



VAPAAT RYHMÄT, NIIDEN TOIMINTA PUILLA JA RESIDUAALINEN
ÄÄRELLISYYS

LuK Oskari Tuomela

Pro gradu -tutkielma
Heinäkuu 2026

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

Tarkastajat:
Dos. Ilkka Törmä
FM, DI Mikko Jaskari

Turun yliopiston laatu järjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -järjestelmällä.

TURUN YLIOPISTO, Matematiikan ja tilastotieteen laitos

Pro gradu -tutkielma

Pääaine: Matematiikka

Tekijä: Oskari Tuomela

Otsikko: Vapaat ryhmät, niiden toiminta puilla ja residuaalinen äärellisyys

Ohjaaja: Dos. Ilkka Törmä

Sivumäärä: 27 sivua

Aika: Heinäkuu 2026

Tässä tutkielmassa tutkitaan vapaita ryhmiä ja niiden ominaisuuksia. Erityisesti tarkastelun kohteina ovat vapaiden ryhmien toiminnot puille ja vapaiden ryhmien residuaalinen äärellisyys.

Tutkielman kolmannessa luvussa määritellään vapaat ryhmät ja tutustutaan niiden konstruktion. Tämän jälkeen määritellään vapaan ryhmän aste Cantor-Bernsteinin lauseen avulla. Lisäksi tutustutaan sanojen redusoiuihin muotoihin ja esitellään Kleinin Ping-Pong lemma.

Tutkielman neljännessä luvussa tutustutaan graafeihin, erityisesti puihin. Tämän jälkeen esitellään joukon S generoiman ryhmän G Cayleyn graafi $\Gamma(G, S)$ ja tarkastellaan ryhmän toimintaa puilla.

Tutkielman viimeisessä luvussa tutkitaan residuaalista äärellisyyttä ja osoitetaan, että kaikki vapaat ryhmät ovat residuaalisesti äärellisiä.

Asiasanat: algebra, ryhmät, vapaat ryhmät, ryhmän toiminta, graafit, residuaalinen äärellisyys.

Sisällys

1	Johdanto	1
2	Ryhmäteorian peruskäsitteet	1
2.1	Ryhmä	1
2.2	Matriisiryhmät	2
2.3	Homomorfismit ja isomorfismit	3
2.4	Zornin lemma	3
2.5	Sanojen tulo	4
3	Vapaat ryhmät	4
3.1	Vapaiden ryhmien määritelmä ja konstruktio	4
3.2	Vapaan ryhmän aste	10
3.3	Redusoidut muodot	12
3.4	Kleinin Ping-Pong lemma	13
4	Vapaiden ryhmien toiminnot puille	15
4.1	Puut	15
4.2	Cayleyn graafi	19
4.3	Ryhmän toiminta puilla	19
5	Residuaalinen äärellisyys	22
5.1	Määritelmä ja esimerkkejä	22
5.2	Residuaalisesti äärellisten ryhmien stabiilisuusominaisuudet	24
5.3	Vapaiden ryhmien residuaalinen äärellisyys	25

1 Johdanto

Tämän tutkielman tarkoituksena on tutustua vapaisiin ryhmiin ja niiden ominaisuuksiin. Erityisesti tarkastelun kohteina ovat vapaiden ryhmän toiminnot puille sekä vapaiden ryhmien residuaalinen äärellisyys.

Luvussa 2 määritellään algebraan ja ryhmäteoriaan liittyviä termejä, jotta ne ovat selvillä tutkielman muissa luvuissa.

Luvussa 3 esitellään vapaat ryhmät ja niihin liittyviä ominaisuuksia. Vapaat ryhmät ovat ryhmiä, joiden alkioiden välillä ei ole relaatioita (ne ovat *vapaita* relaatioista). Vapaan ryhmän alkiot esitetään sanoina. Esimerkiksi joukon $S = \{a, b\}$ generoiman vapaan ryhmän $F(S)$ alkiot ovat sanat, jotka koostuvat kirjaimista a ja b sekä näiden käänteisalkioista a^{-1} ja b^{-1} . Tällaisia sanoja ovat muun muassa $a, b, aa, bb, ab, bab, aba, ab^{-1}ab$ ja $a^{-1}bab^{-1}a$. Lisäksi luvussa määritellään vapaan ryhmän aste Cantor-Bernsteinin lauseen avulla sekä tutustutaan sanojen redusoi-tuihin muotoihin ja esitellään Kleinin Ping-Pong lemma.

Luvussa 4 tutustutaan graafeihin ja tutkitaan ryhmien toimintaa graafeilla. Vuosina 1968-1969 Jean-Pierre Serre esitteli uuden menetelmän kombinatoriseen ryhmäteoriaan. Teorian yleisemmät tulokset ovat puolestaan Hyman Bassin ansiota, joten menetelmää kutsutaan usein Bass-Serre -teoriaksi. [1] Tässä tutkielmassa ollaan kuitenkin kiinnostuneempia teorian sivutuloksesta, että jos ryhmä toimii vapaasti jollekin puulle, se on vapaa ryhmä. Tämän avulla löydetään myös toinen tapa perustella, että vapaan ryhmän aliryhmät ovat myös vapaita ryhmiä.

Luvussa 5 perehdytään residuaalisesti äärellisiin ryhmiin, jotka ovat tärkeitä useilla matematiikan aloilla. Kuten nimestä voi päätellä, residuaalisesti äärelliset ryhmät ovat äärellisten ryhmien yleistys. Alaluvussa 5.1 ne määritellään ryhmiksi, joiden alkiot voidaan erottaa toisistaan äärellisten tekijäryhmien avulla, mutta on olemassa monia vastaavia määritelmiä. Lisäksi luvussa 5 tutkitaan, ovatko vapaat ryhmät residuaalisesti äärellisiä. [5]

Luku 2 perustuu pääosin teokseen [2], luvut 3 ja 5 teokseen [5] ja luku 4 teokseen [1].

Tutkielmassa on hyödynnetty tekoälyä lähdemateriaalin englanninkielisten termien kääntämiseen suomen kielelle.

2 Ryhmäteorian peruskäsitteet

Tämän luvun tarkoituksena on määritellä algebraan ja ryhmäteoriaan liittyviä termejä, joita hyödynnetään seuraavissa luvuissa. Alaluvut 2.1-2.4 perustuvat Dummitin ja Footen teokseen Abstract Algebra [2] ja alaluku 2.5 Ceccherini-Silbersteinin ja Coornaertin teokseen Cellular Automata and Groups [5].

2.1 Ryhmä

Määritelmä 1. *Ryhmä* G on epätyhjä joukko, joka suljettu jonkin binäärioperaation $*$ suhteen ja täyttää seuraavat ehdot:

1. $(a * b) * c = a * (b * c)$ kaikille $a, b, c \in G$ eli $*$ on assosiatiivinen.
2. On olemassa alkio e , jolle $a * e = e * a = a$ kaikille $a \in G$. Tätä alkioa

kutsutaan *identiteettialkioksi* ja sitä voidaan merkitä Id_G .

3. Jokaiselle $a \in G$ on olemassa *käänteisalkio* $a^{-1} \in G$, jolle $a * a^{-1} = a^{-1} * a = \epsilon$.

Jos ryhmä on lisäksi kommutatiivinen eli kaikille $a, b \in G$ $a * b = b * a$, niin ryhmää kutsutaan *Abelin ryhmäksi*.

Esimerkki 1. a) Joukot $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ja $\mathbb{C}$ ovat Abelin ryhmiä operaation $+$ (yhteenlasku) suhteen. Tällöin $\epsilon = 0$ ja $a^{-1} = -a$ kaikille a .

b) Joukot $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}, \mathbb{Q}^+$ ja $\mathbb{R}^+$ ovat Abelin ryhmiä operaation $\cdot$ (tulo) suhteen. Tällöin $\epsilon = 1$ ja $a^{-1} = \frac{1}{a}$ kaikille a .

Määritelmä 2. *Monoidi* on joukko, jossa on määritelty binäärioperaatio ja joka täyttää kaikki määritelmässä 1 esitetyt ryhmän ehdot lukuun ottamatta käänteisalkion olemassaolon ehtoa (ehto 3.).

Määritelmä 3. Yhden alkion a generoimaa ryhmää G kutsutaan *sykliseksi ryhmäksi*. Toisin sanoen on olemassa sellainen alkio $a \in G$, että $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$.

Määritelmä 4. *Ryhmän G toiminta* joukossa X on kuvaus joukon $G \times X$ joukkoon X . Tällä kuvauksella on seuraavat ominaisuudet:

1. $g_1 \circ (g_2 \circ x) = (g_1 g_2) \circ x$ kaikille $g_1, g_2 \in G$ ja $x \in X$ ja
2. $1 \circ x = x$ kaikille $x \in X$.

Määritelmä 5. Ryhmän G toiminnan joukossa X *ydin* määritellään joukoksi

$$\text{Ker}(G) = \{g \in G \mid gx = x \text{ kaikille } x \in X\}$$

eli ydin on joukko niiden ryhmän G alkioista, jotka pitävät kaikki joukon X alkiot samoina.

Seuraava määritelmä on lähteestä [4].

Määritelmä 6. Olkoon G ryhmä, joka toimii joukossa S . Olkoon $s \in S$. Joukon S osajoukkoa, joka koostuu kaikista alkioista gs , missä $g \in G$, merkitään Gs ja kutsutaan alkion s *radaksi* ryhmän G suhteen.

2.2 Matriisiryhmät

Kunta on algebrallinen rakenne, jossa kaikki peruslaskutoimitukset $(+, -, \cdot, \div)$ ovat voimassa.

Määritelmä 7. Joukko F on kunta laskutoimituksilla $+$ ja $\cdot$, jos

1. $(F, +)$ on Abelin ryhmä.
2. $(F \setminus \{0\}, \cdot)$ on Abelin ryhmä.
3. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ kaikilla $a, b, c \in F$.

Määritelmä 8. Olkoon $n \in \mathbb{Z}^+$ ja F on kunta. *Yleinen lineaarinen ryhmä* $\text{GL}_n(F)$ on kaikkien $n \times n$ -matriisien, joiden determinantti ei ole nolla, ryhmä eli

$$\text{GL}_n(F) = \{A \mid A \text{ on } n \times n \text{-matriisi, jonka alkiot ovat kunnasta } F \text{ ja } \det A \neq 0\}.$$

Määritelmä 9. *Erityinen lineaarinen ryhmä* $SL_n(F)$ on kaikkien $n \times n$ -matriisien, joiden determinantti on yksi, ryhmä eli

$$SL_n(F) = \{A \mid A \text{ on } n \times n \text{ -matriisi, jonka alkio } A \text{ on } F \text{ ja } \det A = 1\}.$$

2.3 Homomorfismit ja isomorfismit

Määritelmä 10. Kuvaus $f : A \rightarrow B$ tarkoittaa sääntöä, joka liittää yhden lähtöjoukon A alkion maalijoukon B alkioon. Kuvauksen f vaikutusta lähtöjoukon A alkioon a merkitään $f(a)$.

Määritelmä 11. Joukko

$$f(A) = \{b \in B \mid b = f(a), \text{ jollekin } a \in A\}$$

on maalijoukon B osajoukko ja sitä kutsutaan kuvauksen f *kuva*ksi ja se merkitään $\text{Im}(f)$.

Määritelmä 12. Olkoot $(G, *)$ ja $(H, \circ)$ ryhmiä. Kuvausta $\varphi : G \rightarrow H$, jolle

$$\varphi(x * y) = \varphi(x) \circ \varphi(y) \quad \text{kaikille } x, y \in G$$

kutsutaan *homomorfismiksi*. Homomorfismia φ ryhmältä G itselleen eli $\varphi : G \rightarrow G$ kutsutaan myös *endomorfismiksi* [4].

Määritelmä 13. Kuvausta $\varphi : G \rightarrow H$ kutsutaan *isomorfismiksi*, jos φ on homomorfismi ja bijektio.

Määritelmä 14. Olkoon $N \trianglelefteq G$. Tällöin homomorfismia $\pi : G \rightarrow G/N$, jossa $\pi(g) = gN$ kutsutaan *kanoniseksi* (tai *luonnolliseksi*) homomorfismiksi ryhmästä G joukkoon G/N .

2.4 Zornin lemma

Määritelmä 15. Epätyhjän joukon A *osittainen järjestys* on joukon A relaatio $\leq$, jolle pätee seuraavat ominaisuudet:

- (i) $x \leq x$ kaikille $x \in A$ (refleksiivisyys)
- (ii) jos $x \leq y$ ja $y \leq x$, niin $x = y$ kaikille $x, y \in A$ (antisymmetrisyys)
- (iii) jos $x \leq y$ ja $y \leq z$ niin $x \leq z$ kaikille $x, y, z \in A$ (transitiivisuus)

Määritelmä 16. Olkoon A epätyhjä joukko, joka on osittain järjestetty relaatiolla $\leq$.

- (i) Joukon A osajoukkoa B kutsutaan *ketjuksi*, jos kaikille $x, y \in B$ joko $x \leq y$ tai $y \leq x$.
- (ii) Joukon A osajoukon B *yläraja* on sellainen alkio $u \in A$, että $b \leq u$ kaikille $b \in B$.

- (iii) Joukon A *maksimialkio* on sellainen alkio $m \in A$, että jos $m \leq x$, mille tahansa $x \in A$, niin $m = x$.

Seuraavaa lemmaa kutsutaan **Zornin lemmaksi**.

Lemma 1. *Jos A on epätyhjä joukko, jolla on osittainen järjestys, ja jonka jokaisella ketjulla on yläraja niin joukolla A on maksimialkio.*

2.5 Sanojen tulo

Olkoon A joukko.

Sana aakkostojoukossa on joukon

$$A^* = \bigcup_{n \in \mathbb{N}} A^n$$

alkio, missä A^n on joukon A karteeminen tulo itsensä kanssa eli se koostuu kaikista n -monikoista $(a_1, a_2, \dots, a_n)$, missä $a_k \in A$ kaikille $1 \leq k \leq n$. Alkiota A^0 merkitään notaatiolla ϵ ja kutsutaan *tyhjäksi sanaksi*.

Kahden sanan $w = (a_1, a_2, \dots, a_n)$ ja $w' = (a'_1, a'_2, \dots, a'_n)$ tulo ww' määritellään

$$ww' = (a_1, a_2, \dots, a_n, a'_1, a'_2, \dots, a'_n).$$

Koska $\epsilon w = w \epsilon = w$ ja $(ww')w'' = w(w'w'')$ kaikille $w, w', w'' \in A^*$, A^* on monoidi tulolle, ja sen identiteettiialkio on ϵ .

Huomattavaa on, että jokainen sana $w = (a_1, a_2, \dots, a_n) \in A$ voidaan yksikäsitteisesti kirjoittaa joukon $A = A^1$ alkioden tuloina - erityisesti $w = a_1, a_2 \cdots, a_n$.

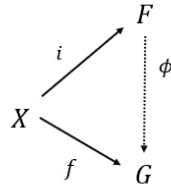
3 Vapaat ryhmät

Tässä luvussa tutustutaan vapaisiin ryhmiin ja niiden konstruktion. Lisäksi selvitetään, mikä on vapaan ryhmän aste ja tutustutaan sanojen redusoiuihin muotoihin. Lisäksi esitetään ja todistetaan Kleinin Ping-Pong lemma, jota hyödynnetään luvussa 5. Luku perustuu Ceccherini-Silbersteinin ja Coornaartin teoksen Cellular Automata and Groups [5] liitteeseen D.

3.1 Vapaiden ryhmien määritelmä ja konstruktio

Määritelmä 17. *Kantaan perustuva vapaa ryhmä* on kolmikko (F, X, i) , missä F on ryhmä, X on joukko ja $i : X \rightarrow F$ on kuvaus joukosta X ryhmään F , joka toteuttaa seuraavan universaaliominaisuuden: jokaiselle ryhmälle G ja mille tahansa kuvaukselle $f : X \rightarrow G$ on olemassa yksikäsitteinen homomorfismi $\phi : F \rightarrow G$, jolle $f = \phi \circ i$.

Ryhmää F kutsutaan *vapaaksi ryhmäksi*, jos on olemassa joukko X ja kuvaus $i : X \rightarrow F$ niin, että kolmikko (F, X, i) on kantaan perustuva vapaa ryhmä. Tällöin sanotaan, että (X, i) on ryhmän F *vapaa kanta* ja F on vapaa ryhmä kannalla (X, i) .



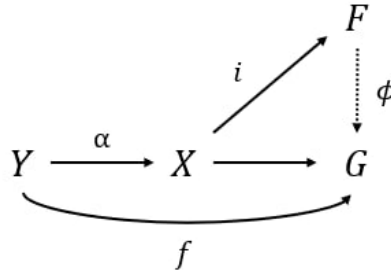
Kuva 1: Kuvaus i joukosta X ryhmään F , kuvaus f joukosta X ryhmään G sekä homomorfismi ϕ ryhmästä F ryhmään G .

Esimerkki 2. Olkoon joukko $X = \{a, b\}$. Tällöin joukon X generoiman vapaan ryhmän F alkiot ovat sanoja, jotka muodostuvat ryhmän S alkioista a ja b sekä näiden käänteisalkioista a^{-1} ja b^{-1} eli ryhmän F alkiot voidaan kirjoittaa

$$a^{i_1} b^{i_2} a^{i_3} b^{i_4} \dots a^{i_{n-1}} b^{i_n},$$

missä $i_k \in \mathbb{Z} \setminus \{0\}$, kaikille $1 \leq k \leq n$.

Huomautus 1. (a) Jos (F, X, i) on kantaan perustuva vapaa ryhmä ja $\alpha : Y \rightarrow X$ on bijektiivinen kuvaus joukolta Y joukkoon X , niin kolmikko $(F, X, \alpha \circ i)$ on myös kantaan perustuva vapaa ryhmä. Itse asiassa, jos $f : Y \rightarrow G$ on kuvaus joukolta Y ryhmään G niin on olemassa sellainen yksikäsitteinen homomorfismi $\phi : F \rightarrow G$, että $f = \phi \circ i \circ \alpha$ nimittäin yksikäsitteinen homomorfismi $\phi : F \rightarrow G$ täyttää ehdon $f \circ \alpha^{-1} = \phi \circ i$.



Kuva 2: Kuvaus i joukosta X ryhmään F , kuvaus f joukosta X ryhmään G sekä homomorfismi ϕ ryhmästä F ryhmään G .

(b) Jos (F, X, i) on kantaan perustuva vapaa ryhmä ja $\psi : F \rightarrow F'$ on isomorfismi ryhmältä F ryhmälle F' niin kolmikko $(F', X, \psi \circ i)$ on kantaan perustuva vapaa ryhmä. Itse asiassa, jos $f : X \rightarrow G$ on kuvaus joukosta X joukkoon G , on olemassa sellainen yksikäsitteinen homomorfismi $\phi' : F' \rightarrow G$, että $f = \phi' \circ \psi \circ i$ nimittäin kuvauksen $\phi' = \phi \circ \psi^{-1}$, antama homomorfismi, missä $\phi : F \rightarrow G$ on yksikäsitteinen homomorfismi, joka toteuttaa ehdon $f = \phi \circ i$.

Lause 1. Olkoon (F, X, i) kantaan perustuva vapaa ryhmä. Tällöin seuraavat ovat voimassa:

- (i) kuvaus i on injektio;
(ii) joukko $i(X)$ generoi ryhmän F ;
(iii) kolmikko (F, X', i') , missä $X' = i(X)$ ja $i' : X' \rightarrow F$ on sisältyiskuvaus, on myös kantaan perustuva vapaa ryhmä.

Todistus. (i) Olkoon x_1 ja x_2 kaksi erillistä joukon X alkia. Tarkastellaan kuvausta $f : X \rightarrow \mathbb{Z}/2\mathbb{Z}$, joka määritellään $f(x) = \bar{0}$, jos $x \neq x_2$ ja $f(x_2) = \bar{1}$. Koska (F, X, i) on kantaan perustuva vapaa ryhmä, on olemassa homomorfismi $\phi : F \rightarrow \mathbb{Z}/2\mathbb{Z}$, jossa $f = \phi \circ i$. Koska $f(x_1) \neq f(x_2)$ niin myös $i(x_1) \neq i(x_2)$, mistä seuraa, että i on injektio.

(ii) Olkoon H joukon $i(X)$ generoima ryhmän F aliryhmä. Tarkastellaan kuvausta $i_* : X \rightarrow H$, joka määritellään $i_*(x) = i(x)$ kaikilla $x \in X$. Koska (F, X, i) on kantaan perustuva vapaa ryhmä, on olemassa homomorfismi $\phi : F \rightarrow H$ niin, että $i_* = \phi \circ i$. Tarkastellaan seuraavaksi sisältyiskuvausta $\rho : H \rightarrow F$. Homomorfismit Id_F ja $\rho \circ \phi$ toteuttavat $\text{Id}_F \circ i = \rho \circ \phi \circ i$. Yksikäsitteisyyden nojalla $\text{Id}_F = \rho \circ \phi$. Tästä voidaan päätellä, että ρ on surjektio eli $H = F$. Näin ollen joukko $i(X)$ generoi ryhmän F .

(iii) Se, että (F, X', i') on kantaan perustuva vapaa ryhmä seuraa suoraan huomautuksesta 1(a), koska $i' = i \circ j^{-1}$, missä $j : X \rightarrow X'$ on bijektiivinen kuvaus, joka määritellään $j(x) = i(x)$ kaikilla $x \in X$. $\square$

Lauseen 1 kohdasta (iii) voidaan päätellä, että jos F on vapaa ryhmä, on olemassa sellainen osajoukko $X \subset F$, että kolmikko (F, X, i) , jossa $i : X \rightarrow F$ on sisältyiskuvaus, on kantaan perustuva vapaa ryhmä. Tällaista osajoukkoa $X \subset F$ kutsutaan tällöin *vapaaksi kantajoukoksi* tai lyhyemmin *kannaksi*.

Esimerkki 3. Olkoon F vapaa ryhmä kannalla $X = \{a, b\}$, missä $a \neq b$ ja $i : X \rightarrow F$ kuvaus, joka on määritelty niin, että

$$i(a) = a, \quad i(b) = b.$$

Tällöin

- (i) Kuvaus i on injektio, koska $i(a) = a \neq b = i(b)$.
(ii) Koska $i(X) = \{a, b\}$ ja vapaan ryhmän F alkiot ovat sanoja, jotka muodostuvat alkioista a ja b sekä näiden käänteisalkioista, generoi joukko $i(X)$ ryhmän F .
(iii) Koska $X' = i(X) = \{a, b\}$ ja $i' : X' \rightarrow F$ on sisältyiskuvaus, (F, X', i') on sama kantaan perustuva vapaa ryhmä kuin (F, X, i) .

Lause 2. Olkoon (F, X, i) kantaan perustuva vapaa ryhmä ja osajoukko $Y \subset X$. Olkoon K osajoukon Y generoima joukon F aliryhmä ja $j : Y \rightarrow K$ kuvaus, joka määritellään $j(y) = i(y)$ kaikille $y \in Y$. Tällöin (K, Y, j) on kantaan perustuva vapaa ryhmä.

Todistus. Olkoon G ryhmä ja $f : Y \rightarrow G$ kuvaus. Osoitetaan, että on olemassa yksikäsitteinen homomorfismi $\phi : K \rightarrow G$, joka toteuttaa ehdon $f = \phi \circ j$. Yksikäsitteisyys seuraa siitä, että $j(Y) = i(Y)$ generoi ryhmän K . Valitaan kuvaus $f' : X \rightarrow G$ laajentamaan kuvausta f . Koska (F, X, i) on kantaan perustuva vapaa

ryhmä, on olemassa homomorfismi $\phi' : F \rightarrow G$, jolle $f' = \phi' \circ i$. Tällöin homomorfismi $\phi = \phi'|_K : K \rightarrow G$ täyttää ehdon $f = \phi \circ j$. Tämä osoittaa, että (K, Y, j) on kantaan perustuva vapaa ryhmä. $\square$

Seuraus 1. *Olkoon i sisällysmiskuvaus ja F vapaa ryhmä kannalla $X \subset F$. Olkoon osajoukko $Y \subset X$ ja olkoon K joukon Y generoima ryhmän F aliryhmä. Tällöin K on vapaa ryhmä kannalla Y .*

Esimerkki 4. Olkoon F joukon $X = \{a, b\}$ generoima vapaa ryhmä ja joukko $Y = \{a\}$ joukon X osajoukko. Tällöin joukon Y generoima aliryhmä $K = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ on ääretön syklinen ryhmä. Määritellään kuvaus $j : Y \rightarrow K$ niin, että $j(a) = i(a) = a$ kaikille $a \in Y$. Tällöin (K, Y, j) on kantaan perustuva vapaa ryhmä.

Lause 3. *Olkoon (F_1, X_1, i_1) ja (F_2, X_2, i_2) kantaan perustuvia vapaita ryhmiä. Oletetaan, että on olemassa bijektiivinen kuvaus $u : X_1 \rightarrow X_2$. Tällöin on olemassa yksikäsitteinen ryhmäisomorfismi $\varphi : F_1 \rightarrow F_2$, jolle pätee $\varphi \circ i_1 = i_2 \circ u$. Kuvaukset on esitetty kuvassa 3.*

$$\begin{array}{ccc} X_1 & \xrightarrow{u} & X_2 \\ i_1 \downarrow & & \downarrow i_2 \\ F_1 & \xrightarrow{\varphi} & F_2 \end{array}$$

Kuva 3: Kuvaus $u : X_1 \rightarrow X_2$, kuvaus $i_1 : X_1 \rightarrow F_1$, kuvaus $i_2 : X_2 \rightarrow F_2$ ja kuvaus $\varphi : F_1 \rightarrow F_2$

Todistus. Koska (F_1, X_1, i_1) on kantaan perustuva vapaa ryhmä, on olemassa sellainen yksikäsitteinen homomorfismi $\varphi : F_1 \rightarrow F_2$, että $i_2 \circ u = \varphi \circ i_1$. Riittää osoittaa, että φ on bijektio. Koska (F_2, X_2, i_2) on kantaan perustuva vapaa ryhmä, on olemassa sellainen homomorfismi $\varphi' : F_2 \rightarrow F_1$, että $i_1 \circ u^{-1} = \varphi' \circ i_2$. Kuvaukset Id_{F_1} ja $\varphi' \circ \varphi$ ovat ryhmän F_1 endomorfismeja toteuttaen ehdot $\text{Id}_{F_1} \circ i_1 = i_1$ ja $(\varphi' \circ \varphi) \circ i_1 = i_1$. Koska (F_1, X_1, i_1) on kantaan perustuva vapaa ryhmä, yksikäsitteisyydestä seuraa, että $\text{Id}_{F_1} = \varphi' \circ \varphi$. Vastaavasti saadaan, että $\varphi \circ \varphi' = \text{Id}_{F_2}$. Tästä seuraa, että φ on bijektio. $\square$

Esimerkki 5. Olkoon F_1 vapaa ryhmä kannalla $X_1 = \{a, b\}$ ja F_2 vapaa ryhmä kannalla $X_2 = \{c, d\}$. Määritellään bijektiivinen kuvaus $u : X_1 \rightarrow X_2$ niin, että $u(a) = c$ ja $u(b) = d$. Lauseen 3 perusteella on olemassa yksikäsitteinen ryhmäisomorfismi $\varphi : F_1 \rightarrow F_2$, jolle pätee $\varphi \circ i_1 = i_2 \circ u$. Tällöin $\varphi(a) = c$ ja $\varphi(b) = d$. Tämä ryhmäisomorfismi vaihtaa generaattorien nimet niin, että ryhmään F_1 kuuluvat sanat muuttuvat ryhmään F_2 kuuluviksi sanoiksi. Esimerkiksi sanasta $a^{-2}ba^2b^{-1}$ tulee sana $c^{-2}dc^2d^{-1}$.

Lause 4. *Olkoon X joukko. Tällöin on olemassa sellaiset ryhmä F ja kuvaus $i : X \rightarrow F$, että kolmikko (F, X, i) on kantaan perustuva vapaa ryhmä.*

Todistus. Olkoon X' sellainen joukko, että se ei jaa alkioita ryhmän X kanssa eli $X \cap X' = \emptyset$ ja γ bijektiivinen kuvaus $\gamma : X \rightarrow X'$. Olkoon $A = X \cup X'$. Määritellään jokaiselle $a \in A$ alkio $\tilde{a} \in A$ asettamalla

$$\tilde{a} = \begin{cases} \gamma(a) & , \text{ kun } a \in X \\ \gamma^{-1}(a) & , \text{ kun } a \in X'. \end{cases}$$

Huomataan, että kuvaus $a \mapsto \tilde{a}$ on joukon A involuutio eli kaikille $a \in A$ pätee $\tilde{\tilde{a}} = a$.

Tarkastellaan seuraavaksi joukkoa A^* , joka koostuu kaikista aakkostojoukon A sanoista.

Sana $w \in A^*$ voidaan saada sanasta $w' \in A^*$ alkeisreduktiolla, jos on olemassa alkio $a \in A$ ja sanat $u, v \in A^*$ niin, että $w = uv$ ja $w' = ua\tilde{a}v$. Koska sanat $w, w' \in A^*$, voimme kirjoittaa $w \sim w'$, jos joko sanan w voi saada alkeisreduktiolla sanasta w' tai sanan w' voi saada sanasta w alkeisreduktiolla. Kun $w, w' \in A^*$, määritellään relaatio $\equiv$ joukolle A^* kirjoittamalla $w \equiv w'$, jos ja vain jos on olemassa kokonaisluku $n \geq 1$ ja sellainen sanojen $w_1, w_2, \dots, w_n \in A^*$ ketju, jossa $w_1 = w$ ja $w_n = w'$ niin, että $w_i \sim w_{i+1}$ kullekin $i = 1, 2, \dots, n-1$. On nopeaa tarkistaa, että $\equiv$ on ekvivalenssirelaatio joukossa A^* . Merkinnällä $[w]$ tarkoitetaan alkion $w \in A^*$ ekvivalenssiluokkaa ja tarkastellaan tekijäjoukkoa $F = A^*/\equiv$ eli joukkoa, joka sisältää kaikki ekvivalenssiluokat $[w], w \in A^*$. Havaitaan, että jos $u, u', v \in A^*$ ja $u \sim u'$, niin $uv \sim u'v$ ja $vu \sim vu'$. Tästä havainnosta seuraa, että jos sanat $u, v, u', v' \in A^*$ toteuttavat ehdot $u \equiv u'$ ja $v \equiv v'$ niin $uv \equiv u'v'$, joten voimme määritellä ekvivalenssiluokkien $[u]$ ja $[v]$ tulon ryhmässä F asettamalla

$$[u][v] = [uv].$$

Osoitetaan, että tästä tulosta saadaan ryhmän F rakenne. Assosiativisuus seuraa suoraan joukon A^* sanojen ketjutuksen assosiativisuudesta. Kaikille $u, v, w \in A^*$ pätee

$$([u][v])[w] = [uv][w] = [(uv)w] = [u(vw)] = [u][vw] = [u]([v][w]).$$

Toisaalta kaikille $w \in A^*$ pätee

$$[\epsilon][w] = [\epsilon w] = [w] \quad \text{ja} \quad [w][\epsilon] = [w\epsilon] = [w],$$

mikä osoittaa, että $[\epsilon]$ on identiteettialkio. Osoitetaan sitten, että jokaisella ryhmän F alkiolla on käänteisalkio. Määritetään sanalle $w = a_1 a_2 \dots a_n \in A^*$, missä $n \geq 0$ ja $a_k \in A$ kaikille $1 \leq k \leq n$, sana $\tilde{w} \in A^*$ siten, että

$$\tilde{w} = \tilde{a}_n \widetilde{a_{n-1}} \dots \tilde{a}_1.$$

Havaitaan, että

$$\begin{aligned} w\tilde{w} &= a_1 a_2 \dots a_n \tilde{a}_n \dots \tilde{a}_2 \tilde{a}_1 \\ &\sim a_1 \dots a_{n-1} \widetilde{a_{n-1}} \dots \tilde{a}_1 \\ &\vdots \\ &\sim a_1 a_2 \tilde{a}_2 \tilde{a}_1 \\ &\sim a_1 \tilde{a}_1 \\ &\sim \epsilon. \end{aligned}$$

Siten saadaan $w\tilde{w} \equiv \epsilon$ eli $[w][\tilde{w}] = [w\tilde{w}] = [\epsilon]$. Samalla tavalla saadaan $[\tilde{w}][w] = [\epsilon]$. Tästä seuraa, että $\tilde{w}$ on sanan $[w]$ käänteissana ryhmän F tulo-operaation suhteen. Tämä osoittaa, että F on ryhmä. Tarkastellaan seuraavaksi kuvausta $i : X \rightarrow F$, joka määrittää siten, että $i(x) = [x]$ kaikille $x \in X$. Jos $w = a_1a_2 \cdots a_n \in A^*$, missä $a_k \in A$ kaikille $1 \leq k \leq n$, niin

$$[w] = [a_1a_2 \cdots a_n] = [a_1][a_2] \cdots [a_n].$$

Koska $[a] = i(a)$, jos $a \in X$ ja $[a] = [\tilde{a}]^{-1} = i(\tilde{a})^{-1}$, jos $a \in X'$, voimme päätellä, että $i(X)$ generoi ryhmän F .

Osoitetaan seuraavaksi, että kolmikko (F, X, i) on kantaan perustuva vapaa ryhmä. Oletetaan, että $f : X \rightarrow G$ on kuvaus joukosta X ryhmään G . Meidän on osoitettava, että on olemassa sellainen yksikäsitteinen homomorfismi $\phi : F \rightarrow G$, että $f = \phi \circ i$. Koska $i(X)$ generoi ryhmän F , homomorfismi on yksikäsitteinen. Konstruoidakseen homomorfismin ϕ on laajennettava kuvausta f kuvauksella $g : A \rightarrow G$ asettamalla

$$g(a) = \begin{cases} f(a) & , \text{ kun } a \in X \\ f(\tilde{a})^{-1} & , \text{ kun } a \in X'. \end{cases}$$

Havaitaan, että $g(\tilde{a}) = g(a)^{-1}$ kaikille $a \in A$. Määrittää nyt kuvaus $\Phi : A^* \rightarrow G$ asettamalla

$$\Phi(w) = g(a_1)g(a_2) \cdots g(a_n)$$

kaikille $w = a_1a_2 \cdots a_n \in A^*$. Tällöin saadaan

$$\Phi(ww') = \Phi(w)\Phi(w') \tag{1}$$

kaikille $w, w' \in A^*$. Lisäksi jos w saadaan sanasta w' jonkin alkeisreduktion avulla eli $w = uv$ ja $w' = ua\tilde{v}$ jollekin $a \in A$ ja $u, v \in A^*$, niin

$$\Phi(w') = \Phi(u)g(a)g(\tilde{a})\Phi(v) = \Phi(u)g(a)g(a)^{-1}\Phi(v) = \Phi(u)\Phi(v) = \Phi(w).$$

Tästä seuraa, että $\Phi(w) = \Phi(w')$ aina, kun $w, w' \in A^*$ toteuttaa ehdon $w \sim w'$. Induktiolla voimme päätellä, että $\Phi(w) = \Phi(w')$ kaikilla sellaisilla $w, w' \in A^*$, että $w \equiv w'$. Täten voimme määrittää kuvauksen $\phi : F \rightarrow G$ asettamalla $\phi([w]) = \Phi(w)$ kaikille $w \in A^*$. Yhtälön (1) avulla saadaan

$$\phi([w][w']) = \phi([ww']) = \Phi([ww']) = \Phi(w)\Phi(w') = \phi([w])\phi([w']).$$

Tällöin ϕ on ryhmähomomorfismi. Toisaalta kaikille $x \in X$ on voimassa

$$\phi \circ i(x) = \phi([x]) = g(x) = f(x),$$

mikä osoittaa, että $\phi \circ i = f$. Näin ollen kolmikko (F, X, i) on kantaan perustuva vapaa ryhmä. $\square$

Esimerkki 6. Sanan $w = a^{-2}ba^2b^{-1}$ kanssa samassa ekvivalenssiluokassa $[w]$ ovat sanat, joista sana w on saatavissa alkeisreduktioilla ja sanat, jotka on saatavissa alkeisreduktioilla sanasta w .

(a) Ekvivalenssiluokkaan $[w]$ kuuluvat esimerkiksi sanat $w' = a^{-2}baa^{-1}a^2b^{-1}$ ja $w'' = a^{-2}ba^{-1}a^3b^{-1}b^3b^{-3} = a^{-2}ba^{-1}aa^2b^{-1}b^3b^{-3}$.

(b) Sana $u = a^2ba^{-2}b^{-1} \notin [w]$, koska sitä ei saa muodostettua alkeisreduktioilla sanasta w eikä siitä saa alkeisreduktioilla muodostettua sanaa w .

3.2 Vapaan ryhmän aste

Kaksi joukkoa X_1 ja X_2 ovat *yhtä mahtavia* eli niillä on sama *kardinaliteetti*, jos on olemassa bijektiivinen kuvaus $u : X_1 \rightarrow X_2$. Jos G_1 ja G_2 ovat ryhmiä, käytetään kaikkien homomorfismien $\phi : G_1 \rightarrow G_2$ joukosta merkintää $\text{Hom}(G_1, G_2)$. Merkitään kaikkien joukon X osajoukkojen joukkoa puolestaan merkinnällä $\mathcal{P}(X)$.

Lemma 2. *Olkoon F vapaa ryhmä kannalla $X \subset F$. Tällöin joukot $\text{Hom}(F, \mathbb{Z}/2\mathbb{Z})$ ja $\mathcal{P}(X)$ ovat yhtä mahtavat.*

Todistus. Koska F on vapaa ryhmä kannalla X , jokainen kuvaus $f : X \rightarrow \mathbb{Z}/2\mathbb{Z}$ voidaan yksikäsitteisesti laajentaa homomorfismiksi $\phi : F \rightarrow \mathbb{Z}/2\mathbb{Z}$. Täten rajoituskuvaus tuottaa bijektion joukosta $\text{Hom}(F, \mathbb{Z}/2\mathbb{Z})$ joukkoon, johon kuuluvat kaikki kuvaukset joukosta X joukkoon $\mathbb{Z}/2\mathbb{Z}$. Tästä seuraa, että joukot $\text{Hom}(F, \mathbb{Z}/2\mathbb{Z})$ ja $\mathcal{P}(X)$ ovat yhtä mahtavat. $\square$

Seuraavaa lausetta kutsutaan **Cantor-Bernsteinin lauseeksi** tai **Schröder-Bernsteinin lauseeksi**. Lauseen todistus on lähteestä [3]

Lause 5. *Olkoon X ja Y kaksi joukkoa. Oletetaan, että on olemassa injektiiviset kuvaukset $f : X \rightarrow Y$ ja $g : Y \rightarrow X$. Tällöin on olemassa bijektiivinen kuvaus $h : X \rightarrow Y$.*

Todistus. Olkoon $f : X \rightarrow Y$ ja $g : Y \rightarrow X$ injektiivisiä kuvauksia. On kätevää olettaa, että joukoilla X ja Y ei ole yhteisiä alkioita. Vaikka näin ei olisikaan, voimme helposti muokata joukkoja siten, että tämä lisäoletus ei aiheuta yleisyyden menetyksiä.

Kutsutaan joukon X alkioita x joukon Y alkion $f(x)$ *vanhemmaksi*. Vastaavasti joukon Y alkio y on joukon X alkion $g(y)$ vanhempi. Tällöin joukon X alkiolla x on äärettömän pituinen sarja *jälkeläisiä* $(f(x), g(f(x)), f(g(f(x))), \dots)$. Vastaavasti joukon Y alkiolla y on äärettömän monta jälkeläistä. Tämän määritelmän mukaan jokainen sarjan jäsen on kunkin sen edeltävän jäsenen jälkeläinen. Sanotaan myös, että kukin sarjan jäsen on kaikkien sen jälkeisten jäsenten *esi-isä*.

Jokaiselle joukon X tai Y alkiolle on oltava joko 1. joukon X alkio, jolla ei ole vanhempaa (nämä *orvot* ovat täsmälleen joukon $X \setminus g(Y)$ alkiot), 2. joukon Y alkio, jolla ei ole vanhempaa (joukon $Y \setminus f(X)$ alkiot) tai 3. esi-isien sarja jatkuu äärettömästi taaksepäin. Olkoon X_X niiden joukon X alkioden joukko, joiden alkuperä on joukossa X eli se koostuu joukon $X \setminus g(Y)$ alkioista sekä niiden sellaisista jälkeläisistä, jotka kuuluvat joukkoon X . Olkoon joukko X_Y puolestaan niiden joukon X alkioden joukko, joiden alkuperä on joukossa Y eli se koostuu niistä joukon X alkioista, jotka ovat joukon $Y \setminus f(X)$ alkioden jälkeläisiä. Olkoon X_∞ niiden joukon X alkioden joukko, joilla ei ole esi-isää, jolla ei olisi vanhempia. Vastaavasti joukko Y voidaan jakaa kolmeen joukkoon Y_X , Y_Y ja Y_∞ .

Jos $x \in X_X$, niin $f(x) \in Y_X$ ja itse asiassa kuvauksen f rajoittuma joukolle X_X on bijektio joukkojen X_X ja Y_X välillä. Jos puolestaan $x \in X_Y$, niin x kuuluu käänteiskuvauksen g^{-1} määrittelyjoukkoon ja $g^{-1}(x) \in Y_Y$. Tällöin kuvauksen g^{-1} rajoittuma joukolle X_Y on bijektio joukkojen X_Y ja Y_Y välillä. Lopuksi, jos $x \in X_\infty$, niin $f(x) \in Y_\infty$ ja kuvauksen f rajoittuma joukolle X_∞ on bijektio joukkojen X_∞ ja Y_∞ välillä. Yhdistämällä nämä kolme bijektiota saadaan, bijektio joukkojen X ja Y väliin. $\square$

Lemma 3. *Olkoon ryhmä F vapaa ryhmä kannalla $X \subset F$. Oletetaan, että joukko X on ääretön. Tällöin joukot X ja F ovat yhtä mahtavat.*

Todistus. Olkoon $A = X \cup X^{-1}$. Koska joukko X generoi ryhmän F , kuvaus $\rho : A^* \rightarrow F$, joka määritellään ehdolla $\rho(a_1, a_2, \dots, a_n) = a_1 a_2 \cdots a_n$ on surjektio. Koska X on ääretön, ovat joukot X , A ja A^* yhtä mahtavia. Soveltamalla lausetta 5 voidaan päätellä, että X ja F ovat yhtä mahtavia. $\square$

Lause 6. *Olkoon F_1 vapaa ryhmä kannalla $X_1 \subset F_1$ ja F_2 vapaa ryhmä kannalla $X_2 \subset F_2$. Tällöin ryhmät F_1 ja F_2 ovat isomorfiset jos ja vain jos joukot X_1 ja X_2 ovat yhtä mahtavat.*

Todistus. Lauseesta 3 seuraa, että joukkojen X_1 ja X_2 yhtä mahtavuus johtaa siihen, että ryhmät F_1 ja F_2 ovat isomorfiset.

Oletetaan, että on olemassa isomorfismi $\alpha : F_1 \rightarrow F_2$. Tällöin α indusoi bijektiivisen kuvauksen joukkojen $\text{Hom}(F_1, \mathbb{Z}/2\mathbb{Z})$ ja $\text{Hom}(F_2, \mathbb{Z}/2\mathbb{Z})$ välille. Lemmasta 2 seuraa, että joukot $\mathcal{P}(X_1)$ ja $\mathcal{P}(X_2)$ ovat yhtä mahtavat. Jos X_1 on ääretön niin silloin myös X_2 on ääretön, jolloin X_1 ja X_2 ovat lemmän 3 perusteella yhtä mahtavia. Toisaalta, jos X_1 on äärellinen niin siitä, että $\mathcal{P}(X_1)$ ja $\mathcal{P}(X_2)$ ovat yhtä mahtavia seuraa, että myös X_2 on äärellinen ja $2^{|X_1|} = 2^{|X_2|}$. Tästä seuraa, että $|X_1| = |X_2|$, jolloin joukot X_1 ja X_2 ovat yhtä mahtavia myös tässä tapauksessa. $\square$

Esimerkki 7. Olkoon F_1 ja F_2 joukkojen $X_1 = \{a, b\}$ ja $X_2 = \{c, d\}$ generoimia kantaan perustuvia vapaita ryhmiä. Koska sekä joukossa X_1 että X_2 on kaksi alkioita, ne ovat yhtä mahtavia. Tällöin vapaiden ryhmien F_1 ja F_2 välillä on isomorfismi $\varphi : F_1 \rightarrow F_2$. Tämä havaittiin myös esimerkissä 5.

Esimerkki 8. Olkoon F_1 ja F_2 joukkojen $X_1 = \{a, b\}$ ja $X_2 = \{a\}$ generoimia kantaan perustuvia vapaita ryhmiä. Koska $|X_1| = 2 \neq 1 = |X_2|$, joukot X_1 ja X_2 eivät ole yhtä mahtavia. Tällöin vapaiden ryhmien F_1 ja F_2 välillä ei ole isomorfismia.

Seuraus 2. *Olkoon F vapaa ryhmä ja joukot $X_1, X_2 \subset F$ ryhmän F kantoja. Tällöin joukot X_1 ja X_2 ovat yhtä mahtavat.*

Lauseesta 4 seuraa, että mielivaltaiselle joukolle X on olemassa kantaan perustuva vapaa ryhmä (F, X, i) . Merkitään notaatiolla F_k vapaata ryhmää, jonka kantana on joukko $\{1, 2, \dots, k\}$ mille tahansa $k \in \mathbb{N}$.

Olkoon F vapaa ryhmä. Seurauksen 2 perusteella kannan $X \subset F$ kardinaliteetti riippuu vain ryhmästä F . Tätä kardinaliteettia kutsutaan ryhmän F *asteeksi*. Lauseen 6 perusteella vapaat ryhmät ovat isomorfisia jos ja vain jos ne ovat samaa astetta. Ryhmä on äärellistä astetta $k \in \mathbb{N}$ oleva vapaa ryhmä jos ja vain jos se on isomorfinen ryhmän F_k kanssa, toisin sanoen sen kannassa on k alkioita.

Esimerkki 9. Olkoon F joukon $X = \{a, b\}$ generoima vapaa ryhmä. Koska $|X| = 2$, joukko X on yhtä mahtava ryhmän F_2 kannan $\{1, 2\}$ kanssa. Tällöin lauseen 6 perusteella F on isomorfinen ryhmän F_k kanssa eli F on astetta 2 oleva vapaa ryhmä.

3.3 Redusoidut muodot

Sanan $w \in A^*$ sanotaan olevan *redusoitu*, jos se ei sisällä muotoa $a\tilde{a}$, missä $a \in A$, olevaa alisanaa eli ei ole olemassa sanaa $w' \in A^*$, jonka voisi saada sanasta w pelkillä alkeisreduktioilla. Huomattavaa on, että tyhjä sana ϵ on redusoitu ja kaikki redusoidun sanan alisanat ovat redusoituja.

Lause 7. *Jokainen relaation $\equiv$ ekvivalenssiluokka sisältää yksikäsitteisen redusoidun sanan.*

Todistus. Selvästi mikä tahansa sana $w \in A^*$ voidaan muuntaa redusoituun muotoon äärellisellä määrällä alkeisreduktioita. Tämä osoittaa redusoidun sanan olemassaolon missä tahansa relaation $\equiv$ ekvivalenssiluokassa.

Todistetaan yksikäsitteisyys. Tarkastellaan aliryhmää $R \subset A^*$, joka koostuu kaikista redusoiduista sanoista. Jokaiselle $a \in A$ ja $r \in R$ määritellään sana $\alpha_a(r)$

$$\alpha_a(r) = \begin{cases} w & , \text{ jos } r = \tilde{a}w, \text{ jollekin } w \in A^*, \\ ar & \text{ muuten.} \end{cases}$$

Huomattavaa on, että sana $\alpha_a(r)$ on aina redusoitu. Siten saadaan kuvaus $\alpha_a : R \rightarrow R$, joka on määritelty kaikille $a \in A$. Osoitetaan, että

$$\alpha_a \circ \alpha_{\tilde{a}} = \alpha_{\tilde{a}} \circ \alpha_a = \text{Id}_R. \quad (2)$$

Olkoon $a \in A$ ja tarkastellaan mielivaltaista alkioita $r \in R$. Jos $r = aw$ jollekin $w \in A^*$, niin $\alpha_{\tilde{a}}(r) = w$ ja siten $\alpha_a(\alpha_{\tilde{a}}(r)) = \alpha_a(w) = aw = r$ (huomattavaa on, että w ei voi alkaa alkiolla $\tilde{a}$, koska r on redusoitu sana). Muussa tapauksessa $\alpha_{\tilde{a}}(r) = \tilde{a}r$ ja siten $\alpha_a(\alpha_{\tilde{a}}(r)) = \alpha_a(\tilde{a}r) = r$. Tästä seuraa, että $\alpha_a \circ \alpha_{\tilde{a}} = \text{Id}_R$. Korvaamalla alkion a alkiolla $\tilde{a}$ tässä yhtälössä saadaan $\alpha_{\tilde{a}} \circ \alpha_a = \text{Id}_R$, koska $\sim$ on joukon A involuutio. Tämä todistaa yhtälön (2).

Yhtälöstä (2) voidaan päätellä, että α_a on bijektio joukossa R kaikille $a \in A$. Asettamalla

$$\rho(w) = \alpha_{a_1} \circ \alpha_{a_2} \circ \cdots \circ \alpha_{a_n}$$

jokaiselle sanalle $w = a_1a_2 \cdots a_n \in A^*$ saadaan monoidi homomorfismi $\rho : A^* \rightarrow \text{Sym}(R)$. On huomioitava, että

$$\rho(r)(\epsilon) = r \quad \text{kaikille } r \in R. \quad (3)$$

Toisaalta yhtälöstä (2) seuraa suoraan, että $\rho(w) = \rho(w')$ aina kun $w, w' \in A^*$ täyttää ehdon $w \equiv w'$. Siten jos r_1 ja r_2 ovat redusoituja sanoja samassa relaation $\equiv$ ekvivalenssiluokassa, saadaan $\rho(r_1) = \rho(r_2)$ ja siten soveltamalla yhtälöä (3) saadaan $r_1 = r_2$. $\square$

Seuraus 3. *Olkoon (F, X, i) kantaan perustuva vapaa ryhmä. Tällöin jokainen alkio $f \in F$ voidaan yksikäsitteisesti kirjoittaa muodossa*

$$f = i(x_1)^{h_1} i(x_2)^{h_2} \cdots i(x_n)^{h_n}, \quad (4)$$

missä $n \geq 0, x_i \in X$ ja $h_i \in \mathbb{Z} \setminus \{0\}$ kaikille $1 \leq i \leq n$ ja $x_i \neq x_{i+1}$ kaikille $1 \leq i \leq n-1$.

Todistus. Oletetaan, että (F, X, i) on lauseen 4 todistuksessa konstruoitu kantaan perustuva vapaa ryhmä. Rakenteen perusteella alkio $f \in F$ on relaation $\equiv$ mukainen ekvivalenssiluokka. Lauseen 7 mukaan tämä ekvivalenssiluokka sisältää redusoidun sanan r , joka voidaan yksikäsitteisesti kirjoittaa

$$r = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n},$$

missä $n \geq 0$, $a_i \in A$ ja $k_i \in \mathbb{N} \setminus \{0\}$ kaikille $1 \leq i \leq n$ ja $a_i \neq a_{i+1}$ kaikille $1 \leq i \leq n-1$. Tällöin saamme yhtälön (4) mukaisen lausekkeen, jossa $x_i = a_i$ ja $h_i = k_i$, jos $a_i \in A$ ja muulloin $x_i = \tilde{a}_i$ ja $h_i = -k_i$. Lausekkeen yksikäsitteisyys seuraa redusoidun sanan $r \in f$ yksikäsitteisyydestä. $\square$

Määritelmä 18. Yhtälön (4) mukaista lauseketta kutsutaan alkion f *reduoiduksi muodoksi* kantaan perustuvassa vapaassa ryhmässä (F, X, i) .

Seuraus 4. Olkoon G ryhmä. Olkoon $U \subset G$ sellainen ryhmän G osajoukko, että

$$u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n} \neq 1_G \quad (5)$$

kaikille $u_1, u_2, \dots, u_n \in U$ ja $k_1, k_2, \dots, k_n \in \mathbb{Z} \setminus \{0\}$, missä $u_i \neq u_{i+1}$ kaikille $1 \leq i \leq n-1$. Tällöin osajoukon U generoima ryhmän G aliryhmä on vapaa ryhmä kannalla U .

Todistus. Olkoon H osajoukon U generoima ryhmän G aliryhmä ja $\iota : U \rightarrow H$ sisältyiskuvaus. Olkoon (F, U, i) kantaan perustuva vapaa ryhmä. Tällöin on olemassa sellainen yksikäsitteinen homomorfismi $\phi : F \rightarrow H$, että $\iota = \phi \circ i$. Koska $\phi(i(U)) = \iota(U) = U$ generoi ryhmän H , ϕ on surjektio. Osoitetaan, että ϕ on myös injektio. Tarkastetaan alkioita $f \in F$ kirjoitettuna redusoidussa muodossa eli muodossa $f = i(u_1)^{h_1} i(u_2)^{h_2} \cdots i(u_n)^{h_n}$, missä $n \geq 0$, $u_i \in U$ ja $h_i \in \mathbb{Z} \setminus \{0\}$ kaikille $1 \leq i \leq n$ ja $u_i \neq u_{i+1}$ kaikille $1 \leq i \leq n-1$. Tällöin $\phi(f) = u_1^{h_1} u_2^{h_2} \cdots u_n^{h_n}$, koska $\phi(i(u_i)) = \iota(u_i) = u_i$ kaikille $1 \leq i \leq n$. Epäyhtälöstä (5) seuraa, että $\phi(f) = 1_H$ jos ja vain jos $n = 0$ eli jos ja vain jos $f = 1_F$. Tämä osoittaa, että ϕ on isomorfismi. Huomautuksesta 1 seuraa, että (H, U, ι) on kantaan perustuva vapaa ryhmä. $\square$

3.4 Kleinin Ping-Pong lemma

Seuraavaa Kleinin Ping-Pong lemmaksi kutsuttua lausetta käytetään usein todistamaan, että ryhmä on vapaa.

Lause 8. Olkoon G ryhmä ja olkoon X generoiva ryhmän G osajoukko, jolla on vähintään kaksi erillistä alkioita. Oletetaan, että G toimii joukossa E ja että on olemassa sellaisten epätyhjien joukon E osajoukkojen, joilla pareittain ei ole yhteisiä alkioita, perhe $(A_x)_{x \in X}$ niin, että

$$x^k \left(\bigcup_{y \in X \setminus \{x\}} A_y \right) \subset A_x \text{ kaikille } x \in X \text{ ja } k \in \mathbb{Z} \setminus \{0\}. \quad (6)$$

Tällöin G on vapaa ryhmä kannalla X .

Todistus. Tarkastellaan alkioita $g \in G$, joka on kirjoitettu epätriviaalina redusoituna sanana generaattorijoukossa X eli muodossa

$$g = x_1^{k_1} x_2^{k_2} \dots x_n^{k_n},$$

missä $n \geq 1$, $x_i \in X$ ja $k_i \in \mathbb{Z} \setminus \{0\}$ kaikilla $1 \leq i \leq n$ ja $x_i \neq x_{i+1}$ kaikilla $1 \leq i \leq n-1$. Seurauksen 4 perusteella, pitää osoittaa, että $g \neq 1_G$.

Oletetaan ensin, että joko joukko X sisältää vähintään kolme alkioita tai joukkoon X kuuluu täsmälleen kaksi alkioita ja $x_1 = x_n$. Tässä tapauksessa on löydettävissä sellainen alkio $y \in X$, että $y \neq x_1$ ja $y \neq x_n$. Soveltamalla ominaisuutta (6) peräkkäin saadaan

$$\begin{aligned} gA_y &= x_1^{k_1} x_2^{k_2} \dots x_{n-2}^{k_{n-2}} x_{n-1}^{k_{n-1}} x_n^{k_n} A_y \\ &\subset x_1^{k_1} x_2^{k_2} \dots x_{n-2}^{k_{n-2}} x_{n-1}^{k_{n-1}} A_{x_n} \\ &\subset x_1^{k_1} x_2^{k_2} \dots x_{n-2}^{k_{n-2}} A_{x_{n-1}} \\ &\subset x_1^{k_1} x_2^{k_2} \dots A_{x_{n-2}} \\ &\dots \\ &\subset x_1^{k_1} x_2^{k_2} A_{x_3} \\ &\subset x_1^{k_1} A_{x_2} \\ &\subset A_{x_1}. \end{aligned}$$

Koska joukot A_y ja A_{x_1} eivät sisällä samoja alkioita ja $A_y \neq \emptyset$, voidaan päätellä, että $g \neq 1_G$.

Tarkastellaan sitten tapausta, jossa joukossa X on täsmälleen kaksi alkioita ja $x_1 \neq x_n$. Tällöin

$$x_1^{k_1} g x_1^{-k_1} = x_1^{2k_1} x_2^{k_2} x_3^{k_3} \dots x_n^{k_n} x_1^{-k_1}$$

on sanan $x_1^{k_1} g x_1^{-k_1}$ redusoitu muoto. Ensimmäisen tapauksen perusteella $x_1^{k_1} g x_1^{-k_1} \neq 1_G$. Voidaan siis päätellä, että tässäkin tapauksessa $g \neq 1_G$. $\square$

Seuraus 5. *Olko F toisen asteen vapaa ryhmä ja kokonaisluku $n \geq 2$. Tällöin ryhmä F sisältää vapaan asteen n aliryhmän.*

Todistus. Oletetaan, että ryhmän F kanta on alkio a ja b . Olko G ryhmän F aliryhmä, jonka generoi osajoukko

$$X = \{a^i b a^{-i} : 0 \leq i \leq n-1\}.$$

Tarkastellaan vasemmanpuoleisen kertolaskun antamaa ryhmän G toimintaa ryhmään F . Määritellään, että jokaiselle $x = a^i b a^{-1} \in X$ aliryhmä $A_x \subset F$ on niiden ryhmän F alkiodien joukko, joiden redusoitu muoto alkaa $a^i b^k$ jollekin $k \in \mathbb{Z} \setminus \{0\}$. Osajoukot $A_x, x \in X$ selvästi toteuttavat lauseen 8 oletukset, joten ryhmä G on vapaa ryhmä kannalla X . $\square$

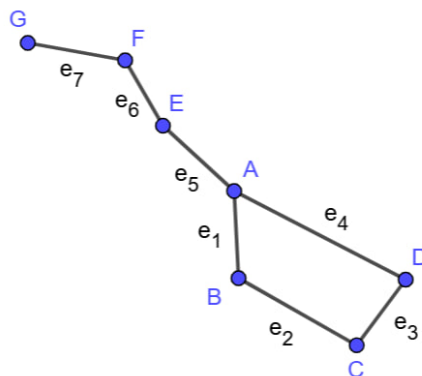
4 Vapaiden ryhmien toiminnot puille

Tässä luvussa tutustutaan graafiteoriaan ja siihen liittyviin käsitteisiin. Lisäksi esitellään Cayleyn graafi ja tarkastellaan mitä tapahtuu, kun ryhmä toimii eri graafeissa. Esitellään myös toinen tapa osoittaa, että vapaan ryhmän aliryhmät ovat vapaita. Luku perustuu Cohenin teoksen Combinatorial Group Theory: A Topological Approach [1] lukuihin 5–8.

4.1 Puut

Määritelmä 19. *Graafi* Γ koostuu kahdesta joukosta, joilla ei ole yhteisiä alkioita. Nämä joukot ovat graafin Γ kärkien joukko $V(\Gamma)$ ja graafin Γ sivujen joukko $E(\Gamma)$. Lisäksi graafin Γ kuuluvat kuvaukset $\sigma : E(\Gamma) \rightarrow V(\Gamma)$ ja $\tau : E(\Gamma) \rightarrow E(\Gamma)$ niin, että kaikille $e \in E(\Gamma)$ $e \neq \bar{e}$ ja $e = \bar{\bar{e}}$. Määritellään myös funktio $\tau : E(\Gamma) \rightarrow V(\Gamma)$ siten, että $e\tau = \bar{e}\sigma$. Tällöin sanotaan, että $e\sigma$ on sivun e *alku* ja $e\tau$ on sivun e *loppu*.

Määritelmä 20. *Polku*, jonka pituus on $n > 0$ graafissa Γ on äärellinen sarja sellaisia sivuja $e_1, e_2, \dots, e_n$, että $e_i\tau = e_{i+1}\sigma$ kaikille $i < n$. Polun alku on sivun e_1 alku eli $e_1\sigma$ ja polun loppu on sivun e_n loppu eli $e_n\tau$. Polun kärjet ovat $e_i\sigma$ kaikille $i \leq n$ sekä $e_n\tau$. Polku, jonka pituus on nolla, koostuu vain kärjestä v ja tällöin v on sekä polun alku että loppu. *Silmukka* on polku, jonka alkuna ja loppuna on sama kärki. Polku on *yksinkertainen*, jos kaikki sen kärjet ovat erillisiä. *Yksinkertainen silmukka* on silmukka, jonka pituus on positiivinen, jonka n kärkeä ovat erillisiä eikä silmukka ole muotoa $e, \bar{e}$. Yksittäinen sivu on silmukka jos ja vain jos se on ympyrä.



Kuva 4: Polku $e_1, e_2, \dots, e_7$.

Esimerkki 10. Kuvassa 4 on esitetty eräs sivuista $e_1, e_2, \dots, e_7$ koostuva polku, jonka pituus on 7. Polun alku $e_1\sigma$ on kärjessä A ja polun loppu $e_7\tau$ on kärjessä G. Kuvan 4 polku ei ole yksinkertainen, koska kärki A on sekä sivun e_1 että sivun e_5 alku. Polku $e_1, \dots, e_4$ muodostaa yksinkertaisen silmukan, jonka alku $e_1\sigma$ ja loppu $e_4\tau$ ovat samassa kärjessä A.

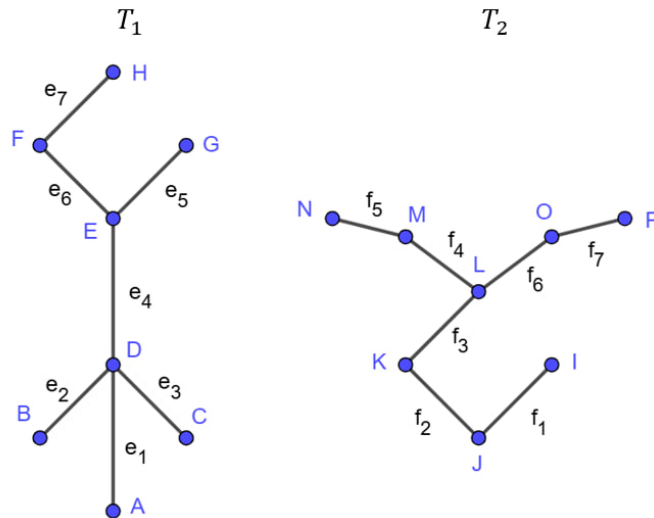
Määritelmä 21. Graafin Γ *aligraafi* Γ_1 koostuu sellaisista osajoukoista $V_1 \subseteq V$ ja $E_1 \subseteq E$, että mille tahansa sivulle $e \in E_1$ pätee $\bar{e} \in E_1$ ja $e\sigma \in V_1$. Tällöin selvästi myös $e\tau \in E_1$ ja Γ_1 on graafi. Selvästi mielivaltaisten graafin Γ aligraafien leikkaukset ja yhdisteet ovat myös graafin Γ aligraafeja. Kun V_1 on kärkijoukon V osajoukko, joukon V_1 virittämän *täyden aligraafin*, jonka kärkijoukko on V_1 , sivujoukko E_1 määritellään

$$E_1 = \{e \mid e\sigma, e\tau \in V_1\}.$$

Määritelmä 22. Graafi Γ on *yhtenäinen*, jos mitkä tahansa graafin Γ kärjet voidaan yhdistää polulla. Yleisemmin mille tahansa graafille Γ voidaan määritellä kärkijoukon V relaatio siten, että kärkien v ja w kärkien välillä on relaatio jos ja vain jos on olemassa polku, joka alkaa kärjestä v ja loppuu kärkeen w . On helppo nähdä, että tämä on ekvivalenssirelaatio. Täysiä aligraafeja, joiden kärkijoukot ovat ekvivalenssiluokkia, kutsutaan graafin Γ *komponenteiksi*.

Määritelmä 23. Polku on *redusoituva*, jos on olemassa sellainen $i \leq n$, että $e_{i+1} = \bar{e}_i$. Muussa tapauksessa polku on *redusoitumaton*. Selvästi redusoituva polku ei ole yksinkertainen. Jos $n > 2$ ja polku on redusoituva, niin $e_1, e_2, \dots, e_{i-1}, e_{i+2}, \dots, e_n$ on myös polku. Erityisesti, jos kaksi kärkeä voidaan yhdistää polulla, niin ne voidaan yhdistää redusoitumattomalla polulla.

Määritelmä 24. *Metsä* on graafi, jonka kaikki positiivisen pituuden silmukat ovat redusoituvia. *Puu* on yhtenäinen metsä. Selvästi metsän kaikki osagraafit ovat metsiä ja graafi on metsä täsmälleen silloin, kun kaikki sen komponentit ovat puita.



Kuva 5: Puiden T_1 ja T_2 muodostama metsä.

Esimerkki 11. Kuvassa 5 on esitetty kahden puun T_1 ja T_2 muodostama metsä. Puu T_1 on graafi, joka koostuu kärjistä A-H ja sivuista $e_1, \dots, e_7$. Puu T_2 puolestaan koostuu kärjistä I-P ja sivuista $f_1, \dots, f_7$. Puista T_1 ja T_2 koostuva metsä ei ole puu,

koska se ei ole yhtenäinen. Sen sijaan puu T_2 on esimerkiksi kärjistä I-L ja sivuista f_1, f_2, f_3 koostuvasta metsästä sekä kärjistä L-P ja sivuista $f_4, \dots, f_7$ koostuvasta metsästä koostuva yhtenäinen metsä.

Kuvassa 4 esitetty polku ei ole metsä, koska siihen kuuluva silmukka $e_1, \dots, e_4$ on redusoitumaton.

Lemma 4. *Olkoon graafi Γ yhtenäinen. Olkoon S sellainen kärkijoukon V epätyhjä alijoukko, että mille tahansa sivulle e , jos $e\sigma \in S$ niin myös $e\tau \in S$. Tällöin $S = V$.*

Todistus. Tarkastellaan kärkeä $v \in S$. Olkoon w mikä tahansa kärki. Koska graafi Γ on yhtenäinen, on olemassa polku $e_1, \dots, e_n$ kärjestä v kärkeen w . Koska $e_1\sigma = v \in S$, voidaan induktiolla helposti nähdä, että jokaisen sivun e_i loppukärki $e_i\tau \in S$. Erityisesti kärki $w = e_n\tau \in S$. Koska w on mielivaltainen kärki, $S = V$. $\square$

Määritelmä 25. *Maksimaalinen metsä* graafissa Γ on sellainen graafin Γ aligraafi F , että F on metsä, mikään muu graafin Γ aligraafi, joka sisältää koko metsän F , ei ole metsä.

Lause 9. *Olkoon metsä F graafin Γ aligraafi. Tällöin on olemassa graafin Γ maksimaalinen metsä, joka sisältää metsän F .*

Todistus. Oletetaan, että graafissa Γ on metsät F_i niin, että kaikille i, j joko $F_i \subseteq F_j$ tai $F_j \subseteq F_i$. Tällöin $\cup F_i$ on metsä. Muulloin yhdiste sisältäisi silmukan. Tämä silmukka kuuluisi äärellisen monen metsän F_i yhdisteeseen, jolloin oletuksen mukaan jokin metsä F_i sisältäisi silmukan. Tämä johtaa ristiriitaan, koska mestässä ei voi olla silmukoita.

Nyt lause seuraa Zornin lemmän 1 perusteella. $\square$

Lause 10. *Olkoon F maksimaalinen metsä graafissa Γ ja olkoon Γ_1 graafin Γ komponentti. Tällöin metsä F sisältää jokaisen graafin Γ kärjen. Lisäksi $F \cap \Gamma_1$ on maksimaalinen metsä komponentissa Γ_1 ja $F \cap \Gamma_1$ on puu.*

Todistus. Oletetaan, että on olemassa sellainen kärki $v \in \Gamma$, että $v \notin F$. Tällöin metsä $F \cup v$ olisi suurempi metsä kuin metsä F , jolloin F ei olisi maksimaalinen metsä.

$F \cap \Gamma_1$ on metsä komponentissa Γ_1 , koska se on metsän F aligraafi. Jos $F \cap \Gamma_1$ ei olisi maksimaalinen metsä komponentissa Γ_1 , olisi olemassa jokin toinen komponentin Γ_1 maksimaalinen metsä F_1 , johon metsä $F \cap \Gamma_1$ kuuluisi kokonaan. Tällöin metsä $F \cup F_1$ olisi graafin Γ metsä, joka sisältäisi kokonaan metsän F . Tällöin F ei olisi maksimaalinen metsä.

Osoitetaan seuraavaksi, että $F \cap \Gamma_1$ on yhtenäinen. Lemman 4 perusteella riittää osoittaa, että minkä tahansa komponentin Γ_1 sivun molemmat päätepisteet ovat samassa metsän F komponentissa. Oletetaan, että näin ei ole. Tarkastellaan sellaista sivua e , jonka alku $e\sigma$ ja loppu $e\tau$ ovat eri metsän F komponenteissa.

Osoitetaan, että tällöin graafi $F \cup \{e, \bar{e}\}$ on metsä. Se on selvästi graafi, koska metsä F sisältää kaikki graafin Γ kärjet. Jos se sisältäisi silmukan, voitaisiin olettaa (tarvittaessa syklistä permutaatioita käyttämällä), että silmukka $e_1, \dots, e_n$, missä $e_r \neq e$ ja $e_r \neq \bar{e}$ kaikilla $r > 1$. Jos $e_1 \neq e$ ja $e_1 \neq \bar{e}$, metsä F sisältäisi silmukan. Jos $e_1 = e$ tai $e_1 = \bar{e}$, niin polku $e_2, \dots, e_n$ osoittaisi, että kärjet $e\sigma$ ja $e\tau$ kuuluisivat

samaan metsän F komponenttiin. Tämä on ristiriidassa oletuksen kanssa. Siis $F \cup \{e, \bar{e}\}$ on metsä. Tällöin se on myös metsää F suurempi metsä, jolloin F ei olisi maksimaalinen metsä. Tällöin metsän $F \cap \Gamma_1$ on oltava yhtenäinen. $\square$

Määritelmä 26. Maksimaalinen metsä yhtenäisessä graafissa on puu, jota kutsutaan *maksimaaliseksi puuksi*. On huomattavaa, että tällöin maksimaalinen metsä sisältää vain yhden puun.

Määritelmä 27. Olkoon kaikille indeksijoukon Λ alkioille λ T_λ graafin Γ sellaisia alipuita, että $T_\lambda \cap T_\mu = \emptyset$, kaikille $\lambda \neq \mu$. Oletetaan, että jokainen kärki kuuluu johonkin puuhun T_λ . Konstruoidaan sitten graafi Δ siten, että graafin Δ kärkijoukko on Λ ja graafin Δ sivujoukko koostuu niistä graafin Γ sivuista, jotka eivät kuulu joukkoon $\cup_{\lambda \in \Lambda} T_\lambda$. Kuvaus $-$ graafissa Γ antaa selvästi kuvauksen $-$ graafissa Δ . Jos e on graafin Δ sivu, jonka alku graafin Γ sivuna tarkasteltuna on puussa T_λ , määritellään sivun e aluksi graafin Δ sivuna kärki λ . Tällöin sanotaan, että graafi Δ saadaan graafista Γ *supistamalla* alipuut T_λ .

Lemma 5. *Olkoon Δ graafi, joka saadaan graafista Γ supistamalla alipuut T_λ . Tällöin graafi Δ on yhtenäinen jos ja vain jos graafi Γ on yhtenäinen ja graafi Δ on metsä jos ja vain jos graafi Γ on metsä.*

Todistus. Olkoon $e_1, \dots, e_n$ polku graafissa Γ . Oletetaan, että joillekin $r < s$ pätee $e_r \notin \cup_\lambda T_\lambda$ ja $e_s \notin \cup_\lambda T_\lambda$, mutta $e_i \in \cup_\lambda T_\lambda$ kaikille $r < i < s$. Jos $e_i \in T_\lambda$ ja $e_{i+1} \in T_\mu$ niin $e_i \tau = e_{i+1} \sigma \in T_\lambda \cap T_\mu$. Tällöin alipuille asetettujen vaatimusten perusteella $\lambda = \mu$. Tästä seuraa, että on olemassa sellainen v , että $e_r \tau \in T_v$ ja $e_s \sigma \in T_v$. Tästä nähdään, että kun polusta $e_1, \dots, e_n$ jätetään pois kaikki sellaiset sivut $e_i \in \cup_\lambda T_\lambda$, saadaan graafin Δ polku.

Oletetaan sitten, että graafin Γ polku on redusoitumaton ja käyttää samoja merkintöjä kuin edellä. Tällöin $e_s \neq \bar{e}_r$, kun $s = r + 1$, koska graafin Γ polku on redusoitumaton. $e_s \neq \bar{e}_r$ myös silloin, kun $s > r + 1$, koska silloin polku $e_{r+1}, \dots, e_{s-1}$ olisi redusoitumaton silmukka puussa T_v . Voidaan siis päätellä, että polku on redusoitumaton myös graafissa Δ .

Aloitetaan nyt redusoitumattomasta graafin Δ polusta $e_1, \dots, e_n$. Tällöin jokaiselle indeksille i on olemassa sellainen μ , että $e_i \tau$ ja $e_{i+1} \sigma$ kuuluvat alipuuhun T_μ graafissa Γ . Tällöin alipuussa T_μ on olemassa redusoitumaton polku p_i kärjestä $e_i \tau$ kärkeen $e_{i+1} \sigma$. Tällöin polku $q = e_1, p_1, e_2, \dots, p_{n-1}, e_n$ on redusoitumaton polku graafissa Γ . Yleisemmin olkoon $e_1 \sigma = \alpha$ ja $e_n \tau = \beta$ graafissa Δ ja olkoot $v \in T_\alpha$ ja $w \in T_\beta$ alipuiden kärkiä graafissa Γ . Tällöin on olemassa sellaiset polut p_0 ja p_n alipuissa T_α ja T_β , että p_0, q, p_n on redusoitumaton polku graafin Γ kärjestä v kärkeen w .

Olkoon Γ yhtenäinen graafi ja α ja β graafin Δ kärkiä. Tarkastellaan graafin Γ kärkiä $v \in T_\alpha$ ja $w \in T_\beta$. Tällöin polku graafin Γ kärjestä v kärkeen w antaa edellä kuvatulla tavalla graafin Δ polun kärjestä α kärkeen β . Tällöin graafi Δ on yhtenäinen.

Olkoon Δ yhtenäinen graafi ja $v \in T_\alpha$ ja $w \in T_\beta$ graafin Γ kärkiä. Tällöin on olemassa graafin Δ polku kärjestä α kärkeen β , joka antaa edellä kuvatulla tavalla graafin Γ polun kärjestä v kärkeen w .

Jos graafi Γ ei ole metsä, se sisältää redusoitumattoman silmukan. Sitä graafissa Δ vastaava polku on tällöin myös redusoitumaton silmukka, jolloin graafi Δ ei ole metsä.

Jos graafi Δ ei ole metsä, on olemassa sellaiset kärjet α ja β , että on olemassa kaksi erillistä redusoitumatonta graafin Δ polkua kärjestä α kärkeen β . Tarkastellaan graafin Γ kärkiä $v \in T_\alpha$ ja $w \in T_\beta$. Nämä polut antavat kaksi erillistä redusoitumatonta graafin Γ polkua kärjestä v kärkeen w , joten graafi Γ ei ole metsä. $\square$

4.2 Cayleyn graafi

Määritelmä 28. Olkoon G ryhmä ja S ryhmän G osajoukko. Olkoon $\Gamma(G, S)$ graafi, jonka kärkijoukko on G ja sivujoukko $G \times S \times \{-1, 1\}$, missä $(g, s, 1)\sigma = g$ ja $(g, s, 1)\tau = gs$ sekä $(g, s, \epsilon) = (g, s, -\epsilon)$ kaikilla $\epsilon = \pm 1$. Tällöin graafia $\Gamma(G, S)$ kutsutaan ryhmän G *Cayleyn graafiksi* joukon S suhteen.

Lemma 6. (i) *Cayleyn graafi $\Gamma(G, S)$ on yhdistetty jos ja vain jos S generoi ryhmän G .*

(ii) *Cayleyn graafi $\Gamma(G, S)$ on metsä jos ja vain jos S generoi vapaasti joukon $\langle S \rangle$.*

(iii) *Cayleyn graafi $\Gamma(G, S)$ on puu jos ja vain jos G on vapaa ryhmä kannalla S .*

Todistus. Olkoon G ryhmä ja S joukko. Tulokset seuraavat suoraan, kun osoitetaan, että mielivaltaisille alkioille $g, h \in G$, alkion $g^{-1}h$ esitysten muodossa $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$, missä $s_i \in S$ ja $\epsilon = \pm 1$, ja niiden polkujen, jotka kulkevat Cayleyn graafin $\Gamma(G, S)$ kärjestä g kärkeen h , välillä on bijektio. Tämä bijektio saa redusoidut sanat vastaamaan redusoitumattomia polkuja ja kuvaa sanan $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$ poluksi $e_1, \dots, e_n$, missä e_r on (g_r, s_r, ϵ_r) . Tässä $g_r = gs_1^{\epsilon_1} \cdots s_{r-1}^{\epsilon_{r-1}}$, jos $\epsilon_r = 1$ ja $g_r = gs_1^{\epsilon_1} \cdots s_r^{\epsilon_r}$, jos $\epsilon_r = -1$. $\square$

4.3 Ryhmän toiminta puilla

Määritelmä 29. Annetaan ryhmän G toimia graafille X . Jos on olemassa sellaiset $g \in G$ ja sivu e , että $ge = \bar{e}$ sanotaan, että ryhmä toimii *käännösten kanssa*. Muussa tapauksessa sanotaan, että ryhmä toimii *ilman käännöksiä*. Selvästi G toimii Cayleyn graafille $\Gamma(G, S)$ ilman käännöksiä.

Määritelmä 30. Olkoon G ryhmä, joka toimii graafille X ilman käännöksiä. Tällöin voidaan muodostaa graafin X *tekijägraafi* ryhmän G suhteen $G \backslash X$ seuraavasti. Määritellään graafin X kärkijoukolle $V(X)$ ekvivalenssirelaatio siten, että $w \equiv v$ täsmälleen silloin, kun $w = gv$ jollakin $g \in G$. Vastaava ekvivalenssirelaatio määritellään graafin X sivujoukolle $E(X)$. Merkitään kärjen v ekvivalenssiluokkaa merkinnällä $[v]$ ja sivun e ekvivalenssiluokkaa merkinnällä $[e]$. Tällöin tekijägraafin $G \backslash X$ kärkijoukko on kaikkien kärkien $v \in V(X)$ ekvivalenssiluokkien $[v]$ joukko ja tekijägraafin $G \backslash X$ sivujoukko on kaikkien sivujen $e \in E(X)$ ekvivalenssiluokkien $[e]$ joukko. Määritellään $[\bar{e}] = [e]$, $[e]\tau = [e\tau]$ ja $[e]\sigma = [e\sigma]$. Selvästi nämä riippuvat vain ekvivalenssiluokasta $[e]$ eivätkä sivun e valinnasta. Ryhmän G on toimittava ilman käännöksiä, jotta varmistutaan siitä, että $[\bar{e}] \neq [e]$.

Määritelmä 31. Olkoon $\rho : X \rightarrow Y$ graafien välinen kuvaus. Jos jokaiselle graafin X kärjelle v ja jokaiselle graafin Y sivulle y , joille pätee $y\sigma = v\rho$, on olemassa sellainen graafin X sivu x , että $x\sigma = v$ ja $x\rho = y$, sanotaan, että ρ on *paikallisesti surjektio*. Jos taas mille tahansa kahdelle eri graafin X sivulle x_1 ja x_2 , joille pätee $x_1\sigma = x_2\sigma$, graafin Y sivut $x_1\rho$ ja $x_2\rho$ ovat erilliset, ρ on *paikallisesti injektio*. Jos kuvaus ρ on sekä paikallisesti surjektio että paikallisesti injektio, ρ on *paikallisesti bijektio*.

Lemma 7. Olkoon $\rho : X \rightarrow Y$ paikallisesti surjektio. Olkoon T puu ja olkoon $f : T \rightarrow Y$ kuvaus puulta T graafin Y . Olkoon a puun T kärki ja olkoon v sellainen graafin X kärki, että $v\rho = af$. Tällöin on olemassa sellainen kuvaus $\varphi : T \rightarrow X$, että $\varphi\rho = f$ ja $a\varphi = v$.

Todistus. Tarkastellaan sellaista paria (T_1, φ_1) , että T_1 on puun T sellainen alipuu, että $a \in T_1$ ja φ_1 on sellainen kuvaus alipuulta T_1 graafille X , että $a\varphi_1 = v$ ja $\varphi_1\rho = f$ alipuussa T_1 . Tällainen pari on olemassa, koska esimerkiksi puu T_1 voisi koostua pelkästään kärjestä a . Tällaisille pareille voidaan antaa osittainen järjestys kirjoittamalla $(T_1, \varphi_1) < (T_2, \varphi_2)$, jos $T_1 \subseteq T_2$ ja φ_1 on kuvauksen φ_2 rajoitus puulle T_1 . Zornin lemmän 1 perusteella on olemassa maksimaalinen pari (T_0, φ_0) ja tulee vain osoittaa, että $T_0 = T$.

Koska T on puu, joko $T_0 = T$ tai jokin puun T kärki ei ole osa puuta T_0 . Jälkimmäisessä tapauksessa on olemassa sellainen sivu e , että $e\sigma \in T_0$ ja $e\tau \notin T_0$ eli on olemassa sellainen sivu e , joka alkaa puusta T_0 ja päättyy puun T_0 ulkopuolelle. Väitteen mukaan on olemassa sellainen graafin X sivu x , jonka alku on $e\sigma\varphi_0$, että $x\rho = ef$. Tällöin voimme laajentaa puun T_0 puuksi $T_1 = T_0 \cup (e, \bar{e}, e\tau)$ ja voimme laajentaa kuvauksen φ_0 puun sellaiseksi T_1 kuvaukseksi φ_1 , että $\varphi_1\rho = f$ puussa T_1 määrittelemällä $e\varphi_1 = x$, $\bar{e}\varphi_1 = \bar{x}$ ja $e\tau\varphi_1 = x\tau$. Tällöin (T_0, φ_0) ei ole maksimaalinen pari. $\square$

Määritelmä 32. Olkoon X G -graafi ja $\rho : X \rightarrow G \setminus X$ luonnollinen kuvaus joukosta X tekijägraafiin $G \setminus X$. Olkoon T maksimaalinen puu tekijägraafissa $G \setminus X$. Lemman 7 perusteella on olemassa sellainen kuvaus $j : T \rightarrow X$, että $j\rho$ on puun T sisältymiskuvaus tekijägraafille $G \setminus X$. Erityisesti ρ määrittelee isomorfismin graafilta Tj puulle T . Tällöin Tj on puu, jota kutsutaan ryhmän G toiminnan graafille X *edustajapuuksi* (engl. *representative tree*).

Määritelmä 33. Ryhmä G toimii graafille X *vapaasti*, jos mille tahansa $g \in G \setminus \text{Id}_G$ ja mille tahansa graafin X kärjelle v pätee $gv \neq v$. Esimerkiksi mille tahansa ryhmälle G ja sen alijoukolle S ryhmä G toimii vapaasti Cayleyn graafille $\Gamma(G, S)$.

Määritelmä 34. Graafin *suunta* on graafin sivujen joukko, johon kuuluu täsmälleen yksi sivu jokaisesta parista $(e, \bar{e})$. Olkoon ryhmällä G toiminta graafille X . Olkoon B graafin $G \setminus X$ suunta ja olkoon $A = B\rho^{-1}$. Jos ryhmä G toimii graafille X ilman käännöksiä, on olemassa suunta A , jolle $GA = A$. Nimittäin kaikille graafin X sivuille e ja ryhmän G alkioille g pätee $\bar{g}e = g\bar{e}$ eli sivun e radalla olevat sivut ovat sen vastakkaisen sivun $\bar{e}$ radan vastakkaiset sivut. Koska G toimii ilman käännöksiä, nämä ovat kaksi eri rataa. Lisätään jompikumpi radoista suuntaan A ja tehdään näin kaikille ratojen pareille.

Lause 11. *Olkoon G ryhmä, joka toimii vapaasti puulle X . Olkoon T kyseisen toiminnan edustajapuu ja olkoon A graafin X sellainen suunta, että $GA = A$. Määritellään joukko S siten, että*

$$S = \{g \in G \setminus Id_G \mid \exists e \in A, \text{ jolle } e\sigma \in T \text{ ja } e\tau \in gT\}.$$

Tällöin G on vapaa ryhmä kannalla S .

Todistus. Havaitaan ensin, että $gT \cap hT = \emptyset$ kaikille $g \neq h$. Muussa tapauksessa voitaisiin valita puun T kärjet v ja w siten, että $gv = hw$. Koska T on edustajapuu, se sisältää vain yhden kärjen kullakin radalta, jolloin $v = w$. Tästä seuraa, että $g = h$, kun G on toimii vapaasti puulla T . Lisäksi jokainen kärki kuuluu johonkin joukkoon gT , missä $g \in G$, koska T on edustajapuu.

Olkoon Y graafi, joka saadaan graafista X supistamalla jokainen puu gT yhdeksi kärjeksi. Lemman 5 perusteella Y on puu. Lemman 6 perusteella riittää osoittaa, että Cayleyn graafi $\Gamma(G, S)$ on isomorfinen graafin Y kanssa.

Määritellään kuvaus Cayleyn graafilta $\Gamma(G, S)$ graafille Y seuraavasti. Graafin Y kärjet voidaan samaistaa puihin gT ja Cayleyn graafin $\Gamma(G, S)$ kärki g kuvataan graafin Y kärkeen gT .

Jokaiselle $s \in S$ on olemassa graafin X sivu e , jolle suunnassa A $e\sigma \in T$ ja $e\tau \in sT$. Jos tällaisia sivuja olisi olemassa kaksi, graafissa Y olisi kaksi erillistä sivua, joilla on sama alku ja loppu. Tämä ei ole mahdollista, joten tällaisia sivuja voi olla vain yksi. Graafin X sivu ge määrittää graafin Y sivun, joka kulkee kärjestä gT kärkeen gsT . Tällöin voidaan kuvata Cayleyn graafin $\Gamma(G, S)$ sivu $(g, s, 1)$ tähän graafin Y sivuun ja sivun $(g, s, 1)$ käänteissivu $(g, s, -1)$ tämän graafin Y sivun käänteissivuksi.

Tämä kuvaus on selvästi graafien välinen kärkijoukon suhteen bijektiivinen kuvaus. Sivuilla $(g, s, 1)$ ja $(h, s', -1)$ on eri kuvat, koska sivun $(g, s, 1)$ kuva $\text{Im}(g, s, 1) \in GA = A$ ja sivun $(h, s, -1)$ kuva $\text{Im}(g, s', -1) \in G\bar{A} = \bar{A}$. Jos $g \neq h$, kahden erillisen sivun kuvilla $\text{Im}(g, s, 1)$ ja $\text{Im}(h, s', 1)$ on eri alkupisteet gT ja hT . Jos $g = h$, niillä on puolestaan eri loppupisteet gsT ja $gs'T$. Täten kuvaus on sivujen suhteen injektio.

Tarkastellaan graafin Y mielivaltaista sivua. Graafin Y määritelmän perusteella se on kuva sellaiselle sivulle e , jonka alku $e\sigma \in gT$ ja loppu $e\tau \in hT$ joillekin $g, h \in G$ ja $g \neq h$. Voidaan olettaa, että $e \in A$, jos tarvittaessa se vaihdetaan sen käänteissivuksi. Tällöin $g^{-1}e \in GA = A$ ja $g^{-1}h \in S$, koska $g^{-1}e$ on sivu, joka alkaa edustajapuusta T ja päättyy puuhun $g^{-1}hT$. Tällöin $(g, g^{-1}h, 1)$ on Cayleyn graafin $\Gamma(G, S)$ sivu, jonka kuva graafissa Y on tarkasteltu sivu. Täten kuvaus on myös surjektio sivujen suhteen. Koska kuvaus on bijektio, Cayleyn graafi $\Gamma(G, S)$ on isomorfinen graafin Y kanssa. $\square$

Yhdistämällä lauseen 6 ja lemmän 4 nähdään, että ryhmä on vapaa jos ja vain jos se toimii vapaasti jollekin puulle. Kun ryhmä toimii vapaasti jollekin puulle, myös mikä tahansa sen aliryhmä toimii vapaasti samalle puulle. Myös näin voidaan nähdä, että mikä tahansa vapaan ryhmän aliryhmä on myös vapaa ryhmä.

5 Residuaalinen äärellisyys

Tässä luvussa tutustutaan residuaaliseen äärellisyyteen ja residuaalisesti äärellisten ryhmien ominaisuuksiin. Lisäksi todistetaan, että kaikki vapaat ryhmät ovat residuaalisesti äärellisiä. Luku perustuu pääosin Ceccherini-Silbersteinin ja Coornaertin teoksen Cellular Automata and Groups [5] lukuun 2.

5.1 Määritelmä ja esimerkkejä

Määritelmä 35. Ryhmä G on *residuaalisesti äärellinen*, jos jokaista alkiota $g \in G, g \neq 1_G$ kohti on olemassa sellainen äärellinen ryhmä F ja homomorfismi $\phi : G \rightarrow F$, että $\phi(g) \neq 1_F$.

Lause 12. Ryhmä G on residuaalisesti äärellinen jos ja vain jos kaikille $g, h \in G$, joille $g \neq h$, on olemassa äärellinen ryhmä F ja sellainen homomorfismi $\phi : G \rightarrow F$, että $\phi(g) \neq \phi(h)$.

Todistus. Valitsemalla $h = 1_G$ nähdään, että jos kaikille $g, h \in G$, joille $g \neq h$, on olemassa äärellinen ryhmä F ja sellainen homomorfismi $\phi : G \rightarrow F$, että $\phi(g) \neq \phi(h)$, ryhmä G on residuaalisesti äärellinen.

Oletetaan sitten, että G on residuaalisesti äärellinen. Olkoon $g, h \in G$ niin, että $g \neq h$. Koska $gh^{-1} \neq 1_G$, on olemassa sellaiset äärellinen ryhmä F ja homomorfismi $\phi : G \rightarrow F$, että $\phi(gh^{-1}) \neq 1_F$. Koska $\phi(gh^{-1}) = \phi(g)(\phi(h))^{-1}$, $\phi(g) \neq \phi(h)$. $\square$

Lause 13. Jokainen äärellinen ryhmä on residuaalisesti äärellinen.

Todistus. Olkoon G äärellinen ryhmä ja tarkastellaan sellaista alkiota $g \in G$, että $g \neq 1_G$. Jos $\phi = \text{Id}_G : G \rightarrow G$ on identiteettikuvaus, saadaan $\phi(g) = g \neq \text{Id}_G$. $\square$

Esimerkki 12. Additiivinen ryhmä $(\mathbb{Z}, +)$ on residuaalisesti äärellinen.

Todistus. Tarkastellaan sellaista alkiota $k \in \mathbb{Z}$, että $k \neq 0$. Valitaan sellainen alkuluku m , että $|k| \leq m$. Tällöin homomorfismi $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ täyttää ehdon $\phi(k) \neq 0$. $\square$

Lause 14. Ryhmä $GL_n(\mathbb{Z})$ on residuaalisesti äärellinen kaikille $n \geq 1$.

Todistus. Olkoon $A = a_{ij} \in GL_n(\mathbb{Z})$ niin, että $A \neq I_n = 1_{GL_n(\mathbb{Z})}$. Valitaan alkuluku m niin, että $|a_{ij}| < m$ kaikille i, j . Tällöin redusoimalla modulo m saadaan homomorfismi $\phi : GL_n(\mathbb{Z}) \rightarrow GL_n(\mathbb{Z}/m\mathbb{Z})$, joka täyttää residuaalisen äärellisyyden ehdon $\phi(A) \neq 1_{GL_n(\mathbb{Z}/m\mathbb{Z})}$. $\square$

Määritelmä 36. Ryhmä G on *jaollinen*, jos jokaiselle alkioille $g \in G$ ja kokonaisluvulle $n \geq 1$, on olemassa sellainen alkio $h \in G$, että $h^n = g$.

Esimerkki 13. Additiiviset ryhmät $\mathbb{Q}, \mathbb{R}$ ja $\mathbb{C}$ ovat jaollisia. Yleisemmin jokainen $\mathbb{Q}$ -vektoriavaruus on jaollinen sen taustalla olevan additiivisen ryhmärakenteen suhteen. Erityisesti jokainen karakteristiikan 0 kunta on jaollinen sen taustalla olevan additiivisen ryhmärakenteen suhteen.

Lemma 8. *Olkoon G jaollinen ryhmä ja F äärellinen ryhmä. Tällöin kaikki homomorfismit $\phi : G \rightarrow F$ ovat triviaaleja.*

Todistus. Olkoon $n = |F|$ ja $g \in G$. Koska G on jaollinen, on löydettävissä sellainen alkio $h \in G$, että $g = h^n$. Jos $\phi : G \rightarrow F$ on homomorfismi, niin $\phi(g) = \phi(h^n) = \phi(h)^n = 1_F$. $\square$

Seuraus 6. *Epätriviaali jaollinen ryhmä ei voi olla residuaalisesti äärellinen.*

Esimerkki 14. Additiivinen ryhmä $\mathbb{Q}$ ei ole residuaalisesti äärellinen, koska se on karakteristiikan 0 kunnan taustalla oleva additiivinen ryhmä.

Lemma 9. *Olkoon G ryhmä ja ryhmä H ryhmän G aliryhmä. Olkoon $K = \bigcap_{g \in G} gHg^{-1}$. Tällöin K on ryhmän G normaali aliryhmä, joka sisältyy ryhmään H . Lisäksi, jos ryhmän H indeksi ryhmässä G on äärellinen, myös ryhmän K indeksi ryhmässä G on äärellinen.*

Todistus. Koska $gHg^{-1} = H$, kun $g = 1_G$, $K \subset H$. Olkoon $\text{Sym}(G/H)$ joukon G/H permutaatioiden ryhmä. Tarkastellaan ryhmän G vasemmanpuoleisen tulon toimintaa joukossa G/H ja olkoon $\rho : G \rightarrow \text{Sym}(G/H)$ kyseinen homomorfismi. Jokaiselle $g \in G$ joukon gH stabilisaattori on gHg^{-1} . Niinpä $K = \text{Ker}(\rho)$, mistä seuraa, että K on ryhmän G normaali aliryhmä. Ryhmä G/K on isomorfinen kuvan $\text{Im}(\rho) \subset \text{Sym}(G/H)$ kanssa. Oletetaan, että ryhmän H indeksi ryhmässä G on äärellinen. Tällöin joukko G/H on äärellinen. Tästä seuraa, että ryhmä $\text{Sym}(G/H)$ on äärellinen. Tästä voidaan päätellä, että ryhmä G/K on äärellinen eli ryhmän K indeksi ryhmässä G on äärellinen. $\square$

Määritelmä 37. Niiden ryhmän G aliryhmien, joiden indeksi on äärellinen ryhmässä G , leikkausta kutsutaan ryhmän G residuaaliseksi aliryhmäksi.

Lause 15. *Olkoon G ryhmä ja N ryhmän G residuaalinen aliryhmä. Tällöin*

(i) *N on ryhmän G kaikkien normaalien aliryhmien, joiden indeksi on äärellinen ryhmässä G , leikkaus.*

(ii) *N on ryhmän G normaali aliryhmä.*

(iii) *G on residuaalisesti äärellinen jos ja vain jos $N = 1_G$.*

Todistus. Olkoon N' on kaikkien niiden ryhmän G normaalien aliryhmien, joiden indeksi on äärellinen ryhmässä G , leikkaus. Triviaalisti $N \subset N'$. Lemman 9 perusteella jos H on ryhmän G aliryhmä ja sen indeksi on äärellinen ryhmässä G , $K = \bigcap_{g \in G} gHg^{-1}$ on ryhmään H sisältyvä ryhmän G normaali aliryhmä, jonka indeksi ryhmässä G on äärellinen. Tästä seuraa, että $N' \subset K \subset H$. Tästä seuraa, että $N' \subset N$, mistä seuraa (i).

(ii) seuraa kohdasta (i), koska ryhmän G normaalien aliryhmien perheen leikkaus on ryhmän G normaali aliryhmä.

Oletetaan, että G on residuaalisesti äärellinen. Olkoon $g \in G$ sellainen alkio, että $g \neq 1_G$. Tällöin on olemassa sellaiset äärellinen ryhmä F ja homomorfismi $\phi : G \rightarrow F$, että $\phi(g) \neq 1_F$. Tällöin $g \notin \text{Ker}(\phi)$. Koska ryhmä $G/\text{Ker}(\phi)$ on

isomorfinen ryhmän F kanssa, aliryhmän $\text{Ker}(\phi)$ indeksi ryhmässä G on äärellinen. Tämä osoittaa, että $N = \{1_G\}$.

Oletetaan sitten, että $N = \{1_G\}$. Olkoon $g \in G$ sellainen alkio, että $g \neq 1_G$. Kohdan (i) perusteella on olemassa sellainen normaali aliryhmä $K \subset G$, jonka indeksi ryhmässä G on äärellinen, että $g \notin K$. Jos $\phi : G \rightarrow G/K$ on kanoninen homomorfismi, $\phi(g) \neq 1_{G/K}$. Tästä seuraa, että ryhmä G on residuaalisesti äärellinen. $\square$

5.2 Residuaalisesti äärellisten ryhmien stabiilisuuksominaisuudet

Lause 16. *Residuaalisesti äärellisen ryhmän kaikki aliryhmät ovat residuaalisesti äärellisiä.*

Todistus. Olkoon G residuaalisesti äärellinen ryhmä ja H ryhmän G aliryhmä. Olkoon $h \in H$ sellainen ryhmän H alkio, että $h \neq 1_G$. Koska G on residuaalisesti äärellinen, on olemassa äärellinen ryhmä F ja sellainen homomorfismi $\phi : G \rightarrow F$, että $\phi(h) \neq 1_F$. Jos $\phi' : H \rightarrow F$ on homomorfismin ϕ rajoitus ryhmälle H , $\phi'(h) = \phi(h) \neq 1_F$. Tästä seuraa, että H on residuaalisesti äärellinen. $\square$

Lause 17. *Olkoon $(G_i)_{i \in I}$ residuaalisesti äärellisten ryhmien perhe. Tällöin niiden suora tulo $G = \prod_{i \in I} G_i$ on residuaalisesti äärellinen.*

Todistus. Olkoon $g = (g_i)_{i \in I} \in G$ sellainen ryhmän G alkio, että $g \neq 1_G$. Tällöin on olemassa sellainen $i_0 \in I$, että $g_{i_0} \neq 1_{G_{i_0}}$. Koska G_{i_0} on residuaalisesti äärellinen, on löydettävissä sellaiset äärellinen ryhmä F ja homomorfismi $\phi : G_{i_0} \rightarrow F$, että $\phi(g_{i_0}) \neq 1_F$. Tarkastellaan homomorfismia $\phi' : G \rightarrow F$, joka määritellään $\phi' = \pi \circ \phi$, missä $\pi : G \rightarrow G_{i_0}$ on projektio ryhmään G_{i_0} . Tällöin $\phi'(g) = \phi(g_{i_0}) \neq 1_F$. Tästä seuraa, että G on residuaalisesti äärellinen. $\square$

Seuraus 7. *Olkoon $(G_i)_{i \in I}$ residuaalisesti äärellisten ryhmien perhe. Tällöin niiden suora summa $G = \bigoplus_{i \in I} G_i$ on residuaalisesti äärellinen.*

Todistus. Tämä on suora seuraus lauseista 16 ja 17, koska G on suoran tulon $P = \prod_{i \in I} G_i$ aliryhmä, joka sisältää kaikki $g = (g_i) \in P$, joille $g_i = 1_{G_i}$ kaikille paitsi äärellisen monelle $i \in I$. $\square$

Seuraus 8. *Jokainen äärellisesti generoitu Abelin ryhmä on residuaalisesti äärellinen.*

Todistus. Jos G on äärellisesti generoitu Abelin ryhmä, on olemassa kokonaisluku $r \geq 0$ ja sellainen äärellinen Abelin ryhmä T , että G on isomorfinen ryhmän $\mathbb{Z}^r \times T$ kanssa. Lauseen 13 ja esimerkin 12 perusteella voimme päätellä, että G on residuaalisesti äärellinen. $\square$

Huomautus 2. Mielivaltainen Abelin ryhmä ei välttämättä ole residuaalisesti äärellinen. Esimerkiksi additiivinen ryhmä $\mathbb{Q}$ ei ole residuaalisesti äärellinen, kuten esimerkissä 14 nähtiin.

Seuraus 9. *Olkoon G ryhmä. Tällöin seuraavat ehdot ovat ekvivalentit:*

- (a) ryhmä G on residuaalisesti äärellinen;
- (b) on olemassa sellaisten äärellisten ryhmien perhe $(F_i)_{i \in I}$, että ryhmä G on isomorfinen suoran tulon $\prod_{i \in I} F_i$ aliryhmän kanssa.

Todistus. Lauseista 13, 16 ja 17 seuraa, että ehdosta (b) seuraa ehto (a).

Oletetaan, että G on residuaalisesti äärellinen. Tällöin jokaiselle $g \in G \setminus \{1_G\}$ on löydettävissä sellaiset äärellinen ryhmä F_g ja homomorfismi $\phi_g : G \rightarrow F_g$, että $\phi_g(g) \neq 1_{F_g}$. Tarkastellaan ryhmää

$$H = \prod_{g \in G \setminus \{1_G\}} F_g.$$

Homomorfismi $\psi : G \rightarrow H$

$$\psi = \prod_{g \in G \setminus \{1_G\}} \phi_g$$

on injektio. Tällöin G on isomorfinen ryhmän H aliryhmän kanssa. Tämä osoittaa, että ehdosta (a) seuraa ehto (b). $\square$

5.3 Vapaiden ryhmien residuaalinen äärellisyys

Tämän luvun tarkoituksena on todistaa, että kaikki vapaat ryhmät ovat residuaalisesti äärellisiä ryhmiä.

Lemma 10. *Matriisien*

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ ja } b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

generoima ryhmän $SL_2(\mathbb{Z})$ aliryhmä on asteen 2 vapaa ryhmä.

Todistus. Ryhmä $GL_2(\mathbb{R})$ luonnollisesti toimii avaruuden $\mathbb{R}^2$ origon kautta kulkevien suorien joukkoon eli projektiiviseen suoraan $P_1(\mathbb{R})$. Epähomogeenisissa koordinaateissa tämän toiminnan vaikutus saadaan kaavalla

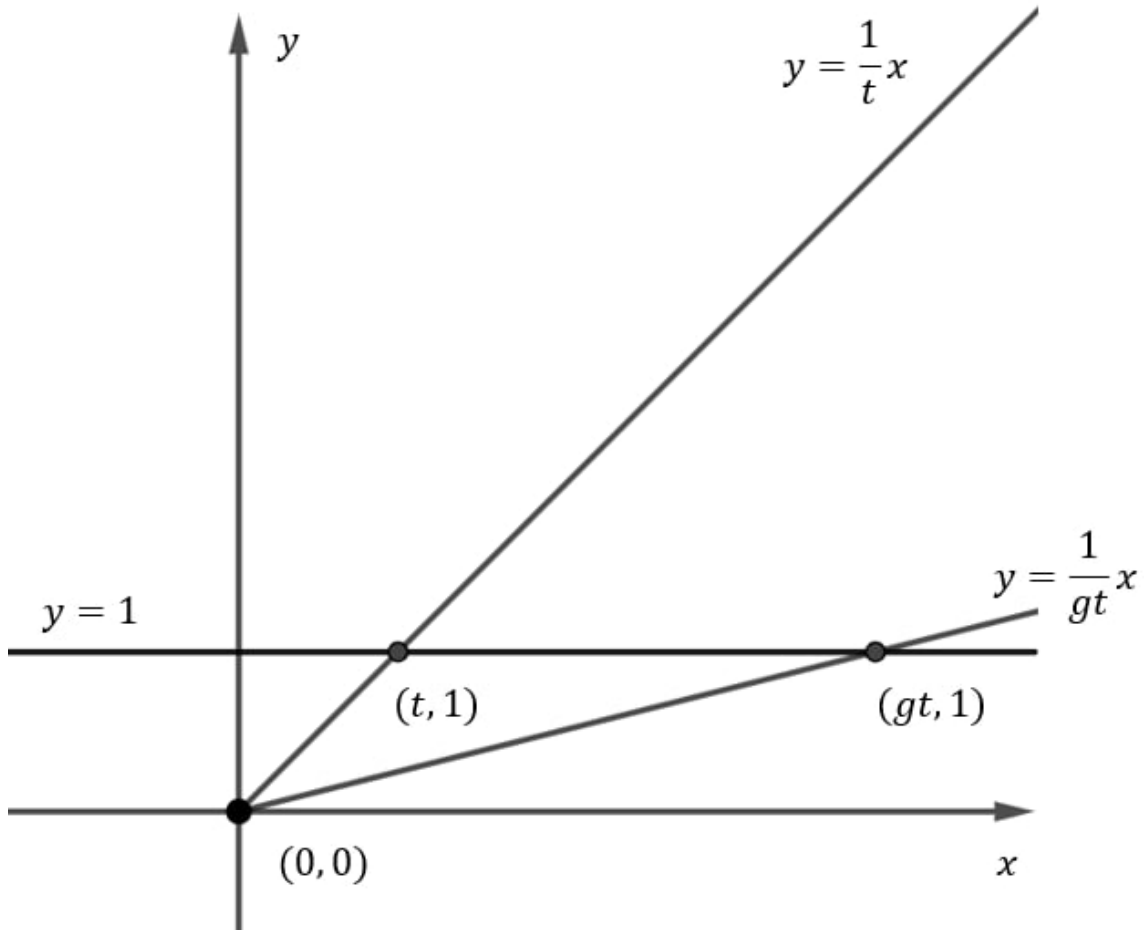
$$gt = \frac{g_{11}t + g_{12}}{g_{21}t + g_{22}},$$

missä $g = g_{ij} \in GL_2(\mathbb{R})$ ja $t \in P_1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ esittää avaruuden $\mathbb{R}^2$ origon kautta kulkevaa suoraa, jonka kulmakerroin on $\frac{1}{t}$. Tämä on esitetty kuvassa 6. Tässä tapauksessa

$$a^k t = t + 2k \quad \text{ja} \quad b^k t = \frac{t}{2kt + 1}$$

kaikille $k \in \mathbb{Z}$. Tarkastellaan seuraavaksi projektiivisten suorien joukon $P_1(\mathbb{R})$ osajoukkoja Y ja Z , missä

$$Y =]-1, 1[\quad \text{ja} \quad Z = P_1(\mathbb{R}) \setminus [-1, 1].$$



Kuva 6: Ryhmän $\text{GL}_2(\mathbb{R})$ toiminta joukkoon $P_1(\mathbb{R})$. Tässä $t = 1$ ja $g = a$.

Kaikille $k \in \mathbb{Z} \setminus \{0\}$ pätee

$$a^k Y =]2k - 1, 2k + 1[\subset Z \quad \text{ja} \quad b^k Z = \left] \frac{1}{2k + 1}, \frac{1}{2k - 1} \right[\subset Y.$$

Soveltamalla Kleinin Ping-Pong lemmaa voidaan päätellä, että a ja b generoivat toisen asteen vapaan ryhmän. $\square$

Lause 18. *Kaikki vapaat ryhmät ovat residuaalisesti äärellisiä.*

Todistus. Lauseen 14 nojalla $\text{GL}_2(\mathbb{Z})$ on residuaalisesti äärellinen. Täten lemmasta 10, seurauksesta 5 ja lauseesta 16 seuraa, että jokainen äärellistä astetta oleva vapaa ryhmä on residuaalisesti äärellinen.

Tarkastellaan mielivaltaista joukkoa X ja olkoon $F(X)$ vapaa ryhmä kannalla X . Olkoon $g \in F(X)$ sellainen ryhmän $F(X)$ alkio, että $g \neq 1_{F(X)}$. Olkoon $Y \subset X$ on sellainen alkioiden $x \in X$ joukko, että x^k esiintyy alkion g redusoidussa muodossa, jollekin $k \in \mathbb{Z} \setminus \{0\}$. Joukon Y generoima aliryhmä $F(Y) \subset F(X)$ on lauseen 2 perusteella vapaa ryhmä kannalla Y , jolloin $g \in F(Y)$. Koska ryhmä $F(Y)$ on äärellistä astetta oleva vapaa ryhmä, se on residuaalisesti äärellinen. Tällöin sellainen

äärellinen ryhmä H ja homomorfismi $\phi : F(Y) \rightarrow H$, että $\phi(g) \neq 1_H$, ovat löydettävissä. Tarkastellaan sellaista yksikäsitteistä homomorfismia $\pi : F(Y) \rightarrow H$, että $\pi(y) = y$ jokaiselle $y \in Y$ ja $\pi(x) = 1_{F(Y)}$ kaikille $x \in X \setminus Y$. Tällöin homomorfismi $\phi \circ \pi : F(X) \rightarrow H$ täyttää ehdon $\phi \circ \pi(g) = \phi(\pi(g)) = \phi(g) \neq 1_H$. Siis $F(X)$ on residuaalisesti äärellinen. $\square$

Viitteet

- [1] Daniel E. Cohen: *Combinatorial Group Theory: A Topological Approach*. Cambridge University Press, London, 1989.
- [2] David S. Dummit & Richard M. Foote: *Abstract Algebra, third edition*. John Wiley & Sons Inc., Hoboken, 2004.
- [3] Paul R. Halmos: *Naive Set Theory*. D. Van Nostrand Company Inc., Princeton, 1960.
- [4] Serge Lang: *Algebra*. Springer-Verlag, New York, 2002.
- [5] Tullio Ceccherini-Silberstein & Michel Coornaert: *Cellular Automata and Groups*. Springer-Verlag Berlin, Heidelberg, 2010.