -aarseks**. Näiteks üleelmise rea term on nii 2-aarne kui 3-aarne. Märgime, et nullaarsed termid on olemas ainult siis, kui $\Omega_0 \neq \emptyset$.

Kui $\mathbf{A}$ on Ω -algebra, siis iga n -aarne (Ω, X) -term tekitab loomulikul viisil ühe n -aarse funktsiooni $A^n \rightarrow A$. Kuna termid defineeriti induktiivselt, tuleb siin samamoodi teha.

Definitsioon 11.7 Kui $t = t(x_1, \dots, x_n) \in F(X) = T(\Omega, X)$ ja $\mathbf{A}$ on Ω -algebra, siis n -aarne funktsioon $t^A : A^n \rightarrow A$ defineeritakse järgmiselt:

1. kui $t = \omega \in \Omega_0$, siis mistahes $a_1, \dots, a_n \in A$ korral $t^A(a_1, \dots, a_n) = 0_\omega^A$, kus 0_ω^A on nullarse tehte ω poolt fikseeritud element hulgas A ,
2. kui $t = x \in X$, siis $x = x_i$ mingi $i \in \{1, \dots, n\}$ korral, ja funktsiooniks t^A võetakse **projektsioon** i -ndale komponendile, s.t. mistahes $a_1, \dots, a_n \in A$ korral

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

3. kui $t = t(x_1, \dots, x_n) = \omega(t_1, \dots, t_s) \in F(X)$ on term, kus $t_1, \dots, t_s$ on termid ja $\omega \in \Omega_s$, siis mistahes $a_1, \dots, a_n \in A$ korral

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

Paneme siin tähele, et eelmises lõigus sisse toodud “fiktiivsete” muutujate lisamine võimaldab meil muuta termid $t, t_1, \dots, t_s$ sama aarsusega n ja samade muutujatega $x_1, \dots, x_n$ termideks, sest termides t_i ei tohi esineda muutujaid, mis ei esine t -s.

Funktsioone t^A nimetatakse **termfunktsioonideks** algebral **A**. Kõigi termfunktsioonide hulka algebral **A** tähistatakse sümboliga T^A .

Märkus 11.8 Termfunktsioonide kohta saab teha järgmised tähelepanekud:

1. Kuna igas termis saab sisalduda vaid lõplik arv muutujaid, siis T^A sisaldab juba loenduva tähestiku X korral kõiki võimalikke termfunktsioone.
2. Kõik algebra **A** tehted ja kõik projektsioonid on termfunktsioonid.
3. Kui vaatleme muutujat $x \in X$ unaarse termina $t = x$, siis tema poolt tekitatud unaarne termfunktsioon (projektsioon) on samasusteisendus, $x^A(a) = a$ iga $a \in A$ korral.
4. Termfunktsioonide hulk on kinnine (mitmemuutuja) funktsioonide kompositsiooni suhtes.

Näide 11.9 Vaatleme täisarvude ringi $\mathbb{Z}$ Ω -algebrana signatuuris $\Omega = \{0, 1\} \cup \{-\} \cup \{+, \cdot\}$. Olgu $X = \{x_1, x_2, x_3\}$.

1. Term $t_1 = t_1(x_1) = ((1 + 1) + 1) \cdot (x_1 \cdot x_1)$ tekitab unaarse termfunktsiooni

$$t_1^{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad a \mapsto 3a^2.$$

2. Term $t_2 = t_2(x_1, x_2) = x_1 + x_2$ tekitab binaarse termfunktsiooni

$$t_2^{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (a, b) \mapsto a + b.$$

See termfunktsioon langeb kujutusena kokku ringi $\mathbb{Z}$ liitmistehtega.

3. Term $t_3 = t_3(x_1, x_2, x_3) = x_2$ tekitab ternaarse termfunktsiooni

$$t_3^{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (a, b, c) \mapsto b$$

(see on otsekorrutise $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ projektsioon teisele komponendile).

4. Erinevatele termidele vastavad termfunktsioonid võivad olla võrdsed. Näiteks $t_4^{\mathbb{Z}} = t_5^{\mathbb{Z}}$, kus

$$t_4 = x_1 + x_2, \quad t_5 = x_2 + x_1,$$

sest täisarvude liitmine on kommutatiivne. Sellisel juhul saame rääkida samasusest, s.t. algebra $\mathbb{Z}$ rahuldab samasust $x_1 + x_2 = x_2 + x_1$ (vt definitsiooni 11.11).

Lause 11.10 Iga Ω -algebra on isomorfne mingi absoluutselt vaba Ω -algebra faktoralgebraga.

TÕESTUS. Vaatleme Ω -algebrat $\mathbf{A}$. Võtame mingi hulga X , mille võimsus on sama kui A võimsus. (Selliseid hulki kindlasti leidub, näiteks võib võtta $X := A$.) Siis leidub bijektiivne kujutus $\rho : X \rightarrow A$. Olgu $\mathbf{F}(\mathbf{X})$ absoluutselt vaba Ω -algebra baasiga X . Defineerime kujutuse $f : F(X) \rightarrow A$ järgmiselt:

$$f(t(x_1, \dots, x_s)) = t^A(\rho(x_1), \dots, \rho(x_s)) \in A$$

iga termi $t(x_1, \dots, x_s) \in F(X)$ korral. See kujutus on surjektiivne, sest iga $a \in A$ korral leidub $x \in X$ nii, et

$$a = \rho(x) = x^A(\rho(x)) = f(x),$$

kus kasutame seda, et termi $t = x$ poolt tekitatud termfunktsioon $x^A : A \rightarrow A$ on samasusteisendus (vt. märkust 11.8).

Näitame, et kujutus f on Ω -algebrate homomorfism. Esiteks, iga $w \in \Omega_0$ korral $w^{F(X)} = w \in F(X)$ ja

$$f(w^{F(X)}) = f(w) = w^A = 0_\omega^A,$$

seega f säilitab null-aarseid tehteid. Olgu nüüd $n \in \mathbb{N}$, $w \in \Omega_n$ ja $t_1, \dots, t_n \in F(X)$. Eelneva kokkuleppe kohaselt võib termi aarsust alati suurendada. Seega kui $\{x_1, \dots, x_s\}$ on kõik muutujad, mis esinevad vähemalt ühes termidest $t_1, \dots, t_n$, siis saame kirjutada, et $t_i = t_i(x_1, \dots, x_s)$, $i = 1, \dots, n$, ning järelikult

$$\begin{aligned} f(\omega^{F(X)}(t_1, \dots, t_n)) &= f(\omega(t_1, \dots, t_n)) && (\text{def. (11.1)}) \\ &= \omega^A(t_1^A(\rho(x_1), \dots, \rho(x_s)), \dots, t_n^A(\rho(x_1), \dots, \rho(x_s))) && (f \text{ def.}) \\ &= \omega^A(f(t_1(x_1, \dots, x_s)), \dots, f(t_n(x_1, \dots, x_s))) && (f \text{ def.}) \\ &= \omega^A(f(t_1), \dots, f(t_n)). \end{aligned}$$

Seega f säilitab ka n -aarseid tehteid ja on homomorfism. Järeldust 11.3 kasutades saame, et $\mathbf{A} \cong \mathbf{F}(\mathbf{X}) / \text{Ker}(f)$. $\square$

Defineerime nüüd samasused ja muutkonnad. Muutkondade uurimine on universaalalgebra üks kesksmaid probleeme.

Definitsioon 11.11 Olgu Ω signatuur ja $u, v \in F(X) = T(\Omega, X)$, kus $X = \{x_1, x_2, \dots\}$ on loenduv hulk. Öeldakse, et Ω -algebral $\mathbf{A}$ kehtib **samasus** $u = v$, kui termidele u ja v vastavad termfunktsioonid on võrdsed, s.t. $u^A = v^A$.

Formaalselt on samasus tegelikult termide paar (u, v) , aga sisulise arusaamise lihtsustamiseks kirjutame selle üles kujul $u = v$. Paneme veel tähele, et termfunktsioonide võrduseks peavad termide u ja v aarsused kokku langema. Kui nad seda ei tee, siis me võime vastavalt varasemale kokkuleppele väiksema aarsusega termi aarsust sobivalt suurendada, lisades vajaliku arvu “fiktiivseid” muutujaid x_i . Siit on ka näha, miks me nõudsimme loenduvat muutujate arvu: me tahame, et oleks võimalik mistahes lõpliku aarsusega terme ja termfunktsioone võrrelda.

Definitsioon 11.12 Ω -algebrate klassi $\mathcal{K}$ nimetatakse **muutkonnaks**, kui leidub selline samasuste hulk S , et klassi $\mathcal{K}$ kuuluvad need ja ainult need algebrad, mis rahuldavad kõiki hulka S kuuluvaid samasusi.

Paljud varem selles kursuses käsitletud algebralised struktuurid moodustavad muutkonna (vt tabelit järgmisel lehel). Samas nii mitmedki tuntud struktuurid ei moodusta (üldiselt) muutkonda, näiteks lõplikud, jaguvad ja lahenduvad rühmad, korpused, injektiivsed ja projektiivsed moodulid.

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

- samasuste abil,
- kinnisuse abil teatavate operatsioonide suhtes.

Märgime, et Ω -algebrate klassi nimetatakse **triviaalseks**, kui see koosneb ainult triviaalsetest algebratest, s.t. ühe-elementilistest algebratest ja tühjast algebrast.

Teoreem 11.13 (Birkhoff) *Mittetriviaalne Ω -algebrate klass on muutkond parajasti siis, kui see on kinnine alamalgebrate, faktoralgebrate ja (mistahes võimsusega) otsekorrutiste võtmise suhtes.*

Birkhoffi teoreemi kutsutakse operatsioonide nimede järgi mõnikord ka *HSP*-teoreemiks (need tähed tulevad terminitest *homomorphic image*, *subalgebra*, *direct product*).

Mistahes Ω -algebra $\mathbf{A}$ puhul leidub vähim Ω -algebrate muutkond $\text{Var}(\mathbf{A})$, mis seda algebrat sisaldab. On võimalik näidata, et

$$\text{Var}(\mathbf{A}) = HSP(\mathbf{A}),$$

s.t. see muutkond koosneb $\mathbf{A}$ otseastmete alamalgebrate homomorfsetest kujutistest (faktoralgebratest).

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	$\Omega_1 = \{\cdot'\}$ $\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $x \cdot x' \cdot x = x, x' \cdot x \cdot x' = x'$
Monoidid	$\Omega_0 = \{1\}$ $\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $1 \cdot x_1 = x_1, x_1 \cdot 1 = x_1$
Rühmad	$\Omega_0 = \{1\}$ $\Omega_1 = \{-1\}$ $\Omega_2 = \{\cdot\}$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $1 \cdot x_1 = x_1, x_1 \cdot 1 = x_1$ $x_1 \cdot x_1^{-1} = 1, x_1^{-1} \cdot x_1 = 1$
Abeli rühmad	$\Omega_0 = \{0\}$ $\Omega_1 = \{-\}$ $\Omega_2 = \{+\}$	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ $0 + x_1 = x_1, x_1 + 0 = x_1$ $x_1 + (-x_1) = 0, (-x_1) + x_1 = 0$ $x_1 + x_2 = x_2 + x_1$
Ringid	$\Omega_0 = \{0\}$ $\Omega_1 = \{-\}$ $\Omega_2 = \{+, \cdot\}$	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ $0 + x_1 = x_1, x_1 + 0 = x_1$ $x_1 + (-x_1) = 0, (-x_1) + x_1 = 0$ $x_1 + x_2 = x_2 + x_1$ $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$ $(x_1 + x_2) \cdot x_3 = x_1 \cdot x_3 + x_2 \cdot x_3$
Võred	$\Omega_2 = \{\wedge, \vee\}$	$x_1 \vee (x_2 \vee x_3) = (x_1 \vee x_2) \vee x_3$ $x_1 \vee x_2 = x_2 \vee x_1$ $x_1 \vee x_1 = x_1$ $(x_1 \vee x_2) \wedge x_1 = x_1$ $x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3$ $x_1 \wedge x_2 = x_2 \wedge x_1$ $x_1 \wedge x_1 = x_1$ $(x_1 \wedge x_2) \vee x_1 = x_1$
S -polügonid	$\Omega_1 = \{\cdot s \mid s \in S\}$	$(x_1 \cdot s) \cdot t = x_1 \cdot (st)$ ($ S ^2$ samasust)
R -moodulid	$\Omega_1 = \{r \cdot \mid r \in R\}$ $\Omega_2 = \{+\}$	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ $0 + x_1 = x_1, x_1 + 0 = x_1$ $x_1 + (-x_1) = 0, -x_1 + x_1 = 0$ $x_1 + x_2 = x_2 + x_1$ $r \cdot (x_1 + x_2) = r \cdot x_1 + r \cdot x_2$ ($ R $ samasust) $(r + s) \cdot x_1 = r \cdot x_1 + s \cdot x_1$ ($ R ^2$ samasust) $r \cdot (s \cdot x_1) = (rs) \cdot x_1$ ($ R ^2$ samasust)
Üheelemendilised algebrad	Ω	$x_1 = x_2$
Kõik algebrad signatuuriga Ω	Ω	$x_1 = x_1$

Väike eesti-inglise algebrasõnastik

Abeli rühm — *abelian group*
ahel — *chain*
alamalgebra — *subalgebra*
alampolügoon — *subact*
alamruum — *subspace*
algebra — *algebra*
algebraalne struktuur — *algebraic structure*
algebraalne tehe — *algebraic operation*
algobjekt — *initial object*
alumine raja — *meet*
automorfism — *automorphism*
baas — *basis*
bimorfism — *bimorphism*
distributiivne võre — *distributive lattice*
distributiivsus — *distributivity*
duaalne kategooria — *opposite category*
endomorfism — *endomorphism*
epimorfism — *epimorphism*
epimorfne kujutis — *epimorphic image*
faktoralgebra — *quotient algebra, factor algebra*
faktorhulk — *quotient set*
faktoriseeruv — *factorisable*
faktorpolügon — *quotient act, factor act*
faktorrühm — *quotient group, factor group*
Greeni seosed — *Green's relations*
homomorfism — *homomorphism*
homomorfismiteoreem — *homomorphism theorem*
ideaal — *ideal*
idempotent — *idempotent*
injektiivne — *injective*
isomorfism — *isomorphism*
isomorfismiteoreem — *isomorphism theorem*
jada — *sequence*
jagamisega ring — *division ring*
jagatis — *quotient*
jaguv — *divisible*
juur — *root*
järjend — *tuple*
järk — *order*
kategooria — *category*
kokorrutis — *coproduct*
kommutatiivne diagramm — *commutative diagram*

kongruents — *congruence*
 kordaja — *coefficient*
 koretraktsioon — *coretraction*
 korpus — *field*
 korpuse karakteristika — *the characteristic of a field*
 korrutis — *product*
 kujutis — *image*
 kõrvalklass — *coset*
 lahutumatu polügon — *indecomposable act*
 lahutuskorpus — *splitting field*
 laiend — *enlargement, extension*
 lame moodul — *flat module*
 lihtne — *simple*
 lineaarkombinatsioon — *linear combination*
 lineaarkujutus — *linear mapping*
 lineaarselt järjestatud hulk — *linearly ordered set*
 lineaarselt sõltumatu — *linearly independent*
 lineaarselt sõltuv — *linearly dependent*
 lineaarteisendus — *linear transformation*
 loomulik projektsioon — *natural projection*
 lõplik korpus — *finite field*
 lõppobjekt — *terminal object*
 lühike täpne jada — *short exact sequence*
 maksimaalne element — *maximal element*
 minimaalne ideaal — *minimal ideal*
 modulaarne võre — *modular lattice*
 monoid — *monoid*
 monomorfism — *monomorphism*
 moodul — *module*
 morfism — *morphism*
 Morita kontekst — *Morita context*
 Morita ekvivalentsus — *Morita equivalence*
 muutkond — *variety*
 n -kohaline tehe — *n -ary operation*
 normaaljagaja — *normal subgroup*
 nullelement — *zero element*
 nullobjekt — *zero object*
 nullvektor — *null vector*
 nõrgad lokaalsed ühikelemendid — *weak local units*
 objekt — *object*
 osaliselt järjestatud hulk — *partially ordered set, poset*
 otseaste — *direct power*
 otsekorrutis — *direct product*
 otsesumma — *direct sum*
 parempoolne ideaal — *right act*

parempoolne kongruents — *right congruence*
 parempoolne moodul — *right module*
 parempoolne polügon — *right act*
 peaideaal — *principal ideal*
 pere — *family*
 perioodiline osa — *torsion subgroup*
 perioodiline rühm — *periodic group*
 permutatsioon — *permutation*
 polügon — *act*
 poolrühm — *semigroup*
 primitiivne idempotent — *primitive idempotent*
 projektiivne — *projective*
 pärisideaal — *proper ideal*
 pöördelement — *inverse element*
 püsipunkt — *fixed point*
 püsiv polügon — *firm act*
 Reesi maatrikspoolrühm — *Rees matrix semigroup*
 retraktsioon — *retraction*
 ring — *ring*
 rühm — *group*
 samasus — *identity*
 signatuur — *signature*
 sisemine otsesumma — *internal direct sum*
 skalaar — *scalar*
 substitutsioon — *permutation*
 sõltumatud tsüklid — *independent cycles*
 tasakaalustatud kujutus — *balanced mapping*
 tehe — *operation*
 tensorkorrutis — *tensor product*
 term — *term*
 termfunktsioon — *term function*
 termine algebra — *term algebra*
 toime — *action*
 transpositsioon — *transposition*
 tsükkel — *cycle*
 tsükliline polügon — *cyclic act*
 tuum — *kernel*
 tõke — *bound*
 täielik alamkategooria — *full subcategory*
 täiesti lihtne poolrühm — *completely simple semigroup*
 täielik võre — *complete lattice*
 täpne — *exact*
 täpne jada — *exact sequence*
 tüüp — *type*
 unitaarne polügon — *unitary act*

universaalalgebra — *universal algebra*
 universaalomadus — *universal property*
 vaba — *free*
 vastandelement — *additive inverse*
 vektor — *vector*
 vektorruum — *vector space, linear space*
 võre — *lattice*
 väline otsesumma — *(external) direct sum*
 väändeta Abeli rühm — *torsion-free abelian group*
 ühikelement — *identity element*
 ühiksubstitutsioon — *identity permutation*
 ülemine raja — *join*
 ülemine tõke — *upper bound*

Indeks

- n -kohaline algebraline tehe, 25
- alamkategooria, 13
 - täielik, 13
- alamvõre, 163
- algebra üle korpuse, 80
- algoritm, 15
- distributiivsuse seadused, 69
- ekvivalentsed kategooriad, 20
- elementaartensor, 105
- endomorfism, 12
- epimorfism, 13
- faktoriseeruv poolrühm, 116
- faktorpolügon, 128
- faktoring, 151
- funktor, 16
 - kontravariantne, 17
 - kovariantne, 16
- funktori samasusteisendus, 20
- Greeni lemma, 119
- Greeni seos, 117
- hom-funktor
 - kontravariantne, 18
 - kovariantne, 18
- idempotent, 113
- injektiivne objekt, 16
- inversne element, 126
- inversne poolrühm, 126
- isomorfism, 14
- isomorfsed objektid, 14
- kategooria, 11
 - suur, 12
 - väike, 12
- kokorrutis, 22, 23
- kokorrutise sisestus, 23
- kokorrutise sisestused, 22
- konkreetne kategooria, 13
- konstantne funktor, 18
- korpus, 69, 145
- korpuse
 - karakteristika, 145
 - laiend, 147
- korpuste isomorfism, 147
- korrutis, 21, 22
- korrutise projektsioon, 22
- lõplik korpus, 145
- lahutumatu polügon, 129
- lihtne korpus, 147
- lihtne poolrühm, 116
- lineaarkombinatsioon, 38
- lineaarkombinatsiooni
 - kordajad, 38
- lineaarkujutus, 30
- lineaarne
 - sõltumatus, 38
 - sõltuvus, 38
- lineaarne ruum, 26
- loomulik isomorfism, 19
- loomulik teisendus, 19
- loomulikult isomorfsed funktorid, 19
- lõppobjekt, 15
- minimaalne vasakpoolne ideaal, 114
- monoid, 113
- monomorfism, 13
- moodul, 85
- morfismide kompositsioon, 11
- Morita ekvivalentsus, 139
- Morita kontekst, 139
- nullobjekt, 15

nullvektor, 27
 nõrgad lokaalsed ühikelemendid, 141

 peaideaal, 115
 polünoomi lahutuskorpus, 152
 polügoni kongruents, 128
 polügonide tensorkorrutis, 135
 poolrühm, 113
 poolrühma ideaal, 114
 poolrühma laiend, 142
 poolrühma ühikelement, 113
 primitiivne idempotent, 119
 projektiivne moodul, 97
 projektiivne objekt, 15
 projektiivne polügon, 131
 pärisideaal, 116
 püsiv polügon, 138

 rühm, 45
 Reesi maatrikspoolrühm, 122
 regulaarne poolrühm, 125
 retrakt, 15
 ring, 69
 ristkülikpoolrühm, 118

 sisestusfunktor, 17
 skalaar, 27
 summa, 22
 suur kategooria, 12

 tasakaalustatud kujutus, 100, 135
 tensor, 105
 tensorkorrutis
 homomorfismide, 106
 moodulite, 100
 universaalomadus, 103
 tsükliline polügon, 128
 täielik alamkategooria, 13
 täiesti lihtne poolrühm, 120

 unitaarne polügon, 127
 unustav funktor, 18

 vastandvektor, 27
 vektor, 27
 vektorruum, 26
 väike kategooria, 12

 ühikfunktor, 17

Kasutatud kirjandus

1. M. Kilp, Algebra I, Eesti Matemaatika Selts, Tartu, 2005.
2. M. Kilp, Algebra II, Tartu, 1998.
3. K. Kaarli, Sissejuhatus universaalalgebrasse, Tartu, 1989.
4. K. Väljako, Idempotentsete ringide Morita ekvivalentsus, Tartu Ülikooli Kirjastus, Tartu, 2025.
5. Y. Chen, K. P. Shum. Projective and indecomposable S -acts, Sci. China Ser. A, 42 (1999), 593–599.
6. V. Laan, Ü. Reimaa, Morita equivalence of factorizable semigroups, Internat. J. Algebra Comput. 29 (2019), 723–741.
7. M. Kilp, O ploskih poligonah (vene keeles), Tartu Riikl. Ül. Toimetised 253 (1970), 66–72.
8. M. V. Lawson, Enlargements of regular semigroups, Proc. Edinburgh Math. Soc. (2) 39 (1996), 425–460.