Sykliset ryhmät

Vilma Karttunen

LuK-tutkielma
Huhtikuu 2024

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Vilma Karttunen: Sykliset ryhmät
LuK-tutkielma, 11 s.
Matematiikka
Huhtikuu 2024

Tässä tutkielmassa esitetään syklisen ryhmän määritelmä sekä siihen liittyviä tuloksia ja esimerkkejä. Tämän jälkeen määritetään syklisten ryhmien aliryhmärakenteeseen liittyviä tärkeimpiä tuloksia ja esimerkkejä. Aliryhmärakennetta tarkastellaan erikseen äärellisille ja äärettömille syklisille ryhmille.

Asiasanat: syklinen ryhmä, syklisen ryhmän aliryhmärakenne.

Sisällys

1 Johdanto

Sykliset ryhmät kuuluvat ryhmäteoriaan, joka on syntynyt lähteessä [1] esiteltyjen neljän eri matematiikan osa-alueen seurauksena. Lagrangen kehittämä klassinen algebra 1770-luvulla toimi ensimmäisenä askeleena kohti ryhmäteoriaa. Hän osoitti, että ryhmän koko k on luvun $n!$ jakaja. Tämä tulos toimi ryhmäteoriassa käytettävän Lagrangen teoreeman lähteenä. Vuonna 1801 Gaussin julkaisemassa Disquisitiones Arithmeticae -kirjassa esitettiin äärellisen Abelin ryhmän ensimmäisiä tuloksia. Tulokset esitettiin lukuteorian asioina, mutta Gaussin todistukset olivat selkeästi nykyaikaisen algebran alkeellisia Abelin ryhmään perustuvia todistuksia. Gauss esitteli myös ensimmäisen kerran syklisen ryhmän määritelmän ja siihen liittyviä tuloksia.

Kolmas ryhmäteoriaa edeltävä tulos on Kleinin vuonna 1872 Erlangenin yliopistossa pitämä luento, jossa käsiteltiin geometrian näkökulmasta erilaisia ryhmiä. Kleinin esittelemä ryhmien käyttö geometriassa toi kertaluvut lopullisesti osaksi geometriaa. Analyysi on viimeinen ryhmäteoriaan johtanut matematiikan osa-alue. Pointcaré ja Klein aloittivat automorfisten funktioiden ja niihin liittyvien ryhmien tutkimisen vuonna 1876. Ryhmäteoria muovautui siis klassisen algebran permutaatioryhmien, lukuteorian Abelin ryhmien sekä geometrian ja analyysin muunnosryhmien seurauksena.

2 Sykliset ryhmät

Syklisessä ryhmässä jokainen ryhmän alkio on jonkin kiinteän alkion potenssi. Syklinen ryhmä on siis yhden alkion generoima. Määritellään seuraavaksi muutamia tärkeitä määritelmiä. Luku perustuu Ikenagan monisteeseen [2].

Määritelmä 2.1. Olkoon G ryhmä ja $g \in G$. Pienin mahdollinen positiivinen kokonaisluku n, jolla $g^n = 1$, on alkion g *kertaluku* eli alkioiden lukumäärä aliryhmässä. Jos ei ole olemassa yhtään positiivista kokonaislukua n, jolla $g^n = 1$, niin alkion g kertaluku on *ääretön*.

Määritelmä 2.2. Jos G on ryhmä ja $g \in G$, niin alkion g *generoima aliryhmä* on $\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$.

Määritelmän 2.3 perusteella yhden alkion generoima ryhmä on syklinen.

Määritelmä 2.3. Ryhmä G on *syklinen*, jos $G = \langle g \rangle$ jollakin $g \in G$. Tällöin g on ryhmän $\langle g \rangle$ generaattori. Jos generaattorin g kertaluku on n, niin myös syklisen ryhmän $G = \langle g \rangle$ kertaluku on n.

Esimerkin 2.4 avulla voidaan tarkastella, millä kokonaisluvuilla ja kokonaisluvuilla modulo n ryhmät ovat syklisiä.

Esimerkki 2.4. Tarkastellaan additiivista ryhmää $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Määritetään, mitkä alkiot generoivat ryhmää. Lasketaan jokaiselle alkiolle n seuraavanlainen lasku, jossa alkiota summataan itseensä. Esimerkiksi kun $n = 3$, niin

$$\begin{aligned}
3 + 3 &\equiv 6 \pmod 7 \\
3 + 3 + 3 = 9 &\equiv 2 \pmod 7 \\
3 + 3 + 3 + 3 = 12 &\equiv 5 \pmod 7 \\
3 + 3 + 3 + 3 + 3 = 15 &\equiv 1 \pmod 7 \\
3 + 3 + 3 + 3 + 3 + 3 = 18 &\equiv 4 \pmod 7 \\
3 + 3 + 3 + 3 + 3 + 3 + 3 = 21 &\equiv 0 \pmod 7.
\end{aligned}$$

Koska jokaisella laskulla saadaan eri tulos, voidaan sanoa, että numero 3 generoi ryhmän $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Tulokset siis kiertävät ikään kuin kehää, jossa käydään läpi luvut 0–6. Käy ilmi, että ryhmässä $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ kaikki muut alkiot paitsi 0 generoivat ryhmää.

Tarkastellaan seuraavaksi ryhmää $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Lasketaan taas jokaiselle alkiolle sama lasku. Esimerkiksi tapauksille $n = 2$ ja $n = 5$ saadaan

$$\begin{aligned}
2 + 2 &\equiv 4 \pmod 6 \\
2 + 2 + 2 = 6 &\equiv 0 \pmod 6 \\
2 + 2 + 2 + 2 = 8 &\equiv 2 \pmod 6 \\
2 + 2 + 2 + 2 + 2 = 10 &\equiv 4 \pmod 6 \\
2 + 2 + 2 + 2 + 2 + 2 = 12 &\equiv 0 \pmod 6
\end{aligned}$$

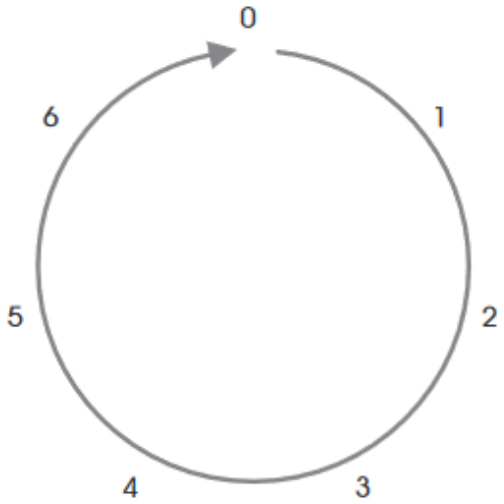
ja

$$\begin{aligned}
5 + 5 = 10 &\equiv 4 \pmod 6 \\
5 + 5 + 5 = 15 &\equiv 3 \pmod 6 \\
5 + 5 + 5 + 5 = 20 &\equiv 2 \pmod 6 \\
5 + 5 + 5 + 5 + 5 = 25 &\equiv 1 \pmod 6 \\
5 + 5 + 5 + 5 + 5 + 5 = 30 &\equiv 0 \pmod 6.
\end{aligned}$$

Laskujen perusteella voidaan huomata, että $n = 5$ generoi ryhmän, koska sen antamissa tuloksissa ryhmän alkiot eivät toistu. Luku 2 puolestaan ei voi olla ryhmän

$\mathbb{Z}_6$ generaattori, koska sama tulos esiintyy useamman kerran. Tällöin ei muodostu sykliä. Kun lasketaan sama lasku kaikilla alkioilla, voidaan todeta, että ryhmää $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ generoivat vain luvut 1 ja 5.

Ikenaga [2] on esittänyt havainnollistavan kuvan syklisestä ryhmästä kertaluvulla 7. Kuvasta voidaan nähdä, että syklisessä ryhmässä tiettyä alkiota keskenään summaamalla päästään lopulta kierroksen ympäri takaisin lukuun 0. Yleisesti voidaan sanoa, että äärellinen syklinen ryhmä muodostaa syklin.



Kuva 1: Syklinen ryhmä kertaluvulla 7.

Määritetään seuraavaksi syklisen ryhmän alkion kertaluku suurimman yhteisen tekijän ja jakoalgoritmin avulla. Ensin annetaan lemma 2.5, jonka perusteella alkion kertaluku m on jokaisen ryhmän identiteettialkion antavan potenssin n jakaja.

Lemma 2.5. *Olkoon G ryhmä ja alkiolla $g \in G$ on kertaluku m. Tällöin $g^n = 1$ jos ja vain jos m on kertaluvun n jakaja.*

Todistus. Oletetaan, että m on kertaluvun n jakaja. Tällöin $n = mq$ jollakin kokonaisluvulla q ja $g^n = (g^m)^q = 1$.

Todistetaan sama toiseen suuntaan. Oletetaan, että $g^n = 1$. Jakoalgoritmin perusteella

$$n = mq + r, \text{ missä } 0 \leq r < m.$$

Tästä seuraa, että

$$g^n = g^{mq+r} = (g^m)^q g^r \text{ joten } 1 = g^r.$$

Tämä on mahdollista vain silloin, kun $r = 0$, sillä m on pienin mahdollinen positiivinen kokonaisluku, jolla $g^m = 1$ ja $r < m$. Tämän perusteella siis $n = qm$, joten m on kertaluvun n jakaja. □

Lause 2.6. *Olkoon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku on n ja $m < n$. Tällöin alkion g^m kertaluku on $\frac{n}{(m,n)}$.*

Todistus. Suurin yhteinen tekijä (m, n) on luvun m jakaja, joten $\frac{m}{(m,n)}$ on kokonaisluku. Tällöin lemman 2.5 mukaan $(g^m)^{\frac{n}{(m,n)}} = 1$, koska n on kokonaisluvun $\frac{mn}{(m,n)}$ jakaja.
Oletetaan, että $(g^m)^k = 1$. Koska lemman 2.5 perusteella n on luvun mk jakaja, voidaan kirjoittaa

$$\frac{n}{(m,n)} \mid k \cdot \frac{m}{(m,n)}.$$

Suurin yhteinen tekijä $(\frac{n}{(m,n)}, \frac{m}{(m,n)}) = 1$, joten kokonaisluvun $\frac{n}{(m,n)}$ täytyy olla luvun k jakaja. Luku $\frac{n}{(m,n)}$ on siis minkä tahansa potenssin $g^m = 1$ jakaja. Tämän perusteella $\frac{n}{(m,n)}$ on alkion g^m kertaluku. □

Lausetta 2.6 jatkavan seurauksen 2.7 avulla voidaan määrittää ryhmän generaattorit.

Seuraus 2.7. *Ryhmän $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ generaattorit ovat ne alkiot $\{0, 1, 2, ..., n-1\}$, joiden ainoa yhteinen tekijä kokonaisluvun n kanssa on luku 1.*

Todistus. Olkoon $m \in \{0, 1, 2, ..., n-1\}$ generaattori kertaluvulla n. Lauseen 2.6 perusteella kertaluku on $\frac{n}{(m,n)}$, joten $n = \frac{n}{(m,n)}$. Tällöin siis suurin yhteinen tekijä $(m, n) = 1$. Osoitetaan tulos vielä toiseen suuntaan. Jos lukujen m ja n suurin yhteinen tekijä $(m, n) = 1$, niin generaattorin m kertaluku on $\frac{n}{(m,n)} = \frac{n}{1} = n$. Ryhmän $\mathbb{Z}_n$ generaattori on siis m. □

Havainnollistetaan ryhmän generaattoreiden määrittämistä seuraavalla esimerkillä 2.8.

Esimerkki 2.8. Ryhmän $\mathbb{Z}_{12}$ kaikki alkiot ovat $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. Näistä alkioista ryhmän $\mathbb{Z}_{12}$ generaattorit ovat 1, 5, 7 ja 11. Kyseisillä alkioilla on vain luku 1 yhteisenä tekijänä luvun 12 kanssa. Esimerkiksi luvuilla 6 ja 12 yhteisiä tekijöitä ovat 1, 2 ja 3, joten luku 6 ei voi olla generaattori.

3 Syklisten ryhmien aliryhmärakenteet

Määritellään yleisen syklisen ryhmän $G = \langle g \rangle$ aliryhmärakenteisiin liittyviä tärkeimpiä tuloksia. Luku perustuu pääosin Conradin monisteeseen [3]. Lause 3.1 on esitelty Ikenagan monisteessa [2].

Lause 3.1. *Syklisen ryhmän kaikki aliryhmät ovat syklisiä.*

Todistus. Olkoon $G = \langle g \rangle$ syklinen alkion g generoima ryhmä, missä $g \in G$. Olkoon H ryhmän G aliryhmä $H < G$ ja $H \neq \{1\}$.

Jotta voidaan näyttää, että aliryhmä H on syklinen, täytyy sille löytää generaattori. Generaattori on pienin alkio, jonka potensseista ryhmä koostuu. Olkoon m pienin positiivinen kokonaisluku, jolla $g^m \in H$. Osoitetaan siis seuraavaksi, että g^m on aliryhmän H generaattori.

Koska $h \in H < G$, toteutuu $h = g^n$ jollekin luvulle n. Jakoalgoritmin mukaan

$$n = mq + r, \text{ missä } 0 \leq r < m.$$

Jakoalgoritmin ja aiempien päätelmien perusteella voidaan kirjoittaa

$$g^n = g^{mq+r} = (g^m)^q \cdot g^r, \text{ joten } h = (g^m)^q \cdot g^r \text{ eli } g^r = (g^m)^{-q} \cdot h.$$

Koska $g^m \in H$, niin $(g^m)^{-q} \in H$. Tästä seuraa, että $(g^m)^{-q} \cdot h \in H$, joten myös $g^r \in H$. Koska g^m on pienin positiivinen alkion g potenssi aliryhmässä H ja $r < m$, täytyy luvun r olla 0. Tämän perusteella jakoalgoritmi on muotoa $n = qm$ ja $h = g^n = (g^m)^q \in \langle g^m \rangle$. On siis todistettu, että g^m on aliryhmän H generaattori, joten H on syklinen. □

Määritetään äärellisen syklisen ryhmän $G = (\mathbb{Z}/(7))^*$ aliryhmät Conradin monisteeseen [3] perustuvan esimerkin 3.2 avulla.

Esimerkki 3.2. Olkoon $G = (\mathbb{Z}/(7))^*$. Ryhmän koko on siis 6. Lasketaan alkioiden peräkkäisiä potensseja, kunnes päästään lukuun 1. Esimerkiksi alkiolle $n = 2$ saadaan

$$2^1 \equiv 2 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$2^3 = 8 \equiv 1 \pmod 7.$$

Kaikki tulokset ovat taulukossa 1.

Taulukko 1: Alkioiden peräkkäiset potenssit.

a	$\langle a \rangle$
1	$\{1\}$
2	$\{2, 4, 1\}$
3	$\{3, 2, 6, 4, 5, 1\}$
4	$\{4, 2, 1\}$
5	$\{5, 4, 6, 2, 3, 1\}$
6	$\{6, 1\}$

Ryhmällä $(\mathbb{Z}/(7))^*$ on siis neljä aliryhmää: $\{1\}$, $\{1, 6\}$, $\{1, 2, 4\}$, $\{1, 2, 3, 4, 5, 6\}$. Jokainen näistä aliryhmistä on syklinen lauseen 3.1 perusteella.

Esimerkin 3.2 kaltainen äärellisen syklisen ryhmän aliryhmien määritys ei ole paras tapa määrittää aliryhmiä, koska siinä esiintyy turhaa toistoa. Samat aliryhmät nimittäin esiintyvät useampaan kertaan, jolloin niiden laskeminen on turhaa. Määritellään seuraavaksi aliryhmien määritystä helpottavia tuloksia.

Lemma 3.3. *Jos g on äärettömän kertaluvun alkio ryhmässä, niin $g^k = g^l$ jos ja vain jos $k = l$.*

Todistus. Tehdään vastaoletus, jossa $g^k = g^l$, kun $k < l$. Tällöin $g^{k-l} = e$, kun $l - k \neq 0$, joten alkiolla g on äärellinen kertaluku. Kertaluvun pitäisi olla ääretön, joten vastaoletus voidaan kumota. Alkiolla g on siis ääretön kertaluku ja $g^k = g^l$, kun $k = l$. □

Lause 3.4 määrittelee äärettömän syklisen ryhmän aliryhmät.

Lause 3.4. *Jokaisella äärettömän syklisen ryhmän ei-triviaalilla aliryhmällä on kaksi generaattoria. Nämä ovat toistensa käänteisluvut. Jos koko ryhmää generoi vain yksi generaattori g, on jokainen aliryhmä muotoa $\langle g^n \rangle$. Tällöin $n \geq 0$ on yksikäsitteinen.*

Todistus. Lauseen 3.1 perusteella kaikki aliryhmät ovat muotoa $\langle g^n \rangle$ jollakin kokonaisluvulla n. Koska $\langle g^n \rangle = \langle g^{-n} \rangle$, niin riittää tarkastella vain tilannetta $n \geq 0$.

Kun $n = 0$, on aliryhmä triviaali. Tällöin $g^0 = 1$ ja halutut johtopäätökset ovat helposti saatavissa. Tarkastellaan siis ei-triviaaleja aliryhmiä. Osoitetaan, että positiiviset kokonaisluvut n ja n' toteuttavat yhtäsuuruuden $\langle g^n \rangle = \langle g^{n'} \rangle$ vain jos $n = n'$. Kun aliryhmät ovat yhtä suuret, täytyy lukujen g^n ja $g^{n'}$ olla toistensa potensseja.

Joillakin luvuilla s ja $t \in \mathbb{Z}$ täytyy siis toteutua $g^n = g^{n's}$ ja $g^{n'} = g^{nt}$. Lemman 3.3 perusteella $n = n's$ ja $n' = nt$, joten n ja n' ovat ovat molemmat toistensa jakajat. Niiden täytyy siis olla yhtä suuret eli $n = n'$. □

Siirrytään tarkastelemaan äärellistä syklistä ryhmää. Lause 3.5 kertoo aliryhmien kokojen ja syklisen ryhmän jakajien välisen yhteyden.

Lause 3.5. *Jokaisen aliryhmän koko jakaa äärellisen syklisen ryhmän koon. Käänteen, jokaista äärellisen syklisen ryhmän positiivista jakajaa kohtaan on olemassa jakajan kokoinen aliryhmä.*

Todistus. Olkoot $G = \langle g \rangle$ ja ryhmän G koko m. Kaikki aliryhmät ovat muotoa $\langle g^k \rangle$, jollakin kokonaisluvulla k. Aliryhmän koko on luvun g^k kertaluku eli väitteen 2.6 perusteella $\frac{m}{(k,m)}$. Aliryhmän koko jakaa siis luvun m.

Merkitään ryhmän koon m positiivista jakajaa merkinnällä d. Koska kertaluku $d = \frac{m}{\frac{m}{d}}$, on kertaluvun d alkio tietyn ryhmän G generaattorin suhteen $g^{m/d}$. Aliryhmän $\langle g^{m/d} \rangle$ koko on siis d. □

Seuraavassa lausessa 3.6 annetaan vahvempi tulos lauseelle 3.5. Lauseen 3.6 mukaan jokaiselle äärellisen syklisen ryhmän koon jakajalle on olemassa tasan yksi jakajan kanssa samankokoinen aliryhmä. Tämä on yksi Conradin [3] esittämistä päätuloksista.

Lause 3.6. *Olkoon $G = \langle g \rangle$ äärellinen syklinen ryhmä, jonka koko on m. Kaikille $k \in \mathbb{Z}$ aliryhmä $\langle g^k \rangle = \langle g^{(k,m)} \rangle$. Mikä tahansa ryhmän G aliryhmä on siis muotoa $\langle g^d \rangle$, missä d on ryhmän koon m positiivinen jakaja. On olemassa vain yksi tietyn kokoinen ryhmän G aliryhmä, koska jakajan d eri arvot muodostavat erikokoiset aliryhmät.*

Todistus. Lauseen 3.1 perusteella kaikki ryhmän G aliryhmät $\langle g^k \rangle$ ovat myös syklisiä. Osoitetaan, että g^k ja $g^{(k,m)}$ generoivat saman aliryhmän näyttämällä, että ne ovat molemmat toistensa potensseja.

Koska $(k, m)|k$, niin g^k on luvun $g^{(k,m)}$ potenssi. Jotta tilanne voidaan osoittaa toiseen suuntaan, käytetään Bezout'n identiteettiä

$$(k, m) = kx + my \text{ joillekin } x, y \in \mathbb{Z}.$$

Bezout'n identiteetin ja yksinkertaistuksen $g^m = g^{\#G} = e$ avulla saadaan

$$g^{(k,m)} = g^{kx} g^{my} = g^{kx}.$$

Koska $d|m$ ja luvulla g^d on positiivinen kertaluku $\frac{m}{d}$, niin $\#\langle g^d \rangle = \frac{m}{d}$. Jos d ja d' olisivat eri suuret ryhmän koon m jakajat, niin $\langle g^d \rangle \neq \langle g^{d'} \rangle$. Positiivisen jakajan d täytyy olla siis yksikäsitteinen, jotta aliryhmät olisivat yhtä suuret. □

Määritetään seuraavaksi, millä ehdolla äärellisen syklisen ryhmän kahdesta aliryhmästä toinen voi olla toisen aliryhmän osajoukko.

Seuraus 3.7. *Olkoon G äärellinen syklinen ryhmä. Aliryhmä H on aliryhmän H' osajoukko $H \subset H'$, jos ja vain jos niiden kertaluvuille pätee $\#H|\#H'$.*

Todistus. Lauseen 3.1 perusteella aliryhmät H ja H' ovat syklisiä. Lauseen 3.5 mukaan, jos H on aliryhmän H' aliryhmä, niin $\#H|\#H'$.

Todistetaan tulos vielä toiseen suuntaan. Oletetaan, että $\#H|\#H'$ pätee. Tällöin lauseen 3.5 mukaan on olemassa aliryhmä $K \subset H'$, jonka koko on $\#H$. Koska H' on äärellisen syklisen ryhmän G aliryhmä, niin myös K on ryhmän G aliryhmä. Aliryhmän K koko on $\#H$. Lauseen 3.6 perusteella ryhmällä G voi olla vain yksi tietyn kokoinen aliryhmä, joten $K = H$. □

Syklisten ryhmien aliryhmärakennetta voidaan verrata lähteessä [4] esitettyyn Lagrangen lauseeseen 3.8.

Lause 3.8. *Äärellisen ryhmän G aliryhmän H kertaluku jakaa ryhmän G kertaluvun eli $[G : H]=\#G \mid \#H$.*

Todistus. Kuvaus $H \to aH$, $h \mapsto ah$ on bijektio, joten kaikkien sivuluokkien aH alkioiden lukumäärä on sama kuin aliryhmän H alkioiden lukumäärä. Koska $[G : H] \in \mathbb{Z}$, niin voidaan kirjoittaa

$$\#G = \sum_{a \in D} \#(aH) = \sum_{a \in D} \#H = [G \ : \ H] \cdot \#H.$$

□

Seurausta 3.7 ja lausetta 3.8 vertaamalla voidaan nähdä, että niissä on paljon samaa. Molemmissa todistetaan aliryhmän olemassaolo kertalukujen jaollisuuden avulla. Lagrangen lauseelle onkin olemassa lähteessä [4] esitetty seuraus, joka yhdistää sen syklisiin ryhmiin.

Seuraus 3.9. *Ryhmä G on syklinen, jos sen kertaluku on alkuluku.*

Todistus. Olkoot g ryhmän G alkio ja $g \neq 1$. Alkion g kertaluku $\#g$ jakaa alkuluvun p ja $\#g > 1$. Tästä seuraa, että $\#g = p$ eli alkion kertaluku on alkuluku. Ryhmä G on siis syklinen. □

Havainnollistetaan vielä syklisen ryhmän aliryhmien ja niiden kertalukujen määritystä sekä niihin liittyvää ristikkomallia esimerkin 3.10 avulla.

Esimerkki 3.10. Olkoon $G = (\mathbb{Z}/(11))^x$ syklinen ryhmä, jonka koko on 10. Lasketaan $2^k \pmod{11}$ jokaiselle ryhmän alkiolle. Esimerkiksi kun $k = 6$, niin $2^k \equiv 9 \pmod{11}$. Kaikki tulokset näkyvät taulukossa 2.

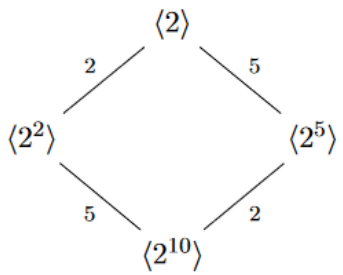
Taulukko 2: Luvun 2 potenssit modulo 11.

k	1	2	3	4	5	6	7	8	9	10
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Ryhmän G aliryhmät ovat

$$\begin{aligned}
\langle 2 \rangle &= \left\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\right\} \\
\langle 2^2 \rangle &= \left\{2^2, 2^4, 2^6, 2^8, 2^{10}\right\} \\
\langle 2^5 \rangle &= \left\{2^5, 2^{10}\right\} \\
\langle 2^{10} \rangle &= \left\{2^{10}\right\}.
\end{aligned}$$

Aliryhmien kertaluvut ovat 10, 5, 2 ja 1. Nämä ovat siis aliryhmien muodostavien alkioiden lukumäärät. Aliryhmät voidaan piirtää ristikkomalliin, jossa koko ryhmä $\langle 2 \rangle$ on ylhäällä ja triviaali aliryhmä $\langle 2^{10} \rangle$ alhaalla. Ne voidaan yhdistää viivoilla, jotka osoittavat aliryhmien välisen indeksin. Esimerkiksi aliryhmässä $\langle 2^2 \rangle$ on 5 alkiota ja aliryhmässä $\langle 2 \rangle$ on 10 alkiota. Niiden välinen indeksi on siis 2.



Taulukon 2 avulla voidaan myös määrittää, mikä aliryhmistä on $\langle 3 \rangle$. Tämä voidaan tehdä kahdella eri tavalla.

Tapa 1: Lasketaan luvun 3 kertaluku ryhmässä G eli pienin positiivinen kokonaisluku k, jolla $3^k \equiv 1 \pmod{11}$:

$$3^1 \equiv 3 \pmod{11}$$
$$3^2 \equiv 9 \pmod{11}$$
$$3^3 \equiv 5 \pmod{11}$$
$$3^4 \equiv 4 \pmod{11}$$
$$3^5 \equiv 1 \pmod{11}.$$

Luvun 3 kertaluku ryhmässä G on siis 5. Sama kertaluku on aliryhmällä $\langle 2^2 \rangle$, joten $\langle 3 \rangle = \langle 2^2 \rangle$.

Tapa 2: Taulukon 2 perusteella $3 \equiv 2^8 \pmod{11}$. Luku 3 generoi siis saman aliryhmän kuin $2^{(8,10)} = 2^2$. Siis $\langle 3 \rangle = \langle 2^2 \rangle$.

Viitteet

[1] I. Kleiner: *A History of Abstract Algebra*.
https://doi.org/10.1007/978-0-8176-4685-1, luettu 21.3.2024

[2] B. Ikenaga: *Cyclic groups*. 2019
https://sites.millersville.edu/bikenaga/abstract-algebra-1/cyclic-groups/cyclic-groups.html, luettu 9.4.2024

[3] K. Conrad: *Subgroups of cyclic groups*.
https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicgp.pdf, luettu 9.4.2024

[4] M. Koppinen: *Algebran peruskurssi I*. Turun yliopisto, 2006