Ryhmän osajoukon generoima aliryhmä ja vapaat ryhmät

LuK-tutkielma
Joose Heinonen
Matemaattisten tieteiden tutkinto-ohjelma
Oulun yliopisto
Kevät 2017

Sisältö

Johdanto

Tutkielma käsittelee ryhmäteoriaa ja siinä määritellään yleisellä tasolla ryhmän osajoukon generoima aliryhmä sekä vapaa ryhmä. Lukijalla tulisi olla riittävä matemaattinen perustietämys ja varsinkin ryhmän käsitteen tunteminen on hyödyksi, vaikka kaikki tutkielmassa tarvittavat ryhmät määritelläänkin tutkielman ensimmäisessä luvussa. Tutkielmassa on käytetty pääasiassa teosta [1], mutta ensimmäisen luvun määritelmien lähteenä on käytetty teosta [2].

Erilaisten tutkielmassa tarvittavien ryhmien määrittelemisen jälkeen siirrytään toisessa luvussa käsittelemään ryhmän osajoukon generoimaa aliryhmää. Luvussa esitellään ryhmän osajoukon generoiman aliryhmän määritelmä ja johdetaan erilaisia esitystapoja kyseiselle aliryhmälle. Aihetta havainnollistetaan kahdella esimerkillä, joiden ratkaisut olen keksinyt itse. Kolmannessa luvussa esitellään vapaan ryhmän käsite.

1 Ryhmät ja aliryhmät

1.1 Ryhmä

Määritelmä 1.1. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G operaatio. Pari $(G, *)$ on *ryhmä*, mikäli seuraavat ehdot ovat voimassa:

1. $(*)$ on binäärinen joukossa G eli
$$a * b \in G$$
aina, kun $a, b \in G$.
2. $(*)$ on assosiatiivinen eli
$$(a * b) * c = a * (b * c)$$
aina, kun $a, b, c \in G$.
3. Joukossa G on sellainen alkio e, että
$$a * e = e * a = a$$
aina, kun $a \in G$. Alkiota e kutsutaan *neutraali- eli ykkösalkioksi.*
4. Aina, kun $a \in G$, on olemassa sellainen alkio $a^{-1} \in G$, että
$$a * a^{-1} = a^{-1} * a = e.$$
Alkiota a^{-1} kutsutaan *alkion a käänteisalkioksi.*

Jos lisäksi $(*)$ on kommutatiivinen eli
$$a * b = b * a$$
aina, kun $a, b \in G$, niin kyseessä on *Abelin ryhmä* eli kommutatiivinen ryhmä.

1.2 Aliryhmä

Määritelmä 1.2. Olkoon $(G, *)$ ryhmä ja $H \subseteq G, H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sitä sanotaan *ryhmän* $(G, *)$ *aliryhmäksi* ja merkitään $(H, *) \leq (G, *)$ tai lyhyemmin $H \leq G$.

Huomautus. Jos $H \leq G$, niin aina ryhmän G neutraalialkio $e_G \in H$.

Käytetään jatkossa ryhmälle $(G, *)$ lyhyempää merkintää G ja ryhmän kahden alkion a ja b väliselle operaatiolle $a * b$ merkintää ab. Esitellään seuraavaksi vielä aliryhmäkriteeri ja sen seuraus, jota hyödynnetään myöhemmin osoitettaessa ryhmän osajoukkoa tämän aliryhmäksi.

Lemma 1.3 (Aliryhmäkriteeri)**.** *Olkoot G ryhmä ja $H \subseteq G, H \neq \emptyset$. Nyt $H \leq G$ jos ja vain jos seuraavat ehdot toteutuvat:*

1. $a, b \in H \Rightarrow ab \in H$;
2. $a \in H \Rightarrow a^{-1} \in H$.

Seuraus 1.4. *Olkoot G ryhmä ja $H \subseteq G, H \neq \emptyset$. Tällöin $H \leq G$ jos ja vain jos ehto*

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

on voimassa.

1.3 Syklinen ryhmä

Olkoon $(G, *)$ ryhmä ja $a \in G$. Kun $n \in \mathbb{Z}^+$, niin määritellään

$$a^n = \underbrace{a * a * \ldots * a}_{n} \text{ ja } a^{-n} = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{n}.$$

Lisäksi asetetaan $a^0 = e$. Tällöin joukko $H = \{a^k \mid k \in \mathbb{Z}\}$ on joukon G osajoukko.

Määritelmä 1.5. Olkoon $a \in G$ ja $H = \{a^k \mid k \in \mathbb{Z}\}$. Tällöin $(H, *)$ on ryhmän $(G, *)$ aliryhmä ja ryhmää H kutsutaan *alkion a generoimaksi sykliseksi ryhmäksi.*

1.4 Symmetrinen ryhmä

Määritelmä 1.6. *Symmetrinen ryhmä* S_n on joukon $N_n = \{1, 2, \ldots, n\}$ kaikkien permutaatioiden muodostama ryhmä, jossa laskutoimituksena on kuvausten yhdistäminen.

2 Ryhmän osajoukon generoima aliryhmä

Tietyn ryhmän syklisen aliryhmän muodostamiseen käytettävä menetelmä on erikoistapaus yleisemmästä menetelmästä, jonka avulla voidaan muodostaa ryhmän mielivaltaisen osajoukon generoima aliryhmä. Syklisen ryhmän tapauksessa generoivana osajoukkona on ryhmän G yhden alkion x muodostama joukko $\{x\}$. Tässä osiossa määritellään aliryhmä, jonka generoijana toimii yhden alkion sijaan mielivaltainen ryhmän G osajoukko A.

Oletetaan, että G on mikä tahansa ryhmä ja joukko A on ryhmän G mielivaltainen osajoukko. Ensiksi osoitetaan aliryhmäkriteerin seurauksen avulla, että mikä tahansa leikkaus ryhmän G aliryhmistä on myös ryhmän G aliryhmä. Tästä seuraa, että joukon A generoima aliryhmä on yksikäsitteisesti pienin ryhmän G aliryhmä, joka sisältää joukon A.

Lause 2.1. *Jos $\mathcal{A}$ on mielivaltainen ryhmän G aliryhmistä koostuva epätyhjä joukko, niin kaikkien joukon $\mathcal{A}$ alkioiden leikkaus on myös ryhmän G aliryhmä.*

Todistus. Olkoon G ryhmä ja olkoon $\mathcal{A}$ mielivaltainen ryhmän G aliryhmistä koostuva epätyhjä joukko. Olkoon lisäksi

$$K = \bigcap_{H \in \mathcal{A}} H.$$

Koska ryhmän G jokainen aliryhmä $H \in \mathcal{A}$ on ryhmän G osajoukko, niin myös näiden aliryhmien leikkaus K on ryhmän G osajoukko eli $K \subseteq G$.

Koska jokainen $H \in \mathcal{A}$ on ryhmän G aliryhmä, niin ryhmän G neutraalialkio $e \in H$ ja täten $e \in K$. Siis $K \neq \emptyset$.

Olkoon $a, b \in K$. Tällöin $a, b \in H$ kaikilla $H \in \mathcal{A}$ ja koska jokainen H on ryhmä, niin $ab^{-1} \in H$ eli $ab^{-1} \in K$. Seurauksen 1.4 nojalla $K \leq G$. □

Määritelmä 2.2. Jos A on ryhmän G mielivaltainen osajoukko, niin *joukon A generoima ryhmän G aliryhmä* on

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

Siis $\langle A \rangle$ on leikkaus kaikista ryhmän G aliryhmistä, jotka sisältävät joukon A. Lauseen 2.1 nojalla $\langle A \rangle$ on ryhmän G aliryhmä, sillä nyt $\mathcal{A} = \{H \leq G \mid A \subseteq H\}$ ja $\mathcal{A}$ on epätyhjä, sillä $A \subseteq G$ ja $G \leq G$ eli $G \in \mathcal{A}$. Koska joukko A sisältyy jokaiseen aliryhmään H, niin joukko A sisältyy myös näiden aliryhmien leikkaukseen eli $A \subseteq \langle A \rangle$.

Aliryhmä $\langle A \rangle$ on nyt yksikäsitteisesti pienin joukon $\mathcal{A}$ alkio, sillä $\langle A \rangle$ on ryhmän G aliryhmä ja $A \subseteq \langle A \rangle$ eli $\langle A \rangle \in \mathcal{A}$, minkä lisäksi kaikki joukon $\mathcal{A}$ alkiot sisältävät kaikkien joukon $\mathcal{A}$ alkioiden leikkauksen eli kaikki joukon $\mathcal{A}$ alkiot sisältävät aliryhmän $\langle A \rangle$. Toisin sanoen kaikki joukon A sisältävät ryhmän G aliryhmät sisältävät aliryhmän $\langle A \rangle$ ja myös kyseinen $\langle A \rangle$ kuuluu tähän aliryhmien joukkoon, joten se on aliryhmistä pienin.

Edellä esitetty määritelmä osoittaa ryhmän G joukon A sisältävän pienimmän aliryhmän olemassaolon ja yksikäsitteisyyden, mutta se ei kerro, millaisia alkioita tämä aliryhmä sisältää. Jotta päästään sanan varsinaisessa merkityksessä generoimaan ryhmän G osajoukon A alkioista ryhmän G aliryhmää, määritellään joukko, joka koostuu osajoukon A alkioiden ja niiden käänteisalkioiden välisistä tuloista. Tämän jälkeen osoitetaan, että kyseisellä menetelmällä muodostettu joukko on itseasiassa sama kuin joukko $\langle A \rangle$. Olkoon

$$\bar{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} \mid n \in \mathbb{Z},\ n \geq 0,\ a_i \in A \text{ ja } \epsilon_i = \pm 1 \text{ jokaisella indeksillä } i\},$$

missä $\bar{A} = \{e\}$, jos $A = \emptyset$. Joukko $\bar{A}$ koostuu siis kaikista joukon A alkioiden ja niiden käänteisalkioiden keskenäisten operaatioiden muodostamista äärellisistä tuloista, joita kutsutaan *sanoiksi*. Huomaa, että alkioiden a_i ei tarvitse olla erillisiä, eli joukon $\bar{A}$ määrittelyssä käytetyssä merkinnässä esimerkiksi a^2 kirjoitetaan muodossa aa.

Lause 2.3. *Jos A on ryhmän G mielivaltainen osajoukko ja joukot $\bar{A}$ ja $\langle A \rangle$ on määritelty kuten edellä, niin $\bar{A} = \langle A \rangle$.*

Todistus. Olkoon G mikä tahansa ryhmä ja A sen mielivaltainen osajoukko.

Osoitetaan ensin, että $\bar{A} \subseteq \langle A \rangle$. Koska $\langle A \rangle$ on ryhmä, joka sisältää joukon A, se sisältää myös jokaisen muotoa $a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n}$ olevan alkion, missä jokainen $a_i \in A$. Nyt jokainen joukon $\bar{A}$ alkio on muotoa $a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n}$, joten jokainen joukon $\bar{A}$ alkio sisältyy joukkoon $\langle A \rangle$. Siis $\bar{A} \subseteq \langle A \rangle$.

Osoitetaan sitten, että $\langle A \rangle \subseteq \bar{A}$. Tähän riittää osoittaa, että $A \subseteq \bar{A}$ ja että $\bar{A}$ on ryhmän G aliryhmä. Tällöin $\bar{A}$ lukeutuu aliryhmiin H ja joukon $\langle A \rangle$ määritelmän nojalla kaikki joukon $\langle A \rangle$ alkiot kuuluvat jokaiseen aliryhmään H, joten kaikkien joukon $\langle A \rangle$ alkioiden täytyy kuulua myös joukkoon $\bar{A}$.

Osoitetaan siis, että $A \subseteq \bar{A}$. Olkoon a joukon A mielivaltainen alkio. Kun $n = 1$, $\epsilon_1 = 1$ ja $a_1 = a$, niin $a \in \bar{A}$. Siis $A \subseteq \bar{A}$.

Osoitetaan vielä, että $\bar{A} \leq G$. Nyt $\bar{A}$ on epätyhjä, sillä kuten edellä todettiin, jos $a \in A$, niin $a \in \bar{A}$ ja jos $A = \emptyset$, niin $\bar{A} = \{e\} \neq \emptyset$. Koska G on ryhmä, joka sisältää joukon A, niin $\bar{A} \subseteq G$.

Olkoon $a, b \in \bar{A}$, missä $a = a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n}$ ja $b = b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$. Nyt alkion b käänteisalkio on $b^{-1} = b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \cdots b_1^{-\delta_1}$, joten

$$ab^{-1} = a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} \cdot b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \cdots b_1^{-\delta_1}.$$

Nyt ab^{-1} on tulo joukon A alkioista korotettuna potenssiin ± 1, joten $ab^{-1} \in \bar{A}$. Seurauksen 1.4 nojalla $\bar{A} \leq G$. Siis $\bar{A} \subseteq \langle A \rangle$ ja $\langle A \rangle \subseteq \bar{A}$, joten $\bar{A} = \langle A \rangle$. $\square$

Käytetään jatkossa merkinnän $\bar{A}$ tilalla merkintää $\langle A \rangle$, sillä näitä määritelmiä voidaan nyt pitää yhtäpitävinä. Nyt esimerkiksi tulot aa, aaa ja aa^{-1} voidaan kirjoittaa yksinkertaisemmin muodossa a^2, a^3 ja e, joten $\langle A \rangle$ voidaan kirjoittaa muodossa

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} \mid n \in \mathbb{Z}^+,\ a_i \in A,\ \alpha_i \in \mathbb{Z} \text{ ja } a_i \neq a_{i+1} \text{ jokaisella indeksillä } i\}.$$

Kun $A = \{x\}$, tämä on myös syklisen ryhmän määritelmä. Tämä osoitetaan Esimerkissä 2.4.

Esimerkki 2.4. Olkoon G ryhmä ja $A = \{x\}$ sen osajoukko eli $x \in G$. Määritetään joukon A generoima aliryhmä $\langle A \rangle$.

Koska joukossa A on vain yksi alkio, niin $a_i = x$ kaikilla indekseillä i. Joukon A generoiman aliryhmän $\langle A \rangle$ määritelmän nojalla $a_i \neq a_{i+1}$, joten kaikki aliryhmän $\langle A \rangle$ alkiot ovat muotoa x^α, missä $\alpha \in \mathbb{Z}$. Siis $\langle A \rangle = \{x^\alpha \mid \alpha \in \mathbb{Z}\}$, mikä on täsmälleen sama kuin alkion x generoiman syklisen ryhmän määritelmä.

Jos G on Abelin ryhmä eli kommutatiivinen ryhmä, voidaan kaikki tietyn alkion a_i eri potenssit koota yhteen. Tällöin esimerkiksi Abelin ryhmän G äärellisen osajoukon $A = \{a_1, a_2, \ldots, a_k\}$ generoima aliryhmä on

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k} \mid \alpha_i \in \mathbb{Z} \text{ kaikilla indekseillä } i\}.$$

Lemma 2.5. *Ryhmä* $(\mathbb{R}^2, +)$ *on Abelin ryhmä.*

Esimerkki 2.6. Olkoon $G = (\mathbb{R}^2, +)$ ja $A = \{(1,0),\ (0,1)\}$ sen osajoukko. Määritetään joukon A generoima aliryhmä $\langle\, A \,\rangle$.

Nyt Lemman 2.5 nojalla G on Abelin ryhmä, joten voidaan käyttää viimeksi esitettyä määritelmää aliryhmälle $\langle\, A \,\rangle$. Merkitään $a_1 = (1,0)$ ja $a_2 = (0,1)$. Yhtälailla voitaisiin tehdä alkioiden järjestyksen valinta toisinpäin, sillä kommutatiivisuuden vuoksi tällä järjestyksellä ei ole väliä.

Joukon A generoiman aliryhmän $\langle\, A \,\rangle$ alkiot ovat siis muotoa $(1,0)^{\alpha_1} + (0,1)^{\alpha_2}$, missä $\alpha_1, \alpha_2 \in \mathbb{Z}$. Olkoon $n \in \mathbb{Z}^+$. Nyt

$$\begin{aligned}(1,0)^n &= \underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{n} \\ &= (\underbrace{1 + 1 + \ldots + 1}_{n}, \underbrace{0 + 0 + \ldots + 0}_{n}) \\ &= (n, 0)\end{aligned}$$

ja vastaavasti

$$(0,1)^n = (0,n).$$

Ryhmän G neutraalialkio on $e = (0,0) = (1,0)^0 = (0,1)^0$. Alkion $(1,0)$ käänteisalkio on $(1,0)^{-1} = (-1,0)$, sillä

$$(-1,0) + (1,0) = (-1+1, 0+0) = (0,0) = e$$

ja kommutatiivisuudesta seuraa, että

$$(1,0) + (-1,0) = e.$$

Vastaavasti alkion $(0,1)$ käänteisalkio on $(0,1)^{-1} = (0,-1)$.

Nyt

$$\begin{aligned}(1,0)^{-n} &= \underbrace{(1,0)^{-1} + (1,0)^{-1} + \ldots + (1,0)^{-1}}_{n} \\ &= \underbrace{(-1,0) + (-1,0) + \ldots + (-1,0)}_{n} \\ &= (\underbrace{-1 + (-1) + \ldots + (-1)}_{n}, \underbrace{0 + 0 + \ldots + 0}_{n}) \\ &= (\underbrace{-1 - 1 - \ldots - 1}_{n}, 0) \\ &= (-n, 0)\end{aligned}$$

ja vastaavasti

$$(0,1)^{-n} = (0,-n).$$

Näin ollen $(1,0)^{\alpha_1} = (\alpha_1, 0)$ kaikilla $\alpha_1 \in \mathbb{Z}$ ja $(0,1)^{\alpha_2} = (0,\alpha_2)$ kaikilla $\alpha_2 \in \mathbb{Z}$, joten joukon A generoiman aliryhmän $\langle\, A \,\rangle$ alkiot ovat muotoa

$$(1,0)^{\alpha_1} + (0,1)^{\alpha_2} = (\alpha_1, 0) + (0, \alpha_2) = (\alpha_1, \alpha_2).$$

Siis $\langle\, A \,\rangle = \{(\alpha_1, \alpha_2) \mid \alpha_1, \alpha_2 \in \mathbb{Z}\} = \mathbb{Z}^2$.

3 Vapaat ryhmät

Tässä osiossa esitellään lyhyesti *vapaa ryhmä* $F(S)$, jonka generoi täysin mielivaltainen joukko S. Edellisessä luvussa generoiva joukko oli jonkin tietyn ryhmän osajoukko, mutta vapaan ryhmän generoivan joukon ei tarvitse toteuttaa mitään tällaisia ehtoja, eli joukko S on "vapaa" relaatioista.

Vapaa ryhmä $F(S)$ koostuu joukon S alkioiden ja niiden käänteisalkioiden yhdessä muodostamista *sanoista*. Huomaa, että nyt sanojen muodostamisessa ei käytetä mitään ryhmäoperaatiota, vaan sanojen muodostaminen tapahtuu vain asettamalla generoija-alkioita peräkkäin. Jos S on esimerkiksi joukko $\{a, b\}$, niin sen generoiman vapaan ryhmän $F(S)$ alkioita ovat esimerkiksi $a, aa, ab, ab^{-1}a$ ja $ba^{-1}ba$ ja kaikkia näitä sanoja pidetään erillisinä.

Jos yhdistetään peräkkäiset samankantaiset potenssit, saadaan esimerkiksi alkiot aa ja abb^{-1} muotoon a^2 ja a. Muodostettuja sanoja voidaan myös ketjuttaa, jolloin esimerkiksi sanat ab^3a ja b^5a^2 muodostavat yhdistettynä sanan $ab^3ab^5a^2$.

Seuraavaksi lähdetään määrittelemään tarkemmin mielivaltaisen joukon S generoimaa vapaata ryhmää $F(S)$. Ainoa ongelma ryhmän $F(S)$ muodostamisessa on osoittaa, että sanojen ketjuttamisoperaatio on hyvin määritelty ja assosiatiivinen. Tätä varten palataan määritelmään, jossa kaikki sanoissa esiintyvät eksponentit ovat joko 1 tai -1.

Olkoon S mielivaltainen joukko ja S^{-1} jokin sellainen joukosta S erillinen joukko, että on olemassa bijektio joukolta S joukolle S^{-1}. Käytetään jokaiselle alkiota $s \in S$ vastaavalle joukon S^{-1} alkiolle merkintää s^{-1} ja vastaavasti jokaista alkiota $t \in S^{-1}$ vastaa joukossa S alkio t^{-1}, jolloin $(s^{-1})^{-1} = s$. Olkoon $\{1\}$ yhden alkion muodostama joukko, joka ei sisälly joukkoon $S \cup S^{-1}$. Määritellään $ss^{-1} = s^{-1}s = 1$ ja $1s = s1 = s$ kaikilla $s \in S$. Olkoon lisäksi $1^{-1} = 1$ ja $x^1 = x$ kaikilla $x \in S \cup S^{-1} \cup \{1\}$.

Merkitään sanaa jonona $(s_1, s_2, s_3, \ldots)$, missä $s_i \in S \cup S^{-1} \cup \{1\}$ ja $s_i = 1$ kaikilla riittävän suurilla indekseillä i. Tällöin jokaiselle sanalle on olemassa sellainen indeksi N, että $s_i = 1$ kaikilla indekseillä $i \geq N$. Siten sanoja voidaan ajatella myös joukon S alkioiden ja niiden käänteisalkioiden äärellisinä tuloina.

Sanojen yksikäsitteisyyden varmistamiseksi otetaan huomioon vain sanat, joissa ei esiinny peräkkäisinä termeinä alkiota ja sen käänteisalkiota. Esimerkiksi sana $baa^{-1}b$ sievenee siis muotoon bb.

Määritelmä 3.1. Sana $(s_1, s_2, s_3, \ldots)$ on *sievennetty*, jos

1. $s_{i+1} \neq s_i^{-1}$ kaikilla indekseillä i, joilla $s_i \neq 1$, ja
2. jos $s_k = 1$ jollakin indeksillä k, niin $s_i = 1$ kaikilla indekseillä $i \geq k$.

Sievennettyä sanaa $(1, 1, 1, \ldots)$ kutsutaan *tyhjäksi sanaksi* ja sille käytetään merkintää 1. Yksinkertaistetaan seuraavaksi sanojen merkintätapaa käyttämällä sievennetylle sanalle $(s_1^{\epsilon_1}, s_2^{\epsilon_2}, \ldots, s_n^{\epsilon_n}, 1, 1, 1, \ldots)$, missä $s_i \in S$ ja $\epsilon_i = \pm 1$, merkintää $s_1^{\epsilon_1} s_2^{\epsilon_2} \ldots s_n^{\epsilon_n}$. Olkoon $F(S)$ joukon S alkioista muodostettujen sievennettyjen sanojen joukko, jolloin S on joukon $F(S)$ osajoukko. Huomaa, että jos $S = \emptyset$, niin $F(S) = \{1\}$.

Nyt voimme esitellä binäärisen operaation joukossa $F(S)$. Operaation määrittelyssä on varmistettava, että kahden sievennetyn sanan välinen tulo on edelleen sievennetty sana. Tällöin esimerkiksi sanojen $ab^{-1}a$ ja $a^{-1}ba$ välisen tulon tulee sieventyä muotoon aa. Olkoon $r_1^{\delta_1} r_2^{\delta_2} \ldots r_m^{\delta_m}$ ja $s_1^{\epsilon_1} s_2^{\epsilon_2} \ldots s_n^{\epsilon_n}$ sievennettyjä sanoja ja oletetaan ensin, että $m \leq n$. Olkoon k sellainen pienin kokonaisluku välillä $1 \leq k \leq m+1$, että $s_k^{\epsilon_k} \neq r_{m-k+1}^{-\delta_{m-k+1}}$. Tällöin näiden sievennettyjen sanojen tuloksi määritellään

$$(r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m})(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = \begin{cases} r_1^{\delta_1} \dots r_{m-k+1}^{\delta_{m-k+1}} s_k^{\epsilon_k} \dots s_n^{\epsilon_n}, & \text{jos } k \leq m \\ s_{m+1}^{\epsilon_{m+1}} \dots s_n^{\epsilon_n}, & \text{jos } k = m+1 \leq n \\ 1, & \text{jos } k = m+1 \text{ ja } m = n. \end{cases}$$

Tulo määritellään vastaavasti, jos $m \geq n$, joten molemmissa tapauksissa kahden sievennetyn sanan tulo on sievennetty sana.

Lause 3.2. *Joukko $F(S)$ on ryhmä edellä määritellyn binäärisen operaation suhteen.*

Todistus. Nyt $F(S) \neq \emptyset$, sillä $s \in F(S)$, jos $s \in S$ ja $F(S) = \{1\}$, jos $S = \emptyset$. Alkio $1 \in F(S)$ on neutraalialkio, sillä $1s = s1 = s$ kaikilla $s \in F(S)$. Sievennetyn sanan $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n} \in F(S)$ käänteisalkio on sievennetty sana $s_n^{-\epsilon_n} s_{n-1}^{-\epsilon_{n-1}} \dots s_1^{-\epsilon_1} \in F(S)$, sillä

$$(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n})(s_n^{-\epsilon_n} s_{n-1}^{-\epsilon_{n-1}} \dots s_1^{-\epsilon_1}) = (s_n^{-\epsilon_n} s_{n-1}^{-\epsilon_{n-1}} \dots s_1^{-\epsilon_1})(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = 1.$$

Enää täytyy osoittaa, että joukon $F(S)$ operaatio on assosiatiivinen. Tätä varten määritellään kaikille $s \in S \cup S^{-1} \cup \{1\}$ kuvaus $\sigma_s : F(S) \to F(S)$, missä

$$\sigma_s(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = \begin{cases} s \cdot s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}, & \text{jos } s_1^{\epsilon_1} \neq s^{-1} \\ s_2^{\epsilon_2} s_3^{\epsilon_3} \dots s_n^{\epsilon_n}, & \text{jos } s_1^{\epsilon_1} = s^{-1}. \end{cases}$$

Nyt $\sigma_{s^{-1}}(s \cdot s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = s^{-1} \cdot s \cdot s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n} = s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$, kun $s_1^{\epsilon_1} \neq s^{-1}$ ja $\sigma_{s^{-1}}(s_2^{\epsilon_2} s_3^{\epsilon_3} \dots s_n^{\epsilon_n}) = s^{-1} \cdot s_2^{\epsilon_2} s_3^{\epsilon_3} \dots s_n^{\epsilon_n} = s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$, kun $s_1^{\epsilon_1} = s^{-1}$, joten yhdistetty kuvaus $\sigma_{s^{-1}} \circ \sigma_s$ on identtinen kuvaus joukolta $F(S)$ itselleen. Kuvaus σ_s on siis bijektio ja täten joukon $F(S)$ permutaatio.

Olkoon $A(S)$ joukolla $F(S)$ määritellyn symmetrisen ryhmän aliryhmä, jonka generoi joukko $\{\sigma_s \mid s \in S\}$. Tällöin aliryhmän $A(S)$ kaikki alkiot ovat luvun 2 mukaan muotoa $\sigma_{s_1}^{\epsilon_1} \circ \sigma_{s_2}^{\epsilon_2} \circ \dots \circ \sigma_{s_n}^{\epsilon_n}$. Nyt kuvaus

$$s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n} \mapsto \sigma_{s_1}^{\epsilon_1} \circ \sigma_{s_2}^{\epsilon_2} \circ \dots \circ \sigma_{s_n}^{\epsilon_n}$$

on bijektio joukolta $F(S)$ joukolle $A(S)$ ja on yhteensopiva binäärioperaatioiden suhteen. Koska $A(S)$ on ryhmänä assosiatiivinen, myös $F(S)$ on assosiatiivinen. Siis $F(S)$ on ryhmä.

□

Esimerkki 3.3. Olkoon $S = \{a, b\}$. Kahden alkion generoiman vapaan ryhmän $F(\{a, b\})$ alkiot ovat tällöin alkioiden a ja b sekä niiden käänteisalkioiden muodostamia äärellisiä sanoja. Siis kaikki vapaan ryhmän $F(\{a, b\})$ alkiot ovat muotoa

$$a^{\alpha_1} b^{\alpha_2} a^{\alpha_3} b^{\alpha_4} \dots a^{\alpha_{n-1}} b^{\alpha_n},$$

missä $\alpha_i \in \mathbb{Z}$, kun $i \in \{1, n\}$ ja $\alpha_i \in \mathbb{Z} \backslash \{0\}$, kun $i \notin \{1, n\}$.

Lähdeluettelo

[1] David S. Dummit, Richard M. Foote: *Abstract Algebra, Second Edition.* John Wiley & Sons, Inc., New York, 1999.

[2] Markku Niemenmaa, Kari Myllylä, Topi Törmä: *802354A Algebran perusteet, Luentorunko, Kevät 2016.*