# Ryhmän esittäminen virittäjien ja relaatioiden avulla

Jenni Sarkki
Pro gradu -tutkielma
Helsingin yliopisto
Matematiikan ja tilastotieteen laitos

12. elokuuta 2013

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

| Tiedekunta/Osasto — Fakultet/Sektion — Faculty | Laitos — Institution — Department |
|---|---|
| Matemaattis-luonnontieteellinen | Matematiikan ja tilastotieteen laitos |

Tekijä — Författare — Author
Jenni Sarkki

Työn nimi — Arbetets titel — Title

Ryhmän esittäminen virittäjien ja relaatioiden avulla

| Oppiaine — Läroämne — Subject | | |
|---|---|---|
| Matematiikka | | |
| Työn laji — Arbetets art — Level | Aika — Datum — Month and year | Sivumäärä — Sidoantal — Number of pages |
| Pro gradu -tutkielma | Elokuu 2013 | 61 s. |

Tiivistelmä — Referat — Abstract

Tässä tutkielmassa näytetään, miten ryhmä voidaan elegantisti ja kompaktisti esittää virittäjien ja relaatioiden avulla. Sitä ennen kuitenkin kerrataan luvussa 2 teoriaa muun muassa ryhmän virittämisen osalta. Luvussa 3 tarkastellaan uusia käsitteitä *sana* ja *vapaa ryhmä*.

Olkoon joukko $S$. Muodostetaan siitä erillinen joukko $S^*$ siten, että jokaista joukon $S$ alkiota $a$ vastaa joukossa $S^*$ täsmälleen yksi alkio $a^*$. Merkitään näiden joukkojen yhdistettä $T$. Muodostetaan äärellisiä jonoja $(a_1, \ldots, a_n)$, joissa jokainen alkio $a_i$ kuuluu joukkoon $T$. Merkitään jonoa lyhyesti $a_1 \ldots a_n$ ja kutsutaan sitä sanaksi joukon $T$ yli. Mikäli lähtökohtana on ryhmä $G$ ja sen osajoukko $S$, niin joukko $S^*$ koostuu joukon $S$ alkioiden $a$ käänteisalkioista $a^{-1}$ ryhmässä $G$, jolloin voidaan merkitä $a^* = a^{-1}$ ja $S^* = S^{-1}$.

Vapaalle ryhmälle on kaksi erilaista määritelmää: epäformaali ja formaali. Epäformaalin määritelmän mukaan ryhmä $F$ on vapaa joukon $S$ suhteen, jos ryhmä $F$ koostuu sellaisista sanoista joukon $T$ yli, että kaikki osasanat $aa^*$ ja $a^*a$ ovat supistettu pois. Tällaisia sanoja kutsutaan supistetuiksi. Formaalin määritelmän mukaan puolestaan ryhmä $F$ on vapaa joukon $S$ suhteen, mikäli mikä tahansa kuvaus $\theta$ joukolta $S$ mielivaltaiselle ryhmälle $G$ laajenee yksikäsitteisesti homomorfismiksi $\theta_1$ ryhmältä $F$ ryhmälle $G$. Alaluvun 3.1 lopussa tutkitaan näiden kahden määritelmän yhteyttä toisiinsa. Alaluvussa 3.2 osoitetaan vielä Nilsenin–Shreierin lause, jonka mukaan jokaisen vapaan ryhmän aliryhmä on myös vapaa.

Näiden myötä siirrytään käsittelemään ryhmän esitystä. Ryhmän $G$ esitys koostuu kahdesta joukosta: virittäjäjoukosta $S$ ja relaattorijoukosta $R$. Relaattorijoukon alkiot ovat supistettuja sanoja joukon $T = S \cup S^{-1}$ yli, eli relaattorijoukko on virittäjäjoukon $S$ suhteen vapaan ryhmän $F$ osajoukko. Ryhmä $G$ saadaan siten, että vapaan ryhmän $F$ alkioista supistetaan pois kaikki osasanat, jotka kuuluvat relaattorijoukon normaaliin sulkeumaan $\overline{R}$. Luvussa 4 annetaan ryhmän esityksen määritelmä ja alaluvussa 4.2 annetaan esimerkkejä erilaisten ryhmien esityksistä.

Relaattorijoukon olemassaolosta seuraa, että ryhmän $G$ sanoilla ei välttämättä ole yksikäsitteinen esitys. Sen sijaan vapaassa ryhmässä, jossa ylimääräisiä relaatioita ei ole, kullakin sanalla on yksikäsitteinen esitys. Yleisessä tapauksessa vapaa ryhmä ei siis ole vaihdannainen eli Abelin ryhmä. Voidaan kuitenkin määritellä myös vapaan Abelin ryhmän käsite. Sen määritelmä esitetään alaluvussa 4.3.

Luvussa 5 käsitellään niin kutsuttuja Cayley-verkkoja, joiden avulla ryhmä voidaan esittää virittäjien ja relaatioiden avulla myös graafisesti. Verkot voivat muun muassa auttaa löytämään uusia relaatioita, jotka pätevät esitetyssä ryhmässä.

Vaikka ryhmän esittäminen virittäjien ja relaatioiden avulla on hyvin kompakti tapa, niin joskus esityksen avulla voi olla monimutkaista sanoa edes, ovatko kaksi ryhmän $G$ sanaa $w_1$ ja $w_2$ oikeastaan sama sana. Lopuksi viimeisessä luvussa tutustutaankin Max Dehnin vuonna 1911 esittämiin ryhmän esitykseen liittyviin kolmeen avoimeen ongelmaan: sanaongelma, konjugaattiongelma ja isomorfismiongelma.

Avainsanat — Nyckelord — Keywords
Sana, vapaa ryhmä, virittäjät ja relaatiot, Cayley-verkko

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

# Sisältö

# 1 Johdanto

Ryhmän voi tunnetusti esittää muun muassa kertotaulun avulla. Kun ryhmän mahtavuus ei ole kovin suuri, kertotaulu on kenties suorin ja informatiivisin tapa esittää ryhmä. Tässä tutkielmassa esitämme kuitenkin, miten jopa äärettömiä ryhmiä voidaan esittää elegantisti ja kompaktisti virittäjien ja relaatioiden avulla.

Lukijalta oletamme Algebra I -kurssin tuntemusta, mutta luvussa 2 kertaamme tämän tutkielman näkökulmasta kurssin keskeisimpiä tuloksia ja käsitteitä. Lisäksi otamme käyttöön muutamia käsitteitä ja lauseita, jotka ovat kurssin Algebra I ulkopuolelta, mutta ovat ymmärrettävissä ja todistettavissa kyseisen kurssin taidoilla.

Ennen kuin voimme esittää ryhmän esityksen määritelmän, on tärkeää tutustua käsitteisiin *sana* ja *vapaa ryhmä*. Luvussa 3 ensin käsittelemme sanoja, minkä jälkeen esitämme vapaalle ryhmälle sekä epäformaalin että formaalin määritelmän. Toivomme, että epäformaali määritelmä auttaa lukijaa rakentamaan itselleen vahvan intuition vapaan ryhmän käsitteestä. Formaali määritelmä on sen sijaan abstrakti ja matemaattisesti tarkka. Vapaan ryhmän formaalin määritelmän ymmärtämistä voi myös tukea eräs analogia lineaarialgebran piiristä, jota käsittelemme formaalin määritelmän yhteydessä. On lisäksi tärkeää pohtia kahden eri määritelmän yhteyttä toisiinsa.

Samassa luvussa osoitamme tuloksen, jonka mukaan jokainen vapaan ryhmän aliryhmä on myös vapaa. Tämä tulos tunnetaan Nilsenin–Schreierin lauseena. Nilsen on osoittanut lauseen alunperin vuonna 1921. Hänellä oli kuitenkin lisäoletuksena, että ryhmä on äärellisesti viritetty. Schreier todisti lauseen myöhemmin eri metodein ilman Nilsenin lisäoletusta. Nykyisin Nilsenin–Schreierin lauseelle tunnetaan eri todistuksia muiden muassa topologian alalta, mutta me todistamme lauseen kunnioittaen Schreierin alkuperäistä todistusta.

Luvussa 4 määrittelemme, miten ryhmä voidaan esittää virittäjien ja relaatioiden avulla. Teorian lisäksi käymme läpi myös useita esimerkkejä — osoitamme esitykset muun muassa diedri- ja symmetriaryhmille, joita käsittelemme ensimmäisen kerran jo luvussa 2. Näytämme, miten ryhmän esityksestä voidaan johtaa sen kertotaulu ja toisaalta kertotaulusta sen esitys.

Yleisessä tapauksessa vapaa ryhmä ei ole Abelin ryhmä, mutta voimme erikseen määritellä vapaan Abelin ryhmän käsitteen. Käsittelemme Abelin ryhmiä omassa alaluvussaan, jossa johdamme myös muun muassa syklisen ryhmän esityksen. Vaikka johdamme ryhmille esityksiä, on kuitenkin muistettava, että ryhmän esitys ei ole yksikäsitteinen. Luvun 4 lopussa esitämme vielä Tietze-muunnokset, joiden avulla ryhmän esitys voidaan saattaa erilaiseen muotoon.

Ryhmä voidaan esittää myös graafisesti virittäjien ja relaatioiden avulla. Niin kutsuttuja Cayley-verkkoja käsittelemme luvussa 5. Verkkojen avulla voidaan löytää uusia relaatioita esitetyssä ryhmässä suoraviivaisesti ilman algebrallista pyörittelyä. Vaikka ryhmän esitys virittäjien ja relaatioiden avulla on hyvin kompakti esitys, niin kaikkea sen sisältämää informaatiota voi olla vaikeaa nähdä. Viimeisessä luvussa 6 esitämme lyhyesti Max Dehnin vuonna 1911 esittämät kolme avointa päätösongelmaa: sanaongelman, konjugaattiongelman ja isomorfiaongelman.

Tutkielmassa olemme käyttäneet päälähteenä D. L. Johnsonin teosta *Presentation of Groups*.

# 2 Taustaa

Oletamme lukijalta Algebra I -kurssin tuntemusta. Tässä luvussa kuitenkin kertaamme muutamia määritelmiä, lauseita ja esimerkkejä, joiden tuntemista vaaditaan myöhemmissä luvuissa. Lisäksi tässä luvussa otamme käyttöön kyseisen kurssin ulkopuolelta muutamia määritelmiä, lauseita ja merkintöjä, joiden ymmärtäminen onnistuu Algebra I -kurssin taidoilla.

## 2.1 Ryhmän virittäminen

Olkoon $G$ ryhmä ja $S$ sen jokin osajoukko. Tarkastellaan $G$:n aliryhmiä $H$, jotka sisältävät joukon $S$. Aliryhmien $H$ leikkaus on myös $G$:n aliryhmä — tarkalleen ottaen se on suppein $G$:n aliryhmä, joka sisältää joukon $S$. Tätä ryhmää merkitään $\langle S \rangle$;

$$\langle S \rangle = \bigcap_{S \subset H \leqslant G} H.$$

**Määritelmä 2.1.** Ryhmä $\langle S \rangle$ on *joukon $S$ virittämä $G$:n aliryhmä*. Joukon $S$ alkioita kutsutaan ryhmän $\langle S \rangle$ *virittäjiksi*. Jos joukko $S$ on äärellinen, eli muotoa $S = \{a_1, a_2, \ldots, a_k\}$, niin sanotaan, että ryhmä $\langle S \rangle$ on *äärellisesti viritetty*. Tällöin voidaan merkitä

$$\langle S \rangle = \langle a_1, a_2, \ldots, a_k \rangle.$$

**Lause 2.2.** *Ryhmän $G$ osajoukon $S$ virittämä aliryhmä $\langle S \rangle$ muodostuu kaikista tuloista, joiden tekijät ovat $S$:n alkioita tai niiden käänteisalkioita;*

$$\langle S \rangle = \{a_1 a_2 \ldots a_n \mid n \geq 0, a_i \text{ tai } a_i^{-1} \in S \text{ kaikilla } i\}.$$

*Todistus.* Katso Metsänkylä & Näätänen: *Algebra* (Yliopistopaino, 2009), lause III.3.6. □

Tulo, jossa on 0 tekijää, on niin kutsuttu *tyhjä tulo*. Se on ryhmän $\langle S \rangle$ neutraalialkio, jota additiivisessa notaatiossa merkitään 0, mutta muuten tässä tutkielmassa käytämme merkintää $e$.

*Esimerkki* 2.3. Kokonaislukujen additiivisen ryhmän $(\mathbb{Z}, +)$ virittää alkio 1, sillä jokainen kokonaisluku on summa, jonka summattavat ovat luvut 1 tai $-1$. Toisaalta Bezout'n identiteetin nojalla luku 1 voidaan esittää lineaarikombinaationa sellaisista kokonaisluvuista $a, b \in \mathbb{Z}$, joiden suurin yhteinen tekijä on 1. Täten myös kaksio $\{a, b\}$ virittää kokonaislukuryhmän,

$$\mathbb{Z} = \langle 1 \rangle = \langle a, b \rangle, \text{ kun } a, b \in \mathbb{Z} \text{ ja } \operatorname{syt}(a, b) = 1.$$

Ryhmän virittäjät eivät siis ole yksikäsitteisiä.

**Määritelmä 2.4.** Ryhmää $G$ sanotaan *sykliseksi*, jos se on yhden alkion virittämä. Toisin sanoen $G$ on syklinen, jos on olemassa sellainen $a \in G$, että $G = \langle a \rangle$.

**Lause 2.5.** *Olkoon $G$ alkion $a$ virittämä syklinen ryhmä, $G = \langle a \rangle$. Jos $G$ on äärellistä kertalukua $n \in \mathbb{N}$, niin*

$$G = \{e, a, a^2, \dots a^{n-1}\}$$

*ja $n$ on pienin positiivinen kokonaisuku $r$, jolla $a^r = e$. Jos $G$ on ääretön, niin*

$$G = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$$

*ja kaikki potenssit ovat erisuuria, $a^m \neq a^n$ kaikilla erisuurilla $m, n \in \mathbb{Z}$.*

*Todistus.* Katso Metsänkylä & Näätänen: *Algebra* (Yliopistopaino, 2009), lause III.3.7. □

*Esimerkki* 2.6. Additiivinen jäännösluokkaryhmä modulo $m$ eli $(\mathbb{Z}_m, +)$ on syklinen kaikilla $m \geq 1$;

$$\mathbb{Z}_m = \langle 1_m \rangle = \{0_m, 1_m, 2 \cdot 1_m, \dots, (m-1) \cdot 1_m\} = \{0_m, 1_m, 2, \dots, (m-1)_m\}$$

ja $m$ on pienin positiivinen kokonaisluku $r$, jolla $r \cdot 1_m = r_m = 0_m$.

**Määritelmä 2.7.** Olkoon $G$ ryhmä ja $a \in G$. Alkion $a$ virittämän aliryhmän $\langle a \rangle$ kertalukua sanotaan *alkion $a$ kertaluvuksi* ja merkitään $\operatorname{ord}(a)$;

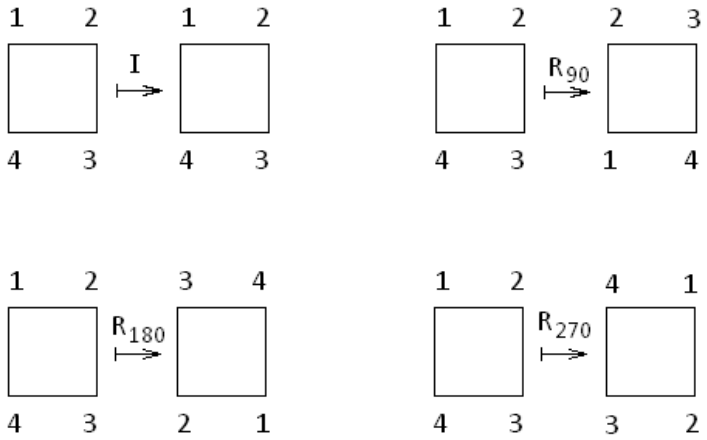
$$\operatorname{ord}(a) = \#\langle a \rangle.$$

**Seuraus 2.8.** *Olkoon $G$ ryhmä ja $a \in G$. Alkion $a$ kertaluku on luonnollinen luku $n$ jos ja vain jos $n$ on pienin positiivinen eksponentti $r$, jolla $a^r = e$.*

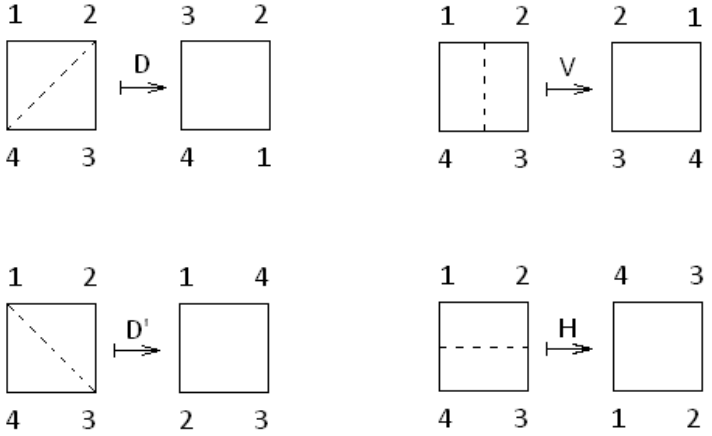
## 2.2 Diedri- ja symmetriaryhmät

Tarkastellaan neliötä tason pistejoukkona. Kun neliötä kierretään keskipisteensä ympäri vastapäivään kulman $0, \frac{\pi}{2}, \pi$ tai $\frac{3\pi}{2}$ verran, niin neliö kuvautuu itselleen, kuten nähdään kuvassa 1. Identtinen kuvaus $I$ vastaa kiertoa kulman 0 verran. Kuvaukset $R_{90}, R_{180}$ ja $R_{270}$ vastaavat puolestaan kiertoja kulmien $\frac{\pi}{2}, \pi$ ja $\frac{3\pi}{2}$ verran.

Lisäksi neliötä voidaan peilata neljällä eri tavalla siten, että se kuvautuu edelleen itselleen. Merkitään näitä eri peilauksia kuvan 2 esittämällä tavalla $D, V, D'$ ja $H$. Kuvaukset $D$ ja $D'$ ovat peilaukset diagonaalien suhteen, $V$ on peilaus pystyakselin ja $H$ vaaka-akselin suhteen. Kierrot ja peilaukset muodostavat ryhmän, jossa laskutoimituksena on kuvausten yhdistäminen. Taulukkoon 1 on koottu ryhmän kertotaulu.




Kuva 1: Neliötä kierretään keskipisteensä ympäri vastapäivään kulmien $0, \frac{\pi}{2}, \pi$ ja $\frac{3\pi}{2}$ verran.




Kuva 2: Neliötä peilataan neljän symmetria-akselinsa ympäri.

**Määritelmä 2.9.** Kiertojen ja peilausten $I, R_{90}, R_{180}, R_{270}, D', H, D, V$ määräämää ryhmää kutsutaan *diedriryhmäksi*;

$$D_4 = (\{I, R_{90}, R_{180}, R_{270}, D', H, D, V\}, \circ).$$

Yleisemmin voidaan määritellä diedriryhmä $D_n$, kun $n \geq 3$. Silloin tutkittava pistejoukko on säännöllinen $n$-kulmio ja kierrot ovat kulman $\frac{2\pi}{n}$ monikertoja.

Tarkastellaan nyt $n$-alkioisen joukon permutaatioita. Olkoon joukko

$$S_n = \{\alpha : J_n \to J_n \mid \alpha \text{ bijektio}\},$$

| $\circ$ | $I$ | $R_{90}$ | $R_{180}$ | $R_{270}$ | $D'$ | $H$ | $D$ | $V$ |
|---|---|---|---|---|---|---|---|---|
| $I$ | $I$ | $R_{90}$ | $R_{180}$ | $R_{270}$ | $D'$ | $H$ | $D$ | $V$ |
| $R_{90}$ | $R_{90}$ | $R_{180}$ | $R_{270}$ | $I$ | $H$ | $D$ | $V$ | $D'$ |
| $R_{180}$ | $R_{180}$ | $R_{270}$ | $I$ | $R_{90}$ | $D$ | $V$ | $D'$ | $H$ |
| $R_{270}$ | $R_{270}$ | $I$ | $R_{90}$ | $R_{180}$ | $V$ | $D'$ | $H$ | $D$ |
| $D'$ | $D'$ | $V$ | $D$ | $H$ | $I$ | $R_{270}$ | $R_{180}$ | $R_{90}$ |
| $H$ | $H$ | $D'$ | $V$ | $D$ | $R_{90}$ | $I$ | $R_{270}$ | $R_{90}$ |
| $D$ | $D$ | $H$ | $D'$ | $V$ | $R_{180}$ | $R_{90}$ | $I$ | $R_{270}$ |
| $V$ | $V$ | $D$ | $H$ | $D'$ | $R_{270}$ | $R_{180}$ | $R_{90}$ | $I$ |

Taulukko 1: Diedriryhmän $D_4$ kertotaulu.

missä $J_n = \{1, 2, \ldots n\}$. Joukko $S_n$ on ryhmä, kun laskutoimituksena on kuvausten yhdistäminen.

**Määritelmä 2.10.** Ryhmää $S_n$ kutsutaan *symmetriaryhmäksi* ja sen aliryhmiä *permutaatioryhmiksi*.

Koska $n$:n symbolin joukolla on $n!$ kappaletta eri permutaatiota, niin ryhmän $S_n$ kertaluku on $n!$.

Permutaatioita voidaan merkitä esimerkiksi

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix},$$

mutta lyhyempi merkintätapa ovat *syklit*. Jos

$$a_1 \mapsto a_2,\ a_2 \mapsto a_3,\ \ldots, a_{r-1} \mapsto a_r,\ a_r \mapsto a_1,\ \text{ja muuten } a \mapsto a,$$

missä $a_i, a \in J_n$ ja kaikki $a_i$ ovat eri alkioita, niin sama voidaan esittää syklinä

$$(a_1 a_2 \ldots a_r),$$

jonka *pituus* on $r$.

*Esimerkki* 2.11.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix} = (142)(36).$$

On huomattava, että permutaation sykliesitys ei ole yksikäsitteinen. Esimerkiksi

$$(142)(36) = (5)(36)(142) = (5)(63)(421).$$

Jos permutaatio koostuu useammasta kuin yhdestä syklistä, niin on syytä lisäksi kiinnittää huomiota syklien järjestykseen. Syklien yhdistäminen on

vaihdannainen vain silloin, jos syklit ovat erilliset. Mikäli permutaatioiden välillä ei ole merkkiä, niin permutaatiot suoritetaan oikealta vasemmalle. Esimerkiksi

$$(12)(23) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (23)(12).$$

Kuitenkin, jos permutaatioiden välillä on merkki $\cdot$, niin permutaatiot suoritetaan vasemmalta oikealle. Siis jos $\alpha$ ja $\beta$ ovat kaksi permutaatiota, niin

$$\alpha \cdot \beta = \beta\alpha.$$

*Esimerkki* 2.12. Numeroidaan neliön kärjet myötäpäivään $1, 2, 3$ ja $4$, kuten kuvissa 1 ja 2. Tällöin neliön kierrot $R_{90}, R_{180}, R_{270}$ ja peilaukset $D', H, D, V$ voidaan samastaa permutaatioiden kanssa:

$$R_{90} = (1234),\ R_{180} = (13)(24),\ R_{270} = (1432),$$
$$D' = (24),\ H = (14)(23),\ D = (13),\ V = (12)(34).$$

**Määritelmä 2.13.** Permutaation sanotaan olevan *tyyppiä* $(r_1, \ldots, r_m)$, jos sen jonkin esityksen syklien pituudet ovat $r_1, \ldots, r_m$.

*Esimerkki* 2.14. Permutaatio $(142)(36) = (5)(36)(142)$ on tyyppiä $(3, 2)$ ja $(1, 2, 3)$.

**Lause 2.15.** *Jos permutaatio $\alpha \in S_n$ on tyyppiä $(r_1, \ldots, r_m)$, niin*

$$\operatorname{ord}(\alpha) = \operatorname{pyj}(r_1, \ldots, r_m).$$

*Todistus.* Katso Metsänkylä & Näätänen: *Algebra* (Yliopistopaino, 2009), Lause IV.4.8. □

Permutaatiota, joka on tyyppiä $(2)$, kutsutaan *transpositioksi*. Havainnollistamme esimerkkien avulla, että transpositiot $(12), (23), \ldots, ((n-1)n)$ virittävät symmetriaryhmän $S_n$:

*Esimerkki* 2.16. Nähdään, että

$$(12345) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (15)(14)(13)(12).$$

Yleisemmin pätee, että mikä tahansa $r$-sykli $(a_1 a_2 \ldots a_r)$ voidaan kirjoittaa $(r-1)$:n transposition yhdisteenä $(1a_r) \ldots (1a_2)$.

*Esimerkki* 2.17. Lisäksi huomataan, että

$$(15) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix} = (12)(23)(34)(45)(34)(23)(12).$$

Yleisemmin mikä tahansa transpositio, joka on muotoa $(1i)$, missä $2 \leq i \leq n$, voidaan kirjoittaa $(12)(23)\dots((i-1)i)((i-2)(i-1))\dots(23)(12)$.

Yhdistämällä edellisten esimerkkien huomiot nähdään, että mikä tahansa symmetriaryhmän $S_n$ permutaatio voidaan kirjoittaa transpositioiden $(12), (23), \dots, ((n-1)n)$ yhdisteenä.

**Seuraus 2.18.** *Transpositiot* $(12), (23), \dots, ((n-1)n)$ *virittävät ryhmän* $S_n$.

Tarkka todistus sivuutetaan.

## 2.3 Suora tulo, kommutaattorialiryhmä ja normaali sulkeuma

**Lause 2.19.** *Olkoon* $G_1$ *ja* $G_2$ *ryhmiä. Niiden karteesinen tulo* $G_1 \times G_2$ *on ryhmä seuraavan laskutoimituksen suhteen:*

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2),$$

*missä* $a_i, b_i \in G_i$.

*Todistus.* Katso Metsänkylä & Näätänen: *Algebra* (Yliopistopaino, 2009), Lause III.2.5. □

**Määritelmä 2.20.** Ryhmää $G_1 \times G_2$ kutsutaan ryhmien $G_1$ ja $G_2$ *suoraksi tuloksi.*

**Määritelmä 2.21.** Olkoon $G$ ryhmä. Alkioita

$$x^{-1}y^{-1}xy,$$

missä $x, y \in G$, kutsutaan *kommutaattoreiksi.* Niiden virittämää ryhmää merkitään $[G, G]$ ja kutsutaan *kommutaattorialiryhmäksi.*

Huomataan, että kommutaattorialiryhmä $[G, G]$ on ryhmän $G$ aliryhmä, sillä kommutaattorit ovat ryhmän $G$ alkioita.

Tässä tutkielmassa käytämme kommutaattorille jatkossa myös merkintää

$$[x, y] \coloneqq x^{-1}y^{-1}xy.$$

**Lause 2.22.** *Kommutaattorialiryhmä* $[G, G]$ *on ryhmän* $G$ *normaali aliryhmä ja tekijäryhmä* $G/[G, G]$ *on Abelin ryhmä.*

*Todistus.* Katso Almkvist: *Algebra* (Studentlitteratur, 1968), exempel A.1.7. □

**Lause 2.23.** *Olkoon* $G$ *ryhmä ja* $N$ *sen normaali aliryhmä. Tekijäryhmä* $G/N$ *on Abelin ryhmä, jos ja vain jos* $[G, G] \leqslant N$.

*Todistus.* Katso Dummit & Foote: *Abstract Algebra* (Prentice-Hall International, 1991), Proposition 5.4.7.(4). □

**Määritelmä 2.24.** Olkoon $G$ ryhmä ja $S$ sen jokin osajoukko. Alkioiden

$$gsg^{-1},$$

missä $g \in G$ ja $s \in S$, virittämää ryhmää $\overline{S}$ kutsutaan *joukon* $S$ *normaaliksi sulkeumaksi ryhmässä* $G$.

Voidaan osoittaa, että normaali sulkeuma $\overline{S}$ on suppein ryhmän $G$ normaali aliryhmä, joka sisältää joukon $S$.

# 3 Vapaa ryhmä

Esitämme alaluvussa 3.1 ensin vapaalle ryhmälle sekä epäformaalin että formaalin määritelmän, minkä jälkeen tutkimme näiden kahden määritelmän yhteyttä toisiinsa. Tämän jälkeen alaluvussa 3.2 osoitamme Nilsenin–Schreierin lauseen.

Tässä luvussa käytämme joukoille ilmaisua *kaksio* tai *kolmio*, kun joukossa on tasan kaksi tai kolme eri alkiota.

## 3.1 Määritelmä

### Sana

Ennen kuin voimme puhua vapaista ryhmistä, on määriteltävä käsitteet *sana* ja *supistettu* sana.

Olkoon $S$ joukko. Joukko-opista tiedetään, että voidaan aina valita sellainen joukosta $S$ erillinen joukko $S^*$, että joukkojen $S$ ja $S^*$ mahtavuudet ovat yhtä suuret. Joukkojen $S$ ja $S^*$ välillä on olemassa bijektio, joka kuvaa joukon $S$ alkion $a$ alkioksi $a^*$. Merkitään näiden joukkojen yhdistettä $T$ eli $T = S \cup S^*$.

Joukon $T$ $n$:nnen karteesisen tulon, $T^n = \underbrace{T \times \ldots \times T}_{n \text{ kappaletta}}$, alkiot ovat $n$-mittaisia *sanoja* joukon $T$ yli. Sanan $w$ pituus $n$ voidaan merkitä $\ell(w) = n$ tai lyhyemmin $w = w_n$. Jos $n = 0$, niin sana on niin kutsuttu *tyhjä sana*, jota merkitään (). Sanoille käytämme yleisesti merkinnän $(a_1, \ldots, a_n)$ sijaan lyhyesti merkintää $a_1 \ldots a_n$.

Sana saattaa sisältää niin kutsuttuja osasanoja $aa^*$ ja $a^*a$, missä $a \in S$. Sana on *supistettu*, jos tällaisia osasanoja ei ole. Olkoon

$$\begin{aligned} W_n &= \{\text{kaikki } n\text{-mittaiset supistetut sanat}\} \\ &= \{w_n = a_1 \ldots a_n \mid a_i \in T, a_i \neq a_{i+1}^* \text{ ja } a_{i+1} \neq a_i^*\}. \end{aligned}$$

*Esimerkki* 3.1. Joukko $W_0$ on yksiö $\{()\}$.

*Esimerkki* 3.2. Muun muassa sanat $abb^*c$, $a^*aac$ ja $ac^*bb^*cc$ ”supistuvat” 2-mittaiseksi supistetuksi sanaksi $ac \in W_2$. Supistaminen voidaan ajatella sanojen projisioimisena supistetuiksi sanoiksi. Jokaista supistettua sanaa vastaa ääretön määrä (supistamattomia) sanoja.

**Määritelmä 3.3.** Olkoot $w_n = a_1 \ldots a_n$ ja $w_m = b_1 \ldots b_m$ supistettuja sanoja. Sana $w_n \cdot w_m$ voidaan muodostaa *yhdistämällä*:

$$w_n \cdot w_m = a_1 \ldots a_n \cdot b_1 \ldots b_m = a_1 \ldots a_{n-r} b_{r+1} \ldots b_m,$$

missä $r$ kappaletta osasanoja $a_n b_1, \ldots, a_{n-r+1} b_r$ ovat supistuneet pois, kunnes $a_{n-r} \neq b_{r+1}^*$ ja $a_{n-r}^* \neq b_{r+1}$.

Yhdistämällä saatu sana $w_n \cdot w_m$ on siis supistettu, $(n+m-2r)$-mittainen sana.

*Esimerkki* 3.4. Olkoot kolmio $S = \{a, b, c\}$ sekä supistetut sanat $w_3 = ab^*c \in W_3$ ja $w_4 = c^*bca^* \in W_4$. Tällöin $w_3 \cdot w_4$ on 3-mittainen supistettu sana

$$w_3 \cdot w_4 = ab^*c \cdot c^*bca^* = aca^* \in W_3$$

ja $w_4 \cdot w_3$ on 5-mittainen supistettu sana

$$w_4 \cdot w_3 = c^*bca^* \cdot ab^*c = c^*bcb^*c \in W_5.$$

Sanojen yhdistäminen ei siis ole vaihdannainen operaatio.

*Esimerkki* 3.5. Olkoot kolmio $S = \{a, b, c\}$ sekä supistetut sanat $w = ab^*ac$ ja $v = c^*a^*ba^*$. Tarkastellaan supistettuja sanoja $w \cdot v$ ja $v \cdot w$:

$$w \cdot v = ab^*ac \cdot c^*a^*ba^* = ()$$
$$v \cdot w = c^*a^*ba^* \cdot ab^*ac = ()$$

Huomataan, että yhdistämällä supistetut sanat $w$ ja $v$ kummin tahansa päin saadaan tyhjä sana $()$.

Joukko $S^*$ konstruoitiin siten, että joukkojen $S$ ja $S^*$ välillä on bijektio. Tällä bijektiolla on myös bijektiivinen käänteiskuvaus, joka kuvaa joukon $S^*$ alkion $a^*$ alkioksi $a^{**} = a$. Koska joukot $S$ ja $S^*$ ovat erillisiä, niin alkio $a^*$ on yksikäsitteisesti määrätty kaikilla $a \in T$.

Olkoon $S$ joukko ja $T = S \cup S^*$. Joukkoa, joka koostuu kaikista supistetuista sanoista joukon $T$ yli, merkitään

$$F = \bigcup_{n \geq 0} W_n.$$

Osoitetaan, että $F$ muodostaa ryhmän, jossa ryhmäoperaationa on yhdistäminen (määritelmä 3.3):

(G0) Kahden supistetun sanan yhdistäminen tuottaa aina supistetun sanan, joten yhdistäminen on määritelty joukossa $F$.

(G1) Olkoot sellaiset sanat $w_\ell, w_m, w_n \in F$, että $w_\ell = a_1 \ldots a_\ell$, $w_m = b_1 \ldots b_m$ ja $w_n = c_1 \ldots c_n$. Osoitetaan, että yhdistäminen toteuttaa liitäntälain, $(w_\ell \cdot w_m) \cdot w_n = w_\ell \cdot (w_m \cdot w_n)$.

Mikäli vähintään yksi sanoista on tyhjä sana (), niin liitäntälaki toteutuu selvästi. Oletetaan siis, että $\ell, m$ ja $n$ ovat positiivisia kokonaislukuja. Oletetaan myös, että yhdistetty sana $w_\ell \cdot w_m$ on $(\ell + m - 2r)$-mittainen ja $w_m \cdot w_n$ on $(m + n - 2s)$-mittainen. Jaetaan tarkastelu kolmeen eri tapaukseen:

$r + s < m$ : Molemmissa tapauksissa saadaan sama supistettu sana,

$$\begin{aligned}(w_\ell \cdot w_m) \cdot w_n &= (a_1 \dots a_\ell \cdot b_1 \dots b_m) \cdot c_1 \dots c_n \\ &= a_1 \dots a_{\ell-r} b_{r+1} \dots b_m \cdot c_1 \dots c_n \\ &= a_1 \dots a_{\ell-r} b_{r+1} \dots b_{m-s} c_{s+1} \dots c_n \\ &= a_1 \dots a_\ell \cdot b_1 \dots b_{m-s} c_{s+1} \dots c_n \\ &= a_1 \dots a_\ell \cdot (b_1 \dots b_m \cdot c_1 \dots c_n) = w_\ell \cdot (w_m \cdot w_n).\end{aligned}$$

$r + s = m$ : Sana $w_m$ supistuu kokonaan pois. Vastaavalla tavalla kuin yllä, molemmissa tapauksissa saadaan sama supistettu sana,

$$(w_\ell \cdot w_m) \cdot w_n = a_1 \dots a_{\ell-r} c_{s+1} \dots c_n = w_\ell \cdot (w_m \cdot w_n).$$

$r + s > m$ : Sana $w_m$ supistuu $r$ termiä yhdisteessä $w_\ell \cdot w_m$ ja $s$ termiä yhdisteessä $w_m \cdot w_n$. Koska $r+s > m$, niin osasana $b_{m-s+1} \dots b_r$ supistuu pois sekä yhdisteessä $w_\ell \cdot w_m$ että $w_m \cdot w_n$. Näin ollen

$$a_{\ell-r+1} \dots a_{\ell-m+s} = b_r^* \dots b_{m-s+1}^* = c_{m-r+1} \dots c_s.$$

Saadaan siis

$$\begin{aligned}(w_\ell \cdot w_m) \cdot w_n &= (a_1 \dots a_\ell \cdot b_1 \dots b_m) \cdot c_1 \dots c_n \\ &= a_1 \dots a_{\ell-r} b_{r+1} \dots b_m \cdot c_1 \dots c_n \\ &= a_1 \dots a_{\ell-r} c_{m-r+1} \dots c_n \\ &= a_1 \dots a_{\ell-m+s} c_s \dots c_n \\ &= a_1 \dots a_\ell \cdot b_1 \dots b_{m-s} c_{s+1} \dots c_n \\ &= a_1 \dots a_\ell \cdot (b_1 \dots b_m \cdot c_1 \dots c_n) = w_\ell \cdot (w_m \cdot w_n).\end{aligned}$$

(G2) Joukkoon $F$ kuuluu tyhjä sana (), joka yhdistettynä minkä tahansa supistetun sanan $w \in F$ kanssa on sana itse,

$$w \cdot () = w = () \cdot w.$$

Joukon $F$ neutraalialkio on siis tyhjä sana ().

(G3) Jokaista supistettua sanaa $w_n = a_1 \dots a_n \in F$ kohti on olemassa sellainen sana $w_n^{-1} = (a_1 \dots a_n)^{-1} = a_n^* \dots a_1^* \in F$, joka yhdistettynä sanan $w$ kanssa tuottaa tyhjän sanan,

$$w \cdot w^{-1} = a_1 \dots a_n \cdot a_n^* \dots a_1^* = () = a_n^* \dots a_1^* \cdot a_1 \dots a_n = w^{-1} \cdot w.$$

Jokaista $F$:n alkiota kohti on siis olemassa käänteisalkio joukossa $F$.

Joukon $T$ alkiot voidaan samastaa 1-mittaisten sanojen kanssa eli $T = W_1$. Koska $a \cdot a^{-1} = ()$ kaikilla $a \in W_1$, niin jokaista 1-mittaista sanaa $a \in W_1$ vastaan on olemassa käänteissana $a^{-1} \in W_n$. Joukon $S$ alkio $a$ samastuu sanan $a \in W_1$ kanssa ja joukon $S^*$ alkio $a^*$ sanan $a^{-1} \in W_1$ kanssa. Joukko $S$ siis sisältyy aina kaikkien supistettujen sanojen joukkoon $F$, $S \subset F$.

**Sana ryhmätilanteessa**

Mikäli lähtökohtana on ryhmä $G$ ja sen osajoukko $S$, niin silloin joukko $S^*$ koostuu joukon $S$ alkioiden $a$ käänteisalkioista $a^{-1}$ ryhmässä $G$. Siis jos $a \in S$, niin $a^{-1} \in S^*$. Voidaan siis merkitä $a^* = a^{-1}$ kaikilla $a \in T$ ja $S^* = S^{-1}$. Vastaavasti tyhjä sana () samastuu neutraalialkion $e$ kanssa, joten myös tyhjälle sanalle voidaan alkaa käyttää merkintää $e$. On muistettava, että joukkojen $S$ ja $S^{-1}$ kuuluu olla erilliset. Näin ollen ryhmän $G$ neutraalialkio $e$ ei saa kuulua joukkoon $S$.

Tehdään ero, milloin puhutaan ryhmän $G$ alkioiden välisestä tulosta ja milloin sanasta joukon $T = S \cup S^{-1}$ yli. Merkintä $a \cdot b$ tarkoittaa ryhmän $G$ alkioiden $a$ ja $b$ tuloa ja $ab$ on sana joukon $T$ yli. Voidaan siis kirjoittaa $a \cdot a^{-1} = e$, mikä pätee kaikille $a \in G$, mutta 2-mittainen sana $aa^{-1}$ ei ole tyhjä sana (), jonka pituus on 0.

Mikä tahansa supistettu sana $a_1 \dots a_n$ voidaan samastaa tuloesityksen $a_1 \cdots a_n$ kanssa, mutta mikä tahansa tuloesitys $a_1 \cdots a_n$ ei välttämättä vastaa supistettua sanaa $a_1 \dots a_n$. Sana on järjestetty jono, joten sen alkioiden ("kirjaimien") lukumäärällä ja järjestyksellä on merkitys. Tulon arvo ei kuitenkaan muutu, vaikka tuloesityksen tekijöiden lukumäärää kasvattaisi neutraalialkiolla $e$ tai osatuloilla $a \cdot a^{-1}$. Abelin ryhmissä myöskään tulontekijöiden järjestyksellä ei ole väliä.

Otetaan käyttöön termi *supistettu tuloesitys*, jolla tarkoitetaan tuloesitystä $a_1 \cdots a_n$ ja jossa tekijänä ei ole neutraalialkiota $e$ eikä tuloja $a \cdot a^{-1}$. Supistetussa tuloesityksessä tulontekijät ja niiden järjestys on kiinnitetty; kaksi supistettua tuloesitystä ovat samat, jos ja vain jos niillä on sama lukumäärä samoja tekijöitä samassa järjestyksessä. Siinä tapauksessa, että tuloesitys on yksikäsitteinen, niin supistettu tuloesitys $a_1 \cdots a_n$ samastuu supistetun sanan $a_1 \dots a_n$ kanssa.

Kun joukko $S$ valitaan ryhmästä $G$ pitäen huolta, että joukot $S$ ja $S^{-1}$ ovat erilliset, niin joukon $T = S \cup S^{-1}$ alkioiden välillä on aina vähintään relaatio $a \cdot a^{-1} = e_G$, missä $a \in S$ tai $a \in S^{-1}$. Sen lisäksi joukon $T$ alkioiden välillä voi olla muitakin relaatioita ryhmässä $G$.

**Määritelmä 3.6.** Olkoon $G$ ryhmä. Valitaan sellainen osajoukko $S$, että neutraalialkio $e_G$ ei sisälly siihen eikä se sisällä sekä alkiota $a$ että $a^{-1}$ millään $a \in G$. Kootaan joukko $S^{-1}$, johon sisältyy kaikki joukon $S$ käänteisalkiot ryhmässä $G$. Joukot $S$ ja $S^{-1}$ ovat siis erilliset. Merkitään niiden yhdistettä $T = S \cup S^{-1}$. Kaikille joukon $T$ alkioille $a, a^{-1} \in T$ pätee ryhmässä $G$ *triviaali relaatio* $a \cdot a^{-1} = e_G$. Mikäli myös jokin muu joukon $T$ alkioiden tulo $a_1 \cdots a_n$, missä $a_1 \cdots a_n$ on supistettu tuloesitys ja $n \geq 2$, tuottaa neutraalialkion ryhmässä $G$, niin sanotaan, että ryhmässä $G$ on *epätriviaali relaatio* $a_1 \cdots a_n = e_G$ joukon $T$ suhteen.

*Esimerkki* 3.7. Olkoon kokonaislukujen additiivinen ryhmä $(\mathbb{Z}, +)$. Valitaan kaksi osajoukkoa $S_1 = \{1\}$ ja $S_2 = \{2, 3\}$. Tällöin $T_1 = \{1, -1\}$ ja $T_2 = \{2, -2, 3, -3\}$. Joukon $T_1$ alkioille pätee vain triviaali relaatio $1 - 1 = 0$. Sen sijaan kokonaislukujen ryhmässä on triviaalien relaatioiden $2 - 2 = 0$ ja $3 - 3 = 0$ lisäksi myös kaksi epätriviaalia relaatiota joukon $T_2$ suhteen:

$$3 + 2 - 3 - 2 = 0 \text{ ja } 3 + 3 - 2 - 2 - 2 = 0,$$

sillä $3 + 2 - 3 - 2$ ja $3 + 3 - 2 - 2 - 2$ ovat supistettuja summaesityksiä.

Esimerkin 2.3 nojalla osajoukot $S_1$ ja $S_2$ virittävät kokonaislukujen ryhmän. Jokainen kokonaisluku voidaan siis ilmaista sekä alkioiden 1 ja $-1$ summana että alkioiden 2 ja 3 lineaarikombinaationa. Esimerkiksi positiivinen kokonaisluku $m$ voidaan esittää seuraavilla tavoilla

$$m = \underbrace{1 + 1 + \ldots + 1}_{m \text{ kappaletta}} = \underbrace{3 - 2 + 3 - 2 + \ldots + 3 - 2}_{m \text{ kappaletta}}.$$

Kuitenkin, koska kokonaislukujen ryhmässä on epätriviaaleja relaatioita joukon $T_2$ suhteen, niin kokonaisluvun $m$ supistettu summaesitys alkioiden 2 ja 3 lineaarikombinaationa ei ole yksikäsitteinen. Tämä nähdään siitä, että

$$1 = 3 - 2 = 3 + 3 + 3 - 2 - 2 - 2 - 2 = \ldots .$$

**Propositio 3.8.** *Olkoon $G$ ryhmä ja $S$ osajoukko, joka virittää ryhmän $G$. Jos ryhmässä $G$ ei ole epätriviaaleja relaatioita joukon $T = S \cup S^{-1}$ suhteen, niin ryhmän $G$ jokaisen alkion supistettu tuloesitys on yksikäsitteinen.*

*Todistus.* Oletetaan, että ryhmässä $G$ ei ole epätriviaaleja relaatioita joukon $T$ suhteen, ja olkoot $a_1 \cdots a_n$ ja $b_1 \cdots b_m$, missä $a_i, b_i \in T$ kaikilla $i$, kaksi sellaista supistettua tuloesitystä alkiolle $w$, että $n > m$. Tällöin

$$a_1 \cdots a_n = b_1 \cdots b_m \text{ eli } a_n^{-1} \cdots a_1^{-1} \cdot b_1 \cdots b_m = e.$$

Koska tuloesitykset $a_1 \cdots a_n$ ja $b_1 \cdots b_m$ ovat supistettuja ja ryhmässä $G$ ei ole epätriviaaleja relaatioita, niin on oltava $a_i^{-1} \cdot b_i = e$ kaikilla $1 \leq i \leq m$ ja $a_j = e$ kaikilla $m < j \leq n$. Tämä on kuitenkin ristiriita, sillä supistetussa tuloesityksessä ei ole tekijänä neutraalialkiota. Saman tulon supistetuissa tuloesityksissä on siis oltava yhtä monta tekijää.

Olkoon siis $a_1 \cdots a_n$ ja $b_1 \cdots b_n$, missä $a_i, b_i \in T$ kaikilla $i$, kaksi sellaista supistettua tuloesitystä alkiolle $w$, joissa on yhtä monta tekijää. Tällöin

$$a_1 \cdots a_n = b_1 \cdots b_n \text{ eli } a_n^{-1} \cdots a_1^{-1} \cdot b_1 \cdots b_n = e.$$

Koska tuloesitykset $a_1 \cdots a_n$ ja $b_1 \cdots b_n$ ovat supistettuja ja ryhmässä $G$ ei ole epätriviaaleja relaatioita, niin on oltava $a_i^{-1} \cdot b_i = e$ eli $a_i = b_i$ kaikilla $i$. Tulon $w$ kahdessa tuloesityksessä, joissa on yhtä monta tekijää, on oltava samat tekijät samassa järjestyksessä.

Jos ryhmässä $G$ ei ole epätriviaaleja relaatioita joukon $T$ suhteen, niin ryhmän $G$ jokaisen tulon supistettu tuloesitys on siis yksikäsitteinen. □

Voidaan tarkastella neutraalialkion supistettuja tuloesityksiä. Tällöin nähdään, että myös käänteinen tulos pätee. Saadaan siis seuraava tulos.

**Seuraus 3.9.** *Ryhmässä $G$, jonka virittää osajoukko $S$, ei ole epätriviaaleja relaatioita joukon $T$ suhteen, jos ja vain jos jokaisella ryhmän $G$ alkiolla on yksikäsitteinen supistettu tuloesitys.*

### Epäformaali määritelmä

**Määritelmä 3.10.** Olkoon $S$ joukko ja $T = S \cup S^*$. Joukko $F$, joka koostuu kaikista supistetuista sanoista joukon $T$ yli, on *vapaa ryhmä joukon $S$ suhteen*, kun laskutoimituksena on supistettujen sanojen yhdistäminen.

Mikäli on tarpeen korostaa, että ryhmä $F$ on vapaa juuri joukon $S$ suhteen, voidaan käyttää myös merkintää $F(S)$.

Huomataan, että minkä tahansa joukon suhteen voidaan konstruoida vapaa ryhmä samaan tyyliin kuin luvun alussa.

Olkoon $G$ ryhmä ja $S$ sen osajoukko. Oletetaan, että jokaisella ryhmän alkioilla on yksikäsitteinen supistettu tuloesitys joukon $T = S \cup S^{-1}$ suhteen. Lauseen 2.2 ja seurauksen 3.9 nojalla joukko $S$ virittää ryhmän $G$ ja ryhmässä $G$ ei ole epätriviaaleja relaatioita joukon $T$ suhteen. Yksikäsitteisestä

tuloesityksestä seuraa, että kaikki ryhmän $G$ alkiot $w = s_1 \cdots s_n$ samastuvat supistettujen sanojen $s_1 \dots s_n$ kanssa.

Lisäksi ryhmän $G$ laskutoimitus $\cdot$ samastuu supistettujen sanojen yhdistämisen kanssa: Olkoot $w_1$ ja $w_2$ ryhmän $G$ alkioita, joilla on yksikäsitteiset supistetut tuloesitykset $w_1 = a_1 \cdots a_n$ ja $w_2 = b_1 \cdots b_m$, missä $a_i, b_i \in T$ kaikilla $i$. Jos $a_{n-i} = b_{i+1}^{-1}$ kaikilla $0 \leq i < r$, mutta $a_{n-r} \neq b_{r+1}^{-1}$, niin

$$w_1 \cdot w_2 = a_1 \cdots a_n \cdot b_1 \cdots b_m = a_1 \cdots a_{n-r} \cdot b_{r+1} \cdots b_m,$$

eli tulolla $w_1 \cdot w_2$ on supistettu tuloesitys $a_1 \cdots a_{n-r} \cdot b_{r+1} \cdots b_m$. Toisaalta alkioiden $w_1$ ja $w_2$ yksikäsitteiset supistetut tuloesitykset $a_1 \cdots a_n$ ja $b_1 \cdots b_m$ samastuvat supistettujen sanojen $w_1 = a_1 \dots a_n$ ja $w_2 = b_1 \dots b_m$ kanssa. Tällöin yhdistämällä saadaan supistettu sana

$$w_1 \cdot w_2 = a_1 \dots a_n \cdot b_1 \dots b_m = a_1 \dots a_{n-r} b_{r+1} \dots b_m.$$

Ryhmä $G$, jonka virittää joukko $S$ ja jossa ei ole epätriviaaleja relaatioita joukon $T = S \cup S^{-1}$ suhteen, samastuu sellaisen ryhmän $F$ kanssa, joka on vapaa joukon $S$ suhteen epäformaalin määritelmän mukaan.

Huomataan, että vapaa ryhmä on aina ääretön ja yleisessä tapauksessa vapaa ryhmä ei ole vaihdannainen, sillä Abelin ryhmässä on epätriviaali relaatio $a \cdot b \cdot a^{-1} \cdot b^{-1} = e$. Käsittelemme vapaita Abelin ryhmiä myöhemmin luvussa 4.3.

### Formaali määritelmä

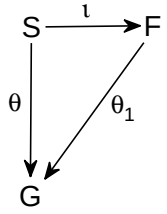
**Määritelmä 3.11.** Olkoon $F$ ryhmä ja $S$ sen osajoukko. Sanotaan, että *ryhmä $F$ on vapaa joukon $S$ suhteen*, jos jokaista ryhmää $G$ ja jokaista kuvausta $\theta : S \to G$ vastaa yksikäsitteisesti sellainen homomorfismi $\theta_1 : F \to G$, että

$$\theta_1(s) = \theta(s),$$

kaikilla $s \in S$.

Ryhmällä $F$ on *rangi* $r$, missä $r$ on joukon $S$ mahtavuus. Ryhmän $F$ rangia merkitään $r(F)$. Vaikka ryhmä voi olla vapaa usean eri joukon suhteen, niin voidaan osoittaa, että ryhmän rangi on yksikäsitteinen. Itse asiassa kaksi vapaata ryhmää ovat isomorfiset, jos ja vain jos niillä on sama rangi. (Katso Johnson: *Topics in the Theory of Group Presentations* (Cambridge University Press, 1980), Theorem 1.1.)

Vapaan ryhmän formaalille määritelmälle löytyy analoginen esimerkki lineaarialgebran piiristä:




Kuva 3: Määritelmän 3.11 kuvauskaavio.

*Esimerkki* 3.12. Olkoon $V$ äärellisulotteinen vektoriavaruus kunnan $K$ yli ja $B$ sen kanta. Tällöin mikä tahansa kuvaus $\tau : B \to W$, missä $W$ on toinen vektoriavaruus saman kunnan $K$ yli, voidaan laajentaa yksikäsitteisesti lineaarikuvauksesi $\tau_1 : V \to W$.

Olkoon nimittäin $\overline{v}$ jokin vektoriavaruuden $V$ vektori. Koska $B$ on $V$:n kanta, niin $\overline{v}$ voidaan esittää yksikäsitteisesti kantavektoreiden $\overline{s}_1, \ldots, \overline{s}_n \in B$ avulla:

$$\overline{v} = a_1\overline{s}_1 + \cdots + a_n\overline{s}_n,$$

missä vakiokertoimet $a_i \in K$ kaikilla $i$. Esityksen olemassaolon ja yksikäsitteisyyden nojalla voidaan määritellä kuvaus

$$\tau_1(\overline{v}) = \tau_1(a_1\overline{s}_1 + \cdots + a_n\overline{s}_n) = a_1\tau(\overline{s}_1) + \cdots + a_n\tau(\overline{s}_n).$$

Kuvaus $\tau_1$ on hyvinmääritelty, sillä jokaista $\overline{v} \in V$ vastaa yksikäsitteinen jono $(a_1, \ldots, a_n)$ ja siten yksikäsitteinen $\tau_1(\overline{v}) \in W$. Lisäksi valitsemalla esimerkiksi $\overline{v} = \overline{s_1}$ on helppo nähdä, että lineaarikuvaus $\tau_1$ laajentaa kuvauksen $\tau$. Laajennus on yksikäsitteinen, sillä $\tau$ määrää, miten avaruuden kanta kuvautuu.

Osoitetaan vielä, että kuvaus $\tau_1$ toteuttaa lineaarikuvauksen ehdon

$$\tau_1(a\overline{x} + b\overline{y}) = a\tau_1(\overline{x}) + b\tau_1(\overline{y}),$$

missä $a, b \in K$ ja $\overline{x}, \overline{y} \in V$. Vektoriavaruuden $V$ vektorit $\overline{x}$ ja $\overline{y}$ voidaan kirjoittaa muodossa $\overline{x} = x_1\overline{s_1} + \cdots + x_n\overline{s_n}$ ja $\overline{y} = y_1\overline{s_1} + \cdots + y_n\overline{s_n}$, missä kaikki skalaarit $x_i$ ja $y_i$ ovat kunnan $K$ alkioita ja vektorit $\overline{s_i}$ kannan $B$

vektorit. Näin ollen

$$\begin{aligned}
\tau_1(a\overline{x} + b\overline{y}) &= \tau_1\left(a(x_1\overline{s_1} + \cdots + x_n\overline{s_n}) + b(y_1\overline{s_1} + \cdots + y_n\overline{s_n})\right) \\
&= \tau_1(ax_1\overline{s_1} + \cdots + ax_n\overline{s_n} + by_1\overline{s_1} + \cdots + by_n\overline{s_n}) \\
&= \tau_1((ax_1 + by_1)\overline{s_1} + \cdots + (ax_n + by_n)\overline{s_n}) \\
&= (ax_1 + by_1)\tau(\overline{s_1}) + \cdots + (ax_n + by_n)\tau(\overline{s_n}) \\
&= ax_1\tau(\overline{s_1}) + \cdots + ax_n\tau(\overline{s_n}) + by_1\tau(\overline{s_1}) + \cdots + by_n\tau(\overline{s_n}) \\
&= a\left(x_1\tau(\overline{s_1}) + \cdots + x_n\tau(\overline{s_n})\right] + b\left[y_1\tau(\overline{s_1}) + \cdots + y_n\tau(\overline{s_n})\right) \\
&= a\tau_1(x_1\overline{s_1} + \cdots + x_n\overline{s_n}) + b\tau_1(y_1\overline{s_1} + \cdots + y_n\overline{s_n}) \\
&= a\tau_1(\overline{x}) + b\tau_1(\overline{y}).
\end{aligned}$$

Vektoriavaruuden kannan vektorit virittävät koko avaruuden ja ovat keskenään lineaarisesti riippumattomia. Myös virittäjistö virittää vektoriavaruuden, mutta se saattaa sisältää vektoreita, jotka ovat keskenään lineaarisesti riippuvia. Mikäli edellisessä esimerkissä $B$ olisi ollut kannan sijasta pelkkä virittäjistö, vektorin $\overline{v}$ esitys $B$:n vektoreiden avulla ei olisi ollut yksikäsitteinen. Poistamalla virittäjistöstä sopivat vektorit, saadaan virittäjistö supistettua kannaksi. On kuitenkin huomattava, että mikäli virittäjistössä on useita toisistaan lineaarisesti riippuvia vektoreita, poistettavat vektorit voidaan valita usealla eri tavalla, joten virittäjistöä ei voi yksikäsitteisesti muuttaa kannaksi. Lisäksi, jos virittäjävektoreiden välillä on lähtöavaruudessa relaatioita, niin lineaarikuvaus, joka laajentaisi alkuperäisen kuvauksen, kuuluisi olla sellainen, että myös kuvapisteet toteuttaisivat samat relaatiot. Tällaista laajennusta ei välttämättä ole olemassa.

Toisaalta mikä tahansa joukko keskenään lineaarisesti riippumattomia vektoreita ei välttämättä viritä avaruutta. Mikäli edellisessä esimerkissä $B$ olisi ollut puolestaan joukko lineaarisesti riippumattomia vektoreita, vektoria $\overline{v}$ ei olisi välttämättä voinut esittää ollenkaan $B$:n vektoreiden lineaarikombinaationa. Tällainen joukko voidaan puolestaan laajentaa kannaksi lisäämällä sopivia vektoreita. Sopivat vektorit eivät kuitenkaan ole yksikäsitteisesti määrättyjä. Näin ollen myöskään vapaata joukkoa ei voi yksikäsitteisesti laajentaa kannaksi. Lisäksi vektorit, joilla vapaiden vektoreiden joukko laajennetaan kannaksi, voidaan kuvata miten tahansa. Tällöin mielivaltainen kuvaus voidaan kyllä laajentaa lineaarikuvaukseksi, mutta ei yksikäsitteisesti.

Tämän analogian valossa on luontevaa tarkastella lisää vapaita ryhmiä.

**Propositio 3.13.** *Olkoon ryhmä $F$ vapaa joukon $S$ suhteen formaalin määritelmän mukaan. Tällöin joukko $S$ virittää ryhmän $F$, $\langle S\rangle = F$.*

*Todistus.* Merkitään inkluusiota $\theta : S \to \langle S\rangle$, jolloin vapaan ryhmän formaalin määritelmän nojalla inkluusio $\theta$ laajenee yksikäsitteisesti homomorfismiksi $\theta_1 : F \to \langle S\rangle$. Joukon $S$ virittämä ryhmä $\langle S\rangle$ sisältyy ryhmään $F$.

Merkitään tätä inkluusiota $\phi : \langle S \rangle \to F$. Tilanteen kuvauskaavio on esitetty kuvassa 4.


Kuva 4: Kun ryhmä $F$ on vapaa joukon $S$ suhteen, niin joukko $S$ virittää ryhmän $F$.

Yhdistetty kuvaus $\phi \circ \theta_1 : F \to F$ laajentaa inkluusion $\iota : S \to F$, mutta niin tekee myös identiteettikuvaus $\mathrm{id} : F \to F$. Koska ryhmä $F$ on vapaa joukon $S$ suhteen, niin laajennus on yksikäsitteinen, joten on oltava $\phi \circ \theta_1 = \mathrm{id}$. Kuvaus $\phi$ on siis surjektio, joten $\langle S \rangle = F$, jolloin $S$ virittää vapaan ryhmän $F$.

□

Huomattavaa on, että jos joukko $S$ ei viritä ryhmää $F$, niin $F$ ei ole vapaa joukon $S$ suhteen. Toisaalta se, että joukko $S$ virittää ryhmän $F$ ei yksinään riitä takaamaan, että ryhmä $F$ on vapaa joukon $S$ suhteen formaalin määritelmän nojalla, kuten nähdään esimerkissä 3.15.

*Esimerkki* 3.14. Olkoot kaksio $S = \{a, b\}$, ryhmä $F$ vapaa ryhmä joukon $S$ suhteen ja ryhmä $G$ mielivaltainen. Näin ollen joukot $S$ ja $S^*$ ovat erilliset ja jokainen supistettu sana $s_1 \dots s_n$ joukon $T = S \cup S^*$ yli samastuu sellaisen yksikäsitteisen supistetun tuloesityksen $s_1 \cdots s_n$ kanssa, missä $s_i \in T = S \cup S^*$ kaikilla $i$.

Olkoon mikä tahansa kuvaus $\theta : S \to G$. Määritellään sellainen kuvaus $\theta_1 : F \to G$, että

$$\begin{aligned} \theta_1(e_F) &= e_G, \\ \theta_1(s) &= \theta(s), \\ \theta_1(s^*) &= \theta(s)^{-1}, \\ \theta_1(s_1 \cdots s_n) &= \theta_1(s_1) \cdots \theta_1(s_n), \end{aligned}$$

missä $s \in S$ ja $s_i \in T$. Kuvaus $\theta_1$ siis laajentaa kuvauksen $\theta$. Esimerkiksi $\theta_1(a^2 \cdot b \cdot a^*) = \theta(a)^2 \cdot \theta(b) \cdot \theta(a)^{-1}$.

Koska supistettu tuloesitys on yksikäsitteinen ja kuvaus $\theta$ on hyvinmääritelty, niin myös kuvaus $\theta_1$ on hyvinmääritelty. Lisäksi se toteuttaa homomorfiaehdon: Olkoot sellaiset $w_n, w_m \in F$, että niillä on (yksikäsitteiset) supistetut tuloesitykset $w_n = a_1 \cdots a_n$ ja $w_m = b_1 \cdots b_m$, missä $a_i, b_i \in T$ kaikilla $i$. Oletetaan, että tulolla $w_n \cdot w_m$ on supistettu tuloesitys, jossa on $n + m - 2r$ tekijää, eli $w_n \cdot w_m = a_1 \cdots a_{n-r} b_{r+1} \cdots b_m$. Tällöin

$$\begin{aligned}
\theta_1(w_n \cdot w_m) &= \theta_1(a_1 \cdots a_{n-r} b_{r+1} \cdots b_m) \\
&= \theta(a_1) \cdots \theta(a_{n-r}) \cdot \theta(b_{r+1}) \cdots \theta(b_m) \\
&= \theta(a_1) \cdots \theta(a_{n-r}) \cdot \theta(a_{n-r+1}) \cdots \theta(a_n) \cdot \theta(b_1) \cdots \theta(b_r) \cdot \theta(b_{r+1}) \cdots \theta(b_m) \\
&= \theta(a_1) \cdots \theta(a_n) \cdot \theta(b_1) \cdots \theta(b_m) \\
&= \theta_1(w_n) \cdot \theta(w_m),
\end{aligned}$$

missä kolmas yhtäsuuruus seuraa kuvauksen $\theta_1$ ominaisuuksista: $\theta(b_{i+1})^{-1} = \theta_1(b_{i+1}^{-1}) = \theta(b_{i+1}^{-1}) = \theta(a_{n-i})$ kaikilla $0 \leq i \leq r$, kun $a_{n-i} = b_{i+1}^{-1}$.

Osoitetaan vielä kuvauksen $\theta_1$ yksikäsitteisyys: Jos $\theta_2$ on toinen homomorfismi, joka laajentaa kuvauksen $\theta$, niin on oltava

$$\theta_2(s) = \theta(s) = \theta_1(s)$$

kaikilla $s \in S$. Toisaalta, koska joukko $S$ virittää ryhmän $F$, niin on oltava $\theta_2(w) = \theta_1(w)$ kaikilla $w \in F$.

Siis kun joukon $T$ alkioiden välillä ei ole epätriviaaleja relaatioita ryhmässä $F = \langle a, b \rangle$, niin $F$ on vapaa formaalin määritelmän mielessä kaksion $S = \{a, b\}$ suhteen ja sen rangi on 2.

Edellisessä esimerkissä kuvaus $\theta_1$ ei olisi hyvinmääritelty, mikäli ryhmässä $F$ olisi epätriviaaleja relaatioita joukon $T$ suhteen. Tämä nähdään myös seuraavassa esimerkissä.

*Esimerkki* 3.15. Olkoot $S = \{a\}$, $F$ alkion $a$ virittämä syklinen ryhmä, jossa pätee epätriviaali relaatio $a^4 = e$, ja ryhmä $G = \mathbb{Z}$. Homomorfismi, joka laajentaisi kuvauksen $\phi : S \to G, a \mapsto 1$, on potenssilain nojalla oltava kuvaus $\theta : F \to G, a^n \mapsto n$. Kuvaus $\theta$ ei kuitenkaan ole kyseisessä tapauksessa hyvinmääritelty:

Epätriviaalin relaation $a^4 = e$ nojalla ryhmässä $F$ pätee $a^5 = a$. Näin ollen $\theta(a) = \theta(a^5) = 5$, vaikka toisaalta $\theta(a) = 1$, mikä on ristiriita. Vapaan ryhmän formaalin määritelmän mukaan ryhmä $F$ ei siis ole vapaa joukon $S$ suhteen.

Vastaava tulos pätee myös yleisesti:

**Propositio 3.16.** *Olkoon ryhmä $F$ vapaa joukon $S$ suhteen vapaan ryhmän formaalin määritelmän mukaan. Tällöin ryhmässä $F$ ei ole epätriviaaleja relaatioita joukon $T$ suhteen.*

*Todistus.* Tehdään vastaoletus: Oletetaan, että neutraalialkiolle $e$ on supistettu tuloesitys $a_1 \cdots a_n$, missä $n \geq 2$, ryhmässä $F$ joukon $T$ suhteen. Olkoon $G = \mathbb{Z}$ ja $\theta$ vakiokuvaus, joka kuvaa kaikki joukon $S$ alkiot vakioksi 1. Näin ollen vapaan ryhmän formaalin määritelmän nojalla on olemassa homomorfismi $\theta_1 : F \to \mathbb{Z}$, joka laajentaa kuvauksen $\theta$. Tällöin

$$\theta_1(e) = \theta_1(a_1 \cdots a_n) = \theta(a_1) + \cdots + \theta(a_n) = 1 + \cdots + 1 = n \neq 0,$$

mikä on ristiriita. Näin ollen vastaoletus on epätosi ja alkuperäinen väite on tosi. □

**Epäformaalin ja formaalin määritelmän yhteys**

Kaksi edellä esitettyä määritelmää vapaalle ryhmälle ovat itse asiassa yhtäpitävät.

Vapaan ryhmän epäformaalin määritelmän nojalla joukko $S$ virittää vapaan ryhmän $F(S)$ ja ryhmässä ei ole epätriviaaleja relaatioita. Esimerkissä 3.14 on esitetty idea, kuinka tällaisessa tapauksessa mielivaltainen kuvaus $\theta : S \to G$, missä $G$ on mikä tahansa ryhmä, laajenee yksikäsitteisesti homomorfismiksi $\theta_1 : F \to G$. Näin ollen epäformaalista määritelmästä seuraa formaali määritelmä.

Toisaalta, jos otamme lähtökohdaksi ryhmän $F$, joka on vapaa joukon $S$ suhteen vapaan ryhmän formaalin määritelmän mukaan, niin proposition 3.13 nojalla joukko $S$ virittää ryhmän $F$. Lisäksi proposition 3.16 nojalla ryhmässä $F$ ei ole epätriviaaleja relaatioita joukon $T$ suhteen. Näin ollen myös formaalista määritelmästä seuraa epäformaali määritelmä: $F$ samastuu $F(S)$:n kanssa, kuten määritelmän 3.10 jälkeen keskustelimme.

## 3.2 Nilsenin–Schreierin lause

Osoitamme ensin lemmat 3.17 – 3.22, minkä jälkeen lemmoja hyödyntäen pääsemme osoittamaan Nilsenin–Schreierin lauseen. Todistamme Nilsenin–Schreierin lauseen vapaille ryhmille, joiden rangi on äärellinen. Todistus kuitenkin laajenee yleiseen tapaukseen Valinta-aksioman nojalla — katso maininta Johnson: *Presentation of Groups* (Cambridge University Press, 1976, 1. painos), sivu 9.

Tässä alaluvussa $F$ on vapaa ryhmä sellaisen joukon $S$ suhteen, jonka mahtavuus on $r$. Merkitään

$$S = \{s_1, \ldots, s_r\},$$
$$T = S \cup S^{-1}.$$

### Ryhmän $F$ alkioiden järjestys

Tässä yhteydessä käytämme merkintää $<$ kuvaamaan alkioiden järjestystä. Järjestetään ensin joukon $T$ alkiot:

$$s_1 < s_2 < \cdots < s_r < s_1^{-1} < s_2^{-1} < \cdots < s_r^{-1}.$$

Ryhmässä $F$ erimittaiset supistetut sanat järjestetään niiden pituuden perusteella: Jos $v$ ja $w$ ovat kaksi erimittaista sanaa ryhmässä $F$, niin

$$v < w, \text{ jos } \ell(v) < \ell(w).$$

Samanmittaiset sanat järjestetään leksikografisesti: Jos

$$v = x_1 \dots x_n \neq y_1 \dots y_n = w,$$

missä $x_i, y_i \in T$ ja $m$ on ensimmäinen indeksi, jolla $x_m \neq y_m$, niin

$$\begin{cases} v < w, \text{ jos } x_m < y_m \\ w < v, \text{ jos } x_m > y_m \end{cases}.$$

Voidaan osoittaa, että vastaava $\leq$ on järjestysrelaatio.

**Lemma 3.17.** *Olkoon ryhmässä $F$ supistettu sana $w$, jonka pituus on vähintään 1. Merkitään $w = x_1 \dots x_n$, missä $x_i \in T$ ja $n \geq 1$. Jos $v$ on sellainen sana ryhmässä $F$, että $v < x_1 \dots x_{n-1}$, niin*

$$v \cdot x_n < w.$$

*Todistus.* Koska $v < x_1 \dots x_{n-1}$, niin joko $\ell(v) < \ell(x_1 \dots x_{n-1})$ tai $\ell(v) = \ell(x_1 \dots x_{n-1})$. Oletetaan ensin, että $\ell(v) < \ell(x_1 \dots x_{n-1}) = n - 1$. Tällöin $\ell(v \cdot x_n) \leq \ell(v) + 1 < n - 1 + 1 = n = \ell(w)$, joten $v \cdot x_n < w$.

Oletetaan nyt, että $\ell(v) = \ell(x_1 \dots x_{n-1})$. Merkitään $v = y_1 \dots y_{n-1}$, missä $y_i \in T$ kaikilla $i$. Koska $v < x_1 \dots x_{n-1}$, niin on olemassa ensimmäinen indeksi $m$, jolla $y_m < x_m$. Jos $y_{n-1} = x_n^{-1}$, niin $\ell(v \cdot x_n) = n - 2 < n = \ell(w)$, jolloin siis $v \cdot x_n < x$. Jos $v \cdot x_n$ ei supistu, niin $\ell(v \cdot x_n) = \ell(w)$. Mutta koska $m$ on viimeinen indeksi, jolla $y_m < x_m$, niin tässäkin tapauksessa $v \cdot x_n < w$.

Väite $v \cdot x_n < w$ pätee siis kaikissa tapauksissa. □

### Schreier-edustajisto

Olkoon $H$ ryhmän $F$ aliryhmä. Jos $x \in F$, niin alkion $x$ määräämä aliryhmän $H$ oikea sivuluokka[1] on osajoukko

$$Hx = \{hx \mid h \in H\}.$$

[1]Huomaa, että Metsänkylän ja Näätäsen tyylistä poiketen käytämme tässä tutkielmassa vasemman sivuluokan sijaan oikeaa sivuluokkaa.

Sivuluokkien ominaisuus on, että kaikilla $x, y \in F$

$$Hx = Hy \text{ tai } Hx \cap Hy = \emptyset.$$

Sivuluokat muodostavat siis ryhmän $F$ osituksen, joten Valinta-aksioman nojalla on olemassa sellainen edustajisto $U$, että jokaiselle $x \in F$ on olemassa yksikäsitteinen alkio $u \in U$, että $x \in Hu$. Siis

$$F = \bigcup_{u \in U} Hu.$$

**Määritelmä 3.18.** Edustajisto $U$ on *Schreier-edustajisto*, jos sillä on ominaisuus:

$$\text{jos } x < y \text{ ja } Hx = Hy, \text{ niin } y \notin U, \tag{3.2.1}$$

missä $x$ ja $y$ ovat sanoja joukon $T$ yli.

Tässä alaluvussa käytämme merkintää $U$ Schreier-edustajistolle.

Koska $He = H \subseteq F$ ja kun ryhmän $F$ alkiot järjestetään, niin $e$ on 0-mittaisena sanana ensimmäinen. Näin ollen neutraalialkio $e$ kuuluu aina Schreier-edustajistoon. Itse asiassa $e$ on ainut aliryhmän $H$ alkio, joka kuuluu Schreier-edustajistoon.

*Esimerkki* 3.19. Olkoon kokonaislukujen additiivinen ryhmä $\mathbb{Z}$ ja sen aliryhmä $5\mathbb{Z}$. Olkoon osajoukko $S = \{1\}$. Joukko $T$ on täten kaksio $\{1, -1\}$ Esimerkissä 3.7 nähtiin, että yksiö $S = \{1\}$ virittää kokonaislukujen ryhmän ja kokonaislukujen ryhmässä ei ole epätriviaaleja relaatioita joukon $T$ suhteen. Näin ollen kokonaislukujen ryhmä on vapaa ryhmä yksiön $S = \{1\}$ suhteen. Lisäksi proposition 3.8 nojalla kokonaisluvuilla on yksikäsitteinen supistettu summaesitys. Näin ollen kokonaisluvut voidaan ajatella sanoiksi joukon $T$ yli.

Joukon $T$ alkioiden järjestys on:

$$1 < -1.$$

Järjestetään tämän jälkeen ryhmän $\mathbb{Z}$ alkiot kuten edellä: 0 on ”tyhjä sana” ja kokonaisluku $n$ on supistettu sana $\underbrace{11\ldots1}_{n \text{ kappaletta}}$, kun $n > 0$, ja $n = \underbrace{-1-1\ldots-1}_{|n| \text{ kappaletta}}$, kun $n < 0$. Koska $1 < -1$, niin $n < -n$. Siis saadaan

$$0 < 1 < -1 < 2 < -2 < 3 < -3 < 4 < -4 < \ldots .$$

Kuten tiedetään, edustajisto ei ole yksikäsitteinen. Nähdään, että

$$\mathbb{Z} = \bigcup_{u \in \{0,1,2,3,4\}} u + 5\mathbb{Z} = \bigcup_{u \in \{5,6,7,8,9\}} u + 5\mathbb{Z} = \bigcup_{u \in \{0,1,-1,2,-2\}} u + 5\mathbb{Z}.$$

Näin ollen esimerkiksi joukot $\{0,1,2,3,4\}, \{5,6,7,8,9\}$ ja $\{0,1,-1,2,-2\}$ ovat edustajistoja kyseisessä tapauksessa. Kuitenkin on olemassa vain yksi edustajisto, joka toteuttaa Schreier-edustajiston ehdon (3.2.1), ja se on kyseisessä tapauksessa joukko $U = \{0,1,-1,2,-2\}$.

Edustajisto on *positiivinen Schreier-edustajisto*, jos sillä on ominaisuus (3.2.1) sillä erotuksella, että $x$ ja $y$ ovatkin sanoja joukon $S$ (eikä joukon $T$) yli. Edellisessä esimerkissä positiivinen Schreier-edustajisto on joukko $U = \{0,1,2,3,4\}$.

**Lemma 3.20.** *Olkoon $n \geq 1$ ja $x_1 \dots x_n$ supistettu $n$-mittainen sana ryhmässä $F$. Tällöin*

$$\textit{jos } x_1 \dots x_n \in U, \textit{ niin } x_1 \dots x_{n-1} \in U.$$

*Todistus.* Osoitetaan väite epäsuorasti: tehdään vastaoletus $x_1 \dots x_{n-1} \notin U$ ja osoitetaan, että siitä seuraa alkuperäisen väitteen negaatio, $x_1 \dots x_n \notin U$.

Joukko $U$ on edustajisto, joten on olemassa sellainen $u \in U$, jolla

$$Hu = Hx_1 \dots x_{n-1}.$$

Oletuksesta $x_1 \dots x_{n-1} \notin U$ ja edustajiston Schreier-ominaisuudesta (3.2.1) seuraa, että $u < x_1 \dots x_{n-1}$. Lemman 3.17 nojalla tällöin $u \cdot x_n < x_1 \dots x_n$. Lisäksi on olemassa sellainen $v \in U$, että $Hv = Hu \cdot x_n$ ja $v \leq u \cdot x_n$. Näin ollen $Hv = Hu \cdot x_n = Hx_1 \dots x_n$ ja $v \leq u \cdot x_n < x_1 \dots x_n$. Järjestysrelaation transitiivisuudesta seuraa, että $v < x_1 \dots x_n$, joten $x_1 \dots x_n \notin U$. Siis alkuperäinen väite on tosi. □

### Aliryhmän $H$ osajoukko $A$

Olkoot $u \in U$ ja $x \in T$. Koska $u \cdot x \in F$ ja $U$ on ryhmän $F$ aliryhmän $H$ edustajisto, niin on olemassa yksikäsitteinen $v \in U$ siten, että $u \cdot x \in Hv$. Alkio $v$ on alkioiden $u$ ja $x$ määräämä, joten merkitään sitä

$$\overline{u \cdot x} \coloneqq v.$$

Koska $u \cdot x = h \cdot v$ jollakin $h \in H$, niin $u \cdot x \cdot \overline{u \cdot x}^{-1} = u \cdot x \cdot v^{-1} = h \in H$ kaikilla $u \in U$ ja $x \in T$. Määritellään $H$:n osajoukko

$$A = \{u \cdot x \cdot \overline{u \cdot x}^{-1} \mid u \in U, x \in T\}. \tag{3.2.2}$$

**Lemma 3.21.** *Joukko $A$ virittää ryhmän $H$.*

*Todistus.* Olkoon $x \in H$. Koska $H$ on vapaan ryhmän $F$ aliryhmä, niin $x$ on supistettu sana, joka voidaan kirjoittaa muodossa

$$x = x_1 \dots x_n,$$

missä $x_i \in T$. Koska neutraalialkio kuuluu aina Schreier-edustajistoon, niin Schreier-edustajiston alkiot $u_1, \dots, u_{n+1} \in U$ voidaan määrittää seuraavalla tavalla induktiivisesti:

$$\begin{cases} u_1 = e \\ u_{i+1} = \overline{u_i \cdot x_i}, \text{ kun } i \geq 1 \end{cases}.$$

Tarkastellaan tuloa

$$a_i = u_i \cdot x_i \cdot u_{i+1}^{-1} = u_i \cdot x_i \cdot \overline{u_i \cdot x_i}^{\,-1},$$

missä $1 \leq i \leq n$. Jokainen $u_i \in U$ ja $x_i \in T$, joten joukon $A$ määritelmän (3.2.2) nojalla jokainen $a_i \in A$. Koska $A$ on $H$:n osajoukko ja $H$ on ryhmä, niin ryhmään $H$ kuuluu alkio

$$a_1 \cdots a_n = u_1 \cdot x_1 \cdot u_2^{-1} \cdot u_2 \cdot x_2 \cdot u_3^{-1} \cdot u_3 \cdots u_n^{-1} \cdot u_n \cdot x_n \cdot u_{n+1}^{-1} = u_1 \cdot x_1 x_2 \dots x_n \cdot u_{n+1}^{-1}.$$

Koska $u_1 = e$ ja $x_1 x_2 \dots x_n = x$, niin saadaan

$$x \cdot u_{n+1}^{-1} = a_1 \cdots a_n \in H.$$

On siis olemassa $h \in H$, jolla $x \cdot u_{n+1}^{-1} = h$. Alkiolla $h$ on olemassa käänteisalkio $H$:ssa, joten saadaan $u_{n+1} = h^{-1} \cdot x$, joka on alkio $H$:ssa, koska $x \in H$. Toisaalta $u_{n+1} \in U$. Näin ollen on oltava $u_{n+1} = e$, sillä neutraalialkio $e$ on ainoa alkio $U$:ssa, jolla $He = H$.

Olemme siis saaneet osoitettua, että mielivaltainen alkio $x$ ryhmässä $H$ voidaan ilmaista joukon $A$ alkioiden $a_i$ tulona

$$x = a_1 \cdots a_n.$$

Tällöin lauseen 2.2 nojalla joukko $A$ virittää ryhmän $H$. □

### Joukon $A$ ominaisuuksia

Tutustutaan tarkemmin joukon $A$ ominaisuuksiin. Tässä alaluvussa merkintä $u \cdot x \in UT \setminus U$ tarkoittaa, että $u \in U$, $x \in T$ ja $u \cdot x \notin U$.

**Lemma 3.22.** *(i) Kaikilla $u \in U$ ja $x \in T$ pätee, että $u \cdot x \cdot \overline{u \cdot x}^{\,-1} = e$, jos ja vain jos $u \cdot x \in U$.*

*(ii)* *Kaikilla $u \in U$ ja $x \in T$ pätee $u = \overline{\overline{u \cdot x} \cdot x^{-1}}$.*

*(iii)* *Olkoot $u \cdot x$ ja $v \cdot y \in UT \setminus U$. Merkitään tuloa $w = x \cdot \overline{u \cdot x}^{-1} \cdot v \cdot y$. Tällöin joko*

- *(a)* *$w = ()$, jolloin $x = y^{-1}, v = \overline{u \cdot x}$ ja $u = \overline{v \cdot y}$, tai*
- *(b)* *$w$ on sellainen vähintään 2-mittainen supistettu sana ryhmässä $F$, joka alkaa $x$:llä ja loppuu $y$:hyn.*

*(iv)* *Alkiot $u \cdot x \cdot \overline{u \cdot x}^{-1}$, missä $u \cdot x \in UT \setminus U$, ovat eri alkioita ja niiden muodostama joukko on $B \cup B^{-1}$, missä*

$$B = \{u \cdot x \cdot \overline{u \cdot x}^{-1} \mid u \in U,\ x \in S\} \setminus \{e\} \text{ ja} \tag{3.2.3}$$
$$B^{-1} = \{w^{-1} \mid w \in B\}. \tag{3.2.4}$$

*Todistus.* (i) Olkoot $u \in U$ ja $x \in T$. Tällöin $u \cdot x \cdot \overline{u \cdot x}^{-1} = e$ on ekvivalentti sen kanssa, että $u \cdot x = \overline{u \cdot x}$. Koska $\overline{u \cdot x} \in U$ kaikilla $u \in U$ ja $x \in T$, niin väite pätee.

(ii) Määritelmän nojalla kaikilla $u \in U$ ja $x \in T$ pätee $Hu \cdot x = H\overline{u \cdot x}$. Tästä seuraa, että

$$Hu = H\overline{u \cdot x} \cdot x^{-1} = H\overline{\overline{u \cdot x} \cdot x^{-1}}.$$

Koska $u \in U$ ja $\overline{\overline{u \cdot x} \cdot x^{-1}} \in U$, niin Schreier-edustajiston määritelmän nojalla on oltava $u = \overline{\overline{u \cdot x} \cdot x^{-1}}$.

(iii) Olkoot $u \cdot x$, $v \cdot y \in UT \setminus U$. Koska $\overline{u \cdot x}$, $v \in F$, niin ne voidaan esittää supistettuina sanoina

$$\overline{u \cdot x} = r_1 \dots r_m \text{ ja } v = t_1 \dots t_n,$$

missä $r_i, t_j \in T$ kaikilla $1 \leq i \leq m$ ja $1 \leq j \leq n$. Tarkastellaan sanaa

$$w = x \cdot \overline{u \cdot x}^{-1} v \cdot y = x(r_1 \dots r_m)^{-1} t_1 \dots t_n y = x r_m^{-1} \dots r_1^{-1} t_1 \dots t_n y$$

yksityiskohtaisesti. Tutkitaan ensin, supistuuko alku:

$$\begin{aligned} x^{-1} = r_m^{-1} &\Rightarrow \overline{u \cdot x} \cdot x^{-1} = r_1 \dots r_{m-1} \\ &\Rightarrow \overline{u \cdot x} \cdot x^{-1} \in U \\ &\Rightarrow u = \overline{\overline{u \cdot x} \cdot x^{-1}} = \overline{u \cdot x} \cdot x^{-1} \\ &\Rightarrow u \cdot x = \overline{u \cdot x} \\ &\Rightarrow u \cdot x \in U, \end{aligned}$$

missä kolmas implikaatio seuraa lemmasta 3.20, neljäs implikaatio kohdasta (ii) ja viimeinen implikaatio kohdasta (i). Lopputulos on ristiriidassa oletuksen $u \cdot x \in UT \setminus U$ kanssa, joten implikaatioketjun etujäsen on epätosi. Näin ollen sanan alku ei supistu, $x^{-1} \neq r_m^{-1}$.

Kun tarkastellaan sanan loppua, niin havaitaan vastaavasti, että oletuksesta $t_n = y^{-1}$ ja lemmasta 3.20 seuraa ristiriita $v \cdot y = t_1 \dots t_{n-1} t_n y = t_1 \dots t_{n-1} \in U$, joten myöskään sanan loppu ei supistu, $t_n \neq y^{-1}$.

Otetaan vielä tarkasteluun sana $\overline{u \cdot x}^{-1} \cdot v = r_m^{-1} \dots r_1^{-1} t_1 \dots t_n$. Ei voida sanoa, supistuuko sana, ja jos supistuu, niin kuinka paljon. Täten merkitään osasanaa, joka supistuu sanasta viimeisenä, $r_i^{-1} t_i$ ja jaetaan tarkastelu neljään eri tapaukseen:

(1) Oletetaan, että $i < m$ ja $i < n$. Tällöin

$$\overline{u \cdot x}^{-1} \cdot v = r_m^{-1} \dots r_{i+1}^{-1} t_{i+1} \dots t_n,$$

joten $w$ on supistettu sana $w = x r_m^{-1} \dots r_{i+1}^{-1} t_{i+1} \dots t_n y$, joten pätee väitteen (b)-tapaus.

(2) Oletetaan, että $i = m < n$. Tällöin

$$\overline{u \cdot x}^{-1} \cdot v = t_{m+1} \dots t_n,$$

joten $w = x t_{m+1} \dots t_n y$ tai $w = t_{m+2} \dots t_n y$. Oletetaan, että sanan alku $x t_{m+1}$ supistuu pois eli että $x^{-1} = t_{m+1}$. Oletuksesta $i = m < n$ seuraa, että $t_1 \dots t_m = r_1 \dots r_m = \overline{u \cdot x}$, jolloin jälleen lemman 3.20 ja kohtien (ii) ja (i) nojalla

$$\begin{aligned} \overline{u \cdot x} \cdot x^{-1} = t_1 \dots t_m t_{m+1} \text{ jolloin } & \overline{u \cdot x} \cdot x^{-1} \in U \\ \text{jolloin } & u = \overline{\overline{u \cdot x} \cdot x^{-1}} = \overline{u \cdot x} \cdot x^{-1} \\ \text{jolloin } & u \cdot x = \overline{u \cdot x} \\ \text{jolloin } & u \cdot x \in U, \end{aligned}$$

mikä on ristiriidassa oletuksen $u \cdot x \in UT \setminus U$ kanssa, joten $x t_{m+1}$ ei supistu. Sana $w$ on siis supistettu sana $w = x t_{m+1} \dots t_n y$, joten pätee väitteen (b)-tapaus.

(3) Oletetaan, että $i = n < m$. Tällöin

$$\overline{u \cdot x}^{-1} \cdot v = r_m^{-1} \dots r_{n+1}^{-1},$$

joten $w = x r_m^{-1} \dots r_{n+1}^{-1} y$ tai $w = x r_m^{-1} \dots r_{n+2}^{-1}$. Vastaavalla tavalla kuten edellä oletetaan, että sanan loppu $r_{n+1}^{-1} y$ supistuu pois eli

että $y = r_{n+1}$. Oletuksesta $i = n < m$ seuraa, että $r_1 \dots r_n = t_1 \dots t_n = v$. Näin ollen lemman 3.20 nojalla

$$v \cdot y = r_1 \dots r_n r_{n+1} \in U,$$

sillä $r_1 \dots r_n = \overline{u \cdot x} \in U$. Tämä on kuitenkin ristiriidassa oletuksen $v \cdot y \in UT \setminus U$ kanssa, joten $w = x r_m^{-1} \dots r_{n+1}^{-1} y$. Näin ollen pätee väitteen (b)-tapaus.

(4) Oletetaan, että $i = m = n$. Tällöin

$$\overline{u \cdot x}^{\,-1} \cdot v = e$$

ja $w = xy$ tai $w = e$. Ensimmäisessä tapauksessa pätee väitteen (b)-kohta. Jälkimmäisestä seuraa, että $x = y^{-1}$ ja $v = \overline{u \cdot x}$, jolloin kohdan (ii) nojalla lisäksi $\overline{v \cdot y} = \overline{\overline{u \cdot x} \cdot x^{-1}} = u$. Näin ollen pätee väitteen (a)-tapaus.

Edelliset kohdat osoittavat, että väitteen (b)-tapaus pätee kaikissa tapauksissa paitsi viimeisessä, joka johtaa väitteen (a)-tapaukseen, kun $x = y^{-1}$. Alkuperäinen väite on siis tosi.

(iv) Olkoon $u \cdot x \cdot \overline{u \cdot x}^{\,-1} = v \cdot y \cdot \overline{v \cdot y}^{\,-1}$, missä $u \cdot x$ ja $v \cdot y \in UT \setminus U$. Lisäämällä yhtälöön oikealta puolelta $u^{-1}$ ja vasemmalta puolelta $\overline{v \cdot y} \cdot y^{-1}$ saadaan

$$x \cdot \overline{u \cdot x}^{\,-1} \cdot \overline{v \cdot y} \cdot y^{-1} = u^{-1} \cdot v \cdot y \cdot \overline{v \cdot y}^{\,-1} \cdot \overline{v \cdot y} \cdot y^{-1} = u^{-1} \cdot v.$$

Tutkitaan kohdan (iii) avulla sanaa $x \cdot \overline{u \cdot x}^{\,-1} \cdot \overline{v \cdot y} \cdot y^{-1}$: Kohdan (i) nojalla $v \cdot y \cdot \overline{v \cdot y} \neq e$, joten $v \neq \overline{v \cdot y} \cdot y^{-1}$. Toisaalta kohdasta (ii) seuraa, että $\overline{\overline{v \cdot y} \cdot y^{-1}} = v \neq \overline{v \cdot y} \cdot y^{-1}$, joten $\overline{v \cdot y} \cdot y^{-1} \notin U$. Näin ollen $\overline{v \cdot y} \cdot y^{-1} \in UT \setminus U$, jolloin kohdasta (iii) seuraa, että joko

a) $u^{-1} \cdot v = x \cdot \overline{u \cdot x}^{\,-1} \cdot \overline{v \cdot y} \cdot y^{-1} = e$, jolloin $x = (y^{-1})^{-1} = y$ ja $u = v$, tai

b) $u^{-1} \cdot v = x \cdot \overline{u \cdot x}^{\,-1} \cdot \overline{v \cdot y} \cdot y^{-1} = x \cdots y^{-1}$. Tässä tapauksessa $v \cdot y \cdots x^{-1} = u \in U$, joten lemman 3.20 nojalla $u \cdot x = v \cdot y \cdots \in U$, mikä on ristiriidassa oletuksen kanssa.

Siispä jos $u \cdot x \cdot \overline{u \cdot x}^{-1} = v \cdot y \cdot \overline{v \cdot y}^{-1}$, niin välttämättä $u = v$ ja $x = y$. Alkiot $u \cdot x \cdot \overline{u \cdot x}^{-1}$, missä $u \cdot x \in UT \setminus U$, ovat eri.

Merkitään

$$B_1 = \{u \cdot x \cdot \overline{u \cdot x}^{\,-1} \mid u \in U,\ x \in S^{-1}\} \setminus \{e\}.$$

Osoitetaan, että $B_1 = B^{-1}$. Olkoon $u \cdot x \in US \setminus U$. Tällöin joukon $B^{-1}$ mielivaltaiselle alkiolle pätee

$$(u \cdot x \cdot \overline{u \cdot x}^{-1})^{-1} = \overline{u \cdot x} \cdot x^{-1} \cdot u^{-1} = \overline{u \cdot x} \cdot x^{-1} \cdot \overline{\overline{u \cdot x} \cdot x^{-1}}^{-1}, \quad (3.2.5)$$

missä toinen yhtäsuuruus seuraa kohdasta (ii). Oletuksesta $u \cdot x \notin U$ sekä kohdista (i) ja (ii) seuraa, että

$$u \cdot x \cdot \overline{u \cdot x}^{-1} \neq e \text{ eli } \overline{u \cdot x} x^{-1} \neq u = \overline{\overline{u \cdot x} \cdot x^{-1}}$$
$$\text{eli } \overline{u \cdot x} x^{-1} \overline{\overline{u \cdot x} \cdot x^{-1}}^{-1} \neq e.$$

Koska lisäksi $\overline{u \cdot x} \in U$ ja $x^{-1} \in S^{-1}$, niin $\overline{u \cdot x} \cdot x^{-1} \cdot \overline{\overline{u \cdot x} \cdot x^{-1}}^{-1} \in B_1$.

Näin ollen yhtälöstä (3.2.5) nähdään, että $B^{-1} \subseteq B_1$ ja $B_1 \subseteq B^{-1}$, joten $B_1 = B^{-1}$. Kun $u \cdot x \in UT \setminus U$, niin alkioiden $u \cdot x \cdot \overline{u \cdot x}^{-1}$ muodostama joukko on joukko $B \cup B^{-1}$.

□

**Nilsenin–Schreierin lause**

Nilsenin–Schreierin lauseen todistuksessa hyödynnämme edellä todistettuja lemmoja ja käytämme samoja merkintöjä. Ryhmä $F$ on vapaa joukon $S$ suhteen ja sen rangi on $r$ eli $r(F) = r$. Joukoilla $A$ ja $B$ tarkoitamme edellä määriteltyjä joukkoja

$$A = \{u \cdot x \cdot \overline{u \cdot x}^{-1} \mid u \in U, x \in T\},$$
$$B = \{u \cdot x \cdot \overline{u \cdot x}^{-1} \mid u \in U, x \in S\} \setminus \{e\},$$
$$B^{-1} = \{u \cdot x \cdot \overline{u \cdot x}^{-1} \mid u \in U, x \in S^{-1}\} \setminus \{e\}.$$

Muistetaan lisäksi, että kahdelle permutaatiolle $\alpha$ ja $\beta$ pätee

$$\alpha \cdot \beta = \beta\alpha.$$

**Lause 3.23.** *(Nilsenin–Schreierin lause) Olkoon $F$ vapaa ryhmä ja $H$ sen jokin aliryhmä. Tällöin myös $H$ on vapaa. Lisäksi, jos vapaan ryhmän $F$ rangi on $r$ ja $[F : H] = g$ on äärellinen, niin $H$:n rangi on $(r-1)g + 1$.*

*Todistus.* Osoitetaan ensin, että $H$ on vapaa joukon $B$ suhteen. Lemman 3.21 nojalla $A$ virittää ryhmän $H$. Lauseen 2.2 mukaan ryhmän $H$ alkiot voidaan siis esittää joukon $A$ alkioiden ja käänteisalkioiden tulona. Koska $T = S \cup S^{-1}$ ja $e \in A$, niin $A = B \cup B^{-1} \cup \{e\}$. Täten myös joukko $B$ virittää $H$:n.

Olkoon $b \in H$ ja $b_1 \cdots b_n$ sen supistettu tuloesitys, missä $n \geq 2$ ja jokainen $b_i \in B \cup B^{-1}$, missä joukot $B$ ja $B^{-1}$ ovat erilliset lemman 3.22 kohdan (iv)

nojalla. Koska $b_1 \cdots b_n$ on supistettu tuloesitys, niin $b_i \cdot b_{i+1} \neq e$ ja $b_i \neq e$ kaikilla $i$. Lemman 3.22 kohdan (i) nojalla $u_i \cdot x_i \cdot \overline{u_i \cdot x_i}^{-1} = e$, jos ja vain jos $u_i \cdot x_i \in U$. Voidaan siis merkitä

$$b_i = u_i \cdot x_i \cdot \overline{u_i \cdot x_i}^{-1},$$

missä $u_i \cdot x_i \in UT \setminus U$. Tarkastellaan tuloa

$$b_i \cdot b_{i+1} = (u_i \cdot x_i \cdot \overline{u_i \cdot x_i}^{-1}) \cdot (u_{i+1} \cdot x_{i+1} \cdot \overline{u_{i+1} \cdot x_{i+1}}^{-1})$$

jollakin $1 \leq i < n-1$. Lemman 3.22 kohdan (iii) nojalla tulo $x_i \cdot \overline{u_i \cdot x_i}^{-1} u_{i+1} x_{i+1}$ on joko tyhjä sana () ja pätee $u_i = \overline{u_{i+1} x_{i+1}}$ tai vähintään 2-mittainen supistettu sana $x_i \dots x_{i+1}$ ryhmässä $F$. Ensimmäisessä tapauksessa

$$\begin{aligned} b_i \cdot b_{i+1} &= (u_i \cdot x_i \cdot \overline{u_i \cdot x_i}^{-1}) \cdot (u_{i+1} \cdot x_{i+1} \cdot \overline{u_{i+1} \cdot x_{i+1}}^{-1}) \\ &= u_i \cdot (x_i \cdot \overline{u_i \cdot x_i}^{-1} \cdot u_{i+1} \cdot x_{i+1}) \cdot \overline{u_{i+1} \cdot x_{i+1}}^{-1} \\ &= u_i \cdot e \cdot \overline{u_{i+1} \cdot x_{i+1}}^{-1} \\ &= u_i \cdot \overline{u_{i+1} \cdot x_{i+1}}^{-1} \\ &= (\overline{u_{i+1} \cdot x_{i+1}}) \cdot (\overline{u_{i+1} \cdot x_{i+1}})^{-1} = e, \end{aligned}$$

mikä on ristiriita, sillä $b_1 \cdots b_n$ on supistettu tuloesitys, joten $b_i \cdot b_{i+1} \neq e$. Tällöin tulo $x_i \cdot \overline{u_i \cdot x_i}^{-1} \cdot u_{i+1} \cdot x_{i+1}$ on vähintään 2-mittainen supistettu sana $x_i \dots x_{i+1}$ ryhmässä $F$. Näin ollen

$$\begin{aligned} b_1 \cdots b_n &= (u_1 \cdot x_1 \cdot \overline{u_1 \cdot x_1}^{-1}) \cdot (u_2 \cdot x_2 \cdot \overline{u_2 \cdot x_2}^{-1}) \cdots (u_n \cdot x_n \cdot \overline{u_n \cdot x_n}^{-1}) \\ &= u_1 \cdot (x_1 \cdot \overline{u_1 \cdot x_1}^{-1} \cdot u_2 \cdot x_2) \cdot \overline{u_2 \cdot x_2}^{-1} \cdots u_n \cdot x_n \cdot \overline{u_n \cdot x_n}^{-1} \\ &= u_1 \cdot x_1 \dots x_2 \cdot \overline{u_2 \cdot x_2}^{-1} \cdots u_n \cdot x_n \cdot \overline{u_n \cdot x_n}^{-1} \\ &= u_1 \cdot x_1 \dots (x_2 \cdot \overline{u_2 \cdot x_2}^{-1} u_3 \cdot x_3) \cdot \overline{u_3 \cdot x_3}^{-1} \cdots u_n \cdot x_n \cdot \overline{u_n \cdot x_n}^{-1} \\ &= u_1 \cdot x_1 \dots x_2 \dots x_3 \cdot \overline{u_3 \cdot x_3}^{-1} \cdots u_n \cdot x_n \cdot \overline{u_n \cdot x_n}^{-1} \\ &\quad \vdots \\ &= \cdots x_1 \dots x_2 \dots \ \dots \ \dots x_n \cdots, \end{aligned}$$

joten $b_1 \cdots b_n$ on vähintään $n$-mittainen sana ryhmässä $H$. Näin ollen $b_1 \cdots b_n \neq e$. Joukon $B$ alkioiden välillä ei siis ole epätriviaaleja relaatioita ryhmässä $H$. Ryhmä $H$ on siis vapaa joukon $B$ suhteen.

Osoitetaan lauseen loppuosa ensin siinä tapauksessa, että $H$ on ryhmän $F$ normaali aliryhmä $N$. Olkoon $N$:llä äärellinen määrä $k$ sivuluokkia ryhmässä $F$ eli $[F : N]$. Näytetään, että normaalille aliryhmälle on mahdollista löytää positiivinen Schreier-edustajisto, siis edustajisto $U$, jonka jokainen alkio on supistettu sana $x_1 \dots x_n$ joukon $S$ (eikä joukon $T = S \cup S^{-1}$) yli.

Äärellisessä ryhmässä $F/N$, jonka mahtavuus on siis $k$, pätee Lagrangen teoreeman nojalla $(Nx)^k = N$ kaikilla $x \in F$: Alkion $Nx$ kertaluku $\mathrm{ord}(Nx) = n$ jakaa ryhmän $F/N$ mahtavuuden $k$. Näin ollen $k = qn$ jollakin kokonaisluvulla $q$. Tällöin $(Nx)^k = (Nx)^{qn} = ((Nx)^n)^q = N^q = N$ kaikilla $x \in F$. Tästä seuraa, että $x^k \in N$ kaikilla $x \in F$.

Olkoon $x_1 \dots x_n$ mikä tahansa supistettu sana joukon $T$ yli. Tällöin kaikilla $i$, joilla $x_i^{-1} \in S$, pätee

$$\begin{aligned} Nx_1 \dots x_n &= x_1 \dots x_{i-1}(Nx_i)x_{i+1} \dots x_n \\ &= x_1 \dots x_{i-1}(Nx_i^{-k}x_i)x_{i+1} \dots x_n \\ &= Nx_1 \dots x_{i-1}x_i^{-k+1}x_{i+1} \dots x_n, \end{aligned}$$

missä ensimmäinen ja viimeinen yhtäsuuruus pätevät, sillä $N$ on normaali aliryhmä, ja toinen yhtäsuuruus pätee, sillä $x_i^{-k} = (x_i^{-1})^k \in N$. Kirjoittamalla $x_i^{-k+1} = (x_i^{-1})^{k-1}$ nähdään, että se on supistettu sana joukon $S$ yli. Käymällä läpi jokainen $i$, jolla $x_i^{-1} \in S$, saadaan, että

$$Nx_1 \dots x_n = Nw,$$

missä $w$ on supistettu sana joukon $S$ yli. Merkitään saatua positiivista edustajistoa $U$:lla. Huomataan, että joukon $U$ mahtavuus on $k$, sillä $[F : N] = k$.

Tarkastellaan joukon $B$ alkioita, jotka ovat siis muotoa $u \cdot x \cdot \overline{u \cdot x}^{-1}$, missä $u \in U$ ja $x \in S$. Koska joukon $U$ mahtavuus on $k$ ja kun joukon $S$ mahtavuus on $r$, niin alkioita $u \cdot x$, missä $u \in U$ ja $x \in S$, on olemassa kaiken kaikkiaan $kr$ kappaletta. Lemman 3.22 (iv) nojalla jokainen $u \cdot x \cdot \overline{u \cdot x}^{-1} \neq e$ on eri, joten näytetään, että täsmälleen $k - 1$ kappaletta alkioista on $e$. Lemman 3.22 (i) nojalla riittää osoittaa, että $k - 1$ kappaletta alkioista $u \cdot x$, missä $u \in U$ ja $x \in S$, kuuluu edustajistoon $U$ eli että joukon $US \cap U$ mahtavuus on $k - 1$.

Olkoon $v = x_1 \dots x_n \in U \setminus \{e\}$, missä $n \geq 1$, sana joukon $S$ yli. Koska $U \setminus \{e\} \subset F$, niin lemman 3.20 nojalla tästä seuraa, että myös $x_1 \dots x_{n-1} \in U$. Näin ollen voidaan merkitä $v = u \cdot x_n$, missä $u \in U$ ja $x_n \in S$, joten $v \in US$ ja $v \in U$. Saadaan siis $U \setminus \{e\} \subseteq US \cap U$.

Olkoon nyt $u \cdot x \in US \cap U$. Halutaan osoittaa, että $u \cdot x \neq e$. Tehdään vastaoletus: $u \cdot x = e$ eli $x^{-1} = u \in U$. Tämä on kuitenkin ristiriita, sillä $U$ on positiivinen Schreier-edustajisto ja $x^{-1} \in S^{-1}$. Siis myös $US \cap U \subseteq U \setminus \{e\}$, jolloin $US \cap U = U \setminus \{e\}$. Koska neutraalialkio kuuluu aina Schreier-edustajistoon, niin joukon $U \setminus \{e\}$ mahtavuus on $k - 1$.

Yhdistämällä edelliset tulokset saadaan, että joukon $B$ mahtavuus on kaiken kaikkiaan $kr - (k - 1) = (r - 1)k + 1$. Näin ollen on osoitettu, että ryhmän $F$ normaalin aliryhmän $N$ rangille pätee

$$r(N) = (r - 1)k + 1, \tag{3.2.6}$$

missä $r = r(F)$ ja $k = [F : N]$.

Olkoon $H$ nyt ryhmän $F$ mielivaltainen aliryhmä, jonka indeksi ryhmässä $F$ on $g$ ($< \infty$). Merkitään $H$:n oikeiden sivuluokkien joukkoa $C = \{H, Hv_1, Hv_2, \ldots, Hv_{g-1}\}$, missä $v_i \in F$ kaikilla $i$ ja $v_0 = e$. Määritellään jokaiselle $w \in F$ kuvaus

$$\begin{aligned} \tau_w : C &\to C, \\ Hv &\mapsto Hv \cdot w. \end{aligned}$$

Jokainen $\tau_w$ kuvaa siis sivuluokat toisikseen. Jos $Hv_i \cdot w \neq Hv_j \cdot w$ joillakin $i \neq j$, niin oltava $Hv_i \neq Hv_j$. Kaksi eri sivuluokkaa kuvautuu siis aina eri sivuluokiksi. Koska joukon $C$ mahtavuus on $g$, niin kukin $\tau_w$ vastaa yhtä symmetriaryhmän $S_g$ permutaatiota. Saadaan kuvaus

$$\begin{aligned} \tau : F &\to S_g, \\ w &\mapsto \tau_w, \end{aligned}$$

joka toteuttaa homomorfiaehdon: Olkoon $w_1, w_2 \in F$ ja $Hv \in C$. Tällöin

$$\begin{aligned} \tau_{w_1 \cdot w_2}(Hv) &= Hv \cdot (w_1 \cdot w_2) = Hv \cdot w_1 \cdot w_2 \\ &= (Hv \cdot w_1) \cdot w_2 = \tau_{w_2}(Hv \cdot w_1) \\ &= \tau_{w_2}(\tau_{w_1}(Hv)) = (\tau_{w_2} \circ \tau_{w_1})(Hv) \\ &= (\tau_{w_1} \cdot \tau_{w_2})(Hv). \end{aligned}$$

Huomataan, että ydin $\ker \tau$ sisältyy ryhmään $H$: Olkoon $a \in \ker \tau$. Tällöin

$$\tau_a = \tau(a) = \mathrm{id},$$

sillä identiteettikuvaus id on symmetriaryhmän $S_g$ neutraalialkio. Tästä saadaan, että

$$H = \tau_a(H) = Ha,$$

joten on oltava $a \in H$. Näin ollen $\ker \tau \subseteq H$.

Koska ydin $\ker \tau$ sisältyy ryhmään $H$ ja se on ryhmän $F$ normaali aliryhmä, niin $\ker \tau$ on myös ryhmän $H$ normaali aliryhmä. Merkitään $\ker \tau = N$. Koska $[F : H]$ on äärellinen, niin myös $[H : N]$ on äärellinen – oikeastaan $N$:n indeksi $H$:ssa on enintään $g!$:

Huomataan ensin, että

$$n \in N \;\Leftrightarrow\; \tau(n) = \mathrm{id} \;\Leftrightarrow\; \forall\, i \in \{0, \ldots, g-1\} : Hv_i \cdot n = Hv_i.$$

Koska alkion $v_i$ ei tarvitse kuulua mihinkään tiettyyn edustajistoon, niin oikeastaan: $n \in N$, jos ja vain jos $Hv \cdot n = Hv$ kaikilla $v \in F$. Tutkitaan

tämän nojalla, milloin kaksi aliryhmän $N$ sivuluokkaa ovat samat ryhmässä $H$. Olkoot $h, k \in H$.

$$\begin{aligned} Nh = Nk &\Leftrightarrow h \cdot k^{-1} \in N \Leftrightarrow \forall\, v \in F : Hv \cdot h \cdot k^{-1} = Hv \\ &\Leftrightarrow \forall\, v \in F : Hv \cdot h = Hv \cdot k \\ &\Leftrightarrow \tau_h = \tau_k. \end{aligned}$$

Koska symmetriaryhmässä $S_g$ on kaiken kaikkiaan $g!$ kappaletta eri permutaatioita, niin aliryhmällä $N$ on enintään $g!$ sivuluokkaa ryhmässä $H$. Siis $[H : N] \leq g!$.

Voidaan siis merkitä $[H : N] = h$ $(< \infty)$. Tällöin $[F : N] = [F : H]\,[H : N] = gh$, jolloin yhtälön (3.2.6) nojalla saadaan kaksi yhtälöä:

$$\begin{array}{rcl} N \lhd F,\ [F : N] = gh & \text{joten} & r(N) = (r-1)gh + 1; \\ N \lhd H,\ [H : N] = h & \text{joten} & r(N) = (r(H)-1)h + 1. \end{array}$$

Yhdistämällä nämä saadaan

$$(r-1)gh + 1 = (r(H)-1)h + 1,$$

josta ratkaisemalla saadaan haluttu tulos $r(H) = (r-1)g + 1$. □

# 4 Ryhmän esitys

Tässä luvussa näytämme, miten ryhmä voidaan esittää kompaktisti virittäjien ja relaatioiden avulla. Alaluvussa 4.3 käsittelemme erityisesti Abelin ryhmiä ja alaluvussa 4.4 näytämme, miten ryhmälle voi annetun esityksen lisäksi muodostaa myös muita esityksiä niin kutsuttujen Tietze-muunnosten avulla.

Edellisessä luvussa, kun sanan käsite oli vielä uusi, halusimme tehdä eron sanan ja tulon välille. Sanan ja tuloesityksen välisen yhteyden tarkastelun jälkeen emme enää tässä luvussa tee eroa sanan ja tulon välille.

## 4.1 Määritelmä

Lähdemme liikkeelle ryhmän esityksen tarkasta, mutta epäintuitiivisesta määritelmästä. Tämän jälkeen teemme määritelmän sisällöstä enemmän käyttökelpoisen.

**Määritelmä 4.1.** Olkoon $S$ joukko ja $F$ vapaa ryhmä sen suhteen. Olkoon ryhmän $F$ osajoukko $R$, joka koostuu joistakin supistetuista sanoista $w$ joukon $T = S \cup S^{-1}$ yli. Muodostetaan joukon $R$ normaali sulkeuma $\overline{R}$ ryhmässä $F$, jolloin on olemassa tekijäryhmä $F/\overline{R}$. Merkitään tätä tekijäryhmää $G$. Tällöin voidaan merkitä

$$G = \langle S|R\rangle,$$

missä yhtälön oikea puoli on ryhmän $G$ *esitys*. Joukkoa $S$ kutsutaan ryhmän $G$ *virittäjäjoukoksi* ja joukkoa $R$ *relaattorijoukoksi*.

Ryhmä $G$ koostuu siis sivuluokista $\overline{R}w$ ja sen laskutoimitus seuraa vapaan ryhmän $F$ laskutoimituksesta eli supistettujen sanojen yhdistämisestä:

$$\overline{R}w_1\overline{R}w_n = \overline{R}w_1w_2,$$

missä $w_1$ ja $w_2$ ovat supistettuja sanoja.

Määritellään relaatio

$$w_1 \sim w_2 \Leftrightarrow \overline{R}w_1 = \overline{R}w_2. \tag{4.1.1}$$

Relaatio $\sim$ on ekvivalenssi, mikä seuraa siitä, että sivuluokkien samuus on tunnetusti refleksiivinen, symmetrinen ja transitiivinen relaatio. Jokaiselle ryhmän $F$ sanalle $w$ on näin ollen olemassa ekvivalenssiluokka $[w]$, joka koostuu kaikista supistetuista sanoista $w_i$, jotka ovat relaatiossa $\sim$ sanan $w$ kanssa. Ekvivalenssirelaatio $\sim$ määrää siis ryhmän $F$ osituksen, jossa kaikki sanat $w_i$, jotka kuuluvat samaan sivuluokkaan $\overline{R}w$, on niputettu yhteen. Tutkitaan

seuraavaksi, minkälaisia sanoja kuuluu ekvivalenssiluokkaan $[w_1w_2]$, missä $w_1, w_2 \in F$. Kirjoitetaan ensin relaatio 4.1.1 muodossa

$$[w_1] = [w_2] \Leftrightarrow w_1 \in \overline{R}w_2.$$

Koska normaali sulkeuma $\overline{R}$ on ryhmä, joka sisältää joukon $R$, niin se sisältää myös kaikki käänteisalkiot $r^{-1}$, missä $r \in R$ ja kaikki tulot $r_1 \dots r_n$, missä $r_i \in R \cup R^{-1}$. Muistetaan, että normaalin sulkeuman määritelmän nojalla lisäksi kaikki alkiot

$$wrw^{-1},$$

missä $w \in F$ ja $r \in R$, sekä niiden käänteisalkiot ja tulot sisältyvät normaaliin sulkeumaan $\overline{R}$.

(i) Olkoot $w_1, w_2 \in F$ ja $r \in R$. Tällöin

$$w_1rw_2 = w_1rw_1^{-1}w_1w_2 \in \overline{R}w_1w_2,$$

sillä $w_1rw_1^{-1} \in \overline{R}$. Näin ollen $[w_1rw_2] = [w_1w_2]$ kaikilla $r \in R$.

(ii) Olkoot $w_1, w_2 \in F$ ja $r \in R^{-1}$. Tällöin

$$w_1rw_2 = w_1rw_1^{-1}w_1w_2 = (w_1r^{-1}w_1^{-1})^{-1}w_1w_2 \in \overline{R}w_1w_2,$$

sillä $r^{-1} \in R$ ja $(w_1r^{-1}w_1^{-1})^{-1} \in \overline{R}$. Näin ollen $[w_1rw_2] = [w_1w_2]$ kaikilla $r \in R^{-1}$.

(iii) Olkoot $w_1, w_2 \in F$ ja $r_1, r_2 \in R$. Tällöin

$$w_1r_1r_2w_2 = w_1r_1w_1^{-1}w_1r_2w_1^{-1}w_1w_2 \in \overline{R}w_1w_2,$$

sillä $w_1r_1w_1^{-1}w_1r_2w_1^{-1} \in \overline{R}$. Näin ollen $[w_1r_1r_2w_2] = [w_1w_2]$ kaikilla $r_1, r_2 \in R$.

(iv) Olkoot $w_1, w_2 \in F$ ja $wrw^{-1} \in \overline{R}$. Tällöin

$$w_1wrw^{-1}w_2 = w_1wrw^{-1}w_1^{-1}w_1w_2 = w_1wr(w_1w)^{-1}w_1w_2 \in \overline{R}w_1w_2,$$

sillä $w_1wr(w_1w)^{-1} \in \overline{R}$. Näin ollen $[w_1wrw^{-1}w_2] = [w_1w_2]$ kaikilla $wrw^{-1} \in \overline{R}$.

Jatkamalla tarkastelua edellä esitettyyn tapaan voidaan todeta, että

$$[w_1w_rw_2] = [w_1w_2] \text{ kaikilla } w_r \in \overline{R}.$$

Merkitään jatkossa

$$w := [w] = \overline{R}w.$$

Näin ollen tekijäryhmäkonstruktion lisäksi ryhmän $G$ alla oleva joukko voidaan johtaa myös toisella tavalla:

Jokaisen supistetun sanan $w$ ekvivalenssiluokasta löytyy supistettu sana, josta on "typistetty" pois kaikki osasanat $w_r$, jotka kuuluvat normaaliin sulkeumaan $\overline{R}$. Valitsemalla ekvivalenssiluokan edustajaksi aina tällainen typistetty sana voidaan ajatella, että ryhmä $G$ koostuu kaikista supistetuista ja typistetyistä sanoista. Edellisen luvun teorian valossa voidaan myös sanoa, että normaalin sulkeuman $\overline{R}$ sanoja $w_r$ vastaavat tulot antavat epätriviaaleja relaatioita ryhmässä $G$ joukon $T$ suhteen.

Tarkastellaan vielä ryhmän esitystä $\langle S|R\rangle$.

**Määritelmä 4.2.** Sanotaan, että ryhmä $G$ on *äärellisesti esitetty*, jos sen jonkin esityksen virittäjäjoukon $S$ ja relaattorijoukon $R$ mahtavuudet ovat äärelliset.

Käsittelemme esimerkeissämme vain äärellisesti esitettyjä ryhmiä. Jos $S = \{a_1, \ldots, a_k\}$ ja $R = \{w_1, \ldots, w_m\}$, niin ryhmän esitys voidaan kirjoittaa

$$G = \langle a_1, \ldots, a_k \mid w_1, \ldots, w_m\rangle.$$

Alkioita $a_i$ kutsutaan *virittäjiksi* ja sanoja $w_i$ *relaattoreiksi*.

Jos virittäjä- ja relaattorijoukot ovat äärellisiä, niin ryhmän esitys voidaan kirjoittaa myös

$$G = \langle a_1, \ldots, a_k \mid w_1 = \cdots = w_m = e\rangle, \tag{4.1.2}$$

jolloin yhtälöitä $w_i = e$ kutsutaan *relaatioiksi*.

**Lause 4.3.** *Jokaisella ryhmällä on esitys ja jokainen äärellinen ryhmä on äärellisesti esitetty.*

*Todistus.* Olkoon $G$ mikä tahansa ryhmä, $\widetilde{G}$ ryhmän $G$ alla oleva joukko ja $F$ vapaa ryhmä joukon $\widetilde{G}$ suhteen. Identiteettikuvaus $\mathrm{id} : \widetilde{G} \to G$ laajenee vapaan ryhmän määritelmän nojalla homomorfismiksi $\theta : F \to G$. Tällöin ryhmä $G$ on isomorfinen ryhmän $F/\ker\theta$ kanssa ja sillä on esitys

$$\langle \widetilde{G} | \ker\theta\rangle.$$

Koska $F$ on vapaa ryhmä ja $\ker\theta$ on ryhmän $F$ aliryhmä, niin ryhmä $\ker\theta$ on myös Nilsenin–Schreierin lauseen (lause 3.23) nojalla vapaa. Olkoon

$R$ sellainen joukko, että $\ker\theta$ on vapaa sen suhteen. Näin ollen äärellisellä ryhmällä $G$ on esitys

$$\langle \widetilde{G} | R \rangle,$$

missä virittäjä- ja relaattorijoukot ovat äärelliset. Nilsenin–Schreierin lauseen nojalla saadaan laskettua niiden kertaluvut: jos $\#G = g$, niin $\#\widetilde{G} = g$ ja $\#R = r(\ker\theta) = (g-1)g + 1 = g^2 - g + 1$. □

Edellisessä lauseessa johdimme mielivaltaiselle ryhmälle erään esityksen. Ryhmän esitys ei kuitenkaan ole yksikäsitteinen, kuten myöhemmin nähdään. Yleensä halutaan, että ryhmän esitys on mahdollisimman lyhyt. Emme siis käsittele tässä tutkielmassa tapauksia, joissa virittäjäjoukolla $S$ ja relaattorijoukolla $R$ on yhteisiä alkioita. Mikäli $S \cap R \neq \emptyset$, niin alaluvun 4.4 teorian nojalla ryhmälle $G = \langle S|R\rangle$ saadaan toinen esitys $\langle S'|R'\rangle$, missä $S' \cap R' = \emptyset$.

## 4.2 Eräiden ryhmien esityksiä

*Esimerkki* 4.4. Olkoon ryhmä $F$ vapaa joukon $S$ suhteen. Koska jokaisella ryhmällä on esitys, niin ryhmällä $F$ on esitys

$$F = \langle S \mid \emptyset \rangle,$$

sillä ryhmässä $F$ ei ole epätriviaaleja relaatioita joukon $T = S \cup S^{-1}$ suhteen.

*Esimerkki* 4.5. Jos ryhmän $G$ relaattorijoukko $R$ on epätyhjä, niin ryhmän $G$ alkioilla ei ole yksikäsitteistä esitystä. Olkoon ryhmä

$$G = \langle a, b \mid aba^{-1}b^{-1},\ a^2b^{-3} \rangle.$$

Näin ollen ryhmässä $G$ on epätriviaalit relaatiot $aba^{-1}b^{-1} = e$ (tämä relaatio itse asiassa tekee ryhmän vaihdannaiseksi) ja $a^2b^{-3} = e$, jolloin esimerkiksi

$$ab^{-1} = ab^{-1}e = ab^{-1}a^2b^{-3} = a^3b^{-4}.$$

Huomataan, että olemme saaneet vastaavanlaisen relaation aiemmin esimerkissä 3.7, kun käsittelimme ryhmää $(\mathbb{Z}, +)$ virittäjäjoukon $\{2, 3\}$ suhteen. Silloin

$$3 - 2 = 3 + 3 + 3 - 2 - 2 - 2 - 2.$$

*Esimerkki* 4.6. Olkoon joukko $S = \{a, b\}$, missä on tasan kaksi eri alkiota. Tarkastellaan lisää edellisen esimerkin ryhmää ja verrataan sitä joukon $S$ virittämään vapaaseen ryhmään. Olkoot

$$F = \langle a, b \mid \emptyset \rangle \quad \text{ja} \quad G = \langle a, b \mid aba^{-1}b^{-1},\ a^2b^{-3} \rangle.$$

Ryhmässä $F$ sana $ab^{-1}a^2b^{-2}a^{-1}$ on supistettu, sillä alkiota ei seuraa sen käänteisalkio. Ryhmässä $G$ sana kuitenkin typistyy ja supistuu, sillä ryhmässä $G$ on relaattori $a^2b^{-3}$:

$$ab^{-1}a^2b^{-2}a^{-1} = ab^{-1}(a^2b^{-3})ba^{-1} = ab^{-1}ba^{-1} = e.$$

Toisaalta toteamalla, että

$$ab^{-1}a^2b^{-2}a^{-1} = (ba^{-1})^{-1}(a^2b^{-3})(ba^{-1}) \in \overline{R}$$

voidaan sana typistää pois suoraan.

*Esimerkki* 4.7. Olkoon ryhmä

$$\langle a, b \mid a^4, b^2, (ab)^2 \rangle. \tag{4.2.1}$$

Koska virittäjän $a$ kertaluku on 4, niin sillä on neljä erisuurta potenssia, $e, a, a^2$ ja $a^3$. Vastaavalla tavalla virittäjällä $b$ on kaksi erisuurta potenssia $e$ ja $b$ (missä molemmat $e$ ovat ryhmän neutraalialkiona samat). Lisäksi ryhmän määräävien relaatioiden nojalla

$$abab = e \text{ eli } aba = b \text{ eli } ba = a^3b.$$

Näiden avulla huomataan, että ryhmään (4.2.1) kuuluu täsmälleen 8 alkiota $e, a, a^2, a^3, b, ab, a^2b, a^3b$ ja voidaan perustella ryhmän kertotaulu, joka on esitetty taulukossa 2.

| | $e$ | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $e$ | $ab$ | $a^2b$ | $a^3b$ | $b$ |
| $a^2$ | $a^2$ | $a^3$ | $e$ | $a$ | $a^2b$ | $a^3b$ | $b$ | $ab$ |
| $a^3$ | $a^3$ | $e$ | $a$ | $a^2$ | $a^3b$ | $b$ | $ab$ | $a^2b$ |
| $b$ | $b$ | $a^3b$ | $a^2b$ | $ab$ | $e$ | $a^3$ | $a^2$ | $a$ |
| $ab$ | $ab$ | $b$ | $a^3b$ | $a^2b$ | $a$ | $e$ | $a^3$ | $a^2$ |
| $a^2b$ | $a^2b$ | $ab$ | $b$ | $a^3b$ | $a^2$ | $a$ | $e$ | $a^3$ |
| $a^3b$ | $a^3b$ | $a^2b$ | $ab$ | $b$ | $a^3$ | $a^2$ | $a$ | $e$ |

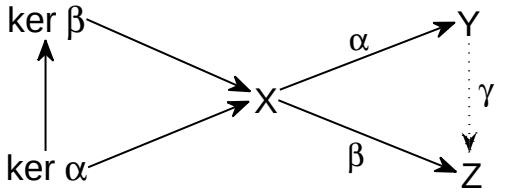
Taulukko 2: Ryhmän 4.2.1 kertotaulu.

Jos virittäjä $a$ vastaa kulman $\frac{\pi}{2}$ kiertoa vastapäivään ja virittäjä $b$ peilausta diagonaalin suhteen, siis määritelmän 2.9 merkintöjä käyttäen $a = R_{90}$ ja $b = D'$, niin $a^2 = R_{180},\ a^3 = R_{270},\ ab = H,\ a^2b = D$ ja $a^3b = V$. Vertaamalla taulukoita 1 ja 2 keskenään nähdään, että ryhmä (4.2.1) esittää diedriryhmää $D_4 = (\{I, R_{90}, R_{180}, R_{270}, D', H, D, V\}, \circ)$.

Myöhemmin käsittelemme yleisemmin diedriryhmän $D_n$ esitystä. Osoitamme ensin kaksi hyödyllistä lemmaa.

**Lemma 4.8.** *Olkoot $X, Y$ ja $Z$ ryhmiä, $\alpha : X \to Y$ epimorfismi ja $\beta : X \to Z$ homomorfismi siten, että $\ker \alpha \subseteq \ker \beta$. Tällöin on olemassa homomorfismi $\gamma : Y \to Z$, jolle pätee $\gamma \circ \alpha = \beta$.*

*Todistus.* Kuvassa 5 on esitetty tilanteen kuvauskaavio. Merkitsemättömät nuolet tarkoittavat inkluusiokuvauksia.




Kuva 5: Lemman 4.8 kuvauskaavio.

Kuvaus $\alpha$ on surjektio, joten jokaista $y \in Y$ kohti on olemassa sellainen $x \in X$, että $\alpha(x) = y$. Määritellään kuvaus $\gamma : Y \to Z$ :

$$\gamma(y) = \gamma(\alpha(x)) = (\gamma \circ \alpha)(x) = \beta(x). \tag{4.2.2}$$

Osoitetaan ensin, että kuvaus $\gamma$ on hyvinmääritelty, eli että sen arvo on riippumaton alkukuvapisteen $x$ valinnasta. Olkoon $x' \in X$ toinen alkukuvapiste $y$:lle, eli $\alpha(x') = y = \alpha(x)$. Kuvaus $\alpha$ on homomorfismi, joten

$$\alpha(x') = \alpha(x) \Leftrightarrow e = \alpha(x')\alpha(x)^{-1} = \alpha(x')\alpha(x^{-1}) = \alpha(x'x^{-1}).$$

Näin ollen $x'x^{-1} \in \ker \alpha \subseteq \ker \beta$, joten $\beta(x'x^{-1}) = e$. Tällöin vastaavasti kuin yllä saadaan

$$\beta(x') = \beta(x) = \gamma(y).$$

Osoitetaan vielä, että $\gamma$ toteuttaa homomorfiaehdon. Olkoot $y_1, y_2 \in Y$ ja $x_1, x_2 \in X$ niiden alkukuvapisteet. Tällöin, koska $\alpha$ on homomorfismi, niin

$$\alpha(x_1x_2) = \alpha(x_1)\alpha(x_2) = y_1y_2.$$

Alkio $x_1x_2 \in X$ on siis alkion $y_1y_2 \in Y$ alkukuvapiste. Kuvaus $\beta$ on homomorfismi, joten kuvauksen $\gamma$ määritelmän (4.2.2) nojalla

$$\gamma(y_1y_2) = \gamma(\alpha(x_1x_2)) = \beta(x_1x_2) = \beta(x_1)\beta(x_2) = \gamma(y_1)\gamma(y_2),$$

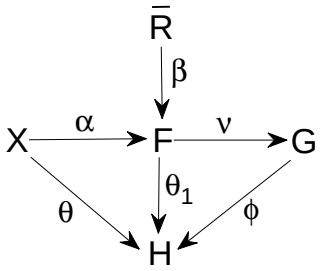
joten $\gamma$ on homomorfismi. □

**Lemma 4.9.** *Olkoon $G$ ryhmä, jolla on äärellinen esitys $\langle X|R\rangle$. Olkoon myös $H$ ryhmä ja kuvaus $\theta : X \to H$. Jokaiselle ryhmän $G$ sanalle $w = x_1 \dots x_n$, missä $x_i \in X$ kaikilla $i$, merkitään $w' = \theta(x_1) \dots \theta(x_n)$. Oletetaan, että $r'$ on ryhmän $H$ neutraalialkio, kun $r \in R$. Tällöin kuvaus*

$$\phi : G \to H,\ w \mapsto w'$$

*on hyvinmääritelty homomorfismi. Jos alkiot $\theta(x_i)$ lisäksi virittävät $H$:n, niin kuvaus $\phi$ on surjektio ja $H$ on ryhmän $G$ homomorfinen kuva, eli $|H| \leq |G|$.*

*Todistus.* Kuvassa 6 on esitetty tilanteen kuvauskaavio. Kuvaukset $\alpha$ ja $\beta$ ovat inkluusiokuvauksia.




Kuva 6: Lemman 4.9 kuvauskaavio.

Olkoon $F$ on vapaa ryhmä joukon $X$ suhteen. Vapaan joukon formaalin määritelmän nojalla kuvaus $\theta : X \to H$ laajenee (yksikäsitteisesti) homomorfismiksi $\theta_1 : F \to H$. Olkoon $r = r_1 \dots r_n \in R$, jolloin $r' = e_H$. Koska

$$r' = \theta(r_1) \dots \theta(r_n) = \theta_1(r_1) \dots \theta_1(r_n) = \theta_1(r_1 \dots r_n) = \theta_1(r),$$

niin oletuksesta seuraa, että $r \in \ker \theta_1$, kun $r \in R$. Oletus voidaan siis kirjoittaa $R \subseteq \ker \theta_1$. Normaali sulkeuma $\overline{R}$ on suppein $F$:n normaali aliryhmä, joka sisältää joukon $R$, joten $R \subseteq \overline{R} \subseteq \ker \phi$.

Olkoon $\nu$ luonnollinen kuvaus $F \to G = F/\overline{R}$. Tällöin $\ker \nu = \overline{R}$. Yhdistetään edelliset tulokset, jolloin saadaan $\ker \nu = \overline{R} \subseteq \ker \theta_1$.

Koska $F, G$ ja $H$ ovat ryhmiä, $\nu : F \to G$ on epimorfismi, $\theta_1 : F \to H$ on homomorfismi ja $\ker \nu \subseteq \ker \theta_1$, niin lemman 4.8 nojalla on olemassa sellainen homomorfismi $\phi_1 : G \to H$, että $\phi_1 \circ \nu = \theta_1$. Tutkitaan vielä, onko $\phi_1$ kuvaus $\phi$.

Olkoon $w = x_1 \dots x_n$, missä $x_i \in X$. Nähdään, että

$$(\phi_1 \circ \nu)(w) = \phi_1(\nu(w)) = \phi_1(\overline{R}w) = \phi_1(w).$$

Toisaalta esimerkin 3.14 mukaisesti homomorfismille $\theta_1$, joka laajentaa kuvauksen $\theta$, pätee

$$\theta_1(w) = \theta_1(x_1)\dots\theta_1(x_n) = \theta(x_1)\dots\theta(x_n) = w',$$

sillä $x_i \in X$. Koska $(\phi_1 \circ \nu)(w) = \theta_1(w)$, niin $\phi_1(w) = w' = \phi(w)$ kaikilla $w \in G$.

Jos alkiot $\theta(x_i)$ virittävät ryhmän $H$, niin kuvaus $\theta_1$ on surjektiivinen. Tällöin myös kuvaus $\phi$ on surjektiivinen, joten $\mathrm{im}(G) = H$. On siis oltava $|H| \leq |G|$. □

**Lemma 4.10.** *Diedriryhmän $D_n$ mahtavuus on $2n$.*

*Todistus.* Diedriryhmän $D_n$ alkiot ovat säännöllisen $n$-kulmion kiertoja ja peilauksia. On olemassa symmetria, joka kuvaa kulmion kärjen 1 kärjeksi $i$. Koska kärki 2 on kärjen 1 vieressä, niin kärki 2 kuvautuu tällöin joko kärjeksi $i-1$ tai $i+1$ (missä $1-1=n$ ja $n+1=1$). Näin ollen on olemassa $n\cdot 2$ mahdollisuutta valita kärkien 1 ja 2 kuvapisteiden sijainti. Symmetriassa riittää määrittää kärkien 1 ja 2 kuvapisteiden sijainti, sillä muiden kärkien kuvapisteiden sijainti määräytyy näiden mukaan. Säännöllisten $n$-kulmioiden symmetrioita on siis olemassa korkeintaan $2n$ kappaletta.

Toisaalta säännöllisellä $n$-kulmiolla on kiertoja ja peilauksia vähintään $2n$ kappaletta. Näin ollen diedriryhmän $D_n$ mahtavuus on $2n$. □

Edellisten lemmojen avulla voimme osoittaa diedriryhmän $D_n$ ja symmetriaryhmän $S_n$ esitykset.

**Lause 4.11.** *Diedriryhmällä $D_n$ on esitys*

$$\langle x, y \mid x^n, y^2, (xy)^2 \rangle. \tag{4.2.3}$$

*Todistus.* Tutkitaan säännöllistä $n$-kulmiota, jonka kärjet on numeroitu myötäpäivään $1, 2, \dots, n$, kuten neliö alaluvun 2.2 kuvissa 1 ja 2. Olkoon kuvaus

$$\begin{aligned} &\theta : \{x, y\} \to D_n, \\ &x \mapsto (12\dots n), \\ &y \mapsto (2n)(3(n-1))\dots, \end{aligned}$$

missä $y$:n kuvan viimeinen transpositio riippuu $n$:n parillisuudesta. Alkio $x$ kuvautuu siis kulman $\frac{2\pi}{n}$ kierroksi (kierto vastapäivään) ja alkio $y$ peilaukseksi sellaisen suoran suhteen, joka kulkee monikulmion keskipisteen ja kärjen 1 kautta.

Nähdään, että

$$\theta(x)\cdot\theta(y)=\theta(y)\theta(x)=(2n)(3(n-1))\dots(12\dots n)=(1n)(2(n-1))\dots,$$

joten lauseesta 2.15 seuraa, että

$$\operatorname{ord}(\theta(x))=n,\ \operatorname{ord}(\theta(y))=2,\ \operatorname{ord}(\theta(x)\cdot\theta(y))=2. \tag{4.2.4}$$

Merkitään ryhmää (4.2.3) $G$:llä. Ryhmällä $G$ on äärellinen esitys ja sen virittäjäjoukolta $\{x,y\}$ on kuvaus $\theta$ toiselle ryhmälle $D_n$. Lisäksi yhtälöiden 4.2.4 ja seurauksen 2.8 mukaan

$$(x^n)'=\theta(x)^n=e,\quad (y^2)'=\theta(y)^2=e,\quad ((xy)^2)'=(\theta(x)\cdot\theta(y))^2=e.$$

Kuva-alkiot $(x^n)', (y^2)'$ ja $((xy)^2)'$ ovat siis $D_n$:n neutraalialkioita. Tällöin lemman 4.9 mukaan on olemassa homomorfismi

$$\phi : G\to D_n.$$

Säännöllisen $n$-kulmion kaikki symmetriat saadaan kahden symmetrian avulla: kulman $\frac{2\pi}{n}$ kierto vastapäivään ja peilaus sellaisen suoran suhteen, joka kulkee monikulmion keskipisteen ja kärjen 1 kautta. Lisäksi siis $\theta(x)$ ja $\theta(y)$ virittävät ryhmän $D_n$. Lemman 4.9 nojalla siis pätee lisäksi, että $\phi$ on surjektio ja $|D_n|\le|G|$.

Toisaalta $G$:n relaattoreista seuraa, että

$$xyxy=e \text{ eli } xyx=y \text{ eli } yx=x^{n-1}y.$$

Koska lisäksi $x^{-1}=x^{n-1}$ ja $y^{-1}=y$, niin jokainen ryhmän $G$ alkio voidaan siis kirjoittaa muodossa

$$x^iy^j,$$

missä $i=0,1,\dots,n-1$ ja $j=0,1$. Näin ollen $|G|\le 2n=|D_n|$.

Koska ryhmien $G$ ja $D_n$ välillä on epimorfismi ja niiden mahtavuudet ovat yhtä suuret, niin ne ovat keskenään isomorfiset. Yhtälö 4.2.3 on siis ryhmän $D_n$ esitys. □

**Lause 4.12.** *Symmetriaryhmällä $S_n$ on esitys*

$$\langle x_1,\dots,x_{n-1}\mid R\cup S\cup T\rangle, \tag{4.2.5}$$

*missä*

$$\begin{aligned}R&=\{x_i^2\mid 1\le i\le n-1\}\\ S&=\{(x_ix_{i+1})^3\mid 1\le i\le n-2\}\\ T&=\{[x_i,x_j]\mid 2\le i+1<j\le n-1\}.\end{aligned}$$

*Todistus.* Merkitään ryhmää (4.2.5) $G_n$. On osoitettava, että ryhmät $S_n$ ja $G_n$ ovat isomorfiset.

Osoitetaan ensin, että on olemassa homomorfismi $G_n \to S_n$. Määritellään kuvaus

$$\theta : \{x_1, \ldots, x_{n-1}\} \to S_n, \;\; x_i \mapsto (i(i+1)),$$

missä $1 \leq i \leq n-1$.

Lauseen 2.15 ja seurauksen 2.8 nojalla

$$(x_i^2)' = (\theta(x_i))^2 = (i(i+1))^2 = e, \text{ missä } 1 \leq i \leq n-1, \qquad \text{ja}$$

$$\begin{aligned}((x_i x_{i+1})^3)' &= (\theta(x_1) \cdot \theta(x_{i+1}))^3 = (\theta(x_{i+1})\theta(x_i))^3 = (((i+1)(i+2))(i(i+1)))^3 \\ &= (i(i+2)(i+1))^3 = e, \text{ missä } 1 \leq i \leq n-2.\end{aligned}$$

Permutaatiot $(i(i+1))$ ja $(j(j+1))$, missä $2 \leq i+1 < j \leq n-1$, ovat erillisiä, joten ne kommutoivat. Tällöin

$$[x_i, x_j]' = [\theta(x_i), \theta(x_j)] = (i(i+1)), (j(j+1))] = e.$$

Relaatiot $R, S$ ja $T$ pätevät siis myös ryhmässä $S_n$. Lisäksi seurauksen 2.18 mukaan transpositiot $\theta(x_1), \theta(x_2) \ldots$ ja $\theta(x_{n-1})$ eli $(12), (23), \ldots$ ja $((n-1)n)$ virittävät ryhmän $S_n$, joten lemman 4.9 nojalla on olemassa epimorfismi $G_n \to S_n$ ja $|S_n| \leq |G_n|$.

Osoitetaan vielä induktion avulla, että $|G_n| \leq n! = |S_n|$. Kun $n = 1$, niin $G_n$ on triviaali ryhmä $\{e\}$, joten $|G_1| = 1 \leq 1!$ ja, kun $n = 2$, niin $G_n$ on syklinen ryhmä $\langle x_1 \mid x_1^2 \rangle = \{e, x\}$, joten $|G_2| = 2 \leq 2!$.

Tehdään nyt induktio-oletus: $G_{n-1} \leq (n-1)!$ ja $n \geq 3$. Olkoon $H$ alkioiden $x_1, \ldots, x_{n-2}$ virittämä $G_n$:n aliryhmä ja määritellään

$$y_0 = e, \; y_i = x_{n-1} \ldots x_{n-i},$$

missä $1 \leq i \leq n-1$. Olkoon joukko

$$A = Hy_0 \cup \cdots \cup Hy_{n-1} = \{hy_i \mid h \in H, \; 1 \leq i \leq n-1\},$$

joka on $G_n$:n osajoukko. Halutaan osoittaa, että $A = G_n$. Koska $A \subseteq G_n$, niin riittää osoittaa, että $G_n \subseteq A$.

Tutkitaan tuloa $hy_i x_j \in Ax_j$, missä $h \in H$, $0 \leq i \leq n-1$ ja $0 \leq j \leq n-1$. Jaetaan tarkastelu kuuteen erilliseen tapaukseen. Relaattorijoukot $R$ ja $S$ koskevat kaikkia $x_i$, missä $1 \leq i \leq n-1$, mutta relaattorijoukossa $T$ on huolehdittava, että alkioiden $x_i$ ja $x_j$ indekseille pätee $i+1 < j$:

(i) Oletetaan, että $i = 0$ ja $j < n - 1$. Tällöin

$$hy_i x_j = hex_j = hx_j \in H.$$

Koska $y_0 = e$, niin $H = Hy_0 \subseteq A$, joten $hy_i x_j \in A$.

(ii) Oletetaan, että $i = 0$ ja $j = n - 1$. Tällöin

$$hy_i x_j = hex_{n-1} = hy_1 \in Hy_1 \subseteq A,$$

joten $hy_i x_j \in A$.

(iii) Oletetaan, että $1 \leq i \leq n - 1$ ja $n - i < j \leq n - 1$. Tällöin

$$\begin{aligned} hy_i x_j &= h(x_{n-1} \dots x_j x_{j-1} \dots x_{n-i}) x_j \\ &= hx_{n-1} \dots x_{j+1} x_j x_{j-1} x_j x_{j-2} \dots x_{n-i} \\ &= hx_{n-1} \dots x_{j-1} x_j x_{j-1} x_{j-2} \dots x_{n-i} \\ &= hx_{j-1} x_{n-1} \dots x_{n-i} \\ &= hx_{j-1} y_i, \end{aligned}$$

missä toinen ja neljäs yhtälö seuraa relaattorijoukosta $T$: $x_n x_m = x_m x_n$, kun $n + 1 < m$. Kolmas yhtälö seuraa puolestaan relaattorijoukoista $R$ ja $S$: $R$:n nojalla $(x_{j-1} x_j)^3 = x_{j-1} x_j x_{j-1} x_j^{-1} x_{j-1}^{-1} x_j^{-1}$, mistä seuraa $S$:n nojalla $x_j x_{j-1} x_j = x_{j-1} x_j x_{j-1}$.

Koska alkiot $x_1, \dots, x_{n-2}$ virittävät ryhmän $H$, niin oletuksen $n - i < j \leq n - 1$ nojalla $x_{j-1} \in H$. Nyt nähdään, että $hy_i x_j = hx_{j-1} y_i \in Hy_i \subseteq A$, joten $hy_i x_j \in A$.

(iv) Oletetaan, että $1 \leq i \leq n - 1$ ja $j = n - i$. Tällöin

$$\begin{aligned} hy_i x_j &= hx_{n-1} \dots x_{n-i+1} x_{n-i} x_{n-i} \\ &= hx_{n-1} \dots x_{n-i+1} x_{n-i}^2 \\ &= hx_{n-1} \dots x_{n-i+1} \\ &= hy_{i-1}, \end{aligned}$$

missä kolmas yhtälö seuraa relaattorijoukosta $R$ ja neljäs yhtälö nähdään helposti, sillä $y_{i-1} = x_{n-1} \dots x_{n-(i-1)} = x_{n-1} \dots x_{n-i+1}$.

Koska $hy_{i-1} \in Hy_{i-1} \subseteq A$, niin $hy_i x_j \in A$.

(v) Oletetaan, että $1 \leq i \leq n - 1$ ja $j = n - i - 1$. Tällöin

$$\begin{aligned} hy_i x_j &= hx_{n-1} \dots x_{n-i} x_{n-i-1} \\ &= hx_{n-1} \dots x_{n-i} x_{n-(i+1)} \\ &= hy_{i+1} \in Hy_{i+1} \subseteq A, \end{aligned}$$

joten $hy_j x_i \in A$.

(vi) Oletetaan, että $1 \leq i \leq n-1$ ja $j < n-i-1$. Tällöin

$$hy_i x_j = hx_{n-1} \dots x_{n-i} x_j.$$

Oletuksesta $j < n-i-1$ seuraa, että $j+1 < n-i$. Koska lisäksi $1 \leq i \leq n-1$, niin $j+1 < n-i \leq n-1$. Näin ollen relaattorijoukon $T$ nojalla

$$hy_i x_j = hx_j y_i.$$

Koska $x_j \in H$, kun $j < n-i-1 < n-1$, niin $hx_j y_i \in Hy_i \subseteq A$, joten $hy_i x_j \in A$.

Olemme osoittaneet, että $hy_i x_j \in A$ kaikilla $h \in H, 0 \leq i \leq n-1$ ja $0 \leq j \leq n-1$, joten $Ax_j \subseteq A$ kaikilla $j$. Toisaalta, koska $R$ sisältyy $G_n$:n relaattorijoukkoon, niin myös jokaiselle käänteisalkiolle $x_j^{-1}$ pätee

$$Ax_j^{-1} = Ax_j \subseteq A,$$

missä $1 \leq j \leq n-1$. Tällöin mille tahansa ryhmän $G_n$ sanalle $w$ pätee $Aw \subseteq A$, mistä seuraa, että $AG_n \subseteq A$.

$H$ on aliryhmä, joten $e \in H$, jolloin nähdään, että joukko $A$ sisältää alkion $ey_0 = e$. Näin ollen

$$G_n = eG_n \subseteq AG_n \subseteq A,$$

joten $A = G_n$.

Aliryhmällä $H$ on samat virittäjäalktiot kuin ryhmällä $G_{n-1}$ ja niissä pätevät relaatiot, jolloin jälleen lemman 4.9 ja induktio-oletuksen nojalla

$$|H| \leq |G_{n-1}| \leq (n-1)!.$$

Toisaalta

$$|G_n| = |A| = |Hy_0 \cup \dots \cup Hy_{n-1}| \leq n|H| \leq n(n-1)! = n!,$$

joten $|G_n| \leq |S_n|$. Yhdistämällä edelliset tulokset saadaan $|G_n| = |S_n|$.

On todistettu, että on olemassa epimorfismi $\theta$ ryhmältä $G_n$ ryhmälle $S_n$. Toisaalta ollaan osoitettu, että ryhmillä $G_n$ ja $S_n$ on sama mahtavuus, joten ryhmät ovat isomorfiset. Symmetriaryhmällä $S_n$ on siis esitys 4.2.5. □

**Määritelmä 4.13.** Ryhmiä, joilla on esitys

$$D(l,m,n) = \langle x, y \mid x^l, y^m, (xy)^n \rangle,$$

kutsutaan von Dyck -ryhmiksi.

*Esimerkki* 4.14. Edellisten lauseiden nojalla huomataan, että diedriryhmä $D_n$ ja symmetriaryhmä $S_3$ ovat von Dyck -ryhmiä,

$$D_n = \langle x, y \mid x^n, y^2, (xy)^2 \rangle = D(n, 2, 2),$$

$$S_3 = \langle x, y \mid x^2, y^2, (xy)^3 \rangle = D(2, 2, 3).$$

**Lause 4.15.** *Jos $G = \langle X|R\rangle$ ja $H = \langle Y|S\rangle$ ovat kaksi esitystä, niin ryhmien $G$ ja $H$ suoralla tulolla $G \times H$ on esitys*

$$\langle X \cup Y \mid R \cup S \cup [X, Y] \rangle, \tag{4.2.6}$$

*missä $[X, Y]$ esittää kommutaattorijoukkoa $\{[x, y] \mid x \in X, y \in Y\}$.*

*Todistus.* Merkitään ryhmää (4.2.6) $D$:llä. Virittäjäjoukot $X$ ja $Y$ sisältyvät ryhmään $D$ ja relaattorijoukot $R$ ja $S$ sisältyvät ryhmän $D$ relaattorijoukkoon. Näin ollen inkluusiokuvaukset $X \to D$ ja $Y \to D$ indusoivat lemman 4.9 nojalla sellaiset homomorfismit $\theta : G \to D$ ja $\phi : H \to D$, että $\theta(r) = e_D$ kaikilla $r \in \overline{R}$ ja $\phi(s) = e_D$ kaikilla $s \in \overline{S}$. Näiden homomorfismien avulla voidaan määritellä kuvaus

$$\alpha : G \times H \to D,\ (g, h) \mapsto \theta(g)\phi(h).$$

Kuvauksen $\alpha$ homomorfisuus seuraa kuvauksien $\theta$ ja $\phi$ homomorfisuudesta: Olkoon $a, c \in G$ ja $b, d \in H$. Näin ollen

$$\begin{aligned}\alpha((a, b)(c, d)) =& \alpha(ac, bd) = \theta(ac)\phi(bd) = \theta(a)\theta(c)\phi(b)\phi(d) \\ =& \theta(a)\phi(b)\theta(c)\phi(d) = \alpha(a, b)\alpha(c, d),\end{aligned}$$

missä neljäs yhtäsuuruus pätee, sillä kommutaattorijoukko $[X, Y]$ sisältyy $D$:n relaattorijoukkoon.

Kommutaattorijoukon $[X, Y]$ ominaisuuksien nojalla pätee myös, että jokainen ryhmän $D$ sana $w$ voidaan kirjoittaa muodossa $w = gh$, missä $g \in G$ ja $h \in H$. Lemmasta 4.9 seuraa, että inkluusio $X \cup Y \to G \times H$ laajenee homomorfismiksi

$$\beta : D \to G \times H,\ w \mapsto (g, h),$$

missä $w = gh \in GH$. Homomorfismilla $\alpha$ on siis käänteiskuvaus $\beta$, joiden yhdisteet $\alpha \circ \beta$ ja $\beta \circ \alpha$ ovat molemmat identiteettikuvauksia. Kuvaus $\alpha$ on siis isomorfismi ja 4.2.6 on suoran tulon $G \times H$ esitys.

□

Aiemmin esimerkissä 4.7 pystyimme päättelemään ryhmän esityksen avulla sen kertotaulun. Entä voiko ryhmän kertotaulusta johtaa ryhmän esityksen?

**Lause 4.16.** *Olkoon $G$ ryhmä, jonka kertolasku on*

$$m : G \times G \to G.$$

*Tällöin ryhmällä $G$ on esitys $\langle X|R\rangle$, missä*

$$\begin{aligned} X &= \text{ ryhmän } G \text{ alla oleva joukko, ja} \\ R &= \{xym(x,y)^{-1} \mid x, y \in G\}. \end{aligned}$$

*Todistus.* Olkoon $M$ ryhmä, jolla on esitys $\langle X|R\rangle$. Relaattorijoukko $R$ koostuu relaatioista, jotka pätevät ryhmässä $G$, joten ryhmissä $M$ ja $G$ on samat neutraalialkiot. Tällöin lemman 4.9 nojalla identiteettikuvaus $X \to G$ laajenee homomorfismiksi $\alpha : M \to G$. Toisaalta homomorfismilla $\alpha$ on käänteiskuvaus

$$\beta : G \to M,\ x \mapsto x,$$

sillä $G \subseteq M$. Koska yhdisteet $\alpha \circ \beta$ ja $\beta \circ \alpha$ ovat molemmat selvästi identiteettikuvauksia, niin $\alpha$ on isomorfismi ja ryhmällä $G$ on esitys $\langle X|R\rangle$. □

## 4.3 Abelin ryhmät

On syytä tutkia vielä erikseen Abelin ryhmiä.

**Lause 4.17.** *Äärellistä kertalukua $n$ olevan syklisen ryhmän esitys on*

$$\langle x|x^n\rangle.$$

*Todistus.* Tarkastellaan vapaan ryhmän $F = \langle x|\emptyset\rangle$ normaalia aliryhmää $\overline{R} = \overline{\{x^n\}}$. Alkiot

$$e, x, x^2, \ldots, x^{n-1}$$

muodostavat aliryhmän $\overline{R}$ positiivisen Schreier-edustajiston $U$ ryhmän $F$ suhteen.

Muistellaan, että $B$ on lemman 3.22 kohdassa (iv) määritelty joukko

$$B = \{ux\overline{ux}^{-1} \mid u \in U,\ x \in S\} \setminus \{e\}.$$

Tässä tapauksessa $S = \{x\}$. Kootaan taulukkon 3 ensimmäiseen sarakkeeseen joukon $U$ alkiot, ensimmäiseen riviin joukon $S$ alkio ja lasketaan toiseen sarakkeeseen seuraaville riveille tulo $ux\overline{ux}^{-1}$, missä $u \in U$ ja $x \in S$.

Lemman 3.22 kohdan (i) nojalla $ux\overline{ux}^{-1} = e$, jos ja vain jos $ux \in U$. Näin ollen saadaan täytettyä taulukon toinen sarake viimeistä riviä lukuunottamatta, sillä $x^{n-i}x \in U$ kaikilla $2 \leq i \leq n$. Viimeisellä rivillä $ux =$

| | $x$ |
|---|---|
| $e$ | $e$ |
| $x$ | $e$ |
| $x^2$ | $e$ |
| $\vdots$ | $\vdots$ |
| $x^{n-2}$ | $e$ |
| $x^{n-1}$ | $x^n$ |

Taulukko 3: Taulukko joukon $B$ määrittämiseksi.

$x^{n-1}x = x^n$. Koska $x^n \in \overline{\{x^n\}}$, niin $\overline{\{x^n\}}x^n = \overline{\{x^n\}}$, jolloin $\overline{ux} = e$. Näin ollen $ux\overline{ux} = x^n e = x^n$.

Taulukosta 3 nähdään, että $B = \{x^n\}$. Lemman 3.21 ja lemman 3.22 kohdan (iv) nojalla joukko $B$ virittää aliryhmän $\overline{R}$, joten

$$\langle x^n \rangle = \overline{\{x^n\}}.$$

Näin ollen $F/\overline{R}$ on yhden alkion virittämä ryhmä ja sen mahtavuus on $n$:

$$F/\overline{R} = \langle x \rangle / \langle x^n \rangle = \{\langle x^n \rangle, \langle x^n \rangle x, \ldots, \langle x^n \rangle x^{n-1}\},$$

ja sillä on esitys

$$\langle x | x^n \rangle.$$

□

*Esimerkki* 4.18. Jäännösluokkaryhmä modulo $n$ on kertalukua $n$ oleva syklinen ryhmä. Edellisestä lauseesta seuraa, että

$$\mathbb{Z}_n = \langle x | x^n \rangle.$$

*Esimerkki* 4.19. Lauseen 4.15 nojalla

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle a, b \mid a^2, b^3, [a, b] \rangle.$$

Virittäjä $a$ on kertalukua 2, joten sillä on kaksi erisuurta potenssia $e$ ja $a$. Vastaavasti virittäjällä $b$ on kolme erisuurta potenssia $e, b$ ja $b^2$ (missä molemmat $e$ on ryhmän $\mathbb{Z}_2 \times \mathbb{Z}_3$ neurtaalialkiona samat). Koska lisäksi $[a, b] = e$, niin ryhmä on vaihdannainen. Näin ollen nähdään, että ryhmään kuuluu täsmälleen kuusi alkiota: $e, a, b, b^2, ab, ab^2$.

Additiiviset ryhmät $\mathbb{Z}_2 \times \mathbb{Z}_3$ ja $\mathbb{Z}_6$ ovat isomorfiset, sillä kun alkio $b$ kuvataan alkioksi $a^2$, niin saadaan ryhmä

$$\{e, a, a^2, (a^2)^2, aa^2, a(a^2)^2\} = \{e, a, \ldots, a^5\} = \langle a | a^6 \rangle = \mathbb{Z}_6.$$

**Lemma 4.20.** *Olkoot $F$ vapaa ryhmä joukon $X$ suhteen sekä $R$ ja $S$ ryhmän $F$ osajoukkoja. Jos $R \subseteq S$, niin on olemassa epimorfismi*

$$\theta : \langle X|R\rangle \to \langle X|S\rangle.$$

*Todistus.* Olkoot $\alpha$ ja $\beta$ kuvaukset:

$$\alpha : F \to F/\overline{R},\ w \mapsto \overline{R}w$$
$$\beta : F \to F/\overline{S},\ w \mapsto \overline{S}w.$$

$F, F/\overline{R}$ ja $F/\overline{S}$ ovat ryhmiä ja kuvaukset $\alpha$ ja $\beta$ ovat surjektiivisia homomorfismeja. Oletuksen nojalla $R \subseteq S$, jolloin myös $\overline{R} \subseteq \overline{S}$. Tästä seuraa, että

$$\ker \alpha = \overline{R} \subseteq \overline{S} = \ker \beta.$$

Näin ollen lemman 4.8 nojalla on olemassa sellainen homomorfismi

$$\theta : F/\overline{R} \to F/\overline{S}$$

että $\theta \circ \alpha = \beta$. Näin ollen kuvauksen $\theta$ surjektiivisuus seuraa kuvauksen $\beta$ surjektiivisuudesta. Kuvaus $\theta$ on siis epimorfismi.

Tekijäryhmän $F/\overline{R}$ esitys on $\langle X|R\rangle$ ja vastaavasti ryhmää $F/\overline{S}$ vastaa esitys $\langle X|S\rangle$. On siis osoitettu, että on olemassa epimorfismi

$$\theta : \langle X|R\rangle \to \langle X|S\rangle.$$

□

Tutustumme lopuksi kommutaattorialiryhmän tekijäryhmään $G/[G,G]$.

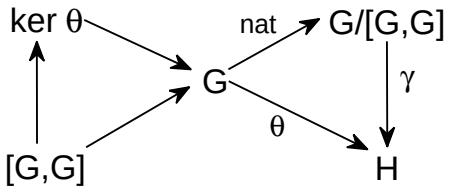
**Lause 4.21.** *Olkoon ryhmällä $G$ esitys $\langle x_1, \ldots, x_n \mid R\rangle$. Tällöin ryhmän $G/[G,G]$ esitys on*

$$\langle x_1, \ldots, x_n \mid R \cup S\rangle, \tag{4.3.1}$$

*missä $S = \{[x_i, x_j] | 1 \leq i < j \leq n\}$.*

*Todistus.* Merkitään ryhmää (4.3.1) $H$:lla. On osoitettava, että ryhmät $H$ ja $G/[G,G]$ ovat isomorfiset.

Ryhmillä $G$ ja $H$ on sama virittäjäjoukko ja $G$:n relaattorijoukko sisältyy $H$:n relaattorijoukkoon. Näin ollen lemmasta 4.20 seuraa, että on olemassa epimorfismi $\theta : G \to H$. Lisäksi on olemassa epimorfismi $\text{nat} : G \to G/[G,G],\ x \mapsto [G,G]x$. Tilanteen kuvauskaavio on kuvassa 7.




Kuva 7: Lauseen 4.21 kuvauskaavio.

Näytetään, että $[G,G] \subseteq \ker(\theta)$: Olkoon $g \in [G,G]$. Alkio $g$ voidaan siis kirjoittaa muodossa $g = [a_1, b_1] \dots [a_n, b_n]$, missä jokainen $a_i, b_i \in G$. Koska $\theta$ on homomorfismi ja $H$ on Abelin ryhmä, niin

$$\begin{aligned}\theta(g) &= \theta([a_1,b_1]\dots[a_n,b_n]) \\ &= \theta(a_1^{-1})\theta(b_1^{-1})\theta(a_1)\theta(b_1)\dots\theta(a_n^{-1})\theta(b_n^{-1})\theta(a_n)\theta(b_n) \\ &= \theta(a_1)^{-1}\theta(b_1)^{-1}\theta(a_1)\theta(b_1)\dots\theta(a_n)^{-1}\theta(b_n)^{-1}\theta(a_n)\theta(b_n) \\ &= \theta(a_1)^{-1}\theta(a_1)\theta(b_1)^{-1}\theta(b_1)\dots\theta(a_n)^{-1}\theta(a_n)\theta(b_n)^{-1}\theta(b_n) \\ &= e,\end{aligned}$$

joten $g \in \ker\theta$. Mielivaltainen ryhmän $[G,G]$ alkio kuuluu siis ytimeen $\ker\theta$, jolloin $[G,G] \subseteq \ker\theta$. Koska $\ker(\text{nat}) = [G,G]$, niin $\ker(\text{nat}) \subseteq \ker(\theta)$. Näin ollen kaikki lemman 4.8 oletukset pätevät, joten on olemassa homomorfismi $\gamma : G/[G,G] \to H$.

Toisaalta lemman 4.9 nojalla kuvauksella $\gamma$ on myös käänteiskuvaus $\gamma'$. Määritellään ensin kuvaus

$$\phi : \{x_1, \dots, x_n\} \to G/[G,G],\ x_i \mapsto [G,G]x_i.$$

Nähdään, että jos $r = r_1 \dots r_m \in R$, missä $r_i \in \{x_1, \dots, x_n\}$ kaikilla $i$, niin

$$\begin{aligned}r' &= \phi(r_1)\dots\phi(r_m) = [G,G]r_1\dots[G,G]r_m \\ &= [G,G](r_1\dots r_m) = [G,G]r = [G,G] = e_{G/[G,G]},\end{aligned}$$

sillä $r = e$ ryhmässä $G$.

Lisäksi, jos $s = [x_i, x_j] \in S$, niin

$$\begin{aligned}s' &= \phi(x_i)^{-1}\phi(x_j)^{-1}\phi(x_i)\phi(x_j) = [G,G]x_i^{-1}[G,G]x_j^{-1}[G,G]x_i[G,G]x_j \\ &= [G,G][x_i,x_j] = [G,G] = e_{G/[G,G]},\end{aligned}$$

sillä $[x_i, x_j] \in [G,G]$.

Tästä nähdään, että ryhmän $H$ määräävät relaatiot pätevät myös ryhmässä $[G, G]$, jolloin lemman 4.9 nojalla on olemassa homomorfismi $\gamma' : H \to G/[G, G]$.

Ryhmät $G/[G, G]$ ja $H$ ovat siis isomorfiset, eli (4.3.1) on kommutaattorialiryhmän tekijäryhmän $G/[G, G]$ esitys. □

### Vapaat Abelin ryhmät

Aiemmin olemme todenneet, että yleisessä tapauksessa vapaa ryhmä $F$ ei ole vaihdannainen. Seuraavaksi tutustumme vielä vapaisiin Abelin ryhmiin.

**Määritelmä 4.22.** Olkoon $F$ ryhmä ja $S$ sen osajoukko. Sanotaan, että $F$ *on vapaa Abelin ryhmä joukon $S$ suhteen*, jos jokaista Abelin ryhmää $G$ ja jokaista kuvausta $\theta : S \to G$ vastaa yksikäsitteisesti sellainen homomorfismi $\theta_1 : F \to G$, että

$$\theta_1(s) = \theta(s),$$

kaikilla $s \in S$.

Vapaan Abelin ryhmän määritelmä poikkeaa siis vapaan ryhmän formaalista määritelmästä (määritelmä 3.11) ainoastaan siten, että mielivaltaisen ryhmän $G$ sijaan vaaditaan mielivaltainen Abelin ryhmä.

**Lause 4.23.** *Olkoon $F$ vapaa ryhmä joukon $X = \{x_1, \ldots, x_n\}$ suhteen ja olkoon joukko*

$$R = \{[x_i, x_j] \mid 1 \leq i < j \leq n\}.$$

*Tällöin*

*(i)* $\overline{R} = [F, F]$,

*(ii)* $F/[F, F] = \langle X|R\rangle$,

*(iii)* $F/[F, F]$ *on vapaa Abelin ryhmä, jonka rangi on $n$,*

*(iv)* $F/[F, F]$ *on isomorfinen $n$:n äärettömän syklisen ryhmän suoran tulon kanssa.*

*Todistus.* (i) Ryhmän $F/\overline{R} = \langle X|R\rangle$ virittäjät kommutoivat keskenään, joten se on selvästi Abelin ryhmä. Tällöin lauseen 2.23 nojalla $[F, F] \leqslant \overline{R}$, joten $[F, F] \subseteq \overline{R}$.

Toisaalta joukon $R$ määritelmän nojalla $R \subseteq [F, F]$, jolloin lauseesta 2.22 seuraa, että $[F, F]$ on ryhmän $F$ normaali aliryhmä. Koska $\overline{R}$ on suppein ryhmän $F$ normaali aliryhmä, joka sisältää joukon $R$, niin on oltava $\overline{R} \subseteq [F, F]$.

Näistä seuraa, että $\overline{R} = [F, F]$, joten alkuperäinen väite on siis tosi.

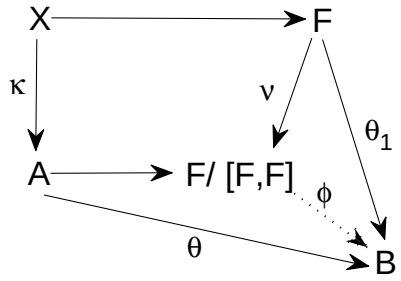
(ii) Väite seuraa suoraan kohdasta (i): $F/[F,F] = F/\overline{R} = \langle X|R\rangle$.

(iii) Määritellään kuvaus

$$\kappa : X \to A,\ x_i \mapsto [F,F]x_i,$$

missä $A = \{[F,F]x_i \mid 1 \leq i \leq n\}$. Kuvauksen kaksi kuva-alkiota $[F,F]x_i$ ja $[F,F]x_j$ ovat samat, jos ja vain jos $x_i x_j^{-1} \in [F,F] = \overline{R}$. Kuitenkin joukon $\overline{R}$ alkioiden tekijöiden $x_i$ eksponenttien summa on aina nolla. Näin ollen $x_i x_j^{-1} \in \overline{R}$, vain jos $i = j$. Joukon $A$ mahtavuus on siis myös $n$. Osoitetaan, että $F/[F,F]$ on vapaa Abelin ryhmä joukon $A$ suhteen.

Kuvassa 8 on kyseisen tilanteen kuvauskaavio. Merkitsemättömät nuolet tarkoittavat inkluusiota, $\nu$ on luonnollinen kuvaus $F \to F/[F,F]$, $B$ on Abelin ryhmä ja $\theta : A \to B$ on mikä tahansa kuvaus. Koska ryhmä $F$ on vapaa joukon $X$ suhteen, niin vapaan ryhmän formaalin määritelmän nojalla on olemassa homomorfismi $\theta_1$, joka laajentaa kuvauksen $\theta \circ \kappa$. Osoitetaan, että on olemassa yksikäsitteinen homomorfismi $\phi : F/[F,F] \to B$, joka laajentaa kuvauksen $\theta$.




Kuva 8: Lauseen 4.23 kohdan (iii) kuvauskaavio.

Olkoon $w \in [F,F]$. Näin ollen voidaan kirjoittaa

$$w = a_1^{-1}b_1^{-1}a_1b_1 \ldots a_n^{-1}b_n^{-1}a_nb_n,$$

missä $a_i, b_i \in F$ kaikilla $i$. Koska ryhmä $B$ on Abelin ryhmä ja kuvaus $\theta_1$ on homomorfismi, niin

$$\begin{aligned}\theta_1(w) &= \theta_1(a_1^{-1}b_1^{-1}ab \ldots a_n^{-1}b_n^{-1}a_nb_n)\\ &= \theta(a_1^{-1})\theta_1(b_1^{-1})\theta(a_1)\theta_1(b_1)\ldots\theta_1(a_n^{-1})\theta_1(b_n^{-1})\theta_1(a_n)\theta(b_n)\\ &= \theta(a_1)^{-1}\theta(a_1)\theta_1(b_1)^{-1}\theta_1(b_1)\ldots\theta_1(a_n)^{-1}\theta_1(a_n)\theta_1(b_n)^{-1}\theta(b_n) = e_B,\end{aligned}$$

joten $[F,F] \subseteq \ker\theta_1$. Toisaalta $\ker\nu = [F,F]$, joten $\ker\nu = [F,F] \subseteq \ker\theta_1$. Koska lisäksi $\nu$ on epimorfismi, niin lemman 4.8 nojalla on olemassa sellainen homomorfismi $\phi : F/[F,F] \to B$, että $\phi\circ\nu = \theta_1$. Muistetaan, että lisäksi $\theta_1 = \theta\circ\kappa$, joten $\phi(\nu(x)) = \theta(\kappa(x))$, kun $x \in X$. Myös kuvaus $\kappa$ on surjektio, joten toisaalta $\phi(a) = \theta(a)$ kaikilla $a \in A$. Näin ollen homomorfismi $\phi$ laajentaa kuvauksen $\theta$.

Homomorfismin $\phi$ yksikäsitteisyys puolestaan seuraa siitä, että joukko $A$ virittää ryhmän $F/[F,F]$. Ryhmä $F/[F,F]$ on siis vapaa ja sen rangi on $n$. Lisäksi lauseen 2.22 nojalla $F/[F,F]$ on Abelin ryhmä.

(iv) Muodostetaan $n$ kappaletta äärettömiä syklisiä ryhmiä,

$$F_m = \langle x_m | \emptyset \rangle,$$

missä $1 \leq m \leq n$. Lauseen 4.15 nojalla

$$\begin{aligned} F_1 \times F_2 &= \langle x_1, x_2 \mid [x_1,x_2] \rangle \\ (F_1 \times F_2) \times F_3 &= \langle x_1, x_2, x_3 \mid [x_1,x_2], [x_1,x_3], [x_2,x_3] \rangle \\ &\vdots \\ F_1 \times \cdots \times F_n &= \langle x_1, \ldots, x_n \mid [x_1,x_2], \ldots, [x_{n-1},x_n] \rangle = \langle X | R \rangle. \end{aligned}$$

Näin ollen kohdasta (ii) seuraa, että väite on tosi.

□

**Seuraus 4.24.** *Jokainen vapaa Abelin ryhmä, jonka rangi on $n$, on isomorfinen $n$:n äärettömän syklisen ryhmän suoran tulon kanssa.*

## 4.4 Tietze-muunnokset

Ryhmän esitys ei ole yksikäsitteinen. Yleensä tavoitellaan mahdollisimman lyhyttä esitystä, jolloin halutaan eroon kaikista turhista virittäjistä ja relaattoreista. Niin kutsuttujen Tietze-muunnosten avulla ryhmän esitys voidaan johtaa toiseen muoton ilman, että ryhmän isomorfialuokka muuttuu.

**Määritelmä 4.25.** Olkoon $G$ ryhmä ja sillä esitys

$$G = \langle X | R \rangle. \tag{4.4.1}$$

Kukin *Tietze-muunnos*, joita merkitään $T1, T2, T3$ ja $T4$, muuttaa esityksen (4.4.1) uuteen muotoon $\langle X' | R' \rangle$.

(T1) Jos $r$ on sana joukon $X$ yli ja relaatio $r = e$ pätee ryhmässä $G$, niin

$$\begin{cases} X' = X \\ R' = R \cup \{r\}. \end{cases}$$

(T2) Jos relaattorijoukossa $R$ on sana $r$, jolle pätee $r = e$ myös ryhmässä $\langle X \mid R \setminus \{r\}\rangle$, niin

$$\begin{cases} X' = X \\ R' = R \setminus \{r\}. \end{cases}$$

(T3) Jos $w$ on sana joukon $X$ yli ja $y$ on symboli, joka ei kuulu joukkoon $X$, niin

$$\begin{cases} X' = X \cup \{y\} \\ R' = R \cup \{y^{-1}w\}. \end{cases}$$

(T4) Jos $y$ on symboli joukossa $X$ ja $w$ on sana joukon $X \setminus \{y\}$ yli, jolle pätee $y^{-1}w \in R$, niin muodostetaan sellainen relaattorijoukko $\widetilde{R}$, että alkuperäisen relaattorijoukon $R$ sanoissa $w$ on korvattu symbolilla $y$. Tällöin

$$\begin{cases} X' = X \setminus \{y\} \\ R' = \widetilde{R}. \end{cases}$$

**Lause 4.26.** *Jokainen Tietze-muunnos $T1$ – $T4$ säilyttää esitetyn ryhmän isomorfismiluokan.*

*Todistus.* Olkoon $G = \langle X|R\rangle$ ja $r \in \overline{R} \setminus R$. Näin ollen ryhmässä $G$ alkio $r$ ei ole relaattori, mutta pätee $r = e$. Inkluusio $X \to \langle X \mid R \cup \{r\}\rangle$ laajenee lemman 4.9 nojalla homomorfismiksi

$$\alpha_1 : \langle X|R\rangle \to \langle X \mid R \cup \{r\}\rangle.$$

Koska $\overline{R} = \overline{R \cup \{r\}}$, niin huomataan, että $\alpha_1$ on itse asiassa isomorfismi. Näin ollen ryhmät $\langle X|R\rangle$ ja $\langle X \mid R \cup \{r\}\rangle$ ovat isomorfiset, joten Tietze-muunnokset $T1$ ja $T2$ säilyttävät isomorfismiluokan.

Olkoon $w$ mielivaltainen sana joukon $X$ yli ja $y$ symboli, joka ei kuulu joukkoon $X$. Inkluusio $X \to \langle X \cup \{y\} \mid R \cup \{y^{-1}w\}\rangle$ laajenee jälleen lemman 4.9 nojalla homomorfismiksi

$$\alpha_2 : \langle X|R\rangle \to \langle X \cup \{y\} \mid R \cup \{y^{-1}w\}\rangle,$$

joka kuvaa bijektiivisesti joukon $X$ alkiot itselleen ja sanan $w$ symboliksi $y$. Kuvaus $\alpha_2$ on siis isomorfismi, mikä osoittaa, että myös Tietze-muunnokset $T3$ ja $T4$ säilyttävät isomorfismiluokan. □

*Esimerkki* 4.27. Von Dyck -ryhmän isomorfialuokka ei ole riippuvainen parametrien järjestyksestä. Näytetään Tietze-muunnosten avulla, että $D(l,m,n) \simeq D(n,m,l)$.

$$
\begin{array}{lrl}
 & & \langle x, y \mid x^l, y^m, (xy)^n \rangle = \\
(T3) & z = xy: & \langle x, y, z \mid x^l, y^m, (xy)^n, xyz^{-1} \rangle = \\
(T1) & z^n: & \langle x, y, z \mid x^l, y^m, (xy)^n, xyz^{-1}, z^n \rangle = \\
(T2) & (xy)^n: & \langle x, y, z \mid x^l, y^m, xyz^{-1}, z^n \rangle = \\
(T1) & zy^{-1}x^{-1}: & \langle x, y, z \mid x^l, y^m, xyz^{-1}, z^n, zy^{-1}x^{-1} \rangle = \\
(T2) & xyz^{-1}: & \langle x, y, z \mid x^l, y^m, z^n, zy^{-1}x^{-1} \rangle = \\
(T4) & x = zy^{-1}: & \langle y, z \mid (zy^{-1})^l, y^m, z^n \rangle = \\
(T3) & t = y^{-1}: & \langle y, z, t \mid (zy^{-1})^l, y^m, z^n, y^{-1}t^{-1} \rangle = \\
(T1) & (zt)^l: & \langle y, z, t \mid (zy^{-1})^l, y^m, z^n, y^{-1}t^{-1}, (zt)^l \rangle = \\
(T2) & (zy^{-1})^l: & \langle y, z, t \mid y^m, z^n, y^{-1}t^{-1}, (zt)^l \rangle = \\
(T1) & t^{-1}y^{-1}: & \langle y, z, t \mid y^m, z^n, y^{-1}t^{-1}, (zt)^l, t^{-1}y^{-1} \rangle = \\
(T2) & y^{-1}t^{-1}: & \langle y, z, t \mid y^m, z^n, (zt)^l, t^{-1}y^{-1} \rangle = \\
(T4) & y = t^{-1}: & \langle z, t \mid t^{-m}, z^n, (zt)^l \rangle = \\
(T1) & t^m: & \langle z, t \mid t^{-m}, z^n, (zt)^l, t^m \rangle = \\
(T2) & t^{-m}: & \langle z, t \mid z^n, t^m, (zt)^l \rangle
\end{array}
$$

Koska Tietze-muunnokset eivät vaikuta esitetyn ryhmän isomorfismiluokkaan, niin

$$D(l,m,n) = \langle x, y \mid x^l, y^m, (xy)^n \rangle \simeq \langle x, y \mid x^n, y^m, (xy)^l \rangle = D(n,m,l).$$

**Lause 4.28.** *Olkoon ryhmälle $G$ annettu kaksi äärellistä esitystä*

$$\langle X|R \rangle \text{ ja } \langle Y|S \rangle.$$

*Esitykset voidaan johtaa toisikseen äärellisen monen Tietze-transformaation avulla.*

*Todistus.* Käsitellään relaatiojoukkoja relaattorijoukkojen sijaan. Merkintä $R = e$ tarkoittaa yhtälöiden $r = e$, missä $r \in R$, muodostamaa joukkoa. Koska $X$ ja $Y$ ovat molemmat ryhmän $G$ virittäjäjoukkoja, niin joukon $X$ alkiot voidaan esittää joukon $Y$ sanoina. Merkitään tätä $X(Y)$. Vastaavasti voidaan kirjoittaa $Y(X)$. Merkinnät

$$X = X(Y) \text{ ja } Y = Y(X)$$

tarkoittavat yhtälöiden $x = y_1 \dots y_n$ ja $y = x_1 \dots x_m$ joukkoja, missä $x \in X$ ja $y_i \in Y$ kaikilla $i$ sekä $y \in Y$ ja $x_i \in X$ kaikilla $i$.

Tietze-muunnosten $T1$ – $T4$ avulla voidaan muokata esitys $\langle X|R\rangle$ esitykseksi $\langle Y|S\rangle$:

$$
\begin{array}{lrll}
 & & \langle X & | \; R(X) = e\rangle \\
(T3) & Y = Y(X): & \langle X \cup Y & | \; R(X) = e,\ \ Y = Y(X)\rangle \\
(T1) & S(Y) = e: & \langle X \cup Y & | \; R(X) = e,\ \ S(Y) = e,\ \ Y = Y(X)\rangle \\
(T1) & X = X(Y): & \langle X \cup Y & | \; R(X) = e,\ \ S(Y) = e,\ \ Y = Y(X),\ \ X = X(Y)\rangle \\
(T4) & X = X(Y): & \langle Y & | \; R(X(Y)) = e,\ \ S(Y) = e,\ \ Y = Y(X(Y))\rangle \\
(T2) & R(X(Y)) = e: & \langle Y & | \; S(Y) = e,\ \ Y = Y(X(Y))\rangle \\
(T2) & Y = Y(X(Y)): & \langle Y & | \; S(Y) = e\rangle,
\end{array}
$$

missä toinen askel pätee, sillä jokainen joukon $Y$ alkio toteuttaa $S(Y) = e$ ryhmässä $G$ ja viimeinen askel pätee, sillä $S(Y) = e$ itse asiassa määrittelee ryhmän $G$.

Koska esitykset $\langle X|R\rangle$ ja $\langle Y|S\rangle$ ovat äärellisiä, niin edellä käytettiin Tietze-muunnoksia äärellisen monta kertaa.

□

# 5 Cayley-verkot

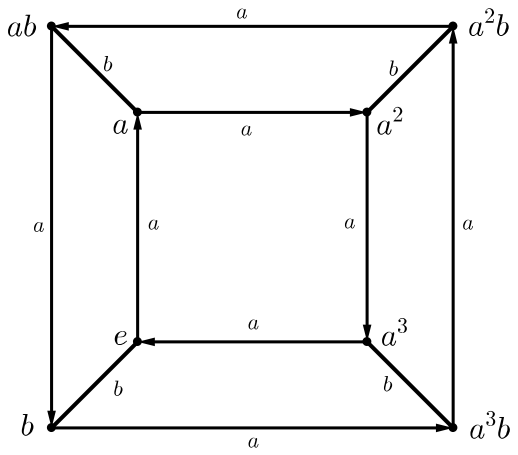
Tässä luvussa esitämme tavan esittää ryhmä virittäjien ja relaatioiden avulla graafisesti. Cayley-verkot ovat yksinkertainen tapa löytää uusia relaatioita, jos ryhmän virittäjä- ja relaattorijoukko ovat pieniä.

Olkoon $G$ ryhmä ja $S$ sen virittäjäjoukko. Cayley-verkossa kukin piste vastaa yhtä ryhmän $G$ alkiota. Jos $a_i$ kuuluu virittäjäjoukkoon $S$ ja $P_1$ ja $P_2$ ovat ryhmän alkioita, niin verkkoon piirretään suunnattu viiva (nuoli) $P_1$:stä $P_2$ :een aina, jos

$$P_2 = a_i P_1.$$

Kustakin pisteestä lähtee siis kutakin virittäjää kohden kaksi viivaa — toinen on suunnattu pisteestä poispäin ja toinen pistettä kohti. Neutraalialkiota $e$ vastaava piste yhdistää virittäjät ja niiden käänteisalkiot. Jos virittäjä $a_i$ on kertalukua kaksi, eli $a_i^2 = e$, niin kahden suunnatun viivan sijaan voidaan piirtää yksi suuntaamaton viiva.

Kukin polku $P$ Cayley-verkon viivoja pitkin vastaa tiettyä sanaa. Esimerkiksi polkua $P$, joka kulkee ensin viivan $a_1$ suuntaan, sitten viivan $a_2$ suuntaa vastaan ja lopuksi viivan $a_3$ suuntaan, on sana $P = a_3 a_2^{-1} a_1$. Polku $P$ johtaa pisteestä $P_1$ pisteeseen $PP_1$.




Kuva 9: Diedriryhmän $D_4$ Cayley-verkko.

Jos ryhmässä pätee epätriviaali relaatio $w = e$, niin polku $w$ on suljettu. Vastaavasti jos jokin polku on suljettu, niin sitä vastaava sana on ryhmän relaattori. Tämän nojalla virittäjä $a_i$ on kertalukua $n$, jos ja vain jos sen polku on syklisesti suunnattu $n$-kulmio, $P = a_i^n$.

*Esimerkki* 5.1. Verrataan kuvaa 9 diedriryhmän $D_4$ esitykseen

$$D_4 = \langle a, b \mid a^4, b^2, (ab)^2 \rangle,$$

missä $a$ on kulman $\frac{\pi}{2}$ kierto vastapäivään ja $b$ peilaus diagonaalin suhteen. Huomataan, että kuva esittää diedriryhmän $D_4$ Cayley-verkkoa: polku $P = a^4$ on syklisesti suunnattu neliö, eli virittäjä $a$ on kertalukua 4. Virittäjää $b$ on merkitty suuntaamattomalla viivalla, joten $b$ on kertalukua 2. Lisäksi kuvasta on helppo nähdä, että $(ab)^2 = e$.

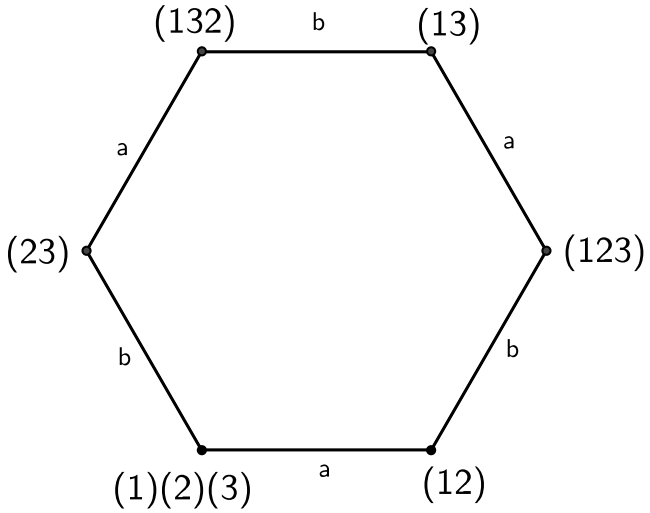
Cayley-verkon avulla on yksinkertaista todeta myös muita ryhmässä päteviä relaatioita. Huomataan esimerkiksi, että polku $ba^2ba$ johtaa samaan pisteeseen kuin polku $a^3$. Ryhmässä $D_4$ pätee siis relaatio $ba^2ba = a^3$.

*Esimerkki* 5.2. Lauseen 4.12 nojalla symmetriaryhmän $S_3$ esitys on

$$\langle a, b \mid a^2, b^2, (ab)^3 \rangle,$$

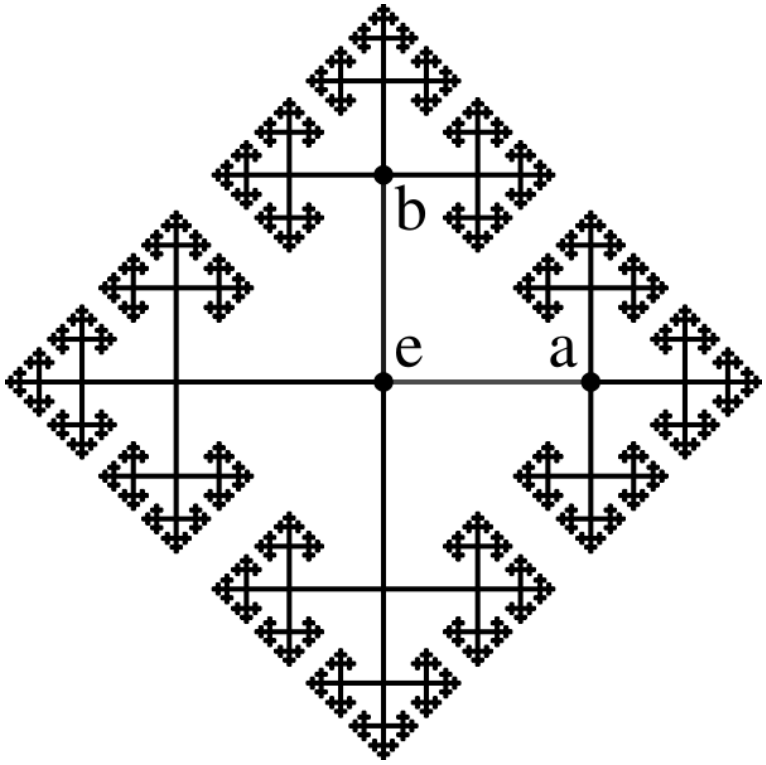
missä virittäjät $a$ ja $b$ ovat seurauksen 2.18 nojalla transpositiot (12) ja (23).

Kuvassa 10 on esitetty symmetriaryhmän $S_3$ Cayley-verkko. Koska transpositiot ovat lauseen 2.15 nojalla kertalukua 2, niin virittäjiä $a$ ja $b$ merkitään suuntaamattomilla viivoilla. Neutraalialkio on permutaatio (1)(2)(3). Cayley-verkon avulla on helppo todeta, että myös relaatio $(ab)^3 = e$ pätee ryhmässä $S_3$.




Kuva 10: Symmetriaryhmän $S_3$ Cayley-verkko. Ryhmän virittäjät ovat $a = (12)$ ja $b = (23)$ sekä neutraalialkio on (1)(2)(3).

*Esimerkki* 5.3. Vapaassa ryhmässä ei ole alkioiden välillä epätriviaaleja relaatioita. Vapaan ryhmän Cayley-verkossa ei siis muodostu suljettuja polkuja, vaan sen Cayley-verkko on loputon puu. Kuvassa 11 on esitetty kahden alkion $a$ ja $b$ virittämä vapaan ryhmän Cayley-verkko.




Kuva 11: Kahden alkion $a$ ja $b$ virittämän vapaan ryhmän Cayley-verkko.[11]

# 6 Avoimia kysymyksiä

Ryhmän esittämiseen virittäjien ja relaatioiden avulla liittyy vielä tärkeitä avoimia kysymyksiä. Max Dehn esitti vuonna 1911 kolme päätösongelmaa [2]: sanaongelman (*word problem*), konjugaattiongelman (*conjugacy problem*) ja isomorfismiongelman (*isomorphism problem*). Geometrian keinoin Dehn itse kehitti sana- ja konjugaattiongelman algoritmin suljettujen suunnistuvien kaksiulotteisten monistojen perusryhmille, joille on yhteistä niin kutsuttu pienten kumoutumisten ominaisuus. Mitään yleistä algoritmia näille ongelmille ei kuitenkaan vielä ole olemassa. Näiden ongelmien tunteminen kuitenkin auttaisi, kun ryhmän esityksestä halutaan saada informaatiota, onko ryhmä esimerkiksi Abelin ryhmä tai äärellinen.

Ongelmat liittyvät ryhmän esitykseen, ei itse ryhmään. On mahdollista, että samalla ryhmällä on kaksi eri esitystä, joista toisessa sanaongelma ratkeaa, mutta toisessa ei. Joskus kuitenkin saatetaan puhua ryhmän ongelmasta. Tällöin voidaan viitata ryhmän niin kutsuttuun standardiesitykseen liittyvästä ongelmasta. Esimerkiksi kahden alkion $a$ ja $b$ virittämän vapaan ryhmän standardiesitys on $\langle a, b\rangle$.

Ensimmäisenä Dehn esitti sanaongelman. Oletetaan tunnetuksi ryhmän $G$ esitys ja olkoot $w_1$ ja $w_2 \in G$. Sanaongelma kysyy, voidaanko sanoa, ovatko nämä mielivaltaiset ryhmän alkiot samat, eli päteekö $w_1 = w_2$? Sanaongelma voidaan esittää myös toisessa muodossa: Esittääkö sana $w = w_1^{-1}w_2$ neutraalialkiota, eli päteekö $w \in \overline{R}$?

Oletetaan jälleen tunnetuksi ryhmän $G$ esitys ja alkiot $w_1$ ja $w_2 \in G$. Konjugaattiongelmassa on kyse siitä, onko mahdollista selvittää, ovatko alkiot $w_1$ ja $w_2$ toistensa konjugaatteja eli onko olemassa sellaista alkiota $a \in G$, että $w_2 = a^{-1}w_1a$. Abelin ryhmille konjugaattiongelma on siis sama kuin sanaongelma. Yleisesti ottaen sanaongelma sisältyy konjugaattiongelmaan, joten on olemassa sellaisia esitysten luokkia, joiden sanaongelma on ratkennut, mutta konjugaattiongelma ei ole.

Sana- ja konjugaattiongelmat ratkeavat esimerkiksi vapaille ryhmille, joiden relaattorijoukko on tyhjä joukko. Sanaongelman ratkaisu on triviaali: Sana $w$ on ykkösalkio, jos ja vain jos se on supistettuna 1.

Luvussa 4.4 osoitimme, että saman ryhmän kaksi äärellistä esitystä voidaan johtaa toisikseen Tietze-muunnoksien avulla. Ei ole kuitenkaan olemassa yleistä algoritmia arvioida, esittävätkö mitkä tahansa kaksi äärellistä esitystä $\langle X|R\rangle$ ja $\langle Y|S\rangle$ samaa ryhmää. Tätä ongelmaa kutsutaan isomorfismiongelmaksi ja se on vaikein kolmesta Dehnin esittämästä ongelmasta.

[2] Päätösongelmassa algoritmilla on kullekin syötteelle kaksi mahdollista tulostetta: kyllä (1) tai ei (0).

# 7 Viitteet


[1] G. Almkvist: *Algebra*, Studentlitteratur, 1968

[2] H. S. M. Coxeter ja W. O. J. Moser: *Generators and Relations for Discrete Groups*, 2. painos, Springer-Verlag, 1964

[3] D. S. Dummit ja R. M. Foote: *Abstract Algebra*, Prentice-Hall International, 1991

[4] D. B. A. Epstein et al: *Word Processing in Groups*, Jones and Bartlett Publishers, 1992

[5] D. L. Johnson: *Presentation of Groups*, Cambridge University Press, 1976

[6] D. L. Johnson: *Topics in the Theory of Group Presentations*, Cambridge University Press, 1980

[7] R. C. Lyndon ja P. E. Schupp: *Combinatorial Group Theory*, Springer-Verlag Berlin Heidelberg, 1977

[8] W. Magnus, A. Karrass ja D. Solitar: *Combinatorial Group Thory – Presentation on Groups in Terms on Generators and Relations*, Interscience Publishers, 1966

[9] T. Metsänkylä ja M. Näätänen: *Algebra*, Yliopistopaino, 2009

[10] `http://www.maths.manchester.ac.uk/∼cwalkden/hyperbolic-geometry/lecture18.pdf` [luettu 12.1.2012]

[11] `http://en.wikipedia.org/wiki/Cayley_graph` [luettu 22.5.2012]