

RÜHMATEORIA

Sügis 2025

Loengukonspekt

Lektor: Valdis Laan

5. detsember 2025. a.

Sisukord

1	Põhimõisted ja -konstruktsioonid	4
1.1	Rühm	4
1.2	Homomorfism	5
1.3	Alamrühm	8
1.4	Dieedri rühm	10
1.5	Rühmade otsekorutis	12
1.6	Kõrvalklassid, Lagrange'i teoreem	13
1.7	Faktorrühm	15
2	Isomorfismiteoreemid	18
3	Rühma elemendi järk ja tsüklilised rühmad	22
3.1	Tsüklilised rühmad	22
3.2	Rühma elemendi järk	24
4	Teisenduste rühmad	26
4.1	Cayley teoreem	26
4.2	Sümmeetrilised rühmad lõplikel hulkadel	27
4.3	Rubiku kuubiku rühm	31
5	Rühma toimed	32
6	Sylowi teoreemid	35
7	Rühmade otsesummad	39
7.1	Sisemised otsesummad üldjuhul	39
7.2	Sisemised ja välised otsesummad	41
7.3	Otsesummad Abeli rühmade korral	42
7.4	Rakendus: 15-ndat järku rühmade kirjeldus	43
8	Perioodilised ja lõplikud Abeli rühmad	45
8.1	Perioodilised Abeli rühmad	45
8.2	Lõplikud Abeli p -rühmad	47
9	Vabad rühmad	50
9.1	Vaba rühma definitsioon	50
9.2	Vaba rühma konstruktsioon	51
10	Lihtsad rühmad	57
11	Lahenduvad rühmad	61
A	Lisa 1: Rühmade esitused tekitajate ja seoste abil	67
B	Lisa 2: Vabad Abeli rühmad	71

Sissejuhatus

Tegemist on 2025. aasta sügisel Tartu Ülikoolis loetud kursuse “Rühmateooria” loengukonspektiga.

Soovin tänada üliõpilast Aleksei Ganyukovi, kes leidis konspektist mitmeid vigu ja aitas neid parandada.

Loengute ajakava

1. Põhimõisted.
2. Põhimõisted.
3. Faktorrühmad.
4. Isomorfismiteoreemid.
5. Tsüklilised rühmad.
6. Teisenduste rühmad.
7. Rühma toimed.
8. Sylowi teoreemid.
9. Sylowi teoreemid.
10. Rühmade otsesummad.
11. Lõplikud Abeli rühmad.
12. Lõplikud Abeli rühmad.
13. Vabad rühmad.
14. Vabad rühmad.
15. Lihtsad rühmad.
16. Lahenduvad rühmad.

1 Põhimõisted ja -konstruktsioonid

1.1 Rühm

Definitsioon 1.1 Rühm on hulk G koos kahekohalise algebralise tehtega $*$, mis rahuldab tingimusi

- G1.** iga $a, b, c \in G$ korral $(a * b) * c = a * (b * c)$;
- G2.** leidub element $e \in G$ nii, et iga $a \in G$ korral $e * a = a = a * e$;
- G3.** iga $a \in G$ jaoks leidub element $a^{-1} \in G$ nii, et $a * a^{-1} = e = a^{-1} * a$.

Elementi e nimetatakse rühma **ühikelemendiks** ja elementi a^{-1} nimetatakse elemendi a **pöördelemendiks**. Tehet $*$ nimetatakse harilikult rühma **korrumisteheteks**.

Märkus 1.2 Kui on rahuldatud ainult tingimus G1, siis öeldakse, et paar $(G, *)$ on **poolrühm**. Kui on rahuldatud tingimused G1 ja G2, siis räägitakse **monoidist**. Muuhulgas võib öelda, et rühm on monoid, mille iga element on pööratav.

Märkus 1.3 Kursusest “Algebra I” teame järgmisi fakte, mille tõestust me siin üle kordama ei hakka.

1. Igas rühma elementidest, korrumistehete märgist ja sulgudest moodustatud korrektses avaldises ei sõltu avaldise väärtus sulgude paigutusest. Tänu sellele võime sellistes avaldistes sulud ära jätta.
2. Rühma ühikelement on üheselt määratud.
3. Rühma iga elemendi pöördelement on üheselt määratud.
4. Rühma $(G, *)$ mistahes elementide a, b korral

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

Edaspidises tähistame rühma ühikelementi enamasti sümboliga 1 (või sümboliga 1_G , kui on vaja rõhutada, et on tegemist rühma G ühikelemendiga) ja kirjutame $a * b$ asemel ab .

Definitsioon 1.4 Rühma, mille tehe on kommutatiivne, nimetatakse **kommutatiivseks** ehk **Abeli rühmaks**.

Näide 1.5 1. $(\mathbb{R} \setminus \{0\}, \cdot)$ ja $(\mathbb{R}^+, \cdot)$ on Abeli rühmad.

2. $(\mathbb{Z}, +)$ ja $(\mathbb{Z}_n, +)$ on Abeli rühmad.

3. Kui X on hulk milles on vähemalt 3 elementi, siis selle hulga bijektiivsete teisenduste hulk $\mathcal{S}(X)$ on mittekommutatatiivne rühm teisenduste järjestakendamise suhtes.

4. Kui K on korpus ja $n \geq 2$, siis n -ndat järku regulaarsete ruutmaatriksite hulk $GL_n(K)$ on mittekommutatatiivne rühm maatriksite korrumistehetega.

5. Ühejuurte hulk $H_n = \{w \in \mathbb{C} \mid w^n = 1\}$ on Abeli rühm kompleksarvude korrumistehetega suhtes.

Rühmades arvutades kasutame edaspidises pidevalt järgmisi arvutusreegleid.

Lemma 1.6 Rühma G mistahes elementide a, b, c korral

$$ab = c \implies a = cb^{-1} \text{ ja } b = a^{-1}c.$$

TÕESTUS. Eeldame, et $ab = c$. Siis

$$cb^{-1} = (ab)b^{-1} = a(bb^{-1}) = a1 = a.$$

Võrduse $b = a^{-1}c$ saab tõestada analoogiliselt. □

Defineerime rühma elementide täisarvulised astmed.

Definitsioon 1.7 Olgu a rühma G element ja k täisarv. Siis

$$a^k := \begin{cases} \underbrace{aa \dots a}_{k \text{ tegurit}}, & \text{kui } k > 0, \\ 1, & \text{kui } k = 0, \\ \underbrace{a^{-1}a^{-1} \dots a^{-1}}_{-k \text{ tegurit}}, & \text{kui } k < 0. \end{cases}$$

Lemma 1.8 Kui a on rühma G element ja $k, l \in \mathbb{Z}$, siis

$$a^k a^l = a^{k+l} \text{ ja } (a^k)^l = a^{kl} = (a^l)^k.$$

Muuhulgas $(a^k)^{-1} = (a^{-1})^k$.

TÕESTUS. Tõestuse jätame iseseisvaks läbimõtlemiseks lugejale. □

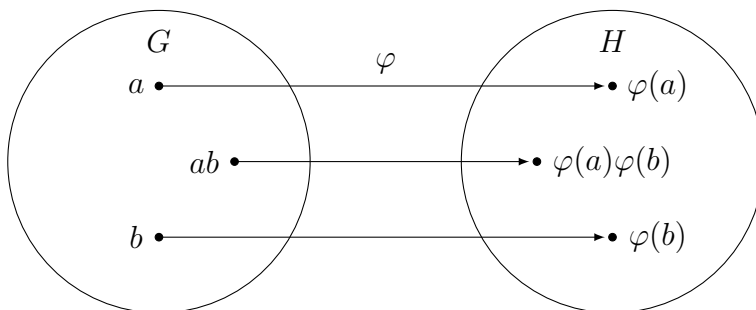
Selles paragrahvis ära toodud arvutusreegleid kasutame edaspidi ilma viitamata.

1.2 Homomorfism

Definitsioon 1.9 Olgu G ja H rühmad. Kujutust $\varphi : G \longrightarrow H$ nimetatakse **rühmade homomorfismiks**, kui iga $a, b \in G$ korral

$$\varphi(ab) = \varphi(a)\varphi(b)$$

(s.t. φ säilitab korrutamist).



Lause 1.10 Kui $\varphi : G \rightarrow H$ on rühmade homomorfism, siis

- $\varphi(1_G) = 1_H$, s.t. φ säilitab ühikelementi;

- iga $a \in G$ korral $\varphi(a^{-1}) = (\varphi(a))^{-1}$, s.t. φ säilitab pöördelmente.

TÕESTUS. Eeldame, et kujutus $\varphi : G \rightarrow H$ säilitab korrutamist. Kuna rühmas G kehtib võrdus $1_G \cdot 1_G = 1_G$, siis rühmas H kehtib tänu eeldusele võrdus $\varphi(1_G)\varphi(1_G) = \varphi(1_G)$. Korrutades selle võrduse mõlemad pooli elemendiga $\varphi(1_G)^{-1}$ ja kasutades rühma tehete omadusi saame võrduse $\varphi(1_G) = 1_H$. Seega φ säilitab ühikelementi. Kui nüüd $a \in G$, siis

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1_G) = 1_H.$$

Analoogiliselt $\varphi(a)\varphi(a^{-1}) = 1_H$. Seega $\varphi(a^{-1}) = (\varphi(a))^{-1}$. $\square$

Näide 1.11 Selles kursuses tähistame sümboliga K^* korpuse K nullist erinevate elementide hulka. Nagu teame, on hulk K^* rühm korpuse korrutamistehte suhtes. Muuhulgas võime vaadelda rühma $\mathbb{R}^*$.

Kujutus

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

on rühmade homomorfism, sest mistahes $x, y \in \mathbb{R}^*$ korral

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

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

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

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

Kas kahe homomorfismi järjestrakendamisel (kui see on võimalik) saame ka homomorfismi? Olgu antud rühmad G, H ja K ning nende vahelised homomorfismid $\varphi : G \rightarrow H$ ja $\psi : H \rightarrow K$. Siis nende kujutuste korrutis $\psi \circ \varphi : G \rightarrow K$ on defineeritud eeskirjaga

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

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

Lause 1.12 Kui $\varphi : G \rightarrow H$ ja $\psi : H \rightarrow K$ on rühmade homomorfismid, siis ka $\psi \circ \varphi$ on rühmade homomorfism.

TÕESTUS. Mistahes $a, b \in G$ korral

$$\begin{aligned} (\psi \circ \varphi)(ab) &= \psi(\varphi(ab)) && (\psi \circ \varphi \text{ def.}) \\ &= \psi(\varphi(a)\varphi(b)) && (\varphi \text{ on homomorfism}) \\ &= \psi(\varphi(a))\psi(\varphi(b)) && (\psi \text{ on homomorfism}) \\ &= (\psi \circ \varphi)(a)(\psi \circ \varphi)(b). && (\psi \circ \varphi \text{ def.}) \end{aligned}$$

$\square$

Definitsioon 1.13 Homomorfismi mingist rühmast iseendasse nimetatakse selle rühma endomorfismiks.

Rühma G kõigi endomorfismide hulka tähistatakse sümboliga $\text{End}(G)$. On selge, et rühma G samasusteisendus id_G on selle rühma endomorfism ja et kahe endomorfismi korrutis on alati defineeritud.

Lause 1.14 Iga rühma G korral on hulk $\text{End}(G)$ monoid kujutuste korrutamise suhtes.

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

Definitsioon 1.15 Bijektiivset homomorfismi nimetatakse **isomorfismiks**.

Definitsioon 1.16 Rühmi G ja H nimetatakse **isomorfseteks**, kui leidub isomorfism $\varphi : G \rightarrow H$.

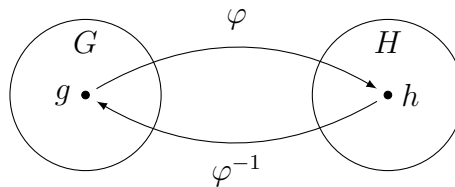
Asjaolu, et rühmad G ja H on isomorfsed, märgitakse kirjutades $G \simeq H$ või $G \cong H$.

Nii nagu ei saa rääkida kõigi hulkade hulgast, ei saa rääkida ka kõigi rühmade hulgast. Küll aga saab rääkida kõigi rühmade klassist.

Lause 1.17 Isomorfisusseos on ekvivalentsiseos kõigi rühmade klassil, s.t. ta on reflekstiivne, sümmeetriline ja transitiivne.

TÕESTUS. On selge, et iga rühma G korral on samasusteisendus $\text{id}_G : G \rightarrow G$ isomorfism ja seega $G \simeq G$. Samuti on selge, et kahe isomorfismi korrutis on isomorfism ja seega on isomorfisusseos transitiivne. Veendume, et seos $\simeq$ on sümmeetriline. Olgu $G \simeq H$ ja leidugu rühmade isomorfism $\varphi : G \rightarrow H$. Kuna φ on bijektiivne, siis on tal olemas pöördkujutus $\varphi^{-1} : H \rightarrow G$, kusjuures mistahes $h \in H$ ja $g \in G$ korral

$$\varphi^{-1}(h) = g \iff \varphi(g) = h. \quad (1)$$



Hulgateooriast teame, et kujutus φ^{-1} on bijektiivne. Jääb veel näidata, et ta on homomorfism. Olgu nüüd $h_1, h_2 \in H$. Kujutuse φ sürjektiivsuse tõttu leiduvad sellised elemendid $g_1, g_2 \in G$, et $\varphi(g_1) = h_1$ ja $\varphi(g_2) = h_2$. Siis

$$\begin{aligned} \varphi^{-1}(h_1 h_2) &= \varphi^{-1}(\varphi(g_1) \varphi(g_2)) \\ &= \varphi^{-1}(\varphi(g_1 g_2)) && (\varphi \text{ on homomorfism}) \\ &= (\varphi^{-1} \circ \varphi)(g_1 g_2) && (\varphi^{-1} \circ \varphi \text{ def.}) \\ &= \text{id}_G(g_1 g_2) && (\varphi^{-1} \circ \varphi = \text{id}_G) \\ &= g_1 g_2 && (\text{id}_G \text{ def.}) \\ &= \varphi^{-1}(h_1) \varphi^{-1}(h_2). && (\text{omadus (1)}) \end{aligned}$$

Seega $\varphi^{-1} : H \rightarrow G$ on rühmade homomorfism ja kokkuvõttes isomorfism. Viimane tähendab, et $H \simeq G$, mida oligi tarvis tõestada. $\square$

Definitsioon 1.18 Bijektiivset endomorfismi nimetatakse **automorfismiks**.

Rühma G kõigi automorfismide hulka tähistatakse sümboliga $\text{Aut}(G)$.

Lause 1.19 Iga rühma G korral on hulk $\text{Aut}(G)$ rühm kujutuste korrutamise suhtes.

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

Näide 1.20 Olgu G rühm ja $x \in G$ mingi element. Siis kujutus

$$\varphi_x : G \longrightarrow G, \quad g \mapsto x^{-1}gx =: g^x$$

on rühma G automorfism. (Miks ta on homomorfism? Mis on tema pöördkujutus?) Automorfisme $\varphi_x, x \in G$, nimetatakse rühma G **siseautomorfismideks**. Elementi g^x nimetatakse elemendi g **kaaselemendiks** x suhtes.

1.3 Alamrühm

Definitsioon 1.21 Rühma G mittetühja alamhulka H nimetatakse **alamrühmaks** (ja kirjutatakse $H \leq G$), kui iga $h, k \in H$ korral $hk \in H$ ja $h^{-1} \in H$.

Sama definitsiooni sõnastatakse mõnikord lühemalt öeldes: rühma mittetühi alamhulk on alamrühm, kui ta on kinnine korrutamise ja pöördlemendi võtmise suhtes. Kui $h \in H \leq G$, siis ka $h^{-1} \in H$ ning järelikult $1_G = hh^{-1} \in H$. Niisiis rühma G iga alamrühm peab sisaldama selle rühma ühikelementi.

Rühma G kõigi alamrühmade hulka tähistatakse $\text{Sub}(G)$.

Rühma G alamrühma H nimetatakse **pärisalamrühmaks**, kui $H \neq G$. Sellisel juhul kirjutatakse $H < G$.

Järgmine lause on lihtsasti tõestatav.

Lause 1.22 Rühma G mittetühja alamhulga H jaoks on järgmised väited samaväärsed:

1. H on G alamrühm;
2. iga $h, k \in H$ korral $hk^{-1} \in H$;
3. iga $h, k \in H$ korral $h^{-1}k \in H$.

Järgmine väide on ilmne.

Lemma 1.23 Kui H on rühma $(G, *)$ alamrühm, siis on H ise ka rühm G korrutamise poolt indutseeritud korrutamistehete $*$ ' suhtes, mis on defineeritud võrdusega

$$h *' k := h * k$$

iga $h, k \in H$ korral.

Reeglina muidugi alamrühma puhul kasutatakse sama tehtemärki nagu terve rühma puhul. Näiteks rühma $(\mathbb{R}, +)$ alamhulk $\mathbb{Z}$ on alamrühm, mida me rühmana tähistame samuti $(\mathbb{Z}, +)$.

Ülesanne 1.24 Näidata, et seos $\leq$ on järjestusseos kõigi rühmade klassil.

Ülesanne 1.25 Veenduda, et hulk

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

on rühma $(GL_n(\mathbb{R}), \cdot)$ alamrühm.

Ülesanne 1.26 Veenduda, et iga rühma G korral on siseautomorfismide hulk

$$\text{Inn}(G) = \{\varphi_x \mid x \in G\}$$

rühma $\text{Aut}(G)$ alamrühm.

Ülesanne 1.27 Leida rühma $(\mathbb{Z}_6, +)$ vähim alamrühm, mis sisaldab elementi $\bar{4}$.

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

$$\iota(h) = h$$

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

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

$$\varphi(H) = \{\varphi(h) \mid h \in H\} \subseteq G.$$

Tihti kirjutatakse $\varphi(H)$ asemel ka $\text{im}(\varphi)$. Tuleb välja, et $\varphi(H)$ on G alamrühm.

Lause 1.28 Kui $\varphi : H \rightarrow G$ on rühmade homomorfism, siis $\varphi(H) \leq G$. Kui φ on üksühene, siis

$$H \simeq \varphi(H).$$

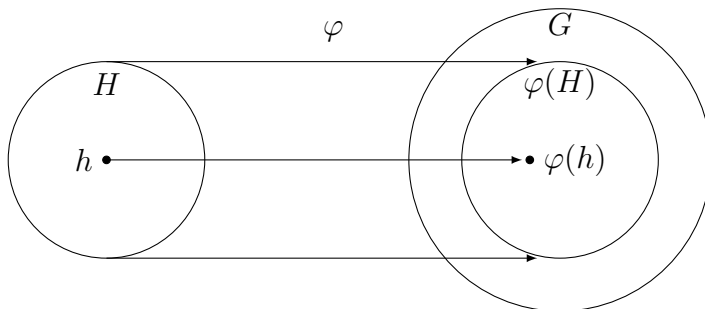
TÕESTUS. Olgu $\varphi(h_1), \varphi(h_2) \in \varphi(H)$, kus $h_1, h_2 \in H$. Kuna φ on homomorfism, siis

$$\varphi(h_1)\varphi(h_2) = \varphi(h_1h_2) \in \varphi(H) \quad \text{ja} \quad \varphi(h_1)^{-1} = \varphi(h_1^{-1}) \in \varphi(H).$$

Seega $\varphi(H)$ on rühma G alamrühm. Kui φ on üksühene, siis kujutus

$$H \rightarrow \varphi(H), \quad h \mapsto \varphi(h)$$

on bijektiivne ja seega rühmade isomorfism.



□

Alamrühmade ühisosa on samuti alamrühm.

Lause 1.29 Kui H_i , $i \in I$ (kus I on mingi mittetühi hulk), on rühma G alamrühmad, siis ka $\bigcap_{i \in I} H_i$ on G alamrühm.

TÕESTUS. Olgu $H := \bigcap_{i \in I} H_i$. Kuna G ühikelement 1_G kuulub igasse alamrühma, siis $1_G \in H \neq \emptyset$. Lisaks sellele

$$\begin{aligned} h, k \in H &\implies (\forall i \in I) h, k \in H_i \implies (\forall i \in I) hk \in H_i \implies hk \in H, \\ h \in H &\implies (\forall i \in I) h \in H_i \implies (\forall i \in I) h^{-1} \in H_i \implies h^{-1} \in H. \end{aligned}$$

□

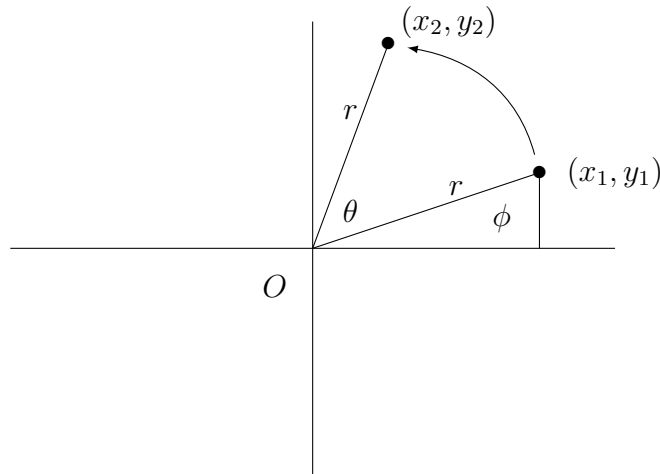
Sellest lausest järeldub, et kui X on rühma G mittetühi alamhulk, siis leidub rühma G vähim alamrühm, mis sisaldab hulka X . Tõepoolest: vaatleme kõikvõimalikke alamrühmi, mis sisaldavad hulka X (selliseid on kindlasti vähemalt üks: G ise), ja võtame nende ühisosa. Seda vähimat alamrühma nimetatakse rühma G **alamhulga X poolt tekitatud alamrühmaks** ja tähistatakse $\langle X \rangle$. Kui $\langle X \rangle = G$, siis öeldakse, et X on G **tekitajate süsteem** (ehk moodustajate süsteem).

1.4 Dieedri rühm

Selles paragrahvis konstrueerime iga $n \in \mathbb{N}$ jaoks rühma $GL_2(\mathbb{R})$ teatud alamrühma, mille elemendid vastavad korrapärase n -nurga pööretele ja peegeldustele.

Olgu tasandil fikseeritud ristkoordinaadistik. Kui punkti $P(x_1, y_1)$ kaugus nullpunktist on r ja nurk x -telje ja selle punkti kohavektori vahel on teravnurk ϕ , siis selle punkti koordinaatide veerg on

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} r \cos \phi \\ r \sin \phi \end{pmatrix}.$$



Kui pöörame tasandit ümber nullpunkti $\theta \in \mathbb{R}$ radiaani võrra vastupäeva, siis liigub see punkt uude kohta, mille koordinaatide veerg on

$$\begin{aligned} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} &= \begin{pmatrix} r \cos(\phi + \theta) \\ r \sin(\phi + \theta) \end{pmatrix} = \begin{pmatrix} r \cos \phi \cos \theta - r \sin \phi \sin \theta \\ r \sin \phi \cos \theta + r \cos \phi \sin \theta \end{pmatrix} \\ &= \begin{pmatrix} x_1 \cos \theta - y_1 \sin \theta \\ x_1 \sin \theta + y_1 \cos \theta \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}. \end{aligned}$$

Nagu näeme saab sellise pöörde korral punktide koordinaate teisendada maatriksiga

$$A(\theta) := \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

vasakult korrutades. Saab näidata, et sama kehtib siis, kui θ on 2., 3. või 4. veerandi nurk.

Paneme tähele, et $A(\theta)^k = A(k\theta)$ iga $k \in \mathbb{N}$ korral, sest tasandi pööramine θ radiaani võrra k korda on sama, mis tasandi pööramine $k\theta$ radiaani võrra üks kord.

Vaatleme maatrikseid

$$J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{ja} \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

kus J väljendab tasandi peegeldamist x -telje suhtes ja E on ühikmaatriks.

Lemma 1.30 *Iga nurga θ korral on $A(\theta)$ pööratav maatriks ja*

$$A(\theta)J = JA(\theta)^{-1}.$$

TÕESTUS. Kuna $|A(\theta)| = \cos^2 \theta + \sin^2 \theta = 1$, siis $A(\theta) \in GL_2(\mathbb{R})$. Lisaks sellele

$$A(\theta)JA(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix} \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = J.$$

Korrutades võrduse $A(\theta)JA(\theta) = J$ mõlemad pooli paremalt maatriksiga $A(\theta)^{-1}$ saamegi soovitud tulemuse. $\square$

Fikseerime nüüd naturaalarvu n ja tähistame

$$A := A\left(\frac{2\pi}{n}\right) = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}.$$

Lause 1.31 *Hulk*

$$D_{2n} = \{E, A, \dots, A^{n-1}, J, JA, \dots, JA^{n-1}\}$$

on rühma $GL_2(\mathbb{R})$ alamrühm, milles on $2n$ elementi.

TÕESTUS. Kõigepealt näitame matemaatilise induktsiooni abil, et iga $k \in \mathbb{N}$ korral

$$JA^k J = A^{-k}. \tag{2}$$

Lemmast 1.30 teame, et $AJ = JA^{-1}$. Korrutades seda võrdust vasakult maatriksiga J saame $JAJ = A^{-1}$ (sest $J^2 = E$). Seega väide kehtib $k = 1$ korral. Eldame, et $k > 1$ ja et väide kehtib $k - 1$ korral. Siis

$$A^{-k} = A^{-(k-1)}A^{-1} = JA^{k-1}JAJ = JA^{k-1}E AJ = JA^k J.$$

Tõestatud omadusest (2) järeldeb, et

$$JA^k JA^k = A^{-k}A^k = E,$$

seega iga $k \in \{0, 1, \dots, n-1\}$ korral JA^k pöördmaatriks on ta ise. Võrdusest $A^n = E$ järeldeb, et A^k pöördmaatriks on A^{n-k} . Seega näeme, et hulk D_{2n} on kinnine pöördelemendi

võtmise suhtes. Jääb veel kontrollida kinnisus korrutamise suhtes. Selleks näitame, et iga $x, y \in D_{2n}$ korral $xy \in D_{2n}$. Vaatleme nelja juhtu, kus $k, l \in \{0, 1, \dots, n-1\}$.

1. $x = A^k, y = A^l$. Siis $xy = A^{k+l} = A^r \in D_{2n}$, kus r on jääk, mis tekib $k+l$ jagamisel n -ga.

2. $x = JA^k, y = A^l$. Siis $xy = JA^{k+l} = JA^r \in D_{2n}$, kus r on samasugune nagu enne.

3. $x = A^k, y = JA^l$. Siis

$$xy = A^k JA^l = JJA^k JA^l = JA^{-k} A^l = JA^{l-k} \in D_{2n}.$$

4. $x = JA^k, y = JA^l$. Siis

$$xy = JA^k JA^l = A^{-k} A^l = A^{l-k} \in D_{2n}.$$

Sellega on tõestatud, et D_{2n} on alamrühm.

On selge, et $|D_{2n}| \leq 2n$. Et tõestada võrdus $|D_{2n}| = 2n$ piisab näidata, et maatriksid $E, A, \dots, A^{n-1}, J, JA, \dots, JA^{n-1}$ on paarikaupa erinevad. Kuna elemendi A järk on n , siis on selge, et $E, A, \dots, A^{n-1}$ on paarikaupa erinevad, nad moodustavad D_{2n} alamrühma, mida tähistame $\langle A \rangle$. Selles alamrühmas on iga maatriksi determinant võrdne 1-ga. Kuna $|JA^k| = |J| \cdot |A^k| = (-1) \cdot 1 = -1$, siis $JA^k \notin \langle A \rangle$. Kui me oletaksime, et $JA^k = JA^l$, kus $k, l \in \{0, 1, \dots, n-1\}$ ja $k \neq l$, siis selle võrduse korrutamisel vasakult maatriksiga J saaksime $A^k = A^l$, mis on vastuolus sellega, et $\langle A \rangle$ elemendid on erinevad. Seega ka $J, JA, \dots, JA^{n-1}$ on paarikaupa erinevad. $\square$

Definitsioon 1.32 Rühma D_{2n} nimetatakse **dieedri rühmaks** järguga $2n$. See koosneb n pöördest $E, A, \dots, A^{n-1}$ ja n peegeldusest $J, JA, \dots, JA^{n-1}$.

Dieedri rühma D_{2n} võib vaadelda sellise korrapärase n -nurga sümmeetriateisenduste rühmana, mille tipud asuvad punktides

$$\begin{pmatrix} \cos \frac{2k\pi}{n} \\ \sin \frac{2k\pi}{n} \end{pmatrix}, \quad \text{kus } k = 0, 1, \dots, n-1.$$

1.5 Rühmade otsekorutus

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

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

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

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

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

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

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

Lause 1.33 Kui G_i , $i \in I$, on rühmad, siis defineerides hulgal $\prod_{i \in I} G_i$ korrumise võrdusega

$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} := (a_i b_i)_{i \in I}$$

(niiöelda komponenthaaval) saame rühma.

TÕESTUS. Korrumamine on assotsiatiiivne, sest

$$((a_i)_{i \in I} \cdot (b_i)_{i \in I}) \cdot (c_i)_{i \in I} = ((a_i b_i) c_i)_{i \in I} = (a_i (b_i c_i))_{i \in I} = (a_i)_{i \in I} \cdot ((b_i)_{i \in I} \cdot (c_i)_{i \in I}).$$

Ühikelemendiks on jada $(1_i)_{i \in I}$, kus 1_i on rühma G_i ühikelement. Jada $(a_i)_{i \in I}$ pöörd-elemendiks on jada $(a_i^{-1})_{i \in I}$. $\square$

Definitsioon 1.34 Rühma $\prod_{i \in I} G_i$ nimetatakse rühmade G_i , $i \in I$, **otsekorrutiseks**.

Näide 1.35 Näiteks rühmade $(\mathbb{Z}_3; +)$ ja $(\mathbb{Z}_7; +)$ otsekorrutises $\mathbb{Z}_3 \times \mathbb{Z}_7$ võib arvutada

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

Lause 1.36 Rühmade otsekorrutise projektsioonid on rühmade homomorfismid.

TÕESTUS. Kui $a = (a_j)_{j \in I}$ ja $b = (b_j)_{j \in I}$ on rühmade otsekorrutise $\prod_{j \in I} G_j$ elemendid, siis iga $i \in I$ korral

$$\pi_i(ab) = \pi_i((a_j b_j)_{j \in I}) = a_i b_i = \pi_i(a) \pi_i(b).$$

$\square$

1.6 Kõrvalklassid, Lagrange'i teoreem

Rühmade faktoriseerimisel kasutatakse teatud alamrühmade kõrvalklasse. Selles paragrahvis uurime kõrvalklasside omadusi ja tõestame nende abil teoreemi, mis on nime saanud prantsuse matemaatiku Joseph-Louis Lagrange'i (1736–1813) järgi. See teoreem annab seose lõpliku rühma alamrühma elementide arvu ja terve rühma elementide arvu vahel.

Definitsioon 1.37 Olgu G rühm ja H tema alamrühm. Siis hulka

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

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

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

Näide 1.38 Vaatleme Abeli rühma $(\mathbb{Z}, +)$. Lihtne on veenduda, et hulk

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

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

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

s.t. arvu 2 jäägiklass mooduli 5 järgi.

Järgmine lause annab ühe võimaluse kõrvalklasside võrdsuse tuvastamiseks.

Lause 1.39 Olgu G rühm, $H \leq G$ ja $a, b \in G$. Siis

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

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

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

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

PIISAVUS. Oletame, et $a^{-1}b \in H$ ja tähistame $h := a^{-1}b$. Siis $b = ah$, millest järeldub, et $bH \subseteq aH$. Korrutades võrdust $b = ah$ paremalt elemendiga h^{-1} saame, et $a = bh^{-1}$, millest järeldub sisalduvus $aH \subseteq bH$. Kokkuvõttes $aH = bH$. $\square$

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

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

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

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

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

$$f(h) := ah$$

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

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

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

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

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

Veendume, et kui hulgal aH ja bH lõikuvad, siis on nad võrdsed. Selleks oletame, et leidub element $g = ah_1 = bh_2 \in aH \cap bH$, kus $h_1, h_2 \in H$. Siis $h_1 = a^{-1}bh_2$ ja $a^{-1}b = h_1h_2^{-1} \in H$, sest H on alamrühm. Lause 1.39 põhjal $aH = bH$. Sellega oleme näidanud, et tegemist on klassijaotusega. Lause 1.41 põhjal teame, et kõik vasakpoolsed kõrvalklassid on sama võimsusega (täpsemalt võimsusega $|H|$). Seega kui neid kõrvalklasse on m tükki, siis

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

ehk naturaalarv $|H|$ jagab naturaalarvu $|G|$. □

1.7 Faktorrühm

Rühmi saab faktoriseerida teatud eriomadustega alamrühmade järgi.

Definitsioon 1.44 Rühma G alamrühma H nimetatakse **normaalseks alamrühmaks** ehk **normaaljagajaks**, kui iga $g \in G$ ja iga $h \in H$ korral $g^{-1}hg \in H$. Sellisel juhul kirjutatakse $H \trianglelefteq G$.

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

Näide 1.46 Kommutatiivse rühma (ehk Abeli rühma) kõik alamrühmad on normaalsed, sest $g^{-1}hg = g^{-1}gh = h \in H$.

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

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

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

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

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

Definitsioon 1.49 Rühma G alamrühma H **indeksiks** rühmas G (tähistus $|G : H|$) nimetatakse H vasakpoolsete kõrvalklasside hulga võimsust.

Lause 1.50 Iga alamrühm indeksiga 2 on normaalne.

TÕESTUS. Olgu H rühma G alamrühm, mille indeks on 2. Siis leidub täpselt 2 vasakpoolset ja täpselt 2 parempoolset kõrvalklassi H järgi. Kuna üks kõrvalklass on H ja kõrvalklassid on lõikumatud, siis teine peab olema $G \setminus H$. Kui $g \in H$, siis $gH = H = Hg$. Kui $g \in G \setminus H$, siis $gH = G \setminus H = Hg$. Seega H on normaalne alamrühm. $\square$

Definitsioon 1.51 Kui $\varphi : G \longrightarrow H$ on rühmade homomorfism, siis hulka

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

nimetatakse homomorfismi φ **tuumaks**.

Lause 1.52 Rühmade homomorfismi $\varphi : G \longrightarrow H$ tuum on rühma G normaalne alamrühm.

TÕESTUS. Lihtne on veenduda, et $\text{Ker } \varphi$ on G alamrühm. Kui $a \in \text{Ker } \varphi$ ja $g \in G$, siis

$$\varphi(g^{-1}ag) = \varphi(g^{-1})\varphi(a)\varphi(g) = \varphi(g)^{-1} \cdot 1_H \cdot \varphi(g) = 1_H$$

ning seega $g^{-1}ag \in \text{Ker } \varphi$. $\square$

Homomorfismi tuuma abil saab otsustada, kas see homomorfism on üksühene.

Lause 1.53 Rühmade homomorfism $\varphi : G \longrightarrow H$ on üksühene parajasti siis, kui $\text{Ker } \varphi = \{1_G\}$.

TÕESTUS. TARVILIKKUS. Olgu φ üksühene ja $a \in \text{Ker } \varphi$. Siis $\varphi(a) = 1_H = \varphi(1_G)$. Üksühesuse tõttu $a = 1_G$ ja seega $\text{Ker } \varphi = \{1_G\}$.

PIISAVUS. Eeldame, et $\text{Ker } \varphi = \{1_G\}$. Kui $\varphi(a) = \varphi(b)$, kus $a, b \in G$, siis

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = 1_H,$$

kust $ab^{-1} \in \text{Ker } \varphi$. Seega $ab^{-1} = 1_G$ ja $a = b$. Oleme näidanud, et φ on üksühene. $\square$

Asume nüüd faktorrühmi moodustama.

Lause 1.54 Kui G on rühm ja $H \trianglelefteq G$, siis defineerides kõrvalklasside hulgal

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

korrutamise eeskirjaga

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

saame rühma.

TÕESTUS. Veendume, et korrutamine on korrektselt defineeritud. Selleks oletame, et $aH = cH$ ja $bH = dH$, kus $a, b, c, d \in G$. Siis $a^{-1}c, b^{-1}d \in H$. Kuna H on normaalne alamrühm, siis

$$(ab)^{-1}(cd) = b^{-1}a^{-1}cd = b^{-1}(a^{-1}c)b \cdot b^{-1}d \in H.$$

Järelikult $(ab)H = (cd)H$, mis tähendab, et korrutis ei sõltu kõrvalklassi esindaja valikust.

Lihtne on näha, et kõrvalklasside korrutamine on assotsiatiivne, et $H = 1H$ on ühikelement ja elemendi aH pöördelement on $a^{-1}H$. $\square$

Definitsioon 1.55 Eelmises lause konstrueeritud rühma G/H nimetatakse rühma G **faktorrühmaks** normaalse alamrühma H järgi.

Lause 1.56 Kui H on rühma G normaalne alamrühm, siis kujutus

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

on surjektiivne rühmade homomorfism, mille tuum on H .

TÕESTUS. Mistahes $a, b \in G$ korral

$$\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b),$$

seega π on homomorfism. Surjektiivsus on ilmne. Tänu järeldusele 1.40 kehtib

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

□

Definitsioon 1.57 Homomorfismi $\pi : G \rightarrow G/H$ nimetatakse rühma G **loomulikuks projektsiooniks** faktorrühmale G/H .

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

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

Kuna pöördelementide osas on vastandelemendid, siis lause 1.39 põhjal mistahes elementide $a, b \in A$ korral

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

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

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

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

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

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

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

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

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

Faktorrühma liitmine on defineeritud võrdusega

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

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

2 Isomorfismiteoreemid

Selles peatükis tõestame rühmade homomorfismiteoreemi ja kolm klassikalist teoreemi, mis käivad isomorfismide kohta teatud faktorrühmade vahel.

Teoreem 2.1 (Homomorfismiteoreem) *Kui $\varphi : G \longrightarrow H$ on rühmade homomorfism, $N \trianglelefteq G$ ja $N \subseteq \text{Ker } \varphi$, siis leidub üheselt määratud rühmade homomorfism $\psi : G/N \longrightarrow H$ nii, et $\psi \circ \pi = \varphi$, kus $\pi : G \longrightarrow G/N$ on loomulik projektsioon.*

TÕESTUS. Defineerime kujutuse $\psi : G/N \longrightarrow H$ võrdusega

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

iga $a \in G$ korral.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ & \searrow \pi & \nearrow \psi \\ & G/N & \end{array}$$

Mistahes $a, b \in G$ korral

$$aN = bN \iff a^{-1}b \in N \implies a^{-1}b \in \text{Ker } \varphi \implies \varphi(a^{-1}b) = 1_H \implies \varphi(a) = \varphi(b),$$

seega ψ on korrektselt defineeritud. Ta on ka homomorfism, sest

$$\psi((aN)(bN)) = \psi(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aN)\psi(bN).$$

Lisaks sellele $(\psi \circ \pi)(a) = \psi(aN) = \varphi(a)$ iga $a \in G$ korral.

Kui ka $\gamma : G/N \longrightarrow H$ on selline homomorfism, et $\gamma \circ \pi = \varphi$, siis $\gamma \circ \pi = \psi \circ \pi$. Järelikult iga $aN \in G/N$ korral

$$\gamma(aN) = (\gamma \circ \pi)(a) = (\psi \circ \pi)(a) = \psi(aN),$$

mis tähendab, et $\gamma = \psi$. Seega ψ on üheselt määratud. □

Järeldus 2.2 *Kui $\varphi : G \longrightarrow H$ on surjektiivne rühmade homomorfism, siis*

$$G/\text{Ker } \varphi \simeq H.$$

TÕESTUS. Rakendame homomorfismiteoreemi olukorras, kus $N = \text{Ker } \varphi$. Meenutame, et lause 1.52 tõttu $\text{Ker } \varphi \trianglelefteq G$. Kujutuse φ surjektiivsusest järeldub ka ψ surjektiivsus. Kui $1_H = \psi(a \text{Ker } \varphi) = \varphi(a)$, siis $a \in \text{Ker } \varphi$ ja $a \text{Ker } \varphi = \text{Ker } \varphi$. Seega $\text{Ker } \psi = \{\text{Ker } \varphi\} = \{N\}$ ja ψ on injektiivne tänu lausele 1.53. Kokkuvõttes ψ on rühmade isomorfism. □

Näide 2.3 Vaatleme rühmade homomorfismi

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

See homomorfism on sürjektiivne, sest arvu $r \in \mathbb{R}^*$ üheks originaaliks φ suhtes on näiteks maatriks

$$\begin{pmatrix} r & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Lisaks sellele

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

Järeldus 2.2 ütleb meile, et

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

Kui H ja K on rühma G mingid alamhulgad siis tähistatakse

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

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

Lemma 2.4 *Kui G on rühm, $H \leq G$ ja $K \trianglelefteq G$, siis $HK \leq G$.*

TÕESTUS. Kuna $1_G = 1_G 1_G \in HK$, siis $HK \neq \emptyset$.

Olgu $h_1 k_1, h_2 k_2 \in HK$, kus $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Kuna $k_1 h_2 \in K h_2 = h_2 K$ (see võrdus kehtib tänu sellele, et $K \trianglelefteq G$), siis leidub selline $k \in K$, et $k_1 h_2 = h_2 k$. Järelikult

$$(h_1 k_1)(h_2 k_2) = h_1 (k_1 h_2) k_2 = h_1 (h_2 k) k_2 = (h_1 h_2)(k k_2) \in HK$$

ning me oleme näidanud, et HK on kinnine korrutamise suhtes.

Kui $hk \in HK$, siis

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

sest $h^{-1} \in H$ ja $(h^{-1})^{-1} k^{-1} h^{-1} \in K$. Seega HK on kinnine ka pöördlemendi võtmise suhtes. $\square$

Meil läheb vaja ka järgmist abitulemust.

Lemma 2.5 *Kui G on rühm, $K \trianglelefteq G$ ja $K \subseteq H \leq G$, siis $K \trianglelefteq H$.*

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

Teoreem 2.6 (Esimene isomorfismiteoreem) *Olgu G rühm, $H \leq G$ ja $K \trianglelefteq G$. Siis*

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

TÕESTUS. Lemma 2.4 põhjal $HK \leq G$. Kuna $K \trianglelefteq G$ ja $K \subseteq HK$, siis lemma 2.5 tõttu $K \trianglelefteq HK$ ja faktorrühm HK/K on olemas.

Defineerime kujutuse $\varphi : H \rightarrow HK/K$ võrdusega

$$\varphi(x) := xK$$

iga $x \in H$ korral. Kuna $\varphi = \pi|_H$, kus $\pi : HK \rightarrow HK/K$ on loomulik projektsioon, siis φ on homomorfism. Kui $(hk)K \in HK/K$, siis $\varphi(h) = hK = h(kK) = (hk)K$, mis tähendab, et φ on pealekujutus. Kasutades järeldust 2.2 võime öelda, et

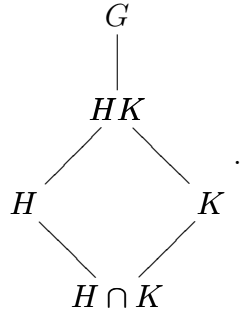
$$\begin{array}{ccc} H & \xrightarrow{\varphi} & HK/K \\ & \searrow \pi' & \nearrow \cong \\ & H/\text{Ker } \varphi & \end{array}$$

Kuna

$$\begin{aligned} x \in \text{Ker } \varphi &\iff x \in H \wedge \varphi(x) = K \iff x \in H \wedge xK = K \\ &\iff x \in H \wedge x \in K \iff x \in H \cap K, \end{aligned}$$

siis $\text{Ker } \varphi = H \cap K$. □

Märkus 2.7 Eelmises teoreemis esinevate alamrühmade vahelisi sisalduvusseoseid illustreerib järgmine diagramm (suuremad alamrühmad on ülevalpool):



Teoreem 2.8 (Teine isomorfismiteoreem) Olgu G rühm, $H \trianglelefteq G$, $K \trianglelefteq G$ ja $K \subseteq H$. Siis

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

TÕESTUS. Kuna $K \trianglelefteq G$, siis tänu lemmale 2.5 ka $K \trianglelefteq H$. Seega on faktorrühmad G/K , H/K ja G/H olemas. Defineerime nüüd kujutuse $\varphi : G/K \rightarrow G/H$ võrdusega

$$\varphi(aK) := aH,$$

$a \in G$. Oletame, et $aK = bK$. Siis $b^{-1}a \in K \subseteq H$. Lause 1.39 põhjal $aH = bH$, mis näitab, et φ on korrektselt defineeritud. Lihtne on näha, et φ on surjektiivne homomorfism. Järelduse 2.2 põhjal

$$(G/K)/\text{Ker } \varphi \cong G/H.$$

$$\begin{array}{ccc}
G/K & \xrightarrow{\varphi} & G/H \\
& \searrow \pi & \nearrow \cong \\
& (G/K)/\text{Ker } \varphi &
\end{array}$$

Mistahes kõrvalklassi $aK \in G/K$, kus $a \in G$, korral

$$aK \in \text{Ker } \varphi \iff \varphi(aK) = H \iff aH = H \iff a \in H \implies aK \in H/K.$$

Viimane implikatsioon on pööratav, sest

$$aK \in H/K \implies (\exists h \in H) aK = hK \implies (\exists k \in K) a = hk \implies a \in H.$$

Järelikult $\text{Ker } \varphi = H/K$ (need hulgad koosnevad samadest elementidest). Sellega on nõutud isomorfism tõestatud. $\square$

Teoreem 2.9 [Kolmas isomorfismiteoreem] Olgu G rühm, $H \trianglelefteq G$, $\pi : G \rightarrow G/H$ loomulik projektsioon, $N \trianglelefteq G/H$ ja $M = \pi^{-1}(N)$. Siis $M \trianglelefteq G$ ja

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

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

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

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

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

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

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

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

Kuna $H \trianglelefteq G$ ja $H \subseteq M$, siis lemma 2.5 põhjal $H \trianglelefteq M$. Veelgi enam,

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

Teise isomorfismiteoreemi põhjal

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

$\square$

Märkus 2.10 Seoseid eelmises teoreemis esinevate alamrühmade vahel illustreerib järgnev diagramm:

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

Teoreem väljendab seda, et faktorrühma faktorrühmad on isomorfsed esialgse rühma (s.t. G) faktorrühmadega.

3 Rühma elemendi järk ja tsüklilised rühmad

3.1 Tsüklilised rühmad

Olgu $(G, \cdot)$ rühm ja $g \in G$. Meenutame, et iga täisarvu k jaoks on defineeritud aste g^k (vt. definitsiooni 1.7) ja kehtivad arvutusreeglid

$$g^{k+l} = g^k \cdot g^l, \quad (g^k)^l = g^{kl}$$

mistahes $k, l \in \mathbb{Z}$ korral.

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

Rühma $(G, \cdot)$ elemendi g korral on hulk $\{g^k \mid k \in \mathbb{Z}\} \subseteq G$ alamrühm, mis sisaldab elementi g . Seega $\langle g \rangle \subseteq \{g^k \mid k \in \mathbb{Z}\}$. Teisest küljest g poolt tekitatud alamrühm $\langle g \rangle$ peab sisaldama kõiki g astmeid. Järelikult

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

Definitsioon 3.1 Rühma $(G, \cdot)$ nimetatakse **tsükliliseks**, kui leidub selline element $g \in G$, et $G = \langle g \rangle$. Seda elementi g nimetatakse tsüklilise rühma **tekitajaks** (ehk **moodustajaks**).

Teisisõnu rühm $(G, \cdot)$ on tsükliline, kui temas leidub selline element g , mille astmetena esituvad kõik selle rühma elemendid: $G = \{g^k \mid k \in \mathbb{Z}\}$. On selge, et iga tsükliline rühm on kommutatiivne, sest mistahes $k, l \in \mathbb{Z}$ korral

$$g^k g^l = g^{k+l} = g^{l+k} = g^l g^k.$$

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

Näide 3.2 • Rühm $(\{1, -1\}, \cdot)$ on tsükliline rühm tekitajaga -1 .

- Rühm $(\mathbb{Z}, +)$ on tsükliline rühm tekitajaga 1 või -1 .
- Rühm $(\mathbb{Z}_n, +)$ on tsükliline rühm tekitajaga $\bar{1}$ (aga sellel rühmal võib olla teisi tekitajaid).
- n -nda astme kompleksarvuliste ühejuurte hulk

$$\sqrt[n]{1} = \left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k \in \{0, 1, \dots, n-1\} \right\}$$

on tsükliline rühm kompleksarvude korrutamise suhtes, mille üheks tekitajaks on ühejuur

$$\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

Meil läheb vaja järgmisi arvuteoreetilisi tulemusi.

Lause 3.3 Kui $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$, siis leiduvad $q, r \in \mathbb{Z}$ nii, et $a = bq + r$ ja $0 \leq r < b$.

Lause 3.4 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 kirjeldab isomorfismi täpsuseni ära kõik tsüklilised rühmad.

Teoreem 3.5 *Sama järku tsüklilised rühmad on isomorfsed, kusjuures*

1. iga lõpmatu tsükliline rühm on isomorfne rühmaga $(\mathbb{Z}, +)$;
2. iga n -elemendiline tsükliline rühm on isomorfne rühmaga $(\mathbb{Z}_n, +)$.

TÕESTUS. Olgu $(G, \cdot)$ rühm ja $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Siis on kaks võimalust.

1) g astmete hulgas pole võrdseid. Siis G on lõpmatu,

$$G = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}. \quad (4)$$

Ei ole raske näha, et kujutus $\varphi : G \rightarrow \mathbb{Z}$, mis on defineeritud võrdusega

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

on isomorfism. Seega $(G, \cdot) \simeq (\mathbb{Z}, +)$,

2) g astmete hulgas on võrdseid. See tähendab, et leiduvad $k, l \in \mathbb{Z}, k \neq l$, nii et $g^k = g^l$. Olgu $k > l$. Siis korrutades võrduse $g^k = g^l$ pooli elemendiga g^{-l} saame $g^{k-l} = g^0 = 1$. Et $k > l$, siis $k - l \in \mathbb{N}$. Olgu n vähim naturaalarv, mille korral $g^n = 1$. Näitame, et

$$G = \{1, g, g^2, \dots, g^{n-1}\}. \quad (5)$$

Selleks tuleb veenduda, et $G \subseteq \{1, g, g^2, \dots, g^{n-1}\}$. Vaatleme rühma G suvalist elementi $g^k \in G$, kus $k \in \mathbb{Z}$. Lause 3.3 põhjal leiduvad sellised $q, r \in \mathbb{Z}$, et $k = nq + r$ ja $0 \leq r < n$. Järelikult

$$g^k = g^{nq+r} = (g^n)^q g^r = 1^q g^r = g^r \in \{1, g, g^2, \dots, g^{n-1}\}$$

ja kehtib võrdus (5).

Veendume veel, et elemendid $1, g, g^2, \dots, g^{n-1}$ on paarikaupa erinevad. Selleks oletame vastuväiteliselt, et $g^k = g^l$, kus $0 \leq l < k \leq n-1$. Siis $g^{k-l} = g^{l-l} = 1$, kus $k-l < n$. See on vastuolus n minimaalsusega. Seega elemendid $1, g, g^2, \dots, g^{n-1}$ peavad olema paarikaupa erinevad ja $|G| = n$.

Tõestame, et $(G, \cdot) \simeq (\mathbb{Z}_n, +)$. Isomorfismiks $\varphi : G \rightarrow \mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ sobib kujutus

$$\varphi(g^k) := \overline{k},$$

$k \in \{0, 1, \dots, n-1\}$. Eespool nägime, et

$$(\forall k, l \in \{0, 1, \dots, n-1\})(g^k = g^l \iff k = l).$$

Seega φ on korrektselt defineeritud ja injektiivne. On selge, et φ on surjektiivne. Näitame, et φ on homomorfism. Mistahes $k, l \in \{0, 1, \dots, n-1\}$ korral olgu $k + l = nq + r$, kus $q, r \in \mathbb{Z}$ ja $0 \leq r < n$. Siis

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = \varphi((g^n)^q g^r) = \varphi(g^r) = \overline{r} = \overline{k+l} = \overline{k} + \overline{l} = \varphi(g^k) + \varphi(g^l).$$

□

3.2 Rühma elemendi järk

Definitsioon 3.6 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 3.7 1. Vaatleme rühmade $(\mathbb{Z}_3, +)$ ja $(\mathbb{Z}, +)$ otsekorrutist $G = \mathbb{Z}_3 \times \mathbb{Z}$. Siis $\text{ord}_G((2, 0)) = 3$ ja $\text{ord}_G((0, 5)) = \infty$.

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

Lagrange'i teoreemist järeldeb vahetult järgmine väide.

Lause 3.8 Lõpliku rühma iga elemendi järk jagab rühma järku.

Teoreemi 3.5 tõestuse põhjal võime öelda, et kehtib järgmine tulemus.

Lause 3.9 Kui rühma $(G, \cdot)$ elemendi g järk on lõplik, siis on see vähim selline naturaalarv n , mille korral $g^n = 1$.

Lause 3.10 Kui g on rühma $(G, \cdot)$ element ja $g^k = 1$ mingi naturaalarvu k korral, siis g järk on lõplik ja jagab arvu k .

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

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

Kuna n on vähim naturaalarv, mille korral $g^n = 1$, siis r ei saa olla naturaalarv, seega $r = 0$, s.t. $k = nq$. Järelikult n jagab arvu k . $\square$

Lause 3.11 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 3.10 põhjal $n \mid ku - 1$. Seega leidub $q \in \mathbb{Z}$ nii, et $ku - 1 = nq$ ehk $ku - nq = 1$. Lause 3.4 põhjal $\text{SÜT}(k, n) = 1$.

PIISAVUS. Olgu $\text{SÜT}(k, n) = 1$. Siis lause 3.4 põhjal leiduvad sellised täisarvud u, v , et $ku + nv = 1$. Järelikult

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

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

Lihtne on veenduda, et kehtib järgmine omadus.

Lemma 3.12 Kui $(G, \cdot)$ on rühm ja $g \in G$, siis $\text{ord}(g) = \text{ord}(g^{-1})$.

Lemma 3.13 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 3.9. Olgu $\text{ord}(g) = mn$. Siis $(g^m)^n = g^{mn} = 1$. Kui oletada, et leidub naturaalarv $n' < n$, mille korral $(g^m)^{n'} = 1$, siis ka $g^{mn'} = 1$ ja $mn' < mn$, mis on vastuolus eeldusega. Seega n on vähim astendaja, mille korral $(g^m)^n = 1$; teiste sõnadega: $\text{ord}(g^m) = n$. $\square$

Tõestatud lemmat läheb muuhulgas vaja aditiivsete rühmade korral.

Järeldus 3.14 Olgu $(A, +)$ rühm, $a \in A$, $m, n \in \mathbb{N}$. Kui $\text{ord}(a) = mn$, siis $\text{ord}(ma) = n$.

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

Lause 3.15 Olgu G mittetriviaalne lõplik rühm. Rühmal G ei ole mittetriviaalseid pärisalamrühmi parajasti siis kui G on algarvulise järguga tsükliline rühm.

TÕESTUS. TARVILIKKUS. Eeldame, et rühmal $G \neq \{1\}$ ei ole mittetriviaalseid pärisalamrühmi. Võtame mingi elemendi $g \in G \setminus \{1\}$. Siis $\langle g \rangle = G$ (seega G on tsükliline) ja $\text{ord}(g) = |G|$. Oletame vastuväiteliselt, et $|G|$ ei ole algarv. Siis $|G| = mn$, kus $m, n \in \mathbb{N}$, $m, n \neq 1$. Lemma 3.13 põhjal

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

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

PIISAVUS. Olgu $G = \{1, g, g^2, \dots, g^{p-1}\}$ tsükliline rühm algarvulise järguga p ja $\{1\} \neq H \leq G$. Siis leidub $k \in \{1, \dots, p-1\}$ nii, et $g^k \in H$. Kuna $\text{SÜT}(k, p) = 1$ (sest p on algarv), siis lause 3.11 põhjal

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

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

4 Teisenduste rühmad

4.1 Cayley teoreem

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

Definitsioon 4.1 Mittetühja hulga X bijektiivseid teisendusi nimetatakse **substitutsioonideks** hulgal X . Nende hulk $\mathcal{S}(X)$ on rühm teisenduste järjestrakendamise suhtes. Seda rühma nimetatakse **sümmeetriliseks rühmaks** hulgal X . Sümmeetriliste rühmade alamrühmi nimetatakse **teisenduste rühmadeks**.

Erijuhul, kus

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

tähistatakse seda rühma sümboliga S_n . Sellest rühmast on varem olnud juttu kursuses “Algebra I”.

Tuleb välja, et iga rühma saab sisestada alamrühmana mingisse sümmeetrilisse rühma. Teiste sõnadega: iga rühm on isomorfne mingi teisenduste rühmaga.

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

Teoreem 4.2 (Cayley teoreem) *Iga rühm on isomorfne mingi sümmeetrilise rühma alamrühmaga.*

TÕESTUS. Tõestuse idee on kasutada lauset 1.28.

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

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

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

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

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

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

Näitame, et φ on rühmade homomorfism. Selleks tuleb veenduda, et mistahes $g, g' \in G$ korral $\varphi(gg') = \varphi(g)\varphi(g')$ ehk $L_{gg'} = L_g L_{g'}$. Viimane võrdus kehtib, sest iga $x \in G$ korral

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

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

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

□

4.2 Sümmeetrilised rühmad lõplikel hulkadel

Vaatleme nüüd substitutsioone lõplikul hulgal $M = \{1, 2, \dots, n\}$ ja nende rühma $(S_n, \circ)$. Selle rühma elemente tähistame väikeste kreeka tähtedega $\sigma, \tau, \dots$.

Substitutsiooni esitamiseks kasutatakse tihti 2-realist ja n -veerulist tabelit, mille esimeses reas on hulga $\{1, 2, \dots, n\}$ elemendid mingis järjekorras ja teises reas on esimeses reas olevate elementide kujutised, seega

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_n) \end{pmatrix}.$$

Nii sellise tabeli esimese rea kui ka teise rea elemendid moodustavad permutatsiooni, s.t. järjendi, milles hulga $\{1, 2, \dots, n\}$ iga element esineb täpselt ühe korra.

Definitsioon 4.3 Substitutsiooni nimetatakse **paarissubstitutsiooniks**, kui inversioonide koguarv permutatsioonides tema esituses tabelina on paarisarv. Vastasel korral nimetatakse seda substitutsiooni **paarituks substitutsiooniks**.

Kursuses “Algebra I” näidatakse ära, et substitutsiooni paarsus ei sõltu tema esitusest tabelina.

Näide 4.4 Leiame substitutsiooni

$$\sigma = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix} \in S_4$$

paarsuse. Kuna $I(2, 3, 4, 1) + I(3, 4, 1, 2) = 3 + 4 = 7$ on paaritu arv, siis σ on paaritu substitutsioon.

Kõige sagedamini esitatakse substitutsioon tabelina nii, et selle esimeses reas on niinimetatud loomulik permutatsioon $(1, 2, 3, \dots, n)$:

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

Sellist tabelit nimetatakse substitutsiooni σ **normaalkujuks**.

Näide 4.5 Leiame substitutsioonide

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \text{ja} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

korrutise $\tau\sigma$ rühmas S_4 . Kuna $(\tau\sigma)(1) = \tau(\sigma(1)) = \tau(2) = 4$, $(\tau\sigma)(2) = \tau(\sigma(2)) = \tau(3) = 3$, $(\tau\sigma)(3) = 1$ ja $(\tau\sigma)(4) = 2$, siis

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Rühma S_n ühikelemendiks on ühiksubstitutsioon

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

Substitutsiooni $\sigma \in S_n$ pöördteisendust nimetatakse σ **pöördsubstitutsiooniks** ja tähistatakse sümboliga σ^{-1} . On selge, et kui

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}, \quad (6)$$

siis

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}, \quad (7)$$

s.t. pöördsubstitutsiooni saamiseks võib σ esituses tabelina read ära vahetada.

Näide 4.6 Kui

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

siis

$$\sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Lause 4.7 *Substitutsioon ja tema pöördsubstitutsioon on sama paarsusega.*

TÕESTUS. Inversioonide koguarv tabelites (6) ja (7) on sama. $\square$

Definitsioon 4.8 Substitutsiooni nimetatakse **tsüklik**, kui ta paigutab mingeid elemente tsükliliselt ümber ning jätab ülejäänud elemendid paigale. Tsükli σ , mis paigutab ümber elemente $i_1, i_2, \dots, i_k$ nii, et

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

tähistame lühidalt

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

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

Definitsioon 4.9 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 kommuteeruvad.

Lihtne on aru saada, et kehtivad järgmised laused.

Lause 4.10 *Iga substitutsiooni saab esitada sõltumatute tsüklite korrutisena. See esitus on ühene tsüklite järjekorra täpsuseni.*

Lause 4.11 *Tsükli järk rühmas S_n on võrdne tema pikkusega.*

Näide 4.12 Rühmas S_9 saame esitada

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

Märgime veel, et näiteks

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

Lause 4.13 *Substitutsiooni järk on võrdne tema sõltumatute tsüklite pikkuste vähima ühiskordsega.*

TÕESTUS. Olgu $\sigma = \zeta_1 \zeta_2 \dots \zeta_k$, kus $\zeta_1, \zeta_2, \dots, \zeta_k \in S_n$ on sõltumatud tsüklid. Olgu l_i tsükli ζ_i pikkus, $i = 1, \dots, k$, ja olgu

$$m := \text{VÜK}(l_1, l_2, \dots, l_k).$$

Siis $l_i \mid m$ ja

$$\sigma^m = (\zeta_1 \zeta_2 \dots \zeta_k)^m = \zeta_1^m \zeta_2^m \dots \zeta_k^m = \varepsilon \varepsilon \dots \varepsilon = \varepsilon.$$

Oletame, et ka $\sigma^r = \varepsilon$, kus $r \in \mathbb{N}$. Siis

$$\varepsilon = (\zeta_1 \zeta_2 \dots \zeta_k)^r = \zeta_1^r \zeta_2^r \dots \zeta_k^r.$$

Kuna tsüklid on sõltumatud, siis peab kehtima $\zeta_1^r = \dots = \zeta_k^r = \varepsilon$. Kuna ζ_i järk on l_i , siis tänu lausele 3.10 $l_i \mid r$ iga $i \in \{1, \dots, k\}$ korral. Seega r on arvude $l_1, \dots, l_k$ ühine kordne. Vähima ühiskordse definitsiooni põhjal $m \mid r$, millest tuleb, et $m \leq r$. Seega m on vähim naturaalarv, mille korral $\sigma^m = \varepsilon$. Seda oligi tarvis tõestada. $\square$

Definitsioon 4.14 Transpositsioon on tsükkel pikkusega 2.

Algebra põhikursuses tõestatakse harilikult järgmine tulemus.

Lause 4.15 ([1], lause 4.3.15) *Transpositsioon on paaritu substitutsioon.*

Lause 4.16 *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 paremalt 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:

$$\sigma_k = \varepsilon \tau_1 \tau_2 \dots \tau_k,$$

kus $\tau_1, \dots, \tau_k$ on transpositsioonid. Kuna ε -ga korrutamine midagi ei muuda, siis iga σ_k on k transpositsiooni korrutis. Et $\sigma_0 = \varepsilon$ 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 4.17 *Olgu $n \geq 2$. Siis on paaris- ja paarituid substitutsioone n elemendist ühepalju.*

Lause 4.18 *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 4.15 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 $\tau_1, \dots, \tau_k$ on transpositsioonid. Induktsiooni eelduse põhjal on korrutise $\tau_1 \tau_2 \dots \tau_{k-1}$ 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 arvud $k - 1$ ja k . Järelikult $\tau_1 \tau_2 \dots \tau_{k-1} \tau_k$ paarsus on sama, mis k paarsus. $\square$

Lause 4.19 *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 4.18 põhjal on tsükkel $(i_1, i_2, \dots, i_k)$ ja arv $k - 1$ sama paarsusega. $\square$

Teoreem 4.20 *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 4.16 põhjal saab σ ja τ esitada paarisarvu transpositsioonide korrutisena. Siis ka $\sigma\tau$ on paarisarvu transpositsioonide korrutis. Tänu lausele 4.18 on $\sigma\tau$ paarissubstitutsioon. Kuna pöördsubstitutsiooni paarsus on sama, mis esialgse oma (vaata lauset 4.7), 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 $\sigma^{-1}\tau\sigma \in A_n$. $\square$

Definitsioon 4.21 Rühma G nimetatakse **lihtsaks**, kui tema ainsad normaalsed alamrühmad on G ja $\{1_G\}$.

Järeldus 4.22 *Kui $n \geq 3$, siis S_n ei ole lihtne.*

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

4.3 Rubiku kuubiku rühm

Kirjeldame ühte konkreetset teisenduste rühma.

Harilikul Rubiku kuubikul on algasendis 6 erivärvilist tahku. Iga tahk koosneb 9 värvilisest ruudukesest. Eesmärk on segatud ruudukestega olekust taastada algasend kasutades selleks tahkude pöördeid.

Pöörete tegemisel me kujutame ette, et hoiame kuubikut nii, et tahkude keskmised ruudud võivad pöörelda küll oma keskpunkti ümber, aga muidu nad oma asendit ei muuda. Näiteks nii, et meie ees oleval tahul on kogu aeg keskmine ruut roheline, parempoolse tahu keskmine ruut on kollane, ülemise tahu keskmine ruut on punane jne.

Rubiku kuubikul on $6 \cdot 8 = 48$ mitte-keskmist ruudukest. Me nummerdame nende positsioonid ära arvudega $1, 2, \dots, 48$. Näiteks nii, et esimese tahu ülemise rea vasakpoolseim koht on numbriga 1, sama rea keskkoht on numbriga 2, sama rea parempoolseim koht on numbriga 3 jne. Siis iga tahu pöörde saab samastada substitutsiooniga rühmast S_{48} . **Rubiku kuubiku rühm** on rühma S_{48} alamrühm, mis on tekitatud järgmise 6 pöörde (= substitutsiooni) poolt:

- F (*front*) — kuubi esimest tahku pööratakse 90° päripäeva;
- B (*back*) — kuubi tagumist tahku pööratakse 90° päripäeva;
- U (*up*) — kuubi ülemist tahku pööratakse 90° päripäeva;
- D (*down*) — kuubi alumist tahku pööratakse 90° päripäeva;
- L (*left*) — kuubi vasakut tahku pööratakse 90° päripäeva;
- R (*right*) — kuubi paremat tahku pööratakse 90° päripäeva.

Ühiksubstitutsiooni tähistame tähega E . Kui me tahame näiteks parempoolset tahku keerata 180° päripäeva, siis sellele vastab rühma element R^2 . Pööre 90° vastupäeva on R^3 . One selge, et kõik selle rühma tekitajad on neljandat järku:

$$F^4 = B^4 = U^4 = D^4 = L^4 = R^4 = E.$$

Seega iga tekitaja pöördelement on tema kuup, nt. $F^{-1} = F^3$. Iga element selles rühmas on tekitajate mingi korrutis, nt. R^2UDF^3 . Substitutsioonide korrutamisele vastab lihtsalt vastavate pöörete jadade sooritamine üksteise järel. Kuubiku lahendamine tähendab selle rühma suvalise elemendi g jaoks tema pöördelemendi leidmist, ilma et me alguses ilmutatult teaks, milliste pöörete tegemisel on g algasendist saadud.

Selle rühma elementide arv on

$$43\,252\,003\,274\,489\,856\,000 = 2^{27}3^{14}5^37^211.$$

Elementide suurim järk on 1260. Näiteks $RU^2D^3BD^3$ on üks sellise järguga element.

5 Rühma toimed

Definitsioon 5.1 Rühma G (vasakpoolseks) **toimeks** hulgal X nimetatakse kujutust

$$G \times X \longrightarrow X, \quad (g, x) \mapsto g \cdot x,$$

mis rahuldab tingimusi

1. $gh \cdot x = g \cdot (h \cdot x)$,
2. $1_G \cdot x = x$

iga $x \in X$ ja $g, h \in G$ korral. Analoogiliselt saab defineerida rühma parempoolse toime hulgal.

Näide 5.2 Iga rühm G toimib iseendal korrutamistehte

$$G \times G \longrightarrow G, \quad (g, h) \mapsto gh$$

abil.

Näide 5.3 Olgu X mittetühi hulk. Sümmeetiline rühm $(\mathcal{S}(X), \circ)$ toimib vasakult hulgal X kujutuse

$$\mathcal{S}(X) \times X \longrightarrow X, \quad (f, x) \mapsto f(x)$$

abil.

Näide 5.4 Olgu $\text{Sub}(G)$ rühma G kõigi alamrühmade hulk. Kui $H \in \text{Sub}(G)$ ja $g \in G$, siis $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \in \text{Sub}(G)$. Defineerides kujutuse

$$G \times \text{Sub}(G) \longrightarrow \text{Sub}(G), \quad (g, H) \mapsto gHg^{-1}$$

saame rühma G toime hulgal $\text{Sub}(G)$.

Näide 5.5 Vaatleme jälle Rubiku kuubiku rühma. Võtame hulgaks X kõikvõimalike saavutatavate kuubiku konfiguratsioonide hulka, kus konfiguratsiooni all mõtleme 48-komponendilist värvide järjedit, kus näiteks i -ndal kohal olev värv "roheline" tähendab seda, et kuubiku i -ndal positsioonil (varem fikseeritud positsioonide nummerduse suhtes) olev ruudukene on parasjagu rohelist värvi. Rakendades kuubikule käesolevas konfiguratsioonis mingit tahu pööret tekib meil uus konfiguratsioon. Niimoodi tekib meil Rubiku kuubiku rühma toime konfiguratsioonide hulgal.

Definitsioon 5.6 Olgu antud rühma G toime hulgal X . Elemendi $x \in X$ **orbiidiks** nimetatakse hulka

$$G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X.$$

Kasutatakse ka tähistust $\text{orb}(x)$. Orbiidi võimsust $|G \cdot x|$ nimetatakse ka selle orbiidi **pikkuseks**.

Näide 5.7 Fikseerime tasandil ühe punkti O ja vaatleme tasandi pöördeid ümber selle punkti nurga $\alpha \in \mathbb{R}$ võrra (möödetuna radiaanides). Kui α on positiivne, siis pöörame päripäeva ja kui α on negatiivne, siis pöörame vastupäeva. See rühm on isomorfne rühmaga $(\mathbb{R}, +)$. Punkti $P \neq O$ orbiidiks on ringjoon, mis läbib punkti P ja mille keskpunkt on punktis O . See orbiit on lõpmatu pikkusega.

Lause 5.8 Olgu antud rühma G toime hulgal X . Siis X on orbiitide lõikumatu ühend.

TÕESTUS. Kuna iga element kuulub enda orbiidile, siis X on orbiitide ühend.

Oletame nüüd, et $x, y \in X$ ja $G \cdot x \cap G \cdot y \neq \emptyset$. Siis leidub $z \in G \cdot x \cap G \cdot y$. Järelikult on olemas sellised elemendid $g, h \in G$, et $z = g \cdot x = h \cdot y$. Siis

$$x = 1_G \cdot x = g^{-1}g \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (h \cdot y) = g^{-1}h \cdot y \in G \cdot y$$

ja analoogiliselt $y \in G \cdot x$. Sellest järeldub kergesti, et $G \cdot x = G \cdot y$. $\square$

Niisiis rühma G toime tekitab hulga X tükelduse.

Definitsioon 5.9 Rühma toimet nimetatakse **transitiivseks**, kui sellel leidub üksainus orbiit. Teiste sõnadega: toime on transitiivne, kui

$$(\forall x, y \in X)(\exists g \in G) x = g \cdot y.$$

Näide 5.10 Rühma G toime iseendal on transitiivne, sest iga $g, h \in G$ korral $g = (gh^{-1})h$.

Näide 5.11 Tasandi vabavektorite rühm $(\mathbb{E}_2, +)$ toimib transitiivselt tasandi punktide hulgal tekitades klassikalises mõttes afinse ruumi.

Definitsioon 5.12 Olgu antud rühma G toime hulgal X . Elemendi $x \in X$ **stabilisaatoriks** selle toime suhteks nimetatakse hulka

$$\text{Stab}(x) = \{g \in G \mid g \cdot x = x\}.$$

Lause 5.13 Olgu antud rühma G toime hulgal X . Elemendi $x \in X$ stabilisaator on rühma G alamrühm.

TÕESTUS. Kuna $1_G \cdot x = x$, siis $1_G \in \text{Stab}(x)$. Kui $g, h \in \text{Stab}(x)$, siis ka $gh \in \text{Stab}(x)$, sest

$$gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x.$$

Samuti $g^{-1} \in \text{Stab}(x)$, sest

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1}g \cdot x = 1_G \cdot x = x.$$

$\square$

Lemma 5.14 Olgu antud rühma G toime hulgal X . Mistahes elementide $x \in X$ ja $g, h \in G$ korral

$$g \cdot x = h \cdot x \iff g^{-1}h \in \text{Stab}(x).$$

TÕESTUS. TARVILIKKUS. Paneme tähele, et

$$\begin{aligned} g \cdot x = h \cdot x &\implies g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (h \cdot x) \\ &\iff g^{-1}g \cdot x = g^{-1}h \cdot x \\ &\iff 1_G \cdot x = g^{-1}h \cdot x \\ &\iff x = g^{-1}h \cdot x \\ &\iff g^{-1}h \in \text{Stab}(x). \end{aligned}$$

PIISAVUS. Kui $g^{-1}h \in \text{Stab}(x)$, siis $g^{-1}h \cdot x = x$. Järelikult

$$g \cdot x = g \cdot (g^{-1}h \cdot x) = gg^{-1}h \cdot x = h \cdot x.$$

$\square$

Teoreem 5.15 (Teoreem orbiidist ja stabilisaatorist) Olgu antud lõpliku rühma G toime lõplikul hulgal X . Siis iga $x \in X$ korral

$$|G| = |G \cdot x| \cdot |\text{Stab}(x)|.$$

TÕESTUS. Vaatleme vasakpoolsete kõrvalklasside hulka

$$G/\text{Stab}(x) = \{g\text{Stab}(x) \mid g \in G\}$$

alamrühma $\text{Stab}(x)$ järgi. Kuna tänu lausele 1.39 ja lemmale 5.14

$$g\text{Stab}(x) = h\text{Stab}(x) \iff g^{-1}h \in \text{Stab}(x) \iff g \cdot x = h \cdot x,$$

siis kujutus

$$\phi : G/\text{Stab}(x) \longrightarrow G \cdot x, \quad g\text{Stab}(x) \mapsto g \cdot x$$

on korrektselt defineeritud ja injektiivne. Vastavalt orbiidi definitsioonile on ta ka surjektiivne. Seega on ϕ bijektiivne, millest järeldub, et $|G \cdot x| = |G/\text{Stab}(x)|$. Kuna kõik kõrvalklassid on tänu Lagrange'i teoreemile võimsusega $|\text{Stab}(x)|$, siis nende arv on arvude $|G|$ ja $|\text{Stab}(x)|$ jagatis. Seega

$$|G \cdot x| = |G/\text{Stab}(x)| = \frac{|G|}{|\text{Stab}(x)|}.$$

□

Selle teoreemi abil saab tõestada järgmise tulemuse orbiitide arvu kohta.

Teoreem 5.16 (Burnside'i lemma) Olgu antud lõpliku rühma G toime lõplikul hulgal X . Siis

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

kus X/G on kõigi orbiitide hulk ja $X^g = \{x \in X \mid g \cdot x = x\}$ on elemendi $g \in G$ poolt fikseeritud X elementide hulk. Teiste sõnadega: orbiitide arv võrdub G elementide poolt fikseeritud X elementide keskmise arvuga.

TÕESTUS. Kehtivad võrdused

$$\begin{aligned} \sum_{g \in G} |X^g| &= |\{(g, x) \in G \times X \mid g \cdot x = x\}| \\ &= \sum_{x \in X} |\text{Stab}(x)| \\ &= \sum_{x \in X} \frac{|G|}{|G \cdot x|} && \text{(teoreem 5.15)} \\ &= |G| \sum_{x \in X} \frac{1}{|G \cdot x|} \\ &= |G| \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|} \\ &= |G| \sum_{A \in X/G} 1 \\ &= |G| \cdot |X/G|. \end{aligned}$$

□

6 Sylowi teoreemid

Definitsioon 6.1 Olgu p algarv. Rühma nimetatakse **p -rühmaks**, kui tema iga elemendi järk on p aste. Alamrühma, mis on p -rühm, nimetatakse **p -alamrühmaks**.

Näide 6.2 Rühm $(\mathbb{Z}_9 \times \mathbb{Z}_{27}, +)$ on 3-rühm, sest tema iga elemendi järk peab olema $9 \cdot 27 = 3^5$ jagaja, seega 3 aste. Rühm $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \dots$ on lõpmatu 3-rühm.

Olgu G lõplik rühm ja p algarv. Siis aritmeetika põhiteoreemi tõttu leiduvad üheselt määratud arvud $m \in \mathbb{N}$ ja $k \in \mathbb{N} \cup \{0\}$ nii, et $|G| = mp^k$ ja $p \nmid m$. Teiste sõnadega: p^k on kõrgeim p aste, mis jagab rühma G järku. Rühma G alamrühma, mille järk on p^k , nimetatakse **Sylowi¹ p -alamrühmaks**.

Teoreem 6.3 (Esimene Sylowi teoreem) *Kui G on lõplik rühm ja p on algarv, siis rühmal G leidub Sylowi p -alamrühm.*

TÕESTUS. Olgu $|G| = mp^k$, kus $m \in \mathbb{N}$, $k \in \mathbb{N} \cup \{0\}$ ja $p \nmid m$. Vaatleme hulka

$$\mathbb{S} = \{S \subseteq G \mid |S| = p^k\}.$$

Meie eesmärk on näidata, et vähemalt üks hulkadest $S \in \mathbb{S}$ on G alamrühm. Hulga $\mathbb{S}$ võimsus on

$$\begin{aligned} N := |\mathbb{S}| &= \binom{mp^k}{p^k} = \frac{mp^k(mp^k - 1) \cdot \dots \cdot (mp^k - p^k + 1)}{1 \cdot 2 \cdot \dots \cdot (p^k - 1) \cdot p^k} \\ &= m \cdot \frac{mp^k - 1}{1} \cdot \frac{mp^k - 2}{2} \cdot \dots \cdot \frac{mp^k - (p^k - 1)}{p^k - 1}. \end{aligned}$$

Tõestame, et $p \nmid N$. Selleks näitame, et iga $i \in \{1, 2, \dots, p^k - 1\}$ ja $j \in \mathbb{N}$ korral

$$p^j \mid i \iff p^j \mid mp^k - i \tag{8}$$

(s.t. viimases murdude korrutises p^j jagab murru nimetajat parajasti siis, kui ta jagab lugejat). Kui $p^j \mid i$, siis $p^j < p^k$, seega $p^j \mid p^k$ ning järelikult $p^j \mid mp^k - i$. Vastupidi, kui oletame, et $p^j \mid mp^k - i$, siis leidub $u \in \mathbb{N}$ nii, et $p^j u = mp^k - i$. Kui oletada, et $j \geq k$, siis $p^k \mid p^k(m - p^{j-k}u) = p^k m - p^j u = i$, mis on võimatu. Järelikult $j < k$ ja $p^j \mid (mp^k - (mp^k - i)) = i$.

Tõestatud omadus (8) ütleb, et pärast p astmete taandamist murrust jäävad järele lugeja ja nimetaja, kus kummaski p ei esine. Seega p ei jaga arvu N .

Vaatleme rühma G toimet $\cdot$ hulgal $\mathbb{S}$, mis on defineeritud võrdusega

$$g \cdot S := gS = \{gs \mid s \in S\},$$

$g \in G$, $S \in \mathbb{S}$. Kujutus $\lambda_g : S \longrightarrow gS$, $s \mapsto gs$, on bijektiivne, seega $|gS| = |S| = p^k$ ja $gS \in \mathbb{S}$. Lihtne on näha, et $\cdot$ on toime. Olgu selle toime orbiidid $O_1, \dots, O_r$. Siis tänu lausele 5.8

$$\begin{aligned} \mathbb{S} &= O_1 \sqcup O_2 \sqcup \dots \sqcup O_r, \\ N = |\mathbb{S}| &= |O_1| + |O_2| + \dots + |O_r|. \end{aligned}$$

¹Peter Ludvig Meidell Sylow (1832–1918) — norra matemaatik

Kuna $p \nmid N$, siis peab leiduma selline $i \in \{1, \dots, r\}$, et $p \nmid |O_i|$. Valime ühe hulga $X \in O_i$ ja vaatleme alamrühma

$$P := \text{Stab}_G(X) = \{g \in G \mid gX = X\} \leq G.$$

Me näitame, et P ongi Sylowi p -alamrühm. Selleks peame tõestama, et $|P| = p^k$. Kuna $p^k \mid |G| = |O_i| \cdot |P|$ (vt. teoreemi 5.15) ja $p \nmid |O_i|$, siis $\text{SÜT}(p^k, |O_i|) = 1$ ja $p^k \mid |P|$, millest järeldub, et $p^k \leq |P|$.

Tõestuse lõpetamiseks on veel vaja tõestada võrratus $|P| \leq p^k$. Kuna P on X -i stabilisaator, siis iga $g \in P$ korral $gX = X$. Seega iga $x \in X$ ja $g \in P$ korral $gx \in X$ ehk $Px \subseteq X$. Järelikult

$$X = \bigcup_{x \in X} Px,$$

kus alamhulgad Px on parempoolsed kõrvalklassid alamrühma $P \leq G$ järgi. Me teame, et kõrvalklassid on lõikumatud ja et nad on kõik sama võimsusega (lause 1.41 ja Lagrange'i teoreemi tõestus). Kuna kujutus $P \rightarrow Px, g \mapsto gx$, on bijektiivne, siis kõik need kõrvalklassid on võimsusega $|P|$. Kui nende kõrvalklasside arv on l , siis $l \cdot |P| = |X|$ ning seega $|P| \mid |X| = p^k$, kust $|P| \leq p^k$. $\square$

Sellest teoreemist saab järeldada Cauchy² teoreemi.

Teoreem 6.4 (Cauchy teoreem) *Kui G on lõplik rühm, mille järk jagub algarvuga p , siis selles rühmas leidub element, mille järk on p .*

TÕESTUS. Olgu $|G| = p^k m$, kus $p \nmid m$ ja $k \in \mathbb{N}$. Esimese Sylowi teoreemi põhjal sisaldab G alamrühma P järguga $p^k > 1$. Valime suvalise elemendi $1 \neq y \in P$. Siis y järk peab jagama P järku ehk arvu p^k , seega $\text{ord}(y) = p^l$, kus $1 \leq l \leq k$. Kuna $\text{ord}(y) = p^{l-1}p$, siis lemma 3.13 põhjal $\text{ord}(y^{p^{l-1}}) = p$. $\square$

Järeldus 6.5 *Lõplik rühm on p -rühm parajasti siis, kui tema järk on p aste.*

TÕESTUS. TARVILIKKUS. Olgu G lõplik p -rühm. Oletame vastuväiteliselt, et $|G|$ ei ole p aste. Siis leidub algarv $q \neq p$ nii, et $q \mid |G|$. Teoreemi 6.4 tõttu peab G -s leiduma element järguga q , mis on vastuolus sellega, et iga elemendi järk peab olema p aste. Järelikult G järk peab olema p aste.

PIISAVUS. Kui $|G| = p^n$, siis lause 3.8 põhjal G iga elemendi järk peab olema p^n jagaja, seega p aste. $\square$

Definitsioon 6.6 Öeldakse, et rühma G alamrühmad H ja K on **kaasalamrühmad**, kui leidub selline $g \in G$, et

$$K = gHg^{-1}.$$

Teiste sõnadega: H ja K on kaasalamrühmad parajasti siis, kui nad on samal orbiidil toime

$$G \times \text{Sub}(G) \rightarrow \text{Sub}(G), \quad (g, L) \mapsto gLg^{-1}$$

suhtes.

²Augustin–Louis Cauchy (1789–1857) — prantsuse matemaatik

Kuna kujutus

$$H \longrightarrow gHg^{-1}, \quad h \mapsto ghg^{-1}$$

on rühmade isomorfism, siis rühma G mistahes kaks kaasalamrühma on isomorfsed, muuhulgas on nad sama võimsusega. Sellest järeldub, et Sylowi p -alamrühma kõik kaasalamrühmad on ka Sylowi p -alamrühmad.

Teoreem 6.7 (Teine Sylowi teoreem) *Olgu G lõplik rühm, $|G| = p^k m$, kus p on algarv ja $p \nmid m$.*

1. Iga alamrühma $K \leq G$, kus $|K| = p^d$, $d \in \mathbb{N}$, ja iga Sylowi p -alamrühma P korral leidub selline $g \in G$, et $gKg^{-1} \leq P$. Teiste sõnadega: Sylowi p -alamrühm sisaldab iga p -alamrühma mõnda kaasalamrühma.

2. Rühma G kõik Sylowi p -alamrühmad on üksteise kaasalamrühmad.

TÕESTUS. 1. Vaatleme vasakpoolsete kõrvalklasside hulka $X := G/P = \{gP \mid g \in G\}$ alamrühma P järgi. Siis

$$|X| = \frac{|G|}{|P|} = \frac{p^k m}{p^k} = m.$$

Defineerime rühma K toime hulgal X võrdusega

$$a \cdot gP := agP,$$

$a \in K$, $g \in G$. Lihtne on veenduda, et see on tõepoolest toime. Siis hulk X on selle toime orbiitide lõikumatu ühend: $X = O_1 \sqcup O_2 \sqcup \dots \sqcup O_r$. Teoreemi 5.15 põhjal iga $i \in \{1, \dots, r\}$ korral $|O_i|$ jagab järku $|K| = p^d$. Seega

$$m = |X| = |O_1| + |O_2| + \dots + |O_r| = p^{e_1} + p^{e_2} + \dots + p^{e_r},$$

kus $0 \leq e_i \leq d$. Kuna $p \nmid m$, siis leidub $j \in \{1, \dots, r\}$ nii, et $e_j = 0$ ehk $|O_j| = p^0 = 1$. Olgu O_j kõrvalklassi $hP \in X$, kus $h \in G$, orbiit. Siis $O_j = \{hP\} = K \cdot hP$, mis tähendab, et iga $a \in K$ korral $ahP = hP$, kust $h^{-1}ah \in P$. Järelikult $h^{-1}Kh \subseteq P$. Kuna K on G alamrühm, siis sellest tuleb välja, et $h^{-1}Kh \leq P$. Me võtame $g := h^{-1}$.

2. Kui K ja P on Sylowi palamrühmad, siis esimese väite põhjal leidub selline $g \in G$, et $gKg^{-1} \leq P$, kusjuures $|gKg^{-1}| = |K| = p^k = |P|$. Järelikult $gKg^{-1} = P$. $\square$

Teoreem 6.8 (Kolmas Sylowi teoreem) *Olgu G lõplik rühm, $|G| = p^k m$, kus p on algarv ja $p \nmid m$. Rühma G Sylowi p -alamrühmade arv jagab arvu m ja on kongruentne 1-ga mooduli p järgi.*

TÕESTUS. Olgu $\text{Syl}_p(G)$ rühma G kõigi Sylowi p -alamrühmade hulk. Esimene Sylowi teoreem ütleb, et see hulk ei ole tühi. Vaatleme hulgal $\text{Syl}_p(G)$ rühma G toimet, mis on defineeritud võrduse

$$g \cdot P := gPg^{-1}$$

abil (öeldakse, et G toimib hulgal $\text{Syl}_p(G)$ konjugeerimise abil). Kui P on Sylowi p -alamrühm, siis on seda ka gPg^{-1} , sest $|gPg^{-1}| = |P| = p^k$. Teine Sylowi teoreem ütleb, et sellel toimel on ainult üks orbiit. Fikseerime ühe Sylowi p -alamrühma H . Siis teoreemi 5.15 põhjal

$$|G| = |\text{Stab}_G(H)| \cdot |G \cdot H| = |\text{Stab}_G(H)| \cdot |\text{Syl}_p(G)|.$$

Tuleb välja, et

$$H \leq \text{Stab}_G(H), \quad (9)$$

sest iga $h \in H$ korral

$$h \cdot H = hHh^{-1} = H. \quad (10)$$

(Viimase võrduse juures $hHh^{-1} \subseteq H$ kehtib tänu sellele, et H on alamrühm ja $H \subseteq hHh^{-1}$ tänu sellele, et iga $h_1 \in H$ korral $h_1 = hh^{-1}h_1hh^{-1}$.) Lagrange'i teoreemi tõttu

$$p^k = |H| \mid |\text{Stab}_G(H)|$$

ehk $p^k u = |\text{Stab}_G(H)|$ mingi $u \in \mathbb{N}$ korral. Kuna

$$p^k m = |G| = p^k u \cdot |\text{Syl}_p(G)|,$$

siis taandades p^k saame, et $m = u \cdot |\text{Syl}_p(G)|$ ja seega $|\text{Syl}_p(G)| \mid m$. Sellega on esimene väide tõestatud.

Vaatleme nüüd rühma H toimet hulgal $\text{Syl}_p(G)$, mis on samuti defineeritud konjugeerimise abil:

$$h \cdot P := hPh^{-1} \quad (11)$$

iga $h \in H$ ja $P \in \text{Syl}_p(G)$ korral. Tänu omadusele (10) teame, et elemendi $H \in \text{Syl}_p(G)$ orbiit on 1-elementiline: $\{H\}$. Näitame, et ükski teine selle toime orbiit ei ole 1-elementiline. Selleks tõestame, et kui elemendi $H' \in \text{Syl}_p(G)$ orbiit on $\{H'\}$ (s.t. iga $h \in H$ korral $hH'h^{-1} = H'$), siis $H' = H$. Eeldamegi, et iga $h \in H$ korral $hH'h^{-1} = H'$. Vaatleme tõestuse esimese osa toime stabilisaatorit

$$\text{Stab}_G(H') = \{g \in G \mid gH'g^{-1} = H'\}.$$

Eelduse põhjal $H \leq \text{Stab}_G(H')$. Samuti teame, et $H' \leq \text{Stab}_G(H')$ (nagu nägime eespool (9) tõestuses). Kuna $\text{Stab}_G(H') \leq G$, siis suurim p aste, mis saab jagada $|\text{Stab}_G(H')|$ järku on p^k . Seega H ja H' on rühma $\text{Stab}_G(H')$ Sylowi p -alamrühmad. Teise Sylowi teoreemi põhjal leidub selline $g \in \text{Stab}_G(H')$, et $gH'g^{-1} = H$. Kuna $g \in \text{Stab}_G(H')$, siis $gH'g^{-1} = H'$. Järelikult $H = H'$.

Nüüd toime (11) orbiitide elementide arvud on p astmed (sest nad peavad jagama arvu $|H| = p^k$), kusjuures täpselt üks orbiit on 1-elementiline. Seega

$$|\text{Syl}_p(G)| = 1 + p^{e_2} + \dots + p^{e_r},$$

kus $1 \leq e_2, \dots, e_r \leq k$, ning järelikult $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$. $\square$

Näide 6.9 Vaatleme paarissubstitutsioonide rühma A_5 . Kuna

$$|A_5| = \frac{5!}{2} = \frac{120}{2} = 60 = 2^2 \cdot 3 \cdot 5,$$

siis selle rühma Sylowi alamrühmad on järkudega 4, 3 ja 5. Uurime näiteks Sylowi 5-alamrühmi. Nende arvu n_5 kohta teame, et $n_5 \mid 12$ ja $n_5 \equiv 1 \pmod{5}$. Seega $n_5 \in \{1, 6\}$. Kui oletada, et leidub ainult üks Sylowi 5-alamrühm P , siis kõik tema kaasalamrühmad gPg^{-1} , $g \in G$, on ka Sylowi 5-alamrühmad ja peaksid seega võrduma P -ga. Siis aga $gP = Pg$ iga $g \in G$ korral, mis tähendab, et P on normaaljagaja. On aga teada, et A_5 on lihtne rühm (vt. [1], teoreem 2.3.3). Saadud vastuolu näitab, et $n_5 = 6$. Näiteks üks neist kuuest Sylowi 5-alamrühmast on tsükli $\sigma = (1, 2, 3, 4, 5)$ poolt tekitatud 5-elementiline alamrühm $\{\varepsilon, \sigma, \sigma^2, \sigma^3, \sigma^4\}$.

7 Rühmade otsesummad

7.1 Sisemised otsesummad üldjuhul

Kõigepealt vaatleme sisemisi otsesummasid suvalise (multiplikatiivse) rühma G alamrühmade korral. Selles paragrahvis tähistab I suvalist mittetühja indeksite hulka, mille abil indekseerime rühma alamrühmi. Ta võib olla nii lõplik kui lõpmatu.

Definitsioon 7.1 Olgu G_i , $i \in I$, rühma G alamrühmad. Öeldakse, et G on nende alamrühmade **sisemine otsesumma** ja kirjutatakse

$$G = \sum_{i \in I} G_i,$$

kui

SO1. iga $i \in I$ korral $G_i \trianglelefteq G$;

SO2. iga $i \in I$ korral $G_i \cap \langle \cup_{j \neq i} G_j \rangle = \{1_G\}$;

SO3. $G = \langle \cup_{i \in I} G_i \rangle$.

Kui G on lõpliku arvu alamrühmade $G_1, \dots, G_n$ sisemine otsesumma, siis kirjutatakse $G = G_1 \dot{+} \dots \dot{+} G_n$.

Teoreem 7.2 Rühm G on oma alamrühmade G_i , $i \in I$, sisemine otsesumma parajasti siis, kui

SO4. iga $i, j \in I$, iga $g \in G_i$ ja iga $h \in G_j$ korral kui $i \neq j$, siis $hg = gh$;

SO5. rühma G iga element $g \neq 1_G$ avaldub tegurite järjekorra täpsuseni üheselt kujul

$$g = g_1 g_2 \dots g_n, \tag{12}$$

kus elemendid $g_1 \in G_{i_1}, \dots, g_n \in G_{i_n}$ on ühikelemendist erinevad ja indeksid $i_1, \dots, i_n \in I$ on paarikaupa erinevad.

TÕESTUS. TARVILIKKUS. Eeldame, et kehtivad **SO1–SO3**.

SO4. Olgu $g \in G_i$, $h \in G_j$, kus $i \neq j$. Vaatleme elementi $h^{-1}g^{-1}hg \in G$. Siis

$$\begin{aligned} G_i \trianglelefteq G &\implies h^{-1}g^{-1}h \in G_i \implies h^{-1}g^{-1}hg \in G_i, \\ G_j \trianglelefteq G &\implies g^{-1}hg \in G_j \implies h^{-1}g^{-1}hg \in G_j. \end{aligned}$$

Järelikult $h^{-1}g^{-1}hg \in G_i \cap G_j \subseteq G_i \cap \langle \cup_{k \neq i} G_k \rangle = \{1_G\}$, kus viimane võrdus kehtib tänu omadusele **SO2**. Kuna $h^{-1}g^{-1}hg = 1_G$, siis $gh = hg$.

SO5. Tingimuse **SO3** põhjal teame, et mistahes elementi $1_G \neq g \in G$ saab esitada korrutisena $g = a_1 a_2 \dots a_m$, kus iga tegur a_l kuulub mingisse alamrühma G_{i_l} , $i_l \in I$, ja ükski tegur ei ole 1_G . Omadus **SO4** lubab selles korrutises tegureid ümber järjestada ja samasse alamrühma kuuluvaid tegureid kokku võtta nii, et tekib esitus (12), kus indeksid on paarikaupa erinevad. Peame veenduma, et selline esitus on ühene. Oletame, et ka

$g = h_1 h_2 \dots h_m$, kus $h_k \in G_{l_k} \setminus \{1_G\}$ iga $k \in \{1, \dots, m\}$ korral. Oletame, et näiteks $l_1 \notin \{i_1, \dots, i_n\}$. Võrdusest $g_1 g_2 \dots g_n = h_1 h_2 \dots h_m$ järeldeb, et

$$h_1 = g_1 g_2 \dots g_n h_m^{-1} \dots h_2^{-1} \in G_{l_1} \cap \langle \cup_{j \neq l_1} G_j \rangle = \{1_G\},$$

mis on vastuolus eeldusega, et $h_1 \neq 1_G$. Seega $l_1 \in \{i_1, \dots, i_n\}$ ja sarnase arutlusega näeme, et $\{l_1, \dots, l_m\} \subseteq \{i_1, \dots, i_n\}$. Analoogiliselt saab näidata, et $\{i_1, \dots, i_n\} \subseteq \{l_1, \dots, l_m\}$ ja seega $\{i_1, \dots, i_n\} = \{l_1, \dots, l_m\}$, muuhulgas $n = m$, sest indeksid on paarikaupa erinevad. Vahetades tegurite järjekorda võime eeldada, et $i_1 = l_1, \dots, i_n = l_n$ ja seega

$$g = g_1 g_2 \dots g_n = h_1 h_2 \dots h_n,$$

kus $g_k, h_k \in G_{i_k}$ iga $k \in \{1, \dots, n\}$ korral.

Tingimuse **SO4** tõttu võime iga $k \in \{1, \dots, n\}$ korral kirjutada

$$g_k g_1 \dots g_{k-1} g_{k+1} \dots g_n = h_k h_1 \dots h_{k-1} h_{k+1} \dots h_n,$$

kust

$$\begin{aligned} h_k^{-1} g_k &= (h_1 \dots h_{k-1} h_{k+1} \dots h_n) (g_1 \dots g_{k-1} g_{k+1} \dots g_n)^{-1} \\ &= h_1 \dots h_{k-1} h_{k+1} \dots h_n g_n^{-1} \dots g_{k+1}^{-1} g_{k-1}^{-1} \dots g_1^{-1} \\ &= (h_1 g_1^{-1}) \dots (h_{k-1} g_{k-1}^{-1}) (h_{k+1} g_{k+1}^{-1}) \dots (h_n g_n^{-1}) \quad (\text{SO4}) \\ &\in G_{i_k} \cap \langle \cup_{j \neq i_k} G_j \rangle = \{1_G\}. \quad (\text{SO2}) \end{aligned}$$

Võrdusest $h_k^{-1} g_k = 1_G$ saame, et $g_k = h_k$ iga $k \in \{1, \dots, n\}$ korral. Sellega on ühesus tõestatud.

PIISAVUS. Eeldame, et kehtivad tingimused **SO4** ja **SO5**.

SO1. Veendume, et $G_i \trianglelefteq G$ iga $i \in I$ korral. Olgu $h \in G_i$ ja $g \in G$ suvalised elemendid. Tingimuse **SO5** tõttu saame g esitada kujul (12). Kui $i \notin \{i_1, \dots, i_n\}$, siis

$$\begin{aligned} g^{-1} h g &= (g_1 \dots g_n)^{-1} h g_1 \dots g_n \\ &= (g_1 \dots g_n)^{-1} g_1 \dots g_n h \quad (\text{SO4}) \\ &= 1_G \cdot h = h \in G_i. \end{aligned}$$

Võib aga juhtuda, et $i \in \{i_1, \dots, i_n\}$. Üldisust kitsendamata eeldame, et $i = i_1$ (seda lubab teha **SO4**). Kuna G_i on G alamrühm ja $g_1, h \in G_i = G_{i_1}$, siis ka $g_1^{-1} \in G_i$ ja $g_1^{-1} h g_1 \in G_i$. Seega

$$\begin{aligned} g^{-1} h g &= (g_2 \dots g_n)^{-1} (g_1^{-1} h g_1) g_2 \dots g_n \\ &= (g_2 \dots g_n)^{-1} (g_2 \dots g_n) (g_1^{-1} h g_1) \quad (\text{SO4}) \\ &= 1_G \cdot g_1^{-1} h g_1 = g_1^{-1} h g_1 \in G_i. \end{aligned}$$

SO2. Vaatleme suvalist elementi

$$g \in G_i \cap \langle \cup_{j \neq i} G_j \rangle.$$

Peame näitama, et $g = 1_G$. Oletame vastuväiteliselt, et $g \neq 1_G$. Kuna $g \in \langle \cup_{j \neq i} G_j \rangle$, siis saame g esitada korrutisena

$$g = g_1 g_2 \dots g_n,$$

kus $g_1 \in G_{k_1}, \dots, g_n \in G_{k_n}$ on ühikelemendid erinevad ja $i \notin \{k_1, \dots, k_n\}$. See on aga vastuolus esituse ühesusega tingimuses **SO5**.

SO3. See järeldeb vahetult tingimusest **SO5**. □

Järeldus 7.3 Rühm G on oma normaalsete alamrühmade H ja K sisemine otsesumma parajasti siis, kui $H \cap K = \{1_G\}$ ja $G = HK$.

TÕESTUS. **TARVILIKKUS.** Kui $G = H \dot{+} K$, siis **SO2** tõttu $H \cap K = H \cap \langle K \rangle = \{1_G\}$. Tingimustest **SO4** ja **SO5** järeldub, et $G \subseteq HK \subseteq G$, seega $G = HK$.

PIISAVUS. Eeldame, et $H \cap K = \{1_G\}$ ja $G = HK$. Kuna iga $g \in G$ on esitatav korrutisena $g = hk$, kus $h \in H$ ja $k \in K$, siis $G = \langle H \cup K \rangle$. Seega tingimused **SO2** ja **SO3** kehtivad. $\square$

Näide 7.4 Nullist erinevate kompleksarvude multiplikatiivne rühm $(\mathbb{C}^*, \cdot)$ on kommutatiivne, seega iga alamrühm on normaalne. See rühm on oma alamrühmade $\mathbb{R}^+$ ja $\{\cos \varphi + i \sin \varphi \mid \varphi \in [0, 2\pi)\}$ sisemine otsesumma. Geomeetriselt väljendudes: kompleksarvude korpuse multiplikatiivne rühm on reaaltelje positiivse suuna ja komplekstasandi ühikringjoone sisemine otsesumma.

7.2 Sisemised ja välised otsesummad

Kui G_i , $i \in I$, on rühmad, siis saab moodustada nende otsekorrutise $\prod_{i \in I} G_i$ defineerides tehted komponenthaaval nii nagu lauses 1.33. Lihtne on näha, et hulk

$$\bigoplus_{i \in I} G_i := \left\{ (a_i)_{i \in I} \in \prod_{i \in I} G_i \mid \text{hulk } \{j \in I \mid a_j \neq 1_{G_j}\} \text{ on lõplik} \right\}$$

on otsekorrutise alamrühm. Seda alamrühma nimetatakse rühmade G_i , $i \in I$, **väliseks otsesummaks**.

On selge, et lõpliku indeksite hulga $I = \{1, 2, \dots, n\}$ korral on väline otsesumma võrdne otsekorrutisega:

$$G_1 \oplus \dots \oplus G_n = G_1 \times \dots \times G_n.$$

Lause 7.5 Kui rühm G on oma paarikaupa erinevate alamrühmade G_i , $i \in I$, sisemine otsesumma, siis

$$G = \sum_{i \in I} G_i \cong \bigoplus_{i \in I} G_i.$$

TÕESTUS. Defineerime kujutuse $\varphi : \bigoplus_{i \in I} G_i \longrightarrow G$ võrdusega

$$\varphi((a_i)_{i \in I}) := \prod_{i \in I} a_i,$$

$(a_i)_{i \in I} \in \bigoplus_{i \in I} G_i$. Korrutise $\prod_{i \in I} a_i$ all peame silmas 1_G ja üldistatud jada $(a_i)_{i \in I}$ nende komponentide korrutist, mis ei võrdu 1_G -ga. Selliseid komponente on lõplik arv ja tänu omadusele **SO4** ei sõltu korrutis tegurite järjekorrast. On võimalik näidata, et φ on rühmade homomorfism.

Tänu tingimusele **SO5** on φ surjektiivne (sest G elemente saab esitada korrutisena) ja injektiivne (sest esitus on ühene). $\square$

7.3 Otsesummad Abeli rühmade korral

Vaatleme nüüd otsesummasid Abeli rühmade korral. Olgu $(A, +)$ Abeli rühm nullelemendiga 0_A ja olgu A_i , $i \in I$, selle alamrühmad. Nagu eestpoolt teada, on Abeli rühmas iga alamrühm normaalne. Lihtne on veenduda, et hulk

$$\sum_{i \in I} A_i = \{a_1 + \dots + a_n \mid n \in \mathbb{N}, i_1, \dots, i_n \in I, a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}\} \subseteq A,$$

mis koosneb hulkadesse A_i , $i \in I$, kuuluvate elementide kõikvõimalikest lõplikest summast, on rühma A alamrühm. Veelgi enam, see on vähim alamrühm, mis sisaldab kõiki hulki A_i , $i \in I$, seega

$$\sum_{i \in I} A_i = \langle \cup_{i \in I} A_i \rangle.$$

Alamrühma $\sum_{i \in I} A_i$ nimetatakse alamrühmade A_i , $i \in I$, **summaks**.

Definitsioon 7.1 võtab nüüd järgmise kuju.

Definitsioon 7.6 Olgu A_i , $i \in I$, Abeli rühma $(A, +)$ alamrühmad. Öeldakse, et A on nende alamrühmade **sisemine otsesumma** ja kirjutatakse

$$A = \sum_{i \in I} A_i,$$

kui

1. iga $i \in I$ korral $A_i \cap \sum_{j \neq i} A_j = \{0_A\}$;
2. $A = \sum_{i \in I} A_i$.

Kuna **SO4** kehtib igas Abeli rühmas, siis teoreem 7.2 omandab järgmise kuju.

Teoreem 7.7 *Abeli rühm $(A, +)$ on oma alamrühmade A_i , $i \in I$, sisemine otsesumma parajasti siis, kui rühma A iga element $a \neq 0_A$ avaldub liidetavate järjekorra täpsuseni üheselt kujul*

$$a = a_1 + a_2 + \dots + a_n,$$

kus $a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}$ on nullelemendist erinevad ja indeksid $i_1, \dots, i_n \in I$ on paari-kaupa erinevad.

Edaspidises läheb meil veel vaja järgmist tulemust.

Lause 7.8 *Abeli rühm $(A, +)$ on oma alamrühmade $A_1, \dots, A_n$ sisemine otsesumma parajasti siis kui*

1. $A = A_1 + \dots + A_n$,
2. *mistahes elementide $a_1 \in A_1, \dots, a_n \in A_n$ korral*

$$a_1 + \dots + a_n = 0 \implies a_1 = \dots = a_n = 0.$$

TÕESTUS. TARVILIKKUS. Eeldame, et $A = A_1 \dot{+} \dots \dot{+} A_n$ ja oletame, et $a_1 + \dots + a_n = 0$, kus $a_1 \in A_1, \dots, a_n \in A_n$. Siis iga $i \in \{1, \dots, n\}$ korral

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

Seega $a_1 = \dots = a_n = 0$.

PIISAVUS. Eeldame, et kehtivad tingimused 1 ja 2. Peame näitama, et kehtib definitsiooni 7.6 esimene tingimus. Oletame, et

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

Siis leiduvad elemendid $a_j \in A_j$, $j \in \{1, \dots, i-1, i+1, \dots, n\}$, nii, et

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

Järelikult

$$a_1 + \dots + a_{i-1} + (-a_i) + a_{i+1} + \dots + a_n = 0.$$

Eelduse tõttu on selles summas kõik liidetavad nullid, muuhulgas $a = 0$. Seega

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

□

7.4 Rakendus: 15-ndat järku rühmade kirjeldus

Nende rühmade kirjeldus järgneb järgmisest üldisemast teoreemist.

Teoreem 7.9 *Kui p ja q on algarvud, kusjuures $p < q$, siis igal rühmal järguga pq on täpselt üks alamrühm järguga q . See alamrühm on normaalne ja seega rühm G ei ole lihtne. Kui $q \not\equiv 1 \pmod{p}$, siis G on tsükliline rühm.*

TÕESTUS. Esimese Sylowi teoreemi põhjal sisaldab G alamrühma H järguga q . Kolmanda Sylowi teoreemi tõttu jagab Sylowi q -alamrühmade arv n_q arvu p ja $n_q \equiv 1 \pmod{q}$. Viimane tähendab seda, et n_q on kujul $1 + kq$, kus $k \in \{0, 1, \dots\}$. Kuna juba $1 + q$ on liiga suur selleks, et jagada arvu p , siis $k = 0$ ja Sylowi q -alamrühmi on ainult üks — see on H . Kuna ka kaasalamrühmad gHg^{-1} , $g \in G$, on Sylowi q -alamrühmad, siis $gHg^{-1} = H$ iga $g \in G$ korral. Järelikult $H \trianglelefteq G$.

Rühmal G leidub ka Sylowi p -alamrühm, olgu see K . Sylowi p -alamrühmade arv n_p jagab arvu q ja $n_p \equiv 1 \pmod{p}$. Seega leidub $k \in \{0, 1, \dots\}$ nii, et $n_p = 1 + kp \mid q$. Kuna q on algarv, siis $1 + kp = q$ või $1 + kp = 1$. Eeldades, et $q \not\equiv 1 \pmod{p}$, peab kehtima võrdus $1 + kp = 1 = n_p$. Nii nagu enne näeme, et $K \trianglelefteq G$.

Kasutame järeldust 7.3 selleks, et näidata, et $G = H \dot{+} K$.

1. Kui $g \in H \cap K$, siis $\text{ord}(g) \mid q = |H|$ ja $\text{ord}(g) \mid p = |K|$. Kuna $\text{SÜT}(p, q) = 1$, siis $\text{ord}(g) = 1$ ja $g = 1_G$. Seega $H \cap K = \{1_G\}$.

2. Näitame, et $G = HK$. Lemma 2.4 tõttu $HK \leq G$. Esimese isomorfismiteoreemi põhjal

$$H \cong H/\{1_G\} = H/(H \cap K) \cong HK/K.$$

Järelikult

$$|H| = |HK/K| = \frac{|HK|}{|K|},$$

kust

$$|HK| = |H| \cdot |K| = qp = |G|.$$

Kuna $HK \subseteq G$, siis peab kehtima võrdus $G = HK$.

Sellega on tõestatud, et $G = H \dot{+} K$. Lause 7.5 ütleb, et

$$G = H \dot{+} K \cong H \oplus K = H \times K.$$

Algarvulise järguga rühm peab olema tsükliline. Seega teoreemi 3.5 põhjal $H \cong \mathbb{Z}_q$ ja $K \cong \mathbb{Z}_p$. Arvuteoorias tõestatakse, et kui $\text{SÜT}(m, n) = 1$, siis $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. Antud juhul

$$G \cong H \times K \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$$

ehk G on tsükliline rühm. □

Järeldus 7.10 *Kõik 15-ndat järku rühmad on tsüklilised.*

TÕESTUS. Paneme tähele, et $15 = 3 \cdot 5$, kus $5 \not\equiv 1 \pmod{3}$. □

Teiste sõnadega: isomorfismi täpsuseni leidub ainult üks 15-elemendiline rühm, see on $(\mathbb{Z}_{15}, +)$.

8 Perioodilised ja lõplikud Abeli rühmad

Selles peatükis käsitleme perioodilisi ja lõplikke Abeli rühmi eesmärgiga anda viimaste kirjeldus. Tuleb välja, et kõik lõplikud Abeli rühmad on saadavad tsüklilistest rühmadest otsesumma konstruktsiooni abil.

8.1 Perioodilised Abeli rühmad

Sarnaselt definitsioonile 1.7 saame defineerida Abeli rühma elemendi täisarvkordsed.

Definitsioon 8.1 Olgu a Abeli rühma $(A, +)$ element ja k täisarv. Siis

$$ka := \begin{cases} \underbrace{a + a + \dots + a}_k, & \text{kui } k > 0, \\ 0, & \text{kui } k = 0, \\ \underbrace{(-a) + (-a) + \dots + (-a)}_{-k}, & \text{kui } k < 0. \end{cases}$$

Lemma 1.8 võtab järgmise kuju.

Lemma 8.2 Kui a, b on Abeli rühma $(A, +)$ elemendid ja $k, l \in \mathbb{Z}$, siis

$$(k + l)a = ka + la, \quad k(a + b) = ka + kb \quad \text{ja} \quad (kl)a = k(la).$$

Muuhulgas $-(ka) = (-k)a$.

Lemma 8.3 Olgu $(A, +)$ Abeli rühm ja p algarv. Siis hulk

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

on rühma A alamrühm.

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

Olgu $a, b \in A_p$, s.t. $\text{ord}(a) = p^k$ ja $\text{ord}(b) = p^l$, kus $k, l \in \mathbb{N} \cup \{0\}$. Siis

$$p^{\max(k,l)}(a + b) = p^{\max(k,l)}a + p^{\max(k,l)}b = 0 + 0 = 0.$$

Lause 3.10 põhjal peab elemendi $a + b$ järk 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 3.12 põhjal $\text{ord}(-a) = \text{ord}(a) = p^k$ ja seega $-a \in A_p$. $\square$

Definitsioon 8.4 Alamrühma A_p nimetatakse Abeli rühma $(A, +)$ p -komponendiks.

Näide 8.5 Abeli rühma $(\mathbb{Z}_{24}, +)$ 3-komponent on alamrühm $\{\bar{8}, \bar{16}, \bar{0}\}$.

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

Definitsioon 8.6 Rühma nimetatakse **perioodiliseks**, kui kõik tema elemendid on lõplikku järku.

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

Näide 8.7 Jäägiklassirühma $(\mathbb{Z}_2, +)$ loenduv otseaste

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

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

Teoreem 8.8 *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 3.4 üldistuse tõttu leiduvad $u_1, \dots, u_n \in \mathbb{Z}$ nii, et $u_1 n_1 + \dots + u_s n_s = 1$. Järelikult

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

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

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

siis lause 3.10 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 $a \in \sum_{p \in \mathbb{P}} A_p$.

Kontrollime veel definitsiooni 7.6 esimest tingimust. 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 kehtib $\text{ord}(a_{p_i}) = p_i^{k_i}$. Tähistame nende järkude korrutist $n = p_1^{k_1} \dots p_s^{k_s}$. 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 , $p \in \mathbb{P}$, sisemine otsesumma. $\square$

8.2 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.

Enne tõestuse juurde minekut mainime, et kui a on Abeli rühma $(A, +)$ element, siis selle elemendi poolt tekitatud alamrühm on

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}.$$

Lõpliku A korral on muidugi ka $\langle a \rangle$ lõplik.

Lause 8.9 *Kui mittetriviaalse lõpliku Abeli rühma C iga nullist erineva elemendi järk on p (s.t. $pC = \{0\}$), siis C on oma tsükliliste alamrühmade sisemine otsesumma.*

TÕESTUS. Võtame elemendi $0 \neq c_1 \in C$. Kui $C = \langle c_1 \rangle$, siis on meil otsesumma ühe otseliidetavaga. Kui $B_1 := \langle c_1 \rangle \subset C$, siis leidub $c_2 \in C \setminus \langle c_1 \rangle$. Vaatleme summat

$$B_2 := B_1 + \langle c_2 \rangle = \langle c_1 \rangle + \langle c_2 \rangle,$$

kus $|\langle c_1 \rangle| = p = |\langle c_2 \rangle|$. Ühisosa $\langle c_1 \rangle \cap \langle c_2 \rangle$ on alamrühm rühmas $\langle c_2 \rangle$, seega selle järk peab olema $p = |\langle c_2 \rangle|$ jagaja. Kui järk oleks p , siis $\langle c_1 \rangle \cap \langle c_2 \rangle = \langle c_2 \rangle$ ehk $c_2 \in \langle c_1 \rangle$, mis on vastuolu. Seega alamrühma $\langle c_1 \rangle \cap \langle c_2 \rangle$ järk on 1 ehk $\langle c_1 \rangle \cap \langle c_2 \rangle = \{0\}$. Sellega oleme tõestanud, et

$$B_2 = \langle c_1 \rangle \dot{+} \langle c_2 \rangle.$$

Kui nüüd $B_2 = C$, siis on vajalik esitus olemas. Vastasel korral leidub element $c_3 \in C \setminus B_2$ ja võime vaadelda summat

$$B_3 = B_2 + \langle c_3 \rangle.$$

Kuna $\langle c_3 \rangle \cap B_2 \leq \langle c_3 \rangle$ ja $c_3 \notin B_2$, siis

$$B_3 = B_2 \dot{+} \langle c_3 \rangle = \langle c_1 \rangle \dot{+} \langle c_2 \rangle \dot{+} \langle c_3 \rangle.$$

Kuna

$$B_1 \subset B_2 \subset B_3 \subset \dots \subseteq C$$

ja rühm C on lõplik, siis lõpliku arvu sammude järel peame jõudma sellise indeksini s , et

$$C = B_s = \langle c_1 \rangle \dot{+} \langle c_2 \rangle \dot{+} \dots \dot{+} \langle c_s \rangle.$$

□

Teoreem 8.10 *Lõplik Abeli p -rühm on oma mingite tsükliliste alamrühmade sisemine otsesumma.*

TÕESTUS. Järelduse 6.5 põhjal on lõpliku Abeli p -rühma järk algarvu p aste. Tõestame teoreemi induktsiooniga rühma järgu järgi. Täpsemalt näitame, et

$$(\forall n \in \mathbb{N})(A \text{ on Abeli rühm ja } |A| = p^n \implies A \text{ on tsükliliste alamrühmade otsesumma}).$$

Alus. Kui Abeli p -rühma järk on p , siis teoreemi 6.4 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 $n \geq 2$. Eeldame, et väide kehtib kõigi Abeli rühmade jaoks järguga p^k , kus $k < n$. Lihtne on näha, et hulk

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

on rühma A alamrühm. Kui $\text{ord}(a) = p^k$, siis järelduse 3.14 põhjal $\text{ord}(pa) = p^{k-1}$, seega pA on samuti p -rühm. Kui oletada, et $pA = A$, siis

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

sest lause 3.8 põhjal on iga A elemendi järk p^n jagaja. Vastuoluline võrdus $A = \{0\}$ näitab, et $pA \subset A$. Kuna pA on lõplik p -rühm, siis $|pA| = p^l$, kus $l < n$. On kaks võimalust.

1. $l = 0$ ehk $pA = \{0\}$. Siis A on tsükliliste alamrühmade otsesumma tänu lausele 8.9.

2. $0 < l < n$ ehk $|pA| = p^l \geq p$. Siis saame rühmale pA rakendada induktsiooni eeldust. Selle põhjal leiduvad nullist erinevad elemendid $pa_1, \dots, pa_r$ rühmas pA nii, et

$$pA = \langle pa_1 \rangle + \dots + \langle pa_r \rangle. \quad (13)$$

Tähistame

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

ja näitame, et see tsükliliste alamrühmade summa on otsesumma. Selleks kasutame lauset 7.8. Oletame, et

$$k_1a_1 + \dots + k_ra_r = 0, \quad (14)$$

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

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

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

kust võrduse (13) 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 (14) saame, et

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

kust võrduse (13) tõttu järeldub, et $pk_i a_i = 0$ iga $i \in \{1, \dots, r\}$ korral, muuhulgas $pk_j a_j = 0$. Olgu $\text{ord}(a_j) = p^e$, $e \in \mathbb{N} \cup \{0\}$. Lause 3.10 põhjal $p^e \mid pk_j$. Kuna $p \nmid k_j$, siis $p^e \mid p$ ehk $e \leq 1$. Järelikult $pa_j = 0$, mis on vastuolus sellega, et pa_j pidi olema nullist erinev.

Kuna võrdusest (14) järeldus, et $k_1a_1 = \dots = k_ra_r = 0$, siis oleme tõestanud, et

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

Tähistame

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

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

$$A = B + C.$$

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

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

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

$$c := a - k_1a_1 - \dots - k_ra_r \in C.$$

See tähendab, et

$$a = (k_1a_1 + \dots + k_ra_r) + c \in B + C.$$

Oleme tõestanud võrduse $A = B + C$.

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

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

on otsesumma, sest $\langle c_1 \rangle$ on tsükliline rühm algarvulise järguga p , seega lause 3.15 põhjal tema alamrühm $B \cap \langle c_1 \rangle$ peab olema triviaalne, $B \cap \langle c_1 \rangle = \{0\}$. Niisiis

$$B_1 = B \dot{+} \langle c_1 \rangle$$

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

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

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

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

□

Teoreemidest 8.8 ja 8.10 saame nüüd järgmise tulemuse.

Teoreem 8.11 *Lõplik Abeli rühm on oma mingite tsükliliste alamrühmade otsesumma.*

Järeldus 8.12 *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 8.13 Vaatleme lõplikku Abeli rühma $A = (\mathbb{Z}_{12}, +)$. Selle rühma p -komponendid on

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

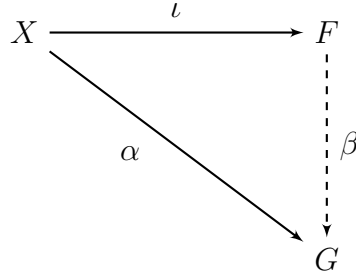
Seega $A = A_2 \dot{+} A_3$. Lause 7.5 põhjal on A isomorfne oma alamrühmade A_2 ja A_3 välise otsesummaga, $A \simeq A_2 \oplus A_3$. Et lõpliku arvu rühmade väline otsesumma on isomorfne nende otsekorrutisega, siis võime öelda, et

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

9 Vabad rühmad

9.1 Vaba rühma definitsioon

Definitsioon 9.1 Olgu F rühm, olgu X mittetühi hulk ja olgu $\iota : X \rightarrow F$ injektiivne kujutus. Öeldakse, et (F, ι) on **vaba rühm hulgal** X , kui iga rühma G ja iga kujutuse $\alpha : X \rightarrow G$ jaoks leidub üheselt määratud rühmade homomorfism $\beta : F \rightarrow G$ nii, et $\beta \circ \iota = \alpha$, s.t. diagramm



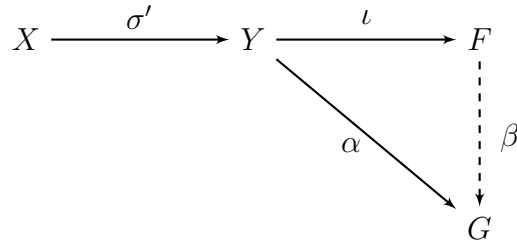
kommuteerub. Rühma nimetatakse **vabaks**, kui ta on vaba mingil hulgal.

Tuleb välja, et rühm on vaba parajasti siis, kui ta on vaba mingil oma alamhulgal.

Lause 9.2 Rühm F on vaba parajasti siis, kui leidub alamhulk $Y \subseteq F$ nii, et (F, ι) on vaba rühm hulgal Y , kus $\iota : Y \rightarrow F$ on sisestus.

TÕESTUS. TARVILIKKUS. Oletame, et F on vaba. Siis leidub hulk $X \neq \emptyset$ ja injektiivne kujutus $\sigma : X \rightarrow F$, mis rahuldab definitsioonis 9.1 kirjeldatud universaalomadust. Tähistame $Y := \sigma(X) \subseteq F$ ja olgu $\iota : Y \rightarrow F$ sisestus. Kujutus $\sigma' : X \rightarrow Y, x \mapsto \sigma(x)$ on bijektiivne ja $\iota \circ \sigma' = \sigma$.

Olgu nüüd $\alpha : Y \rightarrow G$ kujutus mingisse rühma G . Eelduse põhjal leidub üheselt määratud rühmade homomorfism $\beta : F \rightarrow G$ nii, et $\alpha \circ \sigma' = \beta \circ \iota \circ \sigma' = \beta \circ \sigma$. Siis iga $x \in X$ korral $\alpha(\sigma'(x)) = (\beta \circ \iota)(\sigma'(x))$ ning järelikult $\alpha = \beta \circ \iota$.



Oletame, et ka $\gamma : F \rightarrow G$ on rühmade homomorfism, mille korral $\gamma \circ \iota = \alpha$. Siis ka $\gamma \circ \sigma = \gamma \circ \iota \circ \sigma' = \alpha \circ \sigma'$, kust β ühesuse tõttu $\beta = \gamma$.

PIISAVUS. See on ilmne. □

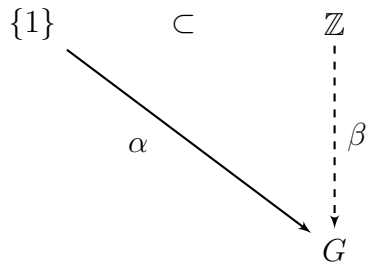
Näide 9.3 Rühm $(\mathbb{Z}, +)$ on vaba rühm hulgal $\{1\} \subset \mathbb{Z}$. Tõepoolest, kui $\alpha : \{1\} \rightarrow G, 1 \mapsto g$, on kujutus rühma G , siis defineerides $\beta : \mathbb{Z} \rightarrow G$ võrdusega

$$\beta(k) := g^k$$

saame rühmade homomorfismi, sest

$$\beta(k+l) = g^{k+l} = g^k g^l = \beta(k)\beta(l),$$

kusjuures $(\beta \circ \iota)(1) = \beta(1) = g^1 = g = \alpha(1)$.



Kui ka $\gamma : \mathbb{Z} \longrightarrow G$ on selline homomorfism, et $\gamma \circ \iota = \alpha$, siis iga $k \in \mathbb{N}$ korral

$$\gamma(k) = \gamma(1 + \dots + 1) = \gamma(1)^k = \alpha(1)^k = g^k = \beta(1)^k = \beta(1 + \dots + 1) = \beta(k)$$

ja $\gamma(-k) = -\gamma(k) = -\beta(k) = \beta(-k)$. Lisaks sellele $\gamma(0) = 1_G = g^0 = \beta(0)$. Seega $\beta = \gamma$.

9.2 Vaba rühma konstruktsioon

Definitsioonist ei paista välja, kas mõni vaba rühm üldse eksisteerib. Järgnevalt me näitamegi, et igal hulgal saab konstrueerida vaba rühma.

Teoreem 9.4 *Kui X on mittetühi hulk, siis leidub rühm F ja injektiivne kujutus $\iota : X \longrightarrow F$ nii, et (F, ι) on vaba rühm hulgal X ja $F = \langle \iota(X) \rangle$.*

TÕESTUS. Võtame ühe hulga, mis on hulgaga X lõikumatu, kuid sama võimsusega. Seda hulka ja tema elemente tähistame

$$X^{-1} = \{x^{-1} \mid x \in X\}.$$

Siin x^{-1} on puhtalt formaalne sümbol, mitte pöördelement mingis rühmas. **Sõnad** tähestikus $X \cup X^{-1}$ on järjestid selle hulga elementidest, mida me lühiduse mõttes kirjutame kujul

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_r^{\varepsilon_r},$$

kus $x_i \in X$, $\varepsilon_i \in \{1, -1\}$ ja $r \geq 0$. Me loeme, et

$$x_i^{\varepsilon_i} = \begin{cases} x_i, & \text{kui } \varepsilon_i = 1, \\ x_i^{-1}, & \text{kui } \varepsilon_i = -1. \end{cases}$$

Kui $r = 0$, siis me loeme, et w on tühi sõna ja me tähistame seda sümboliga 1. Kaks sõna on võrdsed, kui nad on võrdsed järjestitena.

Sõnade $w = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$ ja $v = y_1^{\eta_1} \dots y_s^{\eta_s}$ korrutis defineeritakse järjest kirjutamise ehk konkatenatsiooni abil:

$$wv := x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r} y_1^{\eta_1} \dots y_s^{\eta_s},$$

kusjuures me loeme, et $w1 = w = 1w$. Lisaks sellele defineerime sõna w pöörd sõna

$$w^{-1} := x_r^{-\varepsilon_r} \dots x_1^{-\varepsilon_1}$$

ja loeme, et $1^{-1} = 1$.

Olgu nüüd S kõigi sõnade hulk tähestikus $X \cup X^{-1}$. On selge, et S on monoid, täpsemalt vaba monoid hulgal $X \cup X^{-1}$ (tihti kirjutatakse $S = (X \cup X^{-1})^*$). Defineerime sellel hulgal seose $\sim$ järgmisel viisil. Olgu $w, v \in S$. Ütleme, et $w \sim v$, kui sõnast w on võimalik saada sõna v lõpliku arvu teisenduste abil, mis on järgnevat tüüpi:

(a) mingisse kohta sõnas sümboolite paari xx^{-1} või $x^{-1}x$, kus $x \in X$, lisamine,

(b) sõna mingist kohast sümboolite paari xx^{-1} või $x^{-1}x$, kus $x \in X$, kustutamine.

(Näiteks kui $X = \{x, y, z\}$, siis $xyy^{-1}z^{-1}xy \sim_{(b)} xz^{-1}xy \sim_{(a)} xz^{-1}xx^{-1}xy$.) Teisenduste arv võib olla ka 0, s.t. me loeme, et kui $w = v$, siis $w \sim v$.

Lihtne on aru saada, et seos $\sim$ on ekvivalentsiseos hulgal S . Sõna w ekvivalentsiklassi seose $\sim$ järgi tähistame $[w]$. Vaatleme faktorhulka

$$F := S/\sim = \{[w] \mid w \in S\}.$$

Defineerime hulgal F korrutamistehte võrdusega

$$[w][v] := [wv].$$

Kui $w \sim w'$ ja $v \sim v'$, siis ilmselt ka $wv \sim w'v'$, seega korrutamise definitsioon on korrektne. Korrutamine on assotsiatiivne, sest mistahes sõnade w, v, u korral

$$([w][v])[u] = [wv][u] = [(wv)u] = [w(vu)] = [w][vu] = [w]([v][u]).$$

Selle korrutamise suhtes leidub ühikelement $[1]$, sest iga $[w] \in F$ korral

$$[w][1] = [w1] = [w] = [1w] = [1][w].$$

Kui $w = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$, siis elemendi $[w] \in F$ pöördelemendiks on $[w^{-1}]$, sest

$$[w][w^{-1}] = [x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r} x_r^{-\varepsilon_r} \dots x_1^{-\varepsilon_1}] = [x_1^{\varepsilon_1} \dots x_{r-1}^{\varepsilon_{r-1}} x_{r-1}^{-\varepsilon_{r-1}} \dots x_1^{-\varepsilon_1}] = \dots = [x_1^{\varepsilon_1} x_1^{-\varepsilon_1}] = [1]$$

ja analoogiliselt $[w^{-1}][w] = [1]$. Niisiis oleme näidanud, et F on rühm.

Defineerime kujutuse $\iota : X \longrightarrow F$ võrdusega

$$\iota(x) := [x]$$

iga $x \in X$ korral. Kuna iga $[w] \in F$ on esitatav kujul

$$[w] = [x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}] = [x_1]^{\varepsilon_1} \dots [x_r]^{\varepsilon_r} = \iota(x_1)^{\varepsilon_1} \dots \iota(x_r)^{\varepsilon_r} \in \langle \iota(X) \rangle,$$

siis F on tekitatud alamhulga $\iota(X)$ poolt, $F = \langle \iota(X) \rangle$.

Me näitame, et (F, ι) on vaba rühm hulgal X . Vaatleme kujutust $\alpha : X \longrightarrow G$, kus G on mingi rühm. Defineerime kujutuse $\bar{\beta} : S \longrightarrow G$ võrdusega

$$\bar{\beta}(x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}) := \alpha(x_1)^{\varepsilon_1} \dots \alpha(x_r)^{\varepsilon_r}.$$

Kui mingis sõnas sisaldub korrutis xx^{-1} või $x^{-1}x$, siis $\alpha(x)\alpha(x)^{-1} = 1_G$ või $\alpha(x)^{-1}\alpha(x) = 1_G$, kus 1_G on rühma G ühikelement. Seega kui $w, v \in S$ ja $w \sim v$, siis $\bar{\beta}(w) = \bar{\beta}(v)$ rühmas G . Defineerides nüüd $\beta : F \longrightarrow G$ võrdusega

$$\beta([w]) := \bar{\beta}(w)$$

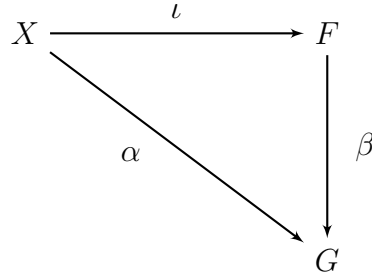
saame korrektselt defineeritud kujutuse. See on rühmade homomorfism, sest mistahes $[w], [v] \in F$ korral

$$\beta([w][v]) = \beta([wv]) = \bar{\beta}(wv) = \bar{\beta}(w)\bar{\beta}(v) = \beta([w])\beta([v]).$$

Kuna iga $x \in X$ korral

$$(\beta \circ \iota)(x) = \beta([x]) = \bar{\beta}(x) = \alpha(x),$$

siis $\beta \circ \iota = \alpha$.

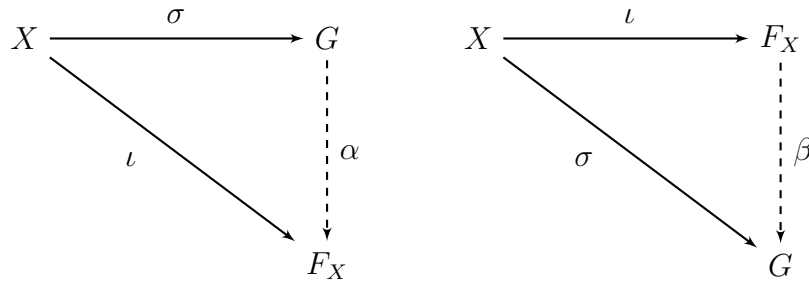


Ühesuse näitamiseks oletame, et ka $\gamma : F \rightarrow G$ on mingi selline rühmade homomorfism, et $\gamma \circ \iota = \alpha$. Siis $\gamma \circ \iota = \beta \circ \iota$ ehk $\gamma(\iota(x)) = \beta(\iota(x))$ iga $x \in X$ korral. Kuna $F = \langle \iota(X) \rangle$, siis $\gamma = \beta$. $\square$

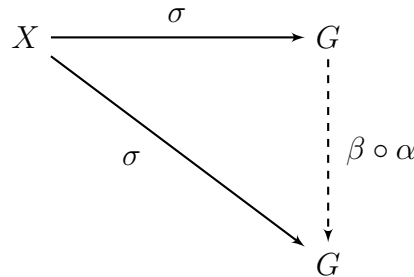
Selles tõestuses konstrueeritud rühma tähistame edaspidises F_X . Tuleb välja, et isomorfismi täpsuseni ongi see rühm ainuke vaba rühm hulgal X .

Lause 9.5 Iga vaba rühm hulgal X on isomorfne rühmaga (F_X, ι) .

TÕESTUS. Olgu ka (G, σ) mingi vaba rühm hulgal X . Kasutades universaalomadusi saame leida rühmade homomorfismid α ja β nii, et kolmnurgad



kommuteeruvad. Siis ka $\beta \circ \alpha \circ \sigma = \beta \circ \iota = \sigma$ ehk kolmnurk



kommuteerub. Kuna ka id_G rahuldab võrdust $id_G \circ \sigma = \sigma$, siis ühesuse tõttu $\beta \circ \alpha = id_G$. Analoogiliselt $\alpha \circ \beta = id_{F_X}$ ning seega on α (ja samuti β) rühmade isomorfism. $\square$

Meie järgmine eesmärk on näidata, et vaba rühma F_X iga elementi saab üheselt esitada teatud kanoonilisel kujul. Selleks läheb vaja teatud abitulemusi.

Definitsioon 9.6 Öeldakse, et sõna w tähestikus $X \cup X^{-1}$ on **taandatud**, kui ta ei sisalda kõrvutiolevate sümbolite paare xx^{-1} ega $x^{-1}x$, kus $x \in X$. Loeme, et ka tühi sõna on taandatud.

On selge, et igast sõnast w on võimalik lõpliku arvu taandamistega (s.t. sammudega tüüpi (b)) saada taandatud sõna w^* . Seejuures $w \sim w^*$. Me kirjutame $w \longrightarrow w'$, kui sõna w' on saadud sõnast w (b)-tüüpi teisenduse (s.t. ühe taandamise) abil. Lisaks sellele kasutame tähistust $w \rightsquigarrow w'$, kui w' on saadud sõnast w lõpliku arvu taandamiste abil. Näiteks $X = \{x, y, z\}$ korral võime taandada:

$$w = xy^{-1}yy^{-1}zz^{-1}x^{-1} \longrightarrow xy^{-1}\underline{zz^{-1}}x^{-1} \longrightarrow xy^{-1}x^{-1} = w^*.$$

Samas taandamisi on enamasti võimalik teha erinevas järjekorras ja tekib küsimus, kas saadav taandatud sõna on üheselt määratud? Tuleb välja, et on. Selle tõestamiseks läheb vaja järgmist lemmat.

Lemma 9.7 *Kui $w \longrightarrow w_1$, $w \longrightarrow w_2$ ja $w_1 \neq w_2$, siis leidub sõna u nii, et $w_1 \longrightarrow u$ ja $w_2 \longrightarrow u$.*

TÕESTUS. Olgu

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_r^{\varepsilon_r}.$$

Kuna w -s on võimalik sooritada kaks erinevat taandamist, siis $r \geq 3$. Olgu w_1 saadud w -st paari $x_k^{\varepsilon_k} x_{k+1}^{\varepsilon_{k+1}} = x_k^{\varepsilon_k} x_k^{-\varepsilon_k}$ taandamisel ja olgu w_2 saadud w -st paari $x_l^{\varepsilon_l} x_{l+1}^{\varepsilon_{l+1}} = x_l^{\varepsilon_l} x_l^{-\varepsilon_l}$ taandamisel. Kuna $w_1 \neq w_2$, siis $k \neq l$. Üldisust kitsendamata võime eeldada, et $k < l$. Kui nüüd $k + 2 \leq l$, siis taandatavad paarid ei lõiku ja on selge, et soovitud u leidub.

Näitame, et juhul $k + 1 = l$ tekib vastuolu. Oletamegi, et $k + 1 = l$. Kui $\varepsilon_k = 1$, siis sõnas w on alamsõna

$$x_k^{\varepsilon_k} x_{k+1}^{\varepsilon_{k+1}} x_{k+2}^{\varepsilon_{k+2}} = x_k x_k^{-1} x_k.$$

Sõna w_1 saamiseks taandatakse sellest alamsõnast 2 esimest tähte ja w_2 saamiseks 2 viimast tähte. Mõlemal juhul jääb alamsõnast järele x_k , mis tähendab, et $w_1 = w_2$, vastuolu. Kui $\varepsilon_k = -1$, siis sõnas w on alamsõna

$$x_k^{\varepsilon_k} x_{k+1}^{\varepsilon_{k+1}} x_{k+2}^{\varepsilon_{k+2}} = x_k^{-1} x_k x_k^{-1},$$

kust saame vastuolu analoogiliselt eelneva juhuga. □

Lemma 9.8 *Iga sõna w jaoks leidub üheselt määratud taandatud sõna w^* nii, et $w \rightsquigarrow w^*$.*

TÕESTUS. Eespool juba märkisime, et selline w^* leidub. Vaja on tõestada selle ühesus. Teeme seda induktsiooniga w pikkuse järgi. Kui sõna pikkus on 0, 1 või 2, siis väide ilmselt kehtib. Olgu $k \geq 2$ ja eeldame, et väide kehtib kõigi sõnade jaoks, mille pikkus on ülimalt k . Vaatleme sõna w , mille pikkus on $k + 1$. On kolm võimalust.

- 1) Sõna w on taandatud. Siis $w^* = w$ on üheselt määratud.
- 2) Sõna w sisaldab täpselt ühte kõrvutiolevate sümbolite paari kujul xx^{-1} või $x^{-1}x$. Taandades selle paari saame sõna u , mille pikkus on väiksem kui k . Induktsiooni eelduse põhjal leidub üheselt määratud w^* nii, et $u \rightsquigarrow w^*$. Iga taandamiste jada, mis viib w -st taandatud sõnani, peab algama u -ga, seega w^* on ka w jaoks ainuke selline sõna, et $w \rightsquigarrow w^*$.
- 3) Sõnas w on võimalik sooritada vähemalt kaks taandamist erinevates kohtades, mis annavad tulemuseks sõnad w_1 ja w_2 . Kui $w_1 = w_2$, siis tähistame $u := w_1 = w_2$. Kui $w_1 \neq w_2$, siis tänu lemmale 9.7 saab sõnad w_1 ja w_2 taandada mingiks sõnaks u . Mõlemal juhul saame u jaoks leida sellise taandatud sõna w^* , et $u \rightsquigarrow w^*$. Kuna ka $w_1 \rightsquigarrow w^*$ ja $w_2 \rightsquigarrow w^*$ ning sõnad w_1, w_2 on lühemad kui w , siis induktsiooni eeldus ütleb, et w^* on ainuke taandatud sõna, mis on võimalik w_1 -st ja w_2 -st taandamise abil saada. Seega ükskõik millisest taandamisest sõnas w alustada, jõuame alati sama taandatud sõnani w^* . □

Teoreem 9.9 *Vabas rühmas $F_X = (X \cup X^{-1})^*/\sim$ sisaldab iga ekvivalentsiklass seose $\sim$ järgi täpselt ühte taandatud sõna tähestikus $X \cup X^{-1}$.*

TÕESTUS. Oletame, et $w \longrightarrow w'$. Siis leiduvad üheselt määratud taandatud sõnad u ja v nii, et $w \rightsquigarrow u$ ja $w' \rightsquigarrow v$. Kuna ka $w \longrightarrow w' \rightsquigarrow v$, siis lemma 9.8 tõttu $u = v$.

Olgu nüüd $w \sim w'$, kus w, w' on taandumatud sõnad. Siis leidub lõplik sõnade jada

$$w = w_0, w_1, w_2, \dots, w_n = w'$$

nii, et iga $i \in \{1, \dots, n\}$ korral w_i on saadud w_{i-1} -st kas taandamise või sümbolite paari lisamise abil. See tähendab, et $w_{i-1} \longrightarrow w_i$ või $w_i \longrightarrow w_{i-1}$. Tänu lemmale 9.8 leidub iga w_i jaoks üheselt määratud taandatud sõna u_i nii, et $w_i \rightsquigarrow u_i$. Tõestuse esimese lõigu põhjal

$$w = u_0 = u_1 = \dots = u_n = w'.$$

□

Järeldus 9.10 *Vabas rühmas F_X kehtib võrdus $[w] = [u]$ parajasti siis, kui $w^* = u^*$.*

TÕESTUS. TARVILIKKUS. Eeldame, et $[w] = [u]$. Kuna taandatud sõnad w^* ja u^* kuuluvad ekvivalentsiklassi $[w]$, siis teoreemi 9.9 tõttu peavad nad olema võrdsed.

PIISAVUS. Eeldame, et $w^* = u^*$. Kuna $w \rightsquigarrow w^*$ ja $u \rightsquigarrow u^*$, siis $[w] = [w^*] = [u^*] = [u]$. □

See järeldus on väga kasulik. See annab meile lihtsa **algoritmi kahe elemendi võrdlemiseks vabas rühmas F_X** : võtame elemendid $[w]$ ja $[u]$, leiame mingil viisil taandatud sõnad w^* ja u^* (seda saab teha lõpliku arvu sammudega) ning võrdleme neid.

Tänu teoreemile 9.9 saab vaba rühma F_X iga elemendi üheselt esitada kujul $[w]$, kus w on taandatud sõna, s.t. $w = y_1^{\varepsilon_1} \dots y_r^{\varepsilon_r}$, kus $y_i \in X$, $\varepsilon_i \in \{1, -1\}$ ja w ei sisalda alamsõnu xx^{-1} ega $x^{-1}x$, kus $x \in X$. (Me lubame siin ka olukorda $r = 0$; sellisel juhul loeme, et w on tühi sõna.) Siis faktorühma tehete definitsioonide põhjal $[w] = [y_1]^{\varepsilon_1} \dots [y_r]^{\varepsilon_r}$. Korrutades kokku kõrvuti olevad tegurid, milles on sama sümbol y_i , saame $[w]$ esitada üheselt kujul

$$[w] = [x_1]^{l_1} \dots [x_s]^{l_s},$$

kus $0 \leq s \leq r$, $l_i \in \mathbb{Z} \setminus \{0\}$, $x_i \in X$ ja $x_i \neq x_{i+1}$. Arvestades $\iota : X \longrightarrow F_X$ definitsiooni võime kirjutada ka

$$[w] = \iota(x_1)^{l_1} \dots \iota(x_s)^{l_s}.$$

Tähistuste lihtsustamiseks kirjutatakse harilikult $[w]$ asemel w . Seega saab rühma F_X iga elemendi w üheselt esitada kujul

$$w = x_1^{l_1} \dots x_s^{l_s},$$

kus $0 \leq s$, $l_i \in \mathbb{Z} \setminus \{0\}$, $x_i \in X$ ja $x_i \neq x_{i+1}$. Sellist esitust nimetatakse elemendi w **normaalkujuks**.

Teoreem 9.11 *Rühm G on vaba parajasti siis, kui leidub alamhulk $X \subseteq G$ nii, et G iga element g on üheselt esitatav kujul*

$$g = x_1^{l_1} x_2^{l_2} \dots x_s^{l_s},$$

kus $s \geq 0$, $l_i \in \mathbb{Z} \setminus \{0\}$, $x_i \in X$ ja $x_i \neq x_{i+1}$.

TÕESTUS. TARVILIKKUS. Oletame, et G on vaba rühm. Lause 9.5 põhjal leidub mingi hulk X nii, et G on isomorfne vaba rühmaga (F_X, ι) . Eelnev arutelu näitab, et F_X elemente saab üheselt esitada kujul

$$z_1^{l_1} z_2^{l_2} \dots z_s^{l_s},$$

kus $s \geq 0$, $l_i \in \mathbb{Z} \setminus \{0\}$, $z_i \in \iota(X)$ ja $z_i \neq z_{i+1}$. Sarnane omadus on siis ka isomorfse rühmal G .

PIISAVUS. Eeldame nüüd, et rühmal G on kirjeldatud omadus. Moodustame vaba rühma (F_X, ι) , kus $\iota : x \mapsto [x]$. Kuna $F_X = \langle \iota(X) \rangle$, siis kujutus

$$\varphi : G \longrightarrow F_X, \quad x_1^{l_1} x_2^{l_2} \dots x_s^{l_s} \mapsto \iota(x_1)^{l_1} \iota(x_2)^{l_2} \dots \iota(x_s)^{l_s}$$

on surjektiivne. Kui $g = x_1^{l_1} x_2^{l_2} \dots x_s^{l_s} \in \text{Ker } \varphi$, siis

$$[1] = \varphi(g) = \iota(x_1)^{l_1} \iota(x_2)^{l_2} \dots \iota(x_s)^{l_s} = [x_1^{l_1} x_2^{l_2} \dots x_s^{l_s}].$$

Tänu sellele, et $x_1^{l_1} x_2^{l_2} \dots x_s^{l_s}$ on taandatud sõna tähestikus $X \cup X^{-1}$, saame järeldusest 9.10, et $x_1^{l_1} x_2^{l_2} \dots x_s^{l_s}$ on tühi sõna. See tähendab, et $s = 0$ ja $g = 1_G$. Seega $\text{Ker } \varphi = \{1_G\}$, mis tähendab seda, et φ on injektiivne.

Saab näidata, et φ on rühmade homomorfism ning kokkuvõttes ka rühmade isomorfism. Järelikult G on vaba rühm. $\square$

Kui alamhulk $X \subseteq G$ on selles lauses kirjeldatud omadusega, siis öeldakse, et X on vaba rühma G **baas**. Teoreem 9.11 ütleb seda, et rühm G on vaba parajasti siis, kui temas leidub alamhulk X nii, et iga G element on saadav X elementidest rühma tehete (korrumise ja pöördlemendi võtmise) abil ühesel viisil.

Vabade rühmade tähtsust rõhutab järgmine tulemus.

Lause 9.12 Iga rühm on vaba rühma epimorfne kujutis. Seega iga rühm on isomorfne vaba rühma faktorrühmaga.

TÕESTUS. Olgu G rühm, võtame hulga $X := G$ ja vaatleme vaba rühma (F_X, ι) . Univeraalomaduse põhjal leidub üheselt määratud rühmade homomorfism $\beta : F_X \longrightarrow G$ nii, et $\beta \circ \iota = id_G$.

$$\begin{array}{ccc} X & \xrightarrow{\iota} & F_X \\ & \searrow id_G & \downarrow \beta \\ & & G \end{array}$$

Kuna id_G on surjektiivne, siis ka β peab olema surjektiivne, teiste sõnadega G on F_X epimorfne kujutis. Homomorfismiteoreemist (vt. järeldust 2.2) saame, et $G \cong F_X / \text{Ker } \beta$. $\square$

10 Lihtsad rühmad

Rühm G on lihtne, kui tema ainsad normaalsed alamrühmad on G ja $\{1_G\}$.

Selles peatükis olgu R kõikjal kommutatiivne ühikelemendiga ring. Me vaatleme maatrikseid üle ringi R . Sümboliga E tähistame ühikmaatriksit, kusjuures selle järk peaks igas olukorras olema selge kontekstist. Iga $n \in \mathbb{N}$, $i, j \in \{1, \dots, n\}$, $i \neq j$ ja $a \in R$ korral tähistame sümboliga $E_{ij}(a)$ sellist n -ndat järku ruutmaatriksit, mis on saadud ühikmaatriksist kohal (i, j) oleva nulli asendamisel elemendiga a . Need on sellised elementaarmaatriksid, millega maatriksit A vasakult korrutades liidetakse A i -ndale reale elemendiga a korrutatud j -s rida.

Definitsioon 10.1 Maatrikseid

$$aE = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a \end{pmatrix},$$

kus $a \in R \setminus \{0\}$, nimetatakse **skalaarmaatriksiteks**.

Definitsioon 10.2 Rühma G alamhulga S **tsentralisaator** on hulk

$$C_G(S) = \{g \in G \mid (\forall s \in S) gs = sg\}.$$

Definitsioon 10.3 Rühma G **tsenter** on hulk

$$Z(G) = C_G(G) = \{g \in G \mid (\forall a \in G) ga = ag\}.$$

Lause 10.4 Alamrühma $SL_n(R)$ tsentralisaator rühmas $GL_n(R)$ koosneb skalaarmaatriksitest.

TÕESTUS. Lihtne on näha, et iga skalaarmaatriks kommuteerub kõigi maatriksitega rühmast $GL_n(R)$. Näitame, et kui maatriks $A = (a_{ij})$ kuulub tsentralisaatorisse, siis ta on skalaarmaatriks. Kui $i \neq j$, siis elementaarmaatriks $E_{ij}(1) \in SL_n(R)$ ning järelikult $E_{ij}(1)A = AE_{ij}(1)$. Kirjutame $E_{ij}(1)$ kujul $E_{ij}(1) = E + E'_{ij}(1)$, kus maatriksis $E'_{ij}(1)$ on kohal (i, j) ringi R ühikelement ja mujal nullid. Siis $(E + E'_{ij}(1))A = A(E + E'_{ij}(1))$, millest distributiivsust ja teisi maatriksite omadusi kasutades saame, et

$$E'_{ij}(1)A = AE'_{ij}(1).$$

Kui $k \neq i$, siis maatriksis $AE'_{ij}(1)$ on kohal (k, j) element a_{ki} ning maatriksis $E'_{ij}(1)A$ on samal kohal element 0. See kehtib suvaliste k ja i , $k \neq i$, korral, seega maatriksis A on väljaspool peadiagonaali nullid. Kohal (i, j) on maatriksis $AE'_{ij}(1)$ element a_{ii} ja maatriksis $E'_{ij}(1)A$ element a_{jj} . See kehtib mistahes i, j korral, seega A peadiagonaali elemendid on omavahel võrdsed. Kuna A on regulaarne, siis peadiagonaalil olev element peab olema nullist erinev. Olemegi saanud, et A on skalaarmaatriks. $\square$

Järeldus 10.5 Iga $n \in \mathbb{N}$ korral

- $Z(GL_n(R)) = \{aE \mid a \in R \setminus \{0\}\};$
- $Z(SL_n(R)) = \{aE \mid a \in R \setminus \{0\}, a^n = 1\}.$

Definitsioon 10.6 Faktorühma

$$PGL_n(R) := GL_n(R)/Z(GL_n(R))$$

nimetatakse n -ndat järku **üldiseks projektiivseks lineaarrühmaks** üle ringi R ja faktorühma

$$PSL_n(R) := SL_n(R)/Z(SL_n(R)) = SL_n(R)/(SL_n(R) \cap Z(GL_n(R)))$$

nimetatakse n -ndat järku **spetsiaalseks projektiivseks lineaarrühmaks** üle ringi R .

Definitsioon 10.7 Olgu K korpus. Matrikseid $E_{ij}(a)$, kus $a \in K^*$ ja $i \neq j$, nimetatakse **transveksioonideks** (ingl. k. *transvection*).

Lemma 10.8 Iga matriks rühmas $SL_n(K)$, kus K on korpus, on transveksioonide korutus.

TÕESTUS. On selge, et kõik transveksioonid kuuluvad rühma $SL_n(K)$ ja et transveksiooni $E_{ij}(a)$ pöördmatriks $E_{ij}(-a)$ on transveksioon.

Olgu $A = (a_{ij}) \in SL_n(K)$. Teisendame selle matriksi ühikmatriksiks *ainult* ridade liitmisteisendustega, mis on samaväärne transveksioonidega vasakult korrutamiseks. Kuna $|A| = 1_K$, siis A esimeses veerus peab leiduma nullist erinev element. Eeldame, et $a_{21} \neq 0$ (kui $a_{21} = 0$, siis liidame teisele reale mingi rea nii, et kohale $(2, 1)$ tekiks nullist erinev element). Nüüd liidame esimesele reale teise rea, mis on korrutatud elemendiga $a_{21}^{-1}(1_K - a_{11})$. Saame matriksi, kus kohal $(1, 1)$ on element 1_K . Selle abil saame muuta nulliks kõik esimese veeru elemendid välja arvatud esimene. Jätkame sarnasel viisil tekitades nulle allapoole peadiagonaali ja hiljem liikudes paremalt vasakule ülespoole peadiagonaali kuni jõuame ühikmatriksini. Nii oleme leidnud transveksioonid $T_1, \dots, T_k$ nii, et $T_k T_{k-1} \dots T_1 A = E$, kust

$$A = (T_k T_{k-1} \dots T_1)^{-1} = T_1^{-1} \dots T_{k-1}^{-1} T_k^{-1}.$$

□

Lause 10.9 Kui normaalne alamrühm $N \trianglelefteq SL_2(\mathbb{R})$ sisaldab transveksiooni, siis $N = SL_2(\mathbb{R})$.

TÕESTUS. Vaatleme transveksiooni $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in N$, kus $a \neq 0$. (Kui $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \in N$, siis on tõestus analoogiline.) Tõestame, et

$$(\forall k \in \mathbb{R}^*) \quad \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in N. \quad (15)$$

Kui see nii on, siis tänu normaalse alamrühma definitsioonile ka

$$N \ni \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix}.$$

See tähendab, et N sisaldab kõiki transveksioone ning järelikult $SL_2(\mathbb{R}) = N$ tänu lemmale 10.8.

Kuna

$$N \ni \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}^{-1} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} x^{-1} & ax \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix}, \quad (16)$$

siis iga $x, y \in \mathbb{R}^*$ korral ka

$$N \ni \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & ay^2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -ay^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a(x^2 - y^2) \\ 0 & 1 \end{pmatrix}, \quad (17)$$

sest N on alamrühm.

Iga reaalarv b on esitatav kahe reaalarvu ruutude vahena:

$$\frac{(b+1)^2}{4} - \frac{(b-1)^2}{4} = \frac{b^2 + 2b + 1 - b^2 + 2b - 1}{4} = \frac{4b}{4} = b.$$

Võttes $k \in \mathbb{R}^*$ saame arvu $a^{-1}k$ esitada ruutude vahena $a^{-1}k = x^2 - y^2$, kus $x, y \in \mathbb{R}$. Seega (17) tõttu

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \cdot a^{-1}k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a(x^2 - y^2) \\ 0 & 1 \end{pmatrix} \in N.$$

□

Lause 10.10 *Faktorühm G/H on lihtne parajasti siis, kui*

$$(\forall N \trianglelefteq G)(H \subset N \implies N = G).$$

TÕESTUS. **TARVILIKKUS.** Eeldame, et G/H on lihtne. Olgu $H \subset N \trianglelefteq G$. Siis on lihtne veenduda, et

$$K := \{aH \mid a \in N\} \trianglelefteq G/H.$$

Kui $c \in N \setminus H$, siis $H \neq cH \in K$ ja seega $\{H\} \subset K$. Kuna G/H on lihtne, siis $K = G/H$. Järelikult iga $g \in G$ jaoks leidub $a \in N$ nii, et $gH = aH$. Et $g \in aH$, siis $g = ah$ mingi $h \in H$ korral. Kuna $H \subset N$ ja N on alamrühm, siis $g \in N$. Seega $G = N$.

PIISAVUS. Eeldame, et $N = G$, kui $H \subset N \trianglelefteq G$. Olgu K faktorühma G/H mittetriviaalne normaaljagaja. Teoreemi 2.9 põhjal

$$H \trianglelefteq M = \pi^{-1}(K) = \{x \in G \mid xH \in K\} \trianglelefteq G,$$

kus $\pi : G \longrightarrow G/H$ on loomulik projektsioon. Kuna $\{H\} \neq K$, siis leidub $y \in G$ nii, et $H \neq yH \in K$, muuhulgas $y \notin H$. Nüüd $y \in M \setminus H$. Eelduse tõttu $M = G$. Seega iga $x \in G$ korral $xH \in K$, mis tähendab, et $G/H = K$. □

Selle paragrahvi põhitulemus on järgmine.

Teoreem 10.11 *Rühm $PSL_2(\mathbb{R})$ on lihtne.*

TÕESTUS. Definiitsiooni põhjal

$$PSL_2(\mathbb{R}) := SL_2(\mathbb{R})/Z(SL_2(\mathbb{R})),$$

kus $Z(SL_2(\mathbb{R})) = \{E, -E\}$. Olgu $N \trianglelefteq SL_2(\mathbb{R})$ ja $Z(SL_2(\mathbb{R})) \subset N$. Tänu lausele 10.10 piisab näidata, et $N = SL_2(\mathbb{R})$. Selleks piisab lause 10.9 põhjal tõestada, et N sisaldab vähemalt ühte transvekttsiooni.

Eelduste põhjal leidub matriks

$$A = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in N \setminus \{E, -E\}.$$

Siis $1 = \det(A) = xt - yz$. Kui A ise on transvekttsioon, siis on kõik korras. Me näitame, et kui A ei ole transvekttsioon, siis ikkagi N peab sisaldama mingit transvekttsiooni. Selleks vaatleme nelja juhtu.

1. $z = 0$. Siis $t = x^{-1}$ ja $A = \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}$. Võttes $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{R})$ näeme, et

$$\begin{aligned} N \ni A \cdot B A^{-1} B^{-1} &= \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & -y \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} x & x+y \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} x^{-1} & -x^{-1}-y \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & -1-xy+x^2+xy \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1+x^2 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

kus viimane matriks on transvekttsioon, kui $-1+x^2 \neq 0$ ehk $x^2 \neq 1$. Võrdus $x^2 = 1$ kehtib parajasti siis, kui $x = 1$ või $x = -1$. Esimesel juhul oleks A transvekttsioon. Teisel juhul

$$N \ni A^2 = \begin{pmatrix} -1 & y \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & y \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -2y \\ 0 & 1 \end{pmatrix}.$$

Viimane matriks on transvekttsioon, sest $y \neq 0$ (muidu $A = -E$).

2. $z \neq 0, y = 0$. Siis $A = \begin{pmatrix} x & 0 \\ z & x^{-1} \end{pmatrix}$. Võttes $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{R})$ näeme, et

$$N \ni B A B^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ z & x^{-1} \end{pmatrix} B^{-1} = \begin{pmatrix} -z & -x^{-1} \\ x & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} x^{-1} & -z \\ 0 & x \end{pmatrix}.$$

Viimane matriks on sellisel kujul nagu juhu 1 matriksid.

3. $z \neq 0, y \neq 0, t = 0$. Siis $A = \begin{pmatrix} x & y \\ -y^{-1} & 0 \end{pmatrix}$. Võttes $B = \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}$ saame, et

$$\begin{aligned} N \ni B A B^{-1} \cdot A^{-1} &= \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix} \begin{pmatrix} x & y \\ -y^{-1} & 0 \end{pmatrix} \begin{pmatrix} 2^{-1} & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & -y \\ y^{-1} & x \end{pmatrix} \\ &= \begin{pmatrix} 2x & 2y \\ -2^{-1}y^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & -2^{-1}y \\ 2y^{-1} & 2x \end{pmatrix} = \begin{pmatrix} 2^2 & -xy+4xy \\ 0 & 2^{-2} \end{pmatrix} = \begin{pmatrix} 4 & 3xy \\ 0 & \frac{1}{4} \end{pmatrix}. \end{aligned}$$

Viimane matriks on sellisel kujul nagu juhu 1 matriksid.

4. $z \neq 0, y \neq 0, t \neq 0$. Kuna $xt - yz = 1$, siis $tx = 1 + yz$. Võttes $B = \begin{pmatrix} 1 & xz^{-1} \\ 0 & 1 \end{pmatrix}$ saame, et

$$\begin{aligned} N \ni B^{-1} A^{-1} B &= B^{-1} \begin{pmatrix} t & -y \\ -z & x \end{pmatrix} \begin{pmatrix} 1 & xz^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -xz^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t & txz^{-1}-y \\ -z & 0 \end{pmatrix} \\ &= \begin{pmatrix} t+x & txz^{-1}-y \\ -z & 0 \end{pmatrix} \begin{pmatrix} t+x & (1+yz)z^{-1}-y \\ -z & 0 \end{pmatrix} = \begin{pmatrix} t+x & z^{-1} \\ -z & 0 \end{pmatrix}. \end{aligned}$$

See on juhtum 3. □

11 Lahenduvad rühmad

Definitsioon 11.1 Rühma G alamrühmade jada

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{k-1} \triangleleft G_k = G,$$

kus iga alamrühm on normaaljagaja järgnevas alamrühmas, nimetatakse rühma G **normaaljadaks**. Faktorrühmi

$$G_{i+1}/G_i, \quad i = 0, 1, \dots, k-1,$$

nimetatakse selle **normaaljada faktoriteks**.

Definitsioon 11.2 Rühma G nimetatakse **lahenduvaks**, kui tal leidub kommutatiivsete faktoritega normaaljada. Muuhulgas ka ühe-elementiline rühm loetakse lahenduvaks.

Näide 11.3 Iga Abeli rühm $G \neq \{1\}$ on lahenduv, sest normaaljada $\{1\} \triangleleft G$ ainuke faktor $G/\{1\} \cong G$ on kommutatiivne.

Näide 11.4 Näitame, et substitutsioonirühm S_3 on lahenduv. Selles rühmas leidub kommutatiivne alamrühm

$$H = \langle (1\ 2\ 3) \rangle = \{(1\ 2\ 3), (1\ 3\ 2), \varepsilon\}.$$

Kuna selle alamrühma indeks on 2, siis on ta tänu lausele 1.50 normaaljagaja rühmas S_3 . Normaaljada

$$\{\varepsilon\} \triangleleft H \triangleleft S_3$$

on kommutatiivsete faktoritega, sest $H/\{\varepsilon\} \cong H$ ja $S_3/H \cong \mathbb{Z}_2$ on kommutatiivsed rühmad.

Tuleb välja, et lahenduvate rühmade klass on kinnine alamrühmade ja faktorrühmade võtmise suhtes.

Lause 11.5 *Lahenduva rühma alamrühm on lahenduv.*

TÕESTUS. Olgu $H \leq G$, kus G on lahenduv rühm. Vaatleme kommutatiivsete faktoritega normaaljada

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{k-1} \triangleleft G_k = G.$$

Iga $i \in \{0, 1, \dots, k\}$ korral defineerime

$$H_i := H \cap G_i \leq G.$$

On selge, et $H_i \subseteq H_{i+1}$ ja seega $H_i \leq H_{i+1}$. Veendume, et $H_i \trianglelefteq H_{i+1}$. Tõepoolest, iga $g \in H_{i+1} = H \cap G_{i+1}$ ja $h \in H_i = H \cap G_i$ korral $g^{-1}hg \in H$ (sest $g \in H$) ja $g^{-1}hg \in G_i$ (sest $G_i \triangleleft G_{i+1}$), seega $g^{-1}hg \in H \cap G_i = H_i$. Niisiis on meil olemas normaaljada

$$\{1\} = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_{k-1} \triangleleft H_k = H.$$

(Kui olla päris täpne, siis normaalgada saame kui jätame selles jadas võrdsetest alamrühmadest alles ühe. Edasist tõestust see siiski ei muuda.) Siis $G_i \trianglelefteq G_{i+1}$, $G_{i+1} \cap H \leq G_{i+1}$ ja alamrühmade vahelisi seoseid iseloomustab diagramm

$$\begin{array}{ccc}
 & G_{i+1} & \\
 & | & \\
 & (G_{i+1} \cap H)G_i & \\
 \swarrow & & \searrow \\
 G_{i+1} \cap H & & G_i \\
 \searrow & & \swarrow \\
 & (G_{i+1} \cap H) \cap G_i &
 \end{array}$$

Nüüd

$$\begin{aligned}
 H_{i+1}/H_i &= (G_{i+1} \cap H)/(G_i \cap H) && (H_j \text{ def.}) \\
 &= (G_{i+1} \cap H)/((G_{i+1} \cap H) \cap G_i) && (G_i \subseteq G_{i+1}) \\
 &\cong (G_{i+1} \cap H)G_i/G_i && (\text{I isomorfismiteoreem}) \\
 &\subseteq G_{i+1}/G_i. && ((G_{i+1} \cap H)G_i \leq G_{i+1})
 \end{aligned}$$

Kuna H_{i+1}/H_i on isomorfne kommutatiivse rühma G_{i+1}/G_i alamrühmaga, siis on ta kommutatiivne. Sellega on tõestatud, et H on lahenduv. $\square$

Lemma 11.6 *Kui G on rühm, $N \trianglelefteq G$ ja $H \leq G$, siis $N \trianglelefteq NG$.*

TÕESTUS. Tänu lemmale 2.4 me teame, et $N \leq NG$. Mistahes $a, b \in N$ ja $g \in G$ korral

$$(ag)^{-1}b(ag) = g^{-1}(a^{-1}ba)g \in g^{-1}Ng = N.$$

Seega $N \trianglelefteq NG$. $\square$

Lause 11.7 *Lahenduva rühma faktorrühm on lahenduv.*

TÕESTUS. Olgu

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{k-1} \triangleleft G_k = G$$

lahenduva rühma G kommutatiivsete faktoritega normaalgada ning olgu $N \trianglelefteq G$. Tahame tõestada, et faktorrühm G/N on lahenduv. Selleks vaatame jada

$$\{1\} = N/N \trianglelefteq NG_1/N \trianglelefteq \dots \trianglelefteq NG_{k-1}/N \trianglelefteq NG_k/N = NG/N = G/N. \quad (18)$$

Siin $N \trianglelefteq NG_i$ tänu lemmale 11.6 ja need faktorid on olemas. Kuna $NG_i \leq NG_{i+1}$, siis teise isomorfismiteoreemi tõestuse põhjal $NG_i/N \trianglelefteq NG_{i+1}/N$ ja

$$\begin{aligned}
 (NG_{i+1}/N) / (NG_i/N) &\cong NG_{i+1}/NG_i && (\text{II isomorfismiteoreem}) \\
 &= (NG_i)G_{i+1}/NG_i && (G_{i+1} = G_iG_{i+1}) \\
 &\cong G_{i+1}/(NG_i \cap G_{i+1}) && (\text{I isomorfismiteoreem}) \\
 &\cong (G_{i+1}/G_i) / ((NG_i \cap G_{i+1})/G_i). && (\text{II isomorfismiteoreem})
 \end{aligned}$$

Kuna G_{i+1}/G_i on kommutatiivne rühm, siis on ka tema faktorrühm kommutatiivne ja seega on jada (18) faktorid kommutatiivsed. $\square$

Lause 11.8 *Mitte triviaalne lihtne rühm on lahenduv parajasti siis, kui ta on isomorfne rühmaga $\mathbb{Z}_p$, kus p on algarv.*

TÕESTUS. **TARVILIKKUS.** Vaatleme lihtsat ja lahenduvat rühma $G \neq \{1\}$. Lihtsuse tõttu leidub rühmal G ainult üks normaaljada: $\{1\} \triangleleft G$. Selle faktor $G/\{1\}$ peab olema kommutatiivne, seega G on kommutatiivne rühm. Lihtsuse tõttu ei tohi tal olla pärisalamrühmi. Seega valides $g \in G \setminus \{1\}$ peab kehtima $\langle g \rangle = G$. Teiste sõnadega: G on tsükliline rühm. Tsüklilised rühmad on kujul $\mathbb{Z}$ või $\mathbb{Z}_n$, kus $n \in \mathbb{N}$. Kuna $\mathbb{Z}$ ei ole lihtne ($2\mathbb{Z} < \mathbb{Z}$), siis $G \cong \mathbb{Z}_n$ mingi $n \geq 2$ korral. Kui n on kordarv, nt. $n = kl$, $k, l \neq 1$, siis $\langle \bar{k} \rangle < \mathbb{Z}_n$ ja $\mathbb{Z}_n$ ei ole lihtne. Seega $G \cong \mathbb{Z}_p$, kus p on algarv.

PIISAVUS. Kuna $(\mathbb{Z}_p, +)$ on kommutatiivne rühm, siis on ta ka lahenduv. $\square$

Saab näidata, et kui $n \geq 5$, siis paarissubstitutsioonide rühm A_n on lihtne. Kui ta oleks lahenduv, siis eelmise lause põhjal ta peaks olema kommutatiivne, mis annaks vastuolu. Seega selline A_n ei ole lahenduv. Kuna $A_n < S_n$, siis ei saa lause 11.5 tõttu ka rühm S_n , kus $n \geq 5$, olla lahenduv.

Lahenduva rühma definitsioon antakse tihti kommutaatorite abil. Vaatlemegi nüüd kommutaatori mõistet ja selle omadusi.

Definitsioon 11.9 Rühma G elementide g ja h **kommutaatoriks** nimetatakse elementi

$$[g, h] := g^{-1}h^{-1}gh.$$

Paneme tähele, et g ja h kommutaator on 1_G parajasti siis, kui $gh = hg$, s.t. elemendid g ja h kommuteeruvad. Üldjuhul kehtib võrdus $gh = hg[g, h]$.

Definitsioon 11.10 Rühma G **kommutaatoralamrühm** ehk **tuletatud alamrühm** $G' = [G, G]$ defineeritakse kui kõigi kommutaatorite $[g, h]$, $g, h \in G$, poolt tekitatud alamrühm rühmas G .

Lemma 11.11 *Kui $\varphi : G \rightarrow H$ on rühmade homomorfism ja $g, h \in G$, siis $[\varphi(g), \varphi(h)] = \varphi([g, h])$.*

TÕESTUS. Tõepoolest,

$$\begin{aligned} [\varphi(g), \varphi(h)] &= \varphi(g)^{-1}\varphi(h)^{-1}\varphi(g)\varphi(h) = \varphi(g^{-1})\varphi(h^{-1})\varphi(g)\varphi(h) \\ &= \varphi(g^{-1}h^{-1}gh) = \varphi([g, h]). \end{aligned}$$

$\square$

Järeldus 11.12 *Kui G on rühm ja $g, h, x \in G$, siis $x^{-1}[g, h]x = [x^{-1}gx, x^{-1}hx]$.*

TÕESTUS. Iga $x \in G$ korral on kujutus

$$G \rightarrow G, \quad g \mapsto x^{-1}gx,$$

rühmade homomorfism. $\square$

Teoreem 11.13 *Kui G on rühm, siis $[G, G] \trianglelefteq G$.*

TÕESTUS. Paneme tähele, et $[g, h]^{-1} = h^{-1}g^{-1}hg = [h, g]$, s.t. kommutaatori pöördelement on kommutaator. Seega alamrühma $[G, G]$ iga element on kujul

$$g = [g_1, h_1][g_2, h_2] \dots [g_n, h_n]$$

ja iga $x \in G$ korral

$$\begin{aligned} x^{-1}gx &= x^{-1}[g_1, h_1]x \cdot x^{-1}[g_2, h_2]x \cdot \dots \cdot x^{-1}[g_n, h_n]x \\ &= [x^{-1}g_1, h_1x][x^{-1}g_2, h_2x] \dots [x^{-1}g_n, h_nx] \in [G, G]. \end{aligned}$$

Seega $[G, G]$ on normaaljagaja. □

Lause 11.14 Olgu G rühm ja $N \trianglelefteq G$. Siis faktorrühm G/N on kommutatiivne parajasti siis, kui $[G, G] \leq N$.

TÕESTUS. Tõepoolest,

$$\begin{aligned} G/N \text{ on kommutatiivne} &\iff (\forall g, h \in G) (gN)(hN) = (hN)(gN) \\ &\iff (\forall g, h \in G) ghN = hgN \\ &\iff (\forall g, h \in G) g^{-1}h^{-1}gh \in N \\ &\iff (\forall g, h \in G) [g, h] \in N \\ &\iff [G, G] \leq N. \end{aligned}$$

□

Järeldus 11.15 Iga rühma G korral on faktorrühm $G/[G, G]$ kommutatiivne.

Teoreem 11.16 Mistahes rühma G , Abeli rühma H ning rühmade homomorfismi $\alpha : G \longrightarrow H$ korral leidub üheselt määratud rühmade homomorfism $\beta : G/[G, G] \longrightarrow H$ nii, et kolmnurk

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/[G, G] \\ & \searrow \alpha & \downarrow \beta \\ & & H \end{array},$$

kus $\pi : g \mapsto g[G, G]$ on loomulik projektsioon, kommuteerub.

TÕESTUS. Olgu $G' = [G, G]$. Kuna H on kommutatiivne, siis iga $g, h \in G$ korral

$$\alpha([g, h]) = [\alpha(g), \alpha(h)] = 1_H.$$

Sellest järeldub, et $G' \subseteq \text{Ker } \alpha$. Homomorfismiteoreemi (teoreem 2.1) põhjal leidub üheselt määratud rühmade homomorfism $\beta : G/G' \longrightarrow H$, mis on defineeritud, võrdusega

$$\beta(gG') := \alpha(g)$$

iga $g \in G$ korral, nii et $\beta\pi = \alpha$. □

Märkus 11.17 See teoreem väljendab seda, et Abeli rühmade kategooria on rühmade kategooria reflektiivne alamkategooria. Teiste sõnadega: funktor, mis viib iga rühma G Abeli rühmaks $G/[G, G]$, on vasakpoolseks kaasfunktoriks sisestusfunktorile Abeli rühmade kategooriasse.

Definitsioon 11.18 Rühma G **tuletatud alamrühmad** $G^{(n)}, n \in \mathbb{N}$, defineeritakse järgmiselt.

1. $G^{(0)} := G$.
2. $G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$ iga $n \in \mathbb{N}$ korral.

Rühma $G^{(n)}$ nimetatakse rühma G **n -indaks tuletatud alamrühmaks** (*the n -th derived subgroup*). Alamrühmade jada

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots$$

nimetatakse rühma G **tuletatud jadaks** (*derived series*).

Rühma tuletatud jada võib olla lõpmatu või lõplik. Osutub, et lõplikud jadad on lahenduvatel rühmadel.

Teoreem 11.19 Rühm G on lahenduv parajasti siis, kui leidub $n \in \mathbb{N}$ nii, et $G^{(n)} = \{1_G\}$.

TÕESTUS. TARVILIKKUS. Eeldame, et G on lahenduv ja olgu

$$\{1\} = G_k \triangleleft G_{k-1} \triangleleft G_{k-2} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$$

kommutatiivsete faktoritega normaalgada. Muuhulgas G/G_0 on kommutatiivne rühm. Lause 11.14 põhjal $G^{(1)} = [G, G] \leq G_1$. Tõestame induktsiooniga, et iga $l \in \{1, \dots, k\}$ korral $G^{(l)} \leq G_l$. Eeldame, et $G^{(m)} \leq G_m$. Lisaks teame, et G_{m+1}/G_m on kommutatiivne. Seega

$$\begin{aligned} G^{(m+1)} &= [G^{(m)}, G^{(m)}] && (G^{(m)} \text{ def.}) \\ &\leq [G_m, G_m] && (G^{(m)} \leq G_m) \\ &\leq G_{m+1}. && (\text{järeldus 11.14}) \end{aligned}$$

Saame, et ka $G^{(k)} \leq G_k = \{1_G\}$, kust $G^{(k)} = \{1_G\}$.

PIISAVUS. Kui leidub selline naturaalarv n , et $G^{(n)} = \{1_G\}$, siis

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots \supseteq G^{(n)} = \{1_G\}$$

on kommutatiivsete faktoritega normaalgada ning seega G on lahenduv. $\square$

Märkus 11.20 Tihti võetaksegi rühma G lahenduvuse defineerimisel aluseks tingimus, et $G^{(n)} = \{1_G\}$ mingi $n \in \mathbb{N}$ korral.

Kasutatud kirjandus

1. M. Kilp, *Algebra II*, Tartu, 1998.
2. D. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, 1982.
3. P. Puusemp, *Üldalgebra alused*, TTÜ kirjastus, Tallinn, 2012.

A Lisa 1: Rühmade esitused tekitajate ja seoste abil

Üks võimalus rühma kirjeldamiseks on näidata ära, kuidas ta tekib vaba rühma faktorühmana. Toome selle kohta ühe lihtsa näite.

Näide A.1 Olgu $X = \{x\}$ ja vaatleme vaba rühma

$$F_X = \{\dots, [x]^{-2}, [x]^{-1}, [1], [x], [x]^2, \dots\}.$$

Lihtne on näha, et hulk $N = \{[x]^{6k} \mid k \in \mathbb{Z}\}$ on selle rühma alamrühm. Kuna see F_X on kommutatiivne rühm, siis on N ka normaaljagaja. Kõrvalklasse N järgi tähistame $[x]^k := [x]^k N$, $k \in \mathbb{Z}$. Ei ole raske näha, et faktorrühm N järgi on

$$G := F_X/N = \{\overline{[1]}, \overline{[x]}, \overline{[x]^2}, \dots, \overline{[x]^5}\}.$$

Selles faktorühmas näiteks

$$\overline{[x]^3} \cdot \overline{[x]^5} = \overline{[x]^3 [x]^5} = \overline{[x]^8} = \overline{[x]^2},$$

sest

$$([x]^2)^{-1} [x]^8 = [x]^{-2} [x]^8 = [x]^6 \in N$$

(vt. lauset 1.39). Enamasti jäetakse sulud ja kriipsud ära ning kirjutatakse lihtsalt

$$G = F_X/N = \{1, x, x^2, \dots, x^5\},$$

aga selles rühmas arvutamisel arvestatakse reeglina $x^6 = 1$. Seega näiteks kirjutatakse

$$x^3 \cdot x^5 =_G x^8 =_G x^6 \cdot x^2 =_G 1 \cdot x^2 =_G x^2.$$

(Siin alaindeks G rõhutab, et arvutused toimuvad rühmas G , mitte aga näiteks rühmas F_X .) Sellises olukorras kirjutatakse tihti

$$G = \langle x \mid x^6 = 1 \rangle.$$

Siin elemendi x kohta öeldakse **tekitaja** (*generator*) ja võrduse $x^6 = 1$ kohta öeldakse **seos** (*relation*). Samuti öeldakse, et on antud rühma G **esitus** (*presentation*) oma tekitaja x ja seose $x^6 = 1$ abil.

Nagu näeme, on G 6-elemendiline tsükliline rühm. Sama mõttekäigu abil saab näidata et iga $n \in \mathbb{N}$ korral omab n -elemendiline tsükliline rühm esitust

$$\langle x \mid x^n = 1 \rangle.$$

Sellistes esitustes võib nii tekitajaid kui seoseid olla mitu. Näiteks võib vaadelda rühma

$$G = \langle r, f \mid r^8 = 1, f^2 = 1, (rf)^2 = 1 \rangle.$$

Anname nüüd sellise konstruktsiooni üldise käsitluse.

Definitsioon A.2 Olgu $R \subseteq G$, kus G on rühm. Tähistame

$$R^G := \{g^{-1}rg \mid g \in G, r \in R\} \subseteq G.$$

Alamhulga R^G poolt tekitatud G alamrühma $\langle R^G \rangle$ nimetatakse hulga R **normaalsulundiks** rühmas G .

Lemma A.3 Rühma G alamhulga R normaalsulund $\langle R^G \rangle$ on rühma G vähim normaal-jagaja, mis sisaldab hulka R .

TÕESTUS. Paneme tähele, et kui $g^{-1}rg \in R^G$, siis $(g^{-1}rg)^{-1} = g^{-1}r^{-1}g$. Seega

$$\langle R^G \rangle = \{g_1^{-1}r_1^{\varepsilon_1}g_1 \dots g_n^{-1}r_n^{\varepsilon_n}g_n \mid n \geq 0, g_i \in G, r_i \in R, \varepsilon_i \in \{1, -1\}\} \leq G.$$

Kui $g \in G$, siis

$$\begin{aligned} & g^{-1} (g_1^{-1}r_1^{\varepsilon_1}g_1 \cdot g_2^{-1}r_2^{\varepsilon_2}g_2 \cdot \dots \cdot g_n^{-1}r_n^{\varepsilon_n}g_n) g \\ &= (g^{-1}g_1^{-1}r_1^{\varepsilon_1}g_1g)(g^{-1}g_2^{-1}r_2^{\varepsilon_2}g_2g) \dots (g^{-1}g_n^{-1}r_n^{\varepsilon_n}g_ng) \\ &= (g_1g)^{-1}r_1^{\varepsilon_1}(g_1g) \cdot (g_2g)^{-1}r_2^{\varepsilon_2}(g_2g) \cdot \dots \cdot (g_ng)^{-1}r_n^{\varepsilon_n}(g_ng) \in \langle R^G \rangle, \end{aligned}$$

s.t. $\langle R^G \rangle$ on normaalne alamrühm. Kuna $r = 1_G^{-1} \cdot r \cdot 1_G$ iga $r \in R$ korral, siis $R \subseteq \langle R^G \rangle$.

Minimaalsuse näitamiseks vaatleme olukorda $R \subseteq H \trianglelefteq G$. Kuna H on normaalne alamrühm, siis iga $g \in G$ ja $r \in R$ korral $g^{-1}rg \in H$. Et H on kinnine pöördelendi võtmise suhtes, siis ka $g^{-1}r^{-1}g \in H$. Kuna H on kinnine korrutamise suhtes, siis näeme, et $\langle R^G \rangle \subseteq H$. $\square$

Definitsioon A.4 Olgu $X \neq \emptyset$ hulk, olgu F_X vaba rühm hulgal X ja olgu $R \subseteq F_X$ mingi alamhulk. **Rühm esitusega**

$$\langle X \mid R \rangle$$

on faktorühm $F_X / \langle R^{F_X} \rangle$. Sellest rühmast võib mõelda kui “kõige vabamast” rühmast, mis on tekitatud hulga X elementide poolt ja mis rahuldab seoseid $r = 1$, $r \in R$.

Kuigi formaalselt on selle faktorühma elementideks kõrvalklassid $[w]N$, kus $N = \langle R^{F_X} \rangle \trianglelefteq F_X$ ja w on sõna tähestikus $X \cup X^{-1}$, siis harilikult (eriti praktilistes arvutustes) kirjutatakse $[w]N$ asemel lihtsalt w .

Näide A.5 Olgu $X = \{x, y\}$ ja $R = \{x^4, y^3, (xy)^2\}$. Siis saame rühma esitusega

$$\langle x, y \mid x^4, y^3, (xy)^2 \rangle.$$

Kuna $x^4, y^3, (xy)^2 \in N = \langle R^{F_X} \rangle$, siis $x^4N = N$, $y^3N = N$ ja $(xy)^2N = N$, mis tähendab, et faktorühmas F_X/N kehtivad võrdused $\overline{x^4} = \overline{1}$, $\overline{y^3} = \overline{1}$ ja $\overline{(xy)^2} = \overline{1}$. Seetõttu pannakse sama esitus tihti kirja kujul

$$\langle x, y \mid x^4 = 1, y^3 = 1, (xy)^2 = 1 \rangle$$

või mõnel teisel samaväärsel kujul, nt.

$$\langle x, y \mid x^4 = 1, y^2 = y^{-1}, xy = y^{-1}x^{-1} \rangle.$$

Järgmine teoreem annab võimaluse homomorfismide defineerimiseks rühmast G , mis on antud mingi oma esitusega, mõnda teise rühma.

Teoreem A.6 Olgu $G = \langle X \mid R \rangle$ ja H rühmad ning olgu $\alpha : X \rightarrow H$ kujutus. Eeldame, et iga $r = [x_1^{\varepsilon_1}x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}] \in R$ korral $\alpha(x_1)^{\varepsilon_1}\alpha(x_2)^{\varepsilon_2} \dots \alpha(x_n)^{\varepsilon_n} = 1_H$. Siis leidub üheselt määratud rühmade homomorfism $\alpha' : G \rightarrow H$ nii, et $\alpha'|_X = \alpha$.

Võrdust $\alpha'|_X = \alpha$ selle teoreemi sõnastuses tuleb tõlgendada nii, et diagramm

$$\begin{array}{ccccc} X & \xrightarrow{\iota} & F_X & \xrightarrow{\pi} & F_X/N = G \\ & \searrow \alpha & & \swarrow \alpha' & \\ & & H & & \end{array}$$

kus $\pi : [w] \mapsto [w]N$ on loomulik projektsioon ja ι on sisestus, kommuteerub ehk iga $x \in X$ korral $\alpha'([x]N) = \alpha(x)$.

TÕESTUS. Olgu (F_X, ι) vaba rühm hulgal X . Universaalomaduse põhjal leidub rühmade homomorfism $\beta : F_X \rightarrow H$ nii, et $\beta \circ \iota = \alpha$.

Kui $r = [x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}] \in R$, siis

$$\begin{aligned} \beta(r) &= \beta([x_1]^{\varepsilon_1} \dots [x_n]^{\varepsilon_n}) && \text{(tehted } F_X\text{-s)} \\ &= \beta([x_1]^{\varepsilon_1}) \dots \beta([x_n]^{\varepsilon_n}) && (\beta \text{ on homomorfism)} \\ &= \beta(\iota(x_1)^{\varepsilon_1}) \dots \beta(\iota(x_n)^{\varepsilon_n}) && (\iota \text{ def.}) \\ &= \beta(\iota(x_1))^{\varepsilon_1} \dots \beta(\iota(x_n))^{\varepsilon_n} && (\beta \text{ on homomorfism)} \\ &= \alpha(x_1)^{\varepsilon_1} \dots \alpha(x_n)^{\varepsilon_n} && (\beta \circ \iota = \alpha) \\ &= 1_H. && \text{(teoreemi eeldus)} \end{aligned}$$

Seega $R \subseteq \text{Ker } \beta$. Kuna $\text{Ker } \beta \trianglelefteq F_X$ ja $N := \langle R^{F_X} \rangle$ on vähim rühma F_X normaaljagaja, mis sisaldab hulka R , siis $N \trianglelefteq \text{Ker } \beta$. Defineerime kujutuse $\alpha' : F_X/N = G \rightarrow H$ võrdusega

$$\alpha'([w]N) := \beta([w]).$$

Oletame, et $[w]N = [u]N$, kus $[w], [u] \in F_X$. Siis $[w]^{-1}[u] = [w^{-1}u] \in N \subseteq \text{Ker } \beta$. Järelikult $1_H = \beta([w^{-1}u]) = \beta([w])^{-1}\beta([u])$, kust $\beta([w]) = \beta([u])$. Seega α' on korrektselt defineeritud.

$$\begin{array}{ccccc} X & \xrightarrow{\iota} & F_X & \xrightarrow{\pi} & F_X/N = G \\ & \searrow \alpha & \downarrow \beta & \swarrow \alpha' & \\ & & H & & \end{array}$$

Kujutus α' on rühmade homomorfism, sest

$$\alpha'([w]N)[u]N) = \alpha'([wu]N) = \beta([wu]) = \beta([w][u]) = \beta([w])\beta([u]) = \alpha'([w]N)\alpha'([u]N).$$

Lisaks sellele

$$\alpha' \circ \pi \circ \iota = \beta \circ \iota = \alpha.$$

Jääb veel tõestada ühesus. Oletame, et ka $\gamma : G \longrightarrow H$ on selline homomorfism, et $\gamma \circ \pi \circ \iota = \alpha$. Siis iga $[x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}]N \in G$ korral

$$\begin{aligned}
\gamma([x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}]N) &= \gamma([x_1]N)^{\varepsilon_1} \dots \gamma([x_n]N)^{\varepsilon_n} && (\gamma \text{ on homomorfism}) \\
&= (\gamma \circ \pi \circ \iota)(x_1)^{\varepsilon_1} \dots (\gamma \circ \pi \circ \iota)(x_n)^{\varepsilon_n} && (\pi, \iota \text{ def.}) \\
&= \alpha(x_1)^{\varepsilon_1} \dots \alpha(x_n)^{\varepsilon_n} && (\gamma \circ \pi \circ \iota = \alpha) \\
&= (\alpha' \circ \pi \circ \iota)(x_1)^{\varepsilon_1} \dots (\alpha' \circ \pi \circ \iota)(x_n)^{\varepsilon_n} && (\alpha = \alpha' \circ \pi \circ \iota) \\
&= \alpha'([x_1]N)^{\varepsilon_1} \dots \alpha'([x_n]N)^{\varepsilon_n} && (\pi, \iota \text{ def.}) \\
&= \alpha'([x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}]N). && (\alpha' \text{ on homomorfism})
\end{aligned}$$

Seega $\gamma = \alpha'$. $\square$

Üldiselt ei ole rühma esituse põhjal lihtne kindlaks teha kui palju selles rühmas on elemente või et kas see rühm on lõplik. Teoreemi A.6 kasutades on seda teatud juhtudel siiski võimalik teha.

Näide A.7 Uurime, kui palju elemente on rühmas

$$G = \langle x, y \mid x^n = 1, y^2 = 1, (xy)^2 = 1 \rangle, \quad (19)$$

kus $n \geq 2$. Vaatleme sõna w tähestikus $\{x, y, x^{-1}, y^{-1}\}$. Kuna $x^n = 1$, siis $x^{-1} =_G x^{n-1}$, mis tähendab seda, et iga x^{-1} esinemise asemel sõnas w saame kirjutada x^{n-1} . Analogiliselt $y =_G y^{-1}$ ja me saame iga y^{-1} asemele kirjutada y . Lõpuks $(xy)^2 =_G 1$ tähendab seda, et $yx =_G x^{-1}y^{-1} =_G x^{n-1}y$. Seega sõna w saab asendada sõnaga kujul $x^k y^l$, kus $k, l \geq 0$. Et $x^n =_G 1$ ja $y^2 =_G 1$, siis saame eeldada, et $0 \leq k \leq n-1$ ja $0 \leq l \leq 1$. (See oleks antud rühma elemendi *normaalkuju*.) Oleme näidanud, et

$$G \subseteq \{x^k y^l \mid 0 \leq k \leq n-1, 0 \leq l \leq 1\},$$

seega $|G| \leq 2n$.

Tõestame ka vastupidise võrratuse. Võtame dieedri rühma D_{2n} . Tuletame meelde, et $|D_{2n}| = 2n$ ning $D_{2n} = \langle A, J \rangle$, kus A ja J on teatud pööratavad (2×2) -maatriksid, mis rahuldavad seoseid

$$A^n = E, \quad J^2 = E \quad \text{ja} \quad AJ = JA^{-1}.$$

Viimane võrdus on samaväärne võrdusega $AJAJ = E$ ehk $(AJ)^2 = E$.

Kujutus

$$\alpha : X = \{x, y\} \longrightarrow D_{2n}, \quad x \mapsto A, \quad y \mapsto J$$

rahuldab teoreemi A.6 eeldusi. Järelikult leidub üheselt määratud rühmade homomorfism $\alpha' : G \longrightarrow D_{2n}$ nii, et diagramm

$$\begin{array}{ccccc}
X & \xrightarrow{\iota_X} & F_X & \xrightarrow{\pi} & G \\
& \searrow \alpha & & & \swarrow \alpha' \\
& & D_{2n} & &
\end{array}$$

kommuteerub. Seega

$$A = \alpha(x) = \alpha'([x]N) \quad \text{ja} \quad J = \alpha(y) = \alpha'([y]N).$$

Kuna $A, J \in \text{Im}(\alpha')$, siis

$$D_{2n} = \langle A, J \rangle \subseteq \text{Im}(\alpha') \subseteq D_{2n},$$

millest järeldub, et α' on surjektiivne. Seega $|G| \geq |D_{2n}| = 2n$. Kokkuvõttes $|G| = 2n$ ja $\alpha' : G \rightarrow D_{2n}$ on rühmade isomorfism. See tähendab, et põhimõtteliselt võiks dieedri rühma D_{2n} defineerida ka esituse (19) abil. Tihti seda tehaksegi.

B Lisa 2: Vabad Abeli rühmad

Sarnaselt vektorruumidega saab Abeli rühmades rääkida lineaarkombinatsioonidest. Ainus vahe on selles, et korpuse elementide asemel on täisarvud.

Definitsioon B.1 Olgu $a_1, \dots, a_n$ Abeli rühma A elemendid ja olgu $k_1, \dots, k_n$ täisarvud. Avaldist

$$k_1 a_1 + \dots + k_n a_n, \tag{20}$$

aga ka selle avaldise poolt määratud rühma A elementi, nimetatakse elementide $a_1, \dots, a_n$ **lineaarkombinatsiooniks**. Arve $k_1, \dots, k_n$ nimetatakse selle lineaarkombinatsiooni **kordajateks**. Lineaarkombinatsiooni nimetatakse **triviaalseks**, kui tema kõik kordajad on nullid.

Definitsioon B.2 Abeli rühma A elementide süsteemi $a_1, \dots, a_n$ nimetatakse

- **lineaarselt sõltumatuks**, kui

$$(\forall k_1, \dots, k_n \in \mathbb{Z})(k_1 a_1 + \dots + k_n a_n = 0 \implies k_1 = \dots = k_n = 0),$$

- **lineaarselt sõltuvaks**, kui ta ei ole lineaarselt sõltumatu.

Lõpmatut elementide süsteemi nimetatakse **lineaarselt sõltumatuks**, kui tema iga lõplik alamsüsteem on lineaarselt sõltumatu.

Vektorruumis on vähemalt kahest vektorist koosnev lõplik vektorite süsteem lineaarselt sõltumatu parajasti siis, kui selle süsteemi mingi vektor avaldub ülejäänud vektorite lineaarkombinatsioonina. Abeli rühmade puhul see nii ei ole.

Näide B.3 Vaatleme Abeli rühmas $\mathbb{Z}$ elementide 2 ja 3 lineaarkombinatsiooni

$$3 \cdot 2 + (-2) \cdot 3 = 0.$$

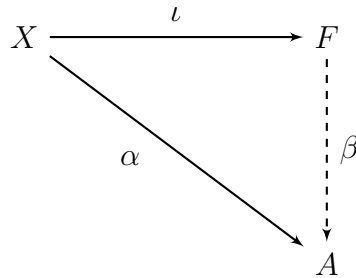
Kuna kordaja $3 \neq 0$, siis see süsteem on lineaarselt sõltuv. Samas kumbki arvudest 2 ja 3 ei avaldu teise lineaarkombinatsioonina.

Definitsioon B.4 Abeli rühma **baasiks** nimetatakse tema lineaarselt sõltumatut moodustajate süsteemi. Abeli rühma nimetatakse **vabaks**, kui temas leidub baas.

On võimalik tõestada, et vaba Abeli rühma mistahes kaks baasi on sama võimsusega. Selles kursuses me seda tõestust ei anna. Vaba Abeli rühma baasi võimsust nimetatakse selle rühma **astakuks**.

Näitame, et vabal Abeli rühmal on omadus, mis on sarnane definitsioonis 9.1 kirjeldatud omadusele.

Lause B.5 Olgu F vaba Abeli rühm baasiga X ja olgu $\iota : X \rightarrow F$ sisestus. Siis iga Abeli rühma A ja iga kujutuse $\alpha : X \rightarrow A$ jaoks leidub üheselt määratud rühmade homomorfism $\beta : F \rightarrow A$ nii, et $\beta \circ \iota = \alpha$, s.t. diagramm



kommuteerub.

TÕESTUS. Olgu $X = \{e_i \mid i \in I\}$ baas. Siis iga $x \in F$ avaldub üheselt lineaarkombinatsioonina $x = k_1 e_{i_1} + \dots + k_n e_{i_n}$, kus $k_1, \dots, k_n \in \mathbb{Z}$ ja $i_1, \dots, i_n \in I$. Defineerime

$$\beta(x) := k_1 \alpha(e_{i_1}) + \dots + k_n \alpha(e_{i_n}).$$

Saab näidata, et β on homomorfism. Iga $i \in I$ korral

$$(\beta \circ \iota)(e_i) = \beta(e_i) = \beta(1e_i) = 1\alpha(e_i) = \alpha(e_i),$$

seega $\beta \circ \iota = \alpha$.

Ühesuse näitamiseks oletame, et ka $\gamma : F \rightarrow A$ on selline homomorfism, et $\gamma \circ \iota = \alpha$. Siis iga $x = k_1 e_{i_1} + \dots + k_n e_{i_n} \in F$ korral

$$\beta(x) = k_1 \alpha(e_{i_1}) + \dots + k_n \alpha(e_{i_n}) = k_1 \gamma(e_{i_1}) + \dots + k_n \gamma(e_{i_n}) = \gamma(k_1 e_{i_1} + \dots + k_n e_{i_n}) = \gamma(x).$$

Seega $\beta = \gamma$. □

Näide B.6 1. Abeli rühm $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}$ komponenthaaval defineeritud liitmise suhtes on vaba, kusjuures baasiks võib võtta $e_1 = (1, 0)$, $e_2 = (0, 1)$ (aga ka näiteks $(1, 0)$, $(0, -1)$). See süsteem on moodustajate süsteem, sest

$$(\forall (k, l) \in \mathbb{Z} \times \mathbb{Z})(k, l) = ke_1 + le_2$$

ja ta on lineaarselt sõltumatu, sest

$$(\forall k, l \in \mathbb{Z})(ke_1 + le_2 = (0, 0) \implies (k, l) = (0, 0) \implies k = 0 \text{ ja } l = 0).$$

2. Rühm $(\mathbb{Z}_2, +)$ ei ole vaba. Selles rühmas $\bar{1}$ on küll moodustajate süsteem, aga ta on lineaarselt sõltuv, sest $2 \cdot \bar{1} = \bar{0}$, kuid $0 \neq 2 \in \mathbb{Z}$.

Järgnev tulemus näitab, et kõik vabad Abeli rühmad on teatud mõttes sarnased näites B.6 vaadeldud Abeli rühmaga.

Teoreem B.7 *Abeli rühm on vaba parajasti siis, kui ta on isomorfne lõpmatute tsükliliste rühmade välise otsesummaga.*

TÕESTUS. PIISAVUS. Teoreemi 3.5 põhjal on kõik lõpmatud tsüklilised rühmad isomorfsed rühmaga $(\mathbb{Z}, +)$. Vaatleme välist otsesummat $\oplus \sum_{i \in I} A_i$, kus $A_i = (\mathbb{Z}, +)$ iga $i \in I$ korral. Tähistame iga $i \in I$ korral $e_i = (x_j)_{j \in I}$, kus

$$x_j = \begin{cases} 1, & \text{kui } j = i, \\ 0, & \text{kui } j \neq i. \end{cases}$$

Lihtne on aru saada, et $\{e_i \mid i \in I\}$ on Abeli rühma $\oplus \sum_{i \in I} A_i$ baas ning seega see rühm on vaba.

TARVILIKKUS. Olgu F vaba Abeli rühm baasiga $e = \{e_i \mid i \in I\}$. On lihtne veenduda, et hulgad $\mathbb{Z}e_i = \{ke_i \mid k \in \mathbb{Z}\} \subseteq F$ on rühma F alamrühmad. Kuna e on moodustajate süsteem, siis iga $a \in F$ jaoks leiduvad $i_1, \dots, i_n \in I$ ja $k_1, \dots, k_n \in \mathbb{Z}$ nii, et

$$a = k_1 e_{i_1} + \dots + k_n e_{i_n} \in \sum_{i \in I} \mathbb{Z}e_i.$$

Seega

$$F = \sum_{i \in I} \mathbb{Z}e_i.$$

Näitame, et see summa on otsesumma. Selleks vaatleme Abeli rühma F moodulina üle ringi $\mathbb{Z}$ ja kontrollime teoreemi ?? tingimust 3. Olgu $i_1, \dots, i_n \in I$ paarikaupa erinevad indeksid, $k_1 e_{i_1} \in \mathbb{Z}e_{i_1}, \dots, k_n e_{i_n} \in \mathbb{Z}e_{i_n}$, ning oletame, et

$$k_1 e_{i_1} + \dots + k_n e_{i_n} = 0.$$

Kuna e on lineaarselt sõltumatu, siis $k_1 = \dots = k_n = 0$ ja seega $k_1 e_{i_1} = \dots = k_n e_{i_n} = 0$. Sellega oleme tõestanud, et

$$F = \sum_{i \in I} \mathbb{Z}e_i.$$

Teoreemi 7.5 põhjal

$$F \simeq \oplus \sum_{i \in I} \mathbb{Z}e_i.$$

Tõestuse lõpetamiseks veendume, et $\mathbb{Z}e_i \simeq \mathbb{Z}$ iga $i \in I$ korral. Selleks vaatleme kujutust

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}e_i, \quad k \mapsto ke_i.$$

Kuna mistahes $k, l \in \mathbb{Z}$ korral

$$f(k + l) = (k + l)e_i = ke_i + le_i = f(k) + f(l),$$

siis f on rühmade homomorfism. On selge, et f on sürjektiivne. Kui $ke_i = f(k) = 0$, siis lineaarselt sõltumatuse tõttu $k = 0$. Seega $\text{Ker}(f) = \{0\}$ ja f on ka injektiivne. Kokkuvõttes f on isomorfism ja rühmad $\mathbb{Z}e_i$, $i \in I$, on lõpmatud tsüklilised rühmad. $\square$

Lause B.8 Iga Abeli rühm on isomorfne mingi vaba Abeli rühma faktorrühmaga.

TÕESTUS. Olgu A suvaline Abeli rühm. Vaatleme hulka A indekseid hulgana ja moodustame välise otsesumma

$$F = \bigoplus_{a \in A} A_a,$$

kus $A_a = (\mathbb{Z}, +)$ on tsüklilised rühmad. Teoreemi B.7 tõttu on F vaba Abeli rühm. Vaatleme kujutust

$$f : F \longrightarrow A, \quad (k_a)_{a \in A} \mapsto \sum_{a \in A} k_a a.$$

Kuna üldistatud jadas $(k_a)_{a \in A}$ esineb lõplik arv nullist erinevaid täisarve, siis summa $\sum_{a \in A} k_a a$ on samuti lõplik. Lihtne on veenduda, et f on rühmade homomorfism. Ta on ka surjektiivne, sest elemendi $a \in A$ originaaliks sobib jada, mille a -komponent on täisarv 1 ja ülejäänud komponendid on nullid. Järeldus 2.2 ütleb, et

$$A \simeq F / \text{Ker}(f).$$

□