Syklinen ryhmä

Pro Gradu -tutkielma

Taava Kuha

Matemaattisten tieteiden laitos

Oulun yliopisto

2016

Sisältö

Johdanto

Tutkielmassa esitetään algebrallisen rakenteen, syklisen ryhmän, teoriaa ja ominaisuuksia. Tutkielman aluksi käydään läpi ryhmäteorian alkeita, jotta varsinaisen aiheen, syklisen ryhmän, ominaisuudet saadaan esitettyä selkeästi ja ymmärrettävästi.

Tutkielman aluksi esitetään ryhmän määritelmä. Käydään läpi ryhmän toteuttamat aksioomat assosiatiivisuus, ykkös- eli neutraalialkion olemassaolo sekä käänteisalkion olemassaolo. Määritellään myös ryhmän kertaluku eli ryhmän alkioiden lukumäärä, joka on oleellisena osana syklisen ryhmän rakenteen määrittämistä.

Seuraavaksi määritellään ryhmän aliryhmä, josta etenkin aliryhmäkriteeri nousee tärkeään osaan. Tutkielmassa käsitellään myös aliryhmän vasemmat ja oikeat sivuluokat, jotta saadaan ymmärrettävästi esitettyä äärellisten ryhmien perustulos, Lagrangen lause. Lopuksi esitetään vielä ryhmäteoriaan oleellisena osana kuuluvat normaali aliryhmä ja tekijäryhmä sekä määritellään ryhmähomomorfismi.

Näiden pohjatietojen jälkeen syvennytään tutkielman aiheeseen, sykliseen ryhmään. Aihetta lähestytään ryhmän alkioiden kokonaislukupotenssien kautta, jonka jälkeen esitetään syklisen ryhmän määritelmä ja lauseet todistuksineen.

Tutkielmassa esitetään tarkasti syklisen ryhmän ominaisuudet. Aluksi käydään läpi syklisen ryhmän kommutatiivisuus, esitetään alkion kertaluvun määrittämät ominaisuudet sekä todistetaan syklisen ryhmän tekijäryhmän syklisyys.

Seuraavaksi syvennytään syklisen ryhmän isomorfisuuteen. Todetaan, että samaa kertalukua olevat sykliset ryhmät ovat isomorfisia keskenään sekä esitetään isomorfisuus niin äärellisessä kuin äärettömässäkin tapauksessa.

Tutkielman lopuksi isompana aihealueena määritellään syklisen ryhmän ali-

ryhmä. Osoitetaan, että syklisen ryhmän aliryhmät voidaan esittää ja luetella tarkasti sekä äärettömässä että äärellisessä tapauksessa. Osoitetaan myös syklisen ryhmän aliryhmän syklisyys sekä aliryhmän normaalisuus.
Tutkielman lähteenä on käytetty pääasiassa teosta [6]. Apuna on käytetty myös useita muita abstraktin algebran julkaisuja ja teoksia.

1 Ryhmäteoriaa

Tässä luvussa käydään läpi ryhmäteorian alkeita, jotka luovat pohjaa varsinaisen aiheen käsittelyyn. Esitetään ryhmän ja aliryhmän määritelmät ja lauseet todistuksineen sekä määritellään normaali aliryhmä, tekijäryhmä ja ryhmähomomorfismi.

1.1 Ryhmän määritelmä

Ryhmä on yhden joukon ja yhden laskutoimituksen muodostava algebrallinen rakenne. Joukon tulee olla suljettu laskutoimituksen suhteen.

Määritelmä 1.1.1. Olkoon S epätyhjä joukko. Kuvaus $S \times S \to S$ on joukon S laskutoimitus eli **binäärinen operaatio**.
Merkitään binääristä operaatiota symbolilla $(*)$. Binäärinen operaatio liittää jokaiseen järjestettyyn pariin $(a, b) \in S \times S$ joukon S erään yksikäsitteisen alkion $a * b$. Nyt siis $a * b \in S$ aina, kun $a, b \in S$. Koska laskutoimituksen arvojoukko on joukon S osajoukko, sanotaan joukon S olevan suljettu laskutoimituksen $(*)$ suhteen.

Määritelmä 1.1.2. Binäärinen operaatio $(*)$ on

i) **assosiatiivinen** (liitännäinen) joukossa S, mikäli $a*(b*c) = (a*b)*c$ aina, kun $a, b, c \in S$,

ii) **kommutatiivinen** (vaihdannainen) joukossa S, mikäli $a * b = b * a$ aina, kun $a, b \in S$.

Määritelmä 1.1.3. Pari $(G, *)$, missä G on epätyhjä joukko ja $(*)$ siihen liittyvä binäärinen operaatio, on **yhden laskutoimituksen algebrallinen struktuuri**.

Määritelmä 1.1.4. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G binäärinen operaatio. Pari $(G, *)$ on **ryhmä** (group), mikäli

G1) operaatio $(*)$ on assosiatiivinen eli

$$a * (b * c) = (a * b) * c$$

aina, kun $a, b, c \in G$;

G2) on olemassa sellainen alkio $e \in G$, että

$$a * e = a = e * a$$

aina, kun $a \in G$. Alkiota e kutsutaan **ykkös- eli neutraalialkioksi** (identity/neutral element);

G3) aina, kun $a \in G$, on olemassa sellainen alkio $b \in G$, että

$$a * b = b * a = e.$$

Alkiota b kutsutaan alkion a **käänteisalkioksi** (inverse element). Ryhmän alkion a käänteisalkiota merkitään symbolilla a^{-1}.

Ryhmä on siis algebrallinen struktuuri, joka toteuttaa aksioomat G1, G2 ja G3.
Jos lisäksi pari $(G, *)$ toteuttaa kommutatiivisuuden ehdon

G4) $a * b = b * a$ aina, kun $a, b \in G$,

niin kyseessä on **Abelin ryhmä** eli kommutatiivinen ryhmä. Jos $a*b = b*a$, niin alkioiden a ja b sanotaan kommutoivan. Jos alkiot a ja b eivät kommutoi, on kyseessä ei-kommutatiivinen ryhmä.

Esimerkki 1.1.5. *Reaalilukujen joukko* $\mathbb{R}$ *ja kompleksilukujen joukko* $\mathbb{C}$ *ovat yhteenlaskun suhteen ryhmiä. Nyt yhteenlasku on assosiatiivinen, neutraalialkiona luku* 0 *ja alkion* a *käänteisalkiona on vastaluku* $-a$.

Joukot $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ *ja* $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ *ovat kertolaskun suhteen ryhmiä. Binäärinen operatio on nyt assosiatiivinen, neutraalialkiona on luku* 1 *ja alkion* $a \neq 0$ *käänteisalkiona käänteisluku* $a^{-1} = \frac{1}{a}$.
Luonnolliset luvut varustettuna yhteenlaskulla ei ole ryhmä. Nyt yhteenlasku on assosiatiivinen ja neutraalialkiona on luku 0, *mutta joukosta puuttuu käänteisalkioita. Esimerkiksi luonnollisella luvulla* 1 *ei ole käänteisalkiota, sillä ei ole olemassa sellaista lunnollista lukua* n, *jolle pätee* $n + 1 = 0$.

Jatkossa ryhmästä $(G, *)$ käytetään merkintää G, mikäli operaatiosta $(*)$ ei ole epäselvyyttä. Ja näin ollen operaatiota $a * b$ merkitään lyhyemmin ab.

Lause 1.1.6. *Olkoon* G *ryhmä. Tällöin*

i) on olemassa yksikäsitteinen neutraalialkio $e \in G$, *jolle* $e * a = a = a * e$ *aina, kun* $a \in G$,

ii) aina kun $a \in G$, *on olemassa yksikäsitteinen käänteisalkio* $a^{-1} \in G$, *jolle* $a * a^{-1} = e = a^{-1} * a$,

iii) yhtälöllä $ax = b$ *on yksikäsitteinen ratkaisu* $x \in G$, *kun* $a, b \in G$,

iv) yhtälöllä $ya = b$ *on yksikäsitteinen ratkaisu* $y \in G$, *kun* $a, b \in G$.

Todistus. Ryhmän määritelmän mukaiset ominaisuudet ovat nyt voimassa.

i) Olkoot e ja e' molemmat ryhmän G neutraalialkioita.
Nyt

$$ee' = e',$$

toisaalta taas

$$ee' = e.$$

Eli saadaan

$$e' = e.$$

Näin ollen neutraalialkio on yksikäsitteinen.

ii) Olkoot a^{-1} ja b alkion a käänteisalkioita.

Siis

$$aa^{-1} = a^{-1}a = e$$

ja

$$ab = ba = e.$$

Tällöin neutraalialkion ja assosiatiivisuuden nojalla saadaan

$$a^{-1} = ea^{-1} = (ba)a^{-1} = b(aa^{-1}) = be = b.$$

Eli kunkin alkion käänteisalkio on yksikäsitteinen.

iii) Olkoon $ax = b$.

Operoimalla yhtälö molemmin puolin vasemmalta alkiolla a^{-1} saadaan

$$a^{-1}(ax) = a^{-1}b.$$

Edelleen assosiatiivisuuden nojalla saadaan

$$(a^{-1}a)x = a^{-1}b,$$

jolloin

$$ex = a^{-1}b$$

eli

$$x = a^{-1}b.$$

Eli yhtälöllä $ax = b$ on yksikäsitteinen ratkaisu x, joka on ryhmän G alkio.

iv) Olkoon $ya = b$.

Operoimalla yhtälö molemmin puolin oikealta alkiolla a^{-1} saadaan

$$(ya)a^{-1} = ba^{-1}.$$

Assosiatiivisuuden nojalla saadaan

$$y(aa^{-1}) = ba^{-1},$$

josta edelleen käänteisalkion olemassaolon nojalla

$$ye = ba^{-1}$$

eli

$$y = ba^{-1}.$$

Eli yhtälöllä $ya = b$ on yksikäsitteinen ratkaisu y, joka on ryhmän G alkio.

□

1.2 Kertaluku

Ryhmän G **kertaluku** (order of G) tarkoittaa joukon G alkioiden lukumäärää. Ryhmän kertalukua merkitään $\mid G \mid$.

Määritelmä 1.2.1. Ryhmää G kutsutaan **äärelliseksi**, jos siinä on äärellinen määrä alkioita. Kun taas ryhmä on **ääretön**, jos alkioita on ääretön määrä.

Esimerkki 1.2.2. *Tarkastellaan ryhmää* $(\mathbb{R}, +)$*. Nyt ryhmän* $\mathbb{R}$ *kertaluku on ääretön, koska sen alkioiden lukumäärä on ääretön. Kyseessä on siis ääretön ryhmä.*

1.3 Aliryhmän määritelmä

Määritelmä 1.3.1. Olkoon $(G, *)$ ryhmä ja $H \subseteq G, H \neq \emptyset$. Jos $(H, *)$ on ryhmä, niin sitä sanotaan ryhmän $(G, *)$ **aliryhmäksi** (subgroup). Tätä aliryhmää merkitään $(H, *) \leq (G, *)$ tai lyhyemmin $H \leq G$.

Lause 1.3.2. ***(Aliryhmäkriteeri).*** *Olkoot G ryhmä ja $H \subseteq G, H \neq \emptyset$. Nyt $H \leq G$ jos ja vain jos seuraavat ehdot ovat voimassa;*

1) kun $a, b \in H$, niin $ab \in H$,

2) jokaisella alkiolla $a \in H$ on olemassa käänteisalkio $a^{-1} \in H$.

Todistus. Todistetaan ensin lause vasemmalta oikealle.
Jos H on ryhmän G aliryhmä, niin H on ryhmä, joten ehdot 1) ja 2) ovat voimassa.
Seuraavaksi todistetaan lause oikealta vasemmalle.
Oletetaan, että ehdot 1) ja 2) ovat voimassa. Ehdosta 1) seuraa, että kyseessä on binäärinen operaatio joukossa H. Koska operaatio on assosiatiivinen ryhmässä G, niin se on assosiatiivinen myös ryhmän G osajoukossa H.
Jos $a \in H$, niin ehdon 2) nojalla $a^{-1} \in H$.
Siten ehdon 1) nojalla $aa^{-1} = e \in H$.
Näin ollen H on ryhmä eli $H \leq G$. □

Lause 1.3.3. *Olkoot G ryhmä ja $H \subseteq G, H \neq \emptyset$. Tällöin $H \leq G$ jos ja vain jos ehto*

3) kun $a, b \in H$, niin $ab^{-1} \in H$

on voimassa.

Todistus. Todistetaan ensin lause vasemmalta oikealle.
Jos $H \leq G$, niin ehto 3) toteutuu, sillä H on ryhmä.
Todistetaan seuraavaksi lause oikealta vasemmalle.
Oletetaan, että ehto 3) on voimassa. Jos $a \in H$, niin ehdon 3) nojalla $aa^{-1} = e \in H$. Edelleen $ea^{-1} = a^{-1} \in H$, joten lauseen 1.3.2 ehto 2) toteutuu.
Jos $a, b \in H$, niin edellisen nojalla $b^{-1} \in H$ ja ehdon 3) nojalla

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

Siten myös lauseen 1.3.2 ehto 1) toteutuu. Näin ollen lauseen 1.3.2 nojalla $H \leq G$. □

1.4 Sivuluokat ja Lagrangen lause

Tässä kappaleessa käydään läpi hyvin tärkeä perustulos äärellisten ryhmien teoriassa, **Lagrangen lause**. Sen perusteella äärellisen ryhmän aliryhmän kertaluku jakaa aina ryhmän kertaluvun. Aluksi esitetään sivuluokkien määritelmä, jota tarvitaan Lagrangen lauseen ymmärrettävään esitykseen.

Määritelmä 1.4.1. Olkoon $(G, *)$ ryhmä ja $(H, *)$ sen aliryhmä. Tällöin alkion $a \in G$ määräämä aliryhmän H **vasen sivuluokka** (left coset) on joukko

$$aH = a * H = \{a * h \mid h \in H\}.$$

Vastaavasti alkion $a \in G$ määräämä aliryhmän H **oikea sivuluokka** (right coset) on joukko

$$Ha = H * a = \{h * a \mid h \in H\}.$$

Kaikki aliryhmän H vasemmat ja oikeat sivuluokat saadaan, kun a käy läpi joukon G kaikki alkiot.

Määritelmä 1.4.2. Olkoon H ryhmän G aliryhmä. Aliryhmän H erillisten vasempien tai oikeiden sivuluokkien lukumäärä on aliryhmän H **indeksi** (index) ryhmässä G. Indeksistä käytetään merkintää $[G : H]$.

Lause 1.4.3. *Olkoon H ryhmän G aliryhmä ja $a, b \in G$. Tällöin*

(i) $a \in aH$,

(ii) $aH = bH$, *jos ja vain jos* $b^{-1}a \in H$,

(iii) joko $aH = bH$ *tai* $aH \cap bH = \emptyset$.

Todistus. (i) Olkoon $a \in G$. Koska $a = ae$ ja $e \in H$, niin $a = ae \in aH$.

(ii) Olkoot $a, b \in G$. Oletetaan ensin, että $aH = bH$. Koska $a \in aH$ ja $aH = bH$, niin on olemassa sellainen $h' \in H$, että $a = bh'$. Tästä

seuraa, että $b^{-1}a = h' \in H$.

Oletetaan seuraavaksi kääntäen, että $b^{-1}a = h' \in H$. Osoitetaan aluksi, että $aH \subseteq bH$. Olkoon $ah \in aH$. Oletuksesta seuraa, että $a = bh'$. Silloin $ah = bh'h \in bH$. Tästä seuraa, että $aH \subseteq bH$.

Seuraavaksi osoitetaan, että $bH \subseteq aH$. Olkoon $bh \in bH$. Oletuksesta $b^{-1}a = h'$ seuraa, että $a(h')^{-1} = b$. Silloin $bh = a(h')^{-1}h \in aH$. Ja siten $bH \subseteq aH$.

Nyt on siis osoitettu, että $aH \subseteq bH$ ja $bH \subseteq aH$, joten voidaan todeta, että $aH = bH$.

(iii) Jos $aH \cap bH = \emptyset$, niin sivuluokat aH ja bH ovat erilliset.

Oletetaan nyt, että $aH \cap bH \neq \emptyset$. Osoitetaan, että $aH = bH$. Koska $aH \cap bH \neq \emptyset$, niin on olemassa sellainen alkio c, että $c \in aH \cap bH$. Tällöin $c \in aH$ ja $c \in bH$, joten on olemassa sellaiset $h_1, h_2 \in H$, että $c = ah_1$ ja $c = bh_2$. Eli saadaan $ah_1 = bh_2$, mistä edelleen saadaan $b^{-1}a = h_2{h_1}^{-1}$. Näin ollen $b^{-1}a \in H$ ja kohdan (ii) nojalla $aH = bH$. Näin on todistettu, että sivuluokat aH ja bH ovat joko erilliset tai samat.

□

Lause 1.4.4. *Olkoon H ryhmän G aliryhmä. Tällöin aliryhmän H kertaluku on sama, kuin minkä tahansa sivuluokan aH tai Ha alkioiden lukumäärä.*

Todistus. Olkoot h_1 ja h_2 aliryhmän H kaksi alkiota. Jos nyt jollekin $a \in G$ pätee

$$ah_1 = ah_2,$$

niin operoimalla puolittain alkion a käänteisalkiolla a^{-1} saadaan

$$h_1 = h_2.$$

Täten jokaisessa sivuluokassa aH on yhtä monta alkiota, kuin aliryhmässä H. □

Lause 1.4.5. ***(Lagrangen lause).*** *Olkoot G äärellinen ryhmä, $H \leq G$ ja n aliryhmän H vasempien sivuluokkien lukumäärä ryhmässä G. Tällöin*

$$\mid G \mid = n \mid H \mid .$$

Eli äärellisessä ryhmässä aliryhmän kertaluku jakaa ryhmän kertaluvun. Lisäksi on voimassa yhtälö

$$[G : H] = \frac{\mid G \mid}{\mid H \mid}.$$

Todistus. Koska G on äärellinen, niin aliryhmän H erillisten vasempien sivuluokkien lukumäärä on myös äärellinen. Olkoon $\{a_1H, a_2H, \ldots, a_nH\}$ aliryhmän H kaikkien erillisten vasempien sivuluokkien joukko ryhmässä G. Tällöin jokaista alkiota $a \in G$ kohti on olemassa sellainen alkio $a_i, 1 \leq i \leq n$, että $aH = a_iH$. Lisäksi lauseen 1.4.3 kohdan (i) nojalla $a \in aH$. Näin ollen jokainen ryhmän G alkio kuuluu yhteen sivuluokista a_iH, joten $G = a_1H \cup a_2H \cup \cdots \cup a_nH$. Lauseen 1.4.3 kohdan (iii) perusteella tämä yhdiste koostuu erillisistä joukoista, jolloin $\mid G \mid = \mid a_1H \mid + \mid a_2H \mid + \cdots + \mid a_nH \mid$. Näin ollen $[G : H] = n$. Lauseen 1.4.4 nojalla $\mid a_iH \mid = \mid H \mid$ aina, kun $1 \leq i \leq n$, joten $\mid G \mid = n \mid H \mid$. Näin ollen $\mid G \mid = [G : H] \mid H \mid$.

□

1.5 Normaali aliryhmä

Määritelmä 1.5.1. Olkoon G ryhmä ja $N \leq G$. Aliryhmää N sanotaan **normaaliksi aliryhmäksi** (normal subgroup), jos sen vasemmat ja oikeat sivuluokat ovat samat eli

$$aN = Na \text{ aina, kun } a \in G.$$

Tällöin merkitään

$$N \trianglelefteq G.$$

Jos N on aito aliryhmä, voidaan käyttää merkintää $N \triangleleft G$.

Lause 1.5.2. *Kommutatiivisen ryhmän jokainen aliryhmä on normaali.*

Todistus. Olkoon G kommutatiivinen ryhmä ja $N \leq G$. Nyt

$$aN = \{an \mid n \in N\}$$

$$= \{na \mid n \in N\}$$

$$= Na.$$

□

Lause 1.5.3. *Ryhmän G aliryhmä N on normaali, jos ja vain jos*

$$aNa^{-1} \subseteq N \text{ aina, kun } a \in G.$$

Todistus. Todistetaan ensin lause vasemmalta oikealle.
Oletetaan, että $N \trianglelefteq G$ eli $aN = Na$ aina, kun $a \in G$. Jos nyt $y \in aNa^{-1} = \{ana^{-1} \mid n \in N\}$, niin alkio y voidaan kirjoittaa muotoon $y = aka^{-1}$, missä $k \in N$. Nyt $ak \in aN$. Koska $aN = Na$, niin tällöin $ak = k'a$, missä $k' \in N$. Joten siis

$$y = aka^{-1} = k'aa^{-1} = k'e = k'.$$

Näin ollen $aNa^{-1} \subseteq N$.
Todistetaan sitten lause oikealta vasemmalle.
Oletetaan, että $aNa^{-1} \subseteq N$ aina, kun $a \in G$. Olkoon nyt $y \in aN$, jolloin $y = an$, missä $n \in N$. Tällöin

$$y = an = ane = ana^{-1}a = (ana^{-1})a$$

eli $y \in Na$, jolloin saadaan $aN \subseteq Na$.
Olkoon nyt $t \in Na$, jolloin $t = ma$, missä $m \in N$. Tällöin

$$t = ma = ema = aa^{-1}ma = a(a^{-1}ma)$$

eli $t \in aN$, jolloin edelleen $Na \subseteq aN$.
Täten $Na = aN$ eli $N \trianglelefteq G$. □

Lause 1.5.4. *Olkoon N ryhmän G normaali aliryhmä. Silloin*

$$aNa^{-1} = N$$

aina, kun $a \in G$.

Todistus. Olkoon $a \in G$. Lauseen 1.5.3 mukaan $aNa^{-1} \subseteq N$ eli nyt myös $a^{-1}Na \subseteq N$.
Nyt $N = a(a^{-1}Na)a^{-1} \subseteq aNa^{-1}$, joten $aNa^{-1} = N$ aina, kun $a \in G$. □

Edellä olevan lauseen nojalla ryhmän G aliryhmän N normaalisuuden ehto on

$$aNa^{-1} = N$$

aina, kun $a \in G$. Usein tämä normaalisuuden ehto on helpompi käyttää, kuin normaalin aliryhmän määritelmän mukainen ehto.

Lause 1.5.5. *Olkoon H ryhmän G aliryhmä. Nyt H on ryhmän G normaali aliryhmä, jos ja vain jos $aha^{-1} \in H$ aina, kun $a \in G$ ja $h \in H$.*

Todistus. Todistetaan ensin lause vasemmalta oikealle.
Eli oletetaan nyt että H on ryhmän G normaali aliryhmä. Olkoon $a \in G$ ja $h \in H$. Oletuksen perusteella ja lauseen 1.5.3 nojalla saadaan, että $aHa^{-1} \subseteq H$ eli $aha^{-1} \in H$ aina, kun $a \in G, h \in H$.
Todistetaan sitten lause oikealta vasemmalle.
Oletetaan, että $aha^{-1} \in H$ aina, kun $a \in G, h \in H$. Oletuksesta seuraa, että $aHa^{-1} \subseteq H$ aina, kun $a \in G$. Lauseen 1.5.3 nojalla H on ryhmän G normaali aliryhmä. □

Määritelmä 1.5.6. Jos ryhmällä G on vain triviaalit normaalit aliryhmät $\{e\}$ ja G, niin G on **yksinkertainen ryhmä** (trivial group).

Määritelmä 1.5.7. Olkoon $N \trianglelefteq G$. Sivuluokkien joukossa $\{aN \mid a \in G\}$ voidaan määritellä operaatio $(*)$ seuraavasti:

$$aN * bN = abN.$$

Osoitetaan, että näin saatu operaatio $(*)$ on hyvin määritelty eli

$$aN * bN = abN$$

on riippumaton sivuluokkien aN ja bN edustajien valinnasta.
Valitaan nyt toiset sellaiset edustajat a' ja b', että

$$aN = a'N$$

ja

$$bN = b'N.$$

Silloin $a \in a'N$, joten on olemassa sellainen $n_1 \in N$, että $a = a'n_1$. Vastaavasti $b \in b'N$ ja on olemassa sellainen $n_2 \in N$, että $b = b'n_2$.
Nyt tulee osoittaa, että $(ab)N = (a'b')N$.
Olkoon $n \in N$. Tällöin operaation assosiatiivisuuden nojalla

$$(ab)n = ((a'n_1)(b'n_2))n = a'n_1b'n_2n.$$

Koska N on normaali aliryhmä, niin jollekkin $n_3 \in N$ on $n_1b' = b'n_3$. Näin ollen

$$(ab)n = a'b'n_3n_2n = a'b'n',$$

missä $n' = n_3n_2n \in N$. Täten $abN \subseteq a'b'N$. Samoin voidaan osoittaa, että $a'b'N \subseteq abN$. Näin ollen operaatio $(*)$ on hyvin määritelty.

Lause 1.5.8. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin $(\{aN \mid a \in G\}, *)$ on ryhmä.*

Todistus. Nyt $aN * bN = abN$ eli $(*)$ on binäärinen operaatio joukossa $\{aN \mid a \in G\}$. Nyt algebrallinen struktuuri $(\{aN \mid a \in G\}, *)$ toteuttaa ryhmän määritelmän vaatimat aksioomat:

G1) Binäärinen operaatio on assosiatiivinen, sillä $(aN * bN) * cN = abN * cN = (ab)cN = a(bc)N = aN * bcN = aN * (bN * cN)$.

G2) Neutraalialkiona on nyt sivuluokka eN, sillä $eN * aN = eaN = aN = aeN = aN * eN$.

G3) Alkion aN käänteisalkio on nyt sivuluokka $a^{-1}N$, sillä $a^{-1}N * aN = a^{-1}aN = eN = N$ ja $aN * a^{-1}N = aa^{-1}N = eN = N$.

Siten $(\{aN \mid a \in G\}, *)$ on ryhmä. □

1.6 Tekijäryhmä

Tekijäryhmä on tiedossa olevasta ryhmästä G ja sen normaalista aliryhmästä N konstruoitu uusi ryhmä.

Määritelmä 1.6.1. Edellisessä lauseessa esiteltyä paria $(\{aN \mid a \in G\}, *)$ kutsutaan ryhmän G **tekijäryhmäksi** (factor group) normaalin aliryhmän N suhteen. Tällaisesta ryhmästä käytetään merkintää

$$G/N.$$

Nyt

$$\mid G/N \mid = \frac{\mid G \mid}{\mid N \mid},$$

mikäli ryhmä G on äärellinen.

Lause 1.6.2. *Olkoon G ryhmä ja N sen normaali aliryhmä. Nyt tekijäryhmän G/N alkiolle gN pätee $(gN)^k = g^kN$ kaikilla $k \in \mathbb{Z}$.*

Todistus. Nyt G on ryhmä ja N on sen normaali aliryhmä, joten operaatio voidaan määritellä sivuluokkien joukossa seuraavasti:

$$g_1N * g_2N = g_1 * g_2N.$$

Kun $k = 0$, niin lauseen 1.5.8 nojalla

$$(gN)^0 = eN = g^0N.$$

Todistetaan seuraavaksi lause tapauksessa $k > 0$. Tällöin saadaan, että

$$(gN)^1 = gN,$$

$$(gN)^2 = gN * gN = ggN = g^2N,$$

$$(gN)^3 = gN * g^2N = gg^2N = g^3N,$$

$$\dots$$

$$(gN)^k = gN * g^{k-1}N = gg^{k-1}N = g^kN,$$

kaikilla $k > 0$.

Olkoon sitten $k < 0$. Voidaan todeta, että $(gN)^{-1} = g^{-1}N$, sillä lauseen 1.5.8 nojalla $g^{-1}N$ on alkion gN käänteisalkio $(gN)^{-1}$. Nyt G on ryhmä, joten $g^{-1} \in G$. Lisäksi todetaan, että kun $k < 0$, niin $-k > 0$ ja lisäksi $(g^{-1})^{-k}N = g^kN$. Näin saadaan

$$(gN)^k = (gN)^{(-1)(-k)} = ((gN)^{-1})^{-k} = (g^{-1}N)^{-k} = (g^{-1})^{-k}N = g^kN.$$

□

1.7 Ryhmähomomorfismi

Määritelmä 1.7.1. Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä. Kuvausta $f : G \to H$ sanotaan **homomorfismiksi** (homomorphism) ryhmältä G ryhmälle H, mikäli

$$f(a \cdot b) = f(a) * f(b)$$

aina, kun $a, b \in G$.

Lause 1.7.2. *Olkoon $f : G \to H$ homomorfismi ja olkoot e_G ja e_H ryhmien G ja H neutraalialkiot. Tällöin*

$$f(e_G) = e_H$$

ja

$$f(a^{-1}) = (f(a))^{-1}$$

aina, kun $a \in G$.

Todistus. Nyt

$$f(e_G) * f(e_G) = f(e_G \cdot e_G) = f(e_G) = f(e_G) * e_H.$$

Eli

$$f(e_G) * f(e_G) = f(e_G) * e_H.$$

Operoidaan nyt molemmat puolet vasemmalta alkiolla $f(e_G)^{-1}$. Saadaan

$$f(e_G) = e_H.$$

Nyt myös

$$f(a^{-1}) * f(a) = f(a^{-1} \cdot a) = f(e_G) = e_H$$

ja

$$f(a) * f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H$$

eli saadaan

$$f(a)^{-1} = f(a^{-1}).$$

□

Määritelmä 1.7.3. Olkoon $f : G \to H$ homomorfismi. Joukkoa

$$Im(f) = f(G) = \{f(x) \mid x \in G\}$$

sanotaan homomorfismin f **kuvaksi** (the image of f) ja joukkoa

$$Ker(f) = \{x \in G \mid f(x) = e_H\}$$

sanotaan homomorfismin **ytimeksi** (the kernel of f).

Määritelmä 1.7.4. Ryhmät $(G, \cdot)$ ja $(H, *)$ ovat **isomorfiset** eli rakenneyhtenevät, mikäli on olemassa bijektio $f : G \to H$, joka toteuttaa ehdon $f(a \cdot b) = f(a) * f(b)$ aina, kun $a, b \in G$. Voidaan myös sanoa, että kuvaus f on bijektiivinen homomorfismi. Tällöin merkitään

$$G \cong H$$

tai täsmällisemmin

$$(G, \cdot) \cong (H, *)$$

ja sanotaan, että kuvaus f on **ryhmäisomorfismi**.

2 Syklinen ryhmä

Tästä alkaa tutkielman aiheen varsinainen käsittely. Syklinen ryhmä G on yhden alkion generoima ryhmä. Ryhmällä G on siis olemassa sellainen alkio a, jonka kokonaislukupotensseina saadaan kaikki ryhmän G alkiot.
Sykliset ryhmät muodostavat yksinkertaisimman luokan kaikkien ryhmien joukossa. Niiden rakenne on hyvin suoraviivainen ja selkeä. Syklinen ryhmä voi sisältää tietyn määrän alkioita tai sitten se voi olla ääretön ryhmä.
Tämän luvun alussa käydään läpi ryhmän alkion kokonaislukupotenssit ja niiden ominaisuudet, jonka jälkeen siirrytään syklisen ryhmän määritelmään ja tuloksiin todistuksineen. Määritelmän jälkeen syvennytään tutkimaan aihetta yksityiskohtaisemmin. Osoitetaan syklisen ryhmän olevan aina Abelin ryhmä, esitetään tuloksia alkion kertaluvun avulla, sekä osoitetaan syklisen ryhmän tekijäryhmän olevan myös aina syklinen.

2.1 Ryhmän alkion kokonaislukupotenssit

Tässä kappaleessa lähestytään syklisen ryhmän määritelmää ryhmän alkion kokonaislukupotenssien kautta. Syklisen ryhmän tarkka määritelmä käydään läpi kappaleessa 2.2

Määritellään ryhmän alkion kokonaislukupotenssit seuraavasti.
Olkoon $(G, *)$ ryhmä ja $a \in G$. Kun $n \in \mathbb{Z}_+$, niin

$$a^n = \underbrace{a * a * \ldots * a}_{n \ kpl}$$

ja

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

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

Jos $x, y \in H$, niin $x = a^m$ ja $y = a^n$ eräillä $m, n \in \mathbb{Z}$. Tällöin myös

$$xy^{-1} = a^m a^{-n} = a^{m-n} \in H.$$

Näin ollen osajoukko H on lauseen 1.3.3 nojalla ryhmän G aliryhmä.
Ryhmää H eli alkion a potenssien joukkoa merkitään symbolilla $\langle a \rangle$, eli

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

Seuraavissa lauseissa 2.1.2 ja 2.1.3 tutkitaan tarkemmin alkion a potenssien joukon $\langle a \rangle$ ominaisuuksia.
Huomioidaan, että ryhmän binäärisen operaation ollessa yhteenlaskunkaltainen, niin termin *potenssien joukon* sijasta on syytä käyttää termiä *monikertojen joukko*. Tällaista joukkoa merkitään

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

Määritelmä 2.1.1. Aliryhmää $\langle a \rangle$ sanotaan **alkion** a **generoimaksi aliryhmäksi**. Tästä voidaan käyttää myös termiä **alkion** a **virittämä aliryhmä**.

Lause 2.1.2. *Olkoon $(G, *)$ ryhmä ja $a \in G$. Tällöin $\langle a \rangle$ on ryhmän G suppein aliryhmä, joka sisältää alkion a.*

Todistus. Todistetaan aluksi, että $\langle a \rangle$ on ryhmän G **aliryhmä**.
Kun asetetaan $k = 1$, saadaan $a^1 = a \in \langle a \rangle$. Näin ollen joukko $\langle a \rangle$ sisältää alkion a.
Olkoot $b, c \in \langle a \rangle$ mielivaltaisesti valitut. Silloin $b = a^k, c = a^l$, missä $k, l \in \mathbb{Z}$.
Voidaan todeta, että

$$c^{-1} = (a^l)^{-1} = a^{-l}.$$

Tästä seuraa, että

$$b * c^{-1} = a^k * a^{-l} = a^{k-l},$$

missä $k - l \in \mathbb{Z}$. Näin ollen

$$b * c^{-1} \in \langle a \rangle.$$

Täten lauseen 1.3.3 nojalla joukko $\langle a \rangle$ on ryhmän G aliryhmä.
Todistetaan vielä, että $\langle a \rangle$ on ryhmän G **suppein aliryhmä**, joka sisältää alkion a.
Suppein aliryhmä tarkoittaa sisältyvyysrelaation suhteen pienintä aliryhmää. Alkion a generoiman aliryhmän tulisi olla siis sellainen aliryhmä, joka sisältyy kaikkiin sellaisiin aliryhmiin, joissa on alkiona a.
Oletetaan, että $M \leq G$ ja $a \in M$. Koska M on ryhmä, niin $a^k \in M$ aina, kun $k \in \mathbb{Z}$. Näin ollen $\langle a \rangle \subseteq M$.
Näin voidaan todeta, että $\langle a \rangle$ on suppein ryhmän G aliryhmä, joka sisältää alkion a. □

Lause 2.1.3. *Olkoon $(G, *)$ ryhmä ja $a \in G$.*

i) Jos $\langle a \rangle$ on äärellinen ryhmä ja merkitään ryhmän $\langle a \rangle$ kertalukua $| \langle a \rangle | = m$, niin

$$\langle a \rangle = \{e, a, a^2, ..., a^{m-1}\}, \tag{1}$$

missä $a^m = e$. Edelleen voidaan todeta, että

$$a^k = e, \qquad \textit{jos ja vain jos} \qquad m \mid k. \tag{2}$$

Yleisemmin esitetään

$$a^k = a^h, \qquad \textit{jos ja vain jos} \qquad k \equiv h \ (mod\ m). \tag{3}$$

ii) Jos $\langle a \rangle$ on ääretön ryhmä, niin

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\},$$

ja kaikki alkion a potenssit a^k ovat pareittain erisuuria.

Todistus. (i) Koska $\langle a \rangle$ on äärellinen, niin kaikki potenssit $a^k, k \geq 0$, eivät voi olla erisuuria. On siis olemassa sellaiset $r, s \in \mathbb{Z}_+$, että $a^r = a^s$ ja $r \neq s$. Valitaan, että $r > s$. Silloin $a^{r-s} = e$, missä $r - s > 0$. Eli on olemassa alkion a positiivinen potenssi, joka on yhtä kuin neutraalialkio e.
Olkoon nyt m pienin sellainen positiivinen kokonaisluku, että $a^m = e$.

1) Todistetaan, että tulos (1) on voimassa.
   Merkitään $H = \{e, a, a^2, ..., a^{m-1}\}$. Tämän luvun alussa todettiin, että alkion a potenssien joukkoa eli alkion a generoimaa aliryhmää merkitään symbolilla $\langle a \rangle$ eli

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

   Selvästi nyt $H \subseteq \langle a \rangle$, joten riittää osoittaa, että $\langle a \rangle \subseteq H$. On siis osoitettava, että $a^k \in H$ kaikilla $k \in \mathbb{Z}$.
   Olkoon $k \in \mathbb{Z}$. Nyt kokonaislukujen jakoalgoritmin mukaan on olemassa kokonaisluvut q ja r, joille pätee $k = qm + r$, missä $0 \leqslant r < m$. Näin ollen

$$a^k = a^{qm+r} = (a^m)^q * a^r = e^q * a^r = e * a^r = a^r \in H.$$

   On siis osoitettu, että

$$\langle a \rangle = \{e, a, a^2, ..., a^{m-1}\}.$$

   Osoitetaan vielä, että ryhmän $\langle a \rangle$ kertaluku $\mid \langle a \rangle \mid = m$. Eli täytyy osoittaa, että mitkään alkion a generoiman aliryhmän alkioista $e, a, a^2, ..., a^{m-1}$ eivät ole samoja.
   Tehdään vastaoletus, että $a^i = a^j$ joillain kokonaisluvuilla i ja j, joille pätee $0 < i < j < m$. Edelleen saadaan $a^{j-i} = e$, jossa $0 < j - i < m$. Tämä on ristiriita, sillä m on pienin positiivinen kokonaisluku, jolla $a^m = e$. Näin ollen $a^i \neq a^j$ aina, kun $i \neq j$ eli kertaluku $\mid \langle a \rangle \mid = m$. Näin ollen tulos (1) on voimassa.

2) Todistetaan, että tulos (2) on voimassa.

Jakoalgoritmin nojalla voidaan merkitä $k = qm + r$, missä $0 \leqslant r < m$. Silloin edelleen $a^k = a^r$. Koska nyt m on pienin sellainen positiivinen kokonaisluku, että $a^m = e$, niin

$$a^k = a^r = e,$$

jos ja vain jos

$$r = 0.$$

Koska $k = qm + r$, niin ehto $r = 0$ on yhtäpitävä ehdon $m \mid k$ kanssa.

3) Voidaan todeta, että

$$a^k = a^h,$$

jos ja vain jos

$$a^{k-h} = e.$$

Josta edelleen kohdan (2) nojalla saadaan, että

$$m \mid k - h,$$

eli

$$k \equiv h \ (mod\ m).$$

(*ii*) Nyt tiedetään, että $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. On siis vain osoitettava, että mitkään potensseista a^k eivät ole samoja.
Tehdään vastaoletus, että $a^k = a^m$ joillakin kokonaisluvuilla k ja m, joille pätee $k > m$. Nyt $a^{k-m} = e$, missä e on neutraalialkio. Nyt kohdan (*i*) nojalla ryhmä $\langle a \rangle$ on äärellinen. Tämä on ristiriita, joten väite on todistettu. Näin lause 2.1.3 on todistettu. □

2.2 Syklisen ryhmän määritelmä

Tässä kappaleessa esitetään syklisen ryhmän tarkka määritelmä sekä osoitetaan syklisen ryhmän kommutatiivisuus.

Määritelmä 2.2.1. Ryhmää G sanotaan **sykliseksi ryhmäksi** (cyclic group), jos on olemassa sellainen alkio $a \in G$, että $G = \{a^n \mid n \in \mathbb{Z}\}$. Tällöin ryhmää G sanotaan **alkion** a **generoimaksi sykliseksi ryhmäksi**, merkitään $G = \langle a \rangle$. Alkiota a kutsutaan ryhmän G **generaattoriksi** (generator).

Syklisen ryhmän nimitys tulee siitä, että kertalukua n olevan syklisen ryhmän $G = \langle a \rangle$ päättymättömän jonon $\ldots, a^{m-1}, a^m, a^{m+1}, \ldots$ mitkä tahansa n peräkkäistä alkiota muodostavat niin sanotun "syklin", joka toistuu samanlaisena siirryttäessä jonossa eteenpäin. Tämä voidaan ilmaista myös seuraavalla selkeällä tavalla:

$$a^k = a^h \Leftrightarrow k \equiv h (mod\ n).$$

Ääretön syklinen ryhmä on siis tässä mielessä eräänlainen rajatapaus, johon sisältyy vain yksi äärettömän pitkä sykli.

Lause 2.2.2. *Syklinen ryhmä on kommutatiivinen eli vaihdannainen. Eli syklinen ryhmä G on aina Abelin ryhmä.*

Todistus. Olkoon G syklinen ryhmä. Oletetaan, että ryhmän G alkio g generoi koko ryhmän eli $G = \langle g \rangle$. Tällöin G on muotoa

$$G = \{g^k \mid k \in \mathbb{Z}\},$$

missä $g \in G$. Olkoot nyt $a, b \in G$. Silloin a ja b ovat muotoa $a = g^s$, $b = g^t$, missä $s, t \in \mathbb{Z}$. Nyt

$$ab = g^s g^t = g^{s+t} = g^t g^s = ba.$$

Näin ollen syklinen ryhmä G on siis Abelin ryhmä. □

Huomataan kuitenkin, että jokainen Abelin ryhmä ei ole syklinen. Esimerkiksi ryhmä $(\mathbb{Z}_8^*, \cdot)$ on Abelin ryhmä, mutta se ei ole syklinen ryhmä.

Esimerkki 2.2.3. *Olkoon $n \in \mathbb{Z}$. Jäännösluokkien joukko $\mathbb{Z}_n$ on syklinen ryhmä, jonka kertaluku on n, kun binäärisenä operaationa on yhteenlasku. Osoitetaan ensin, että jäännösluokkien joukko $\mathbb{Z}_n$ on ryhmä.*
Jäännösluokille pätee seuraava:
Jos $[a]_n, [b]_n \in \mathbb{Z}_n$, niin $[a]_n + [b]_n = [a+b]_n \in \mathbb{Z}_n$.

G1) Olkoot $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$. Nyt

$$([a]_n + [b]_n) + [c]_n = [a+b]_n + [c]_n$$

$$= [(a+b)+c]_n = [a+(b+c)]_n$$

$$= [a]_n + [b+c]_n = [a]_n + ([b]_n + [c]_n),$$

joten jäännösluokkien yhteenlasku on assosiatiivinen.

G2) Neutraalialkiona on nyt $[0]_n$, sillä

$$[0]_n + [a]_n = [0+a]_n = [a]_n$$

ja

$$[a]_n + [0]_n = [a+0]_n = [a]_n$$

kaikilla $[a]_n \in \mathbb{Z}_n$.

G3) Alkion $[a]_n \in \mathbb{Z}_n$ käänteisalkio on $[-a]_n$, sillä

$$[a]_n + [-a]_n = [a-a]_n = [0]_n$$

ja

$$[-a]_n + [a]_n = [-a+a]_n = [0]_n.$$

Eli $(\mathbb{Z}_n, +)$ *on ryhmä.*
Joukko $\mathbb{Z}_n$ *koostuu jäännösluokista* $[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$. *Jos* a *on jokin kokonaisluku, jolle pätee* $0 \leq a \leq n-1$, *niin*

$$[a]_n = \underbrace{[1]_n + [1]_n + \cdots + [1]_n}_{n \qquad kpl}.$$

Tästä seuraa, että alkio $[1]_n$ *generoi ryhmän* $\mathbb{Z}_n$. *Joten siis* $(\mathbb{Z}_n, +)$ *on syklinen. Lisäksi nyt jäännösluokkien lukumäärä on* n, *joten ryhmän* $\mathbb{Z}_n$ *kertaluku* $\mid \mathbb{Z}_n \mid$ *on* n.

2.3 Alkion kertaluku

Tässä kappaleessa määritellään ryhmän alkion kertaluku. Ryhmän kertaluku on kappaleen 1.2 mukaan ryhmän alkioiden lukumäärä, kun taas alkion kertaluku kertoo sen virittämän aliryhmän alkioiden lukumäärästä. Kertaluvulla tarkoitetaan siis kahta eri asiaa, jotka kuitenkin liittyvät toisiinsa.

Määritelmä 2.3.1. Olkoon $(G, *)$ ryhmä ja $a \in G$. Alkion a generoiman syklisen ryhmän $(\langle a \rangle, *)$ kertalukua sanotaan **alkion** a **kertaluvuksi**. Alkion a kertalukua merkitään $ord(a)$, eli

$$ord(a) = \mid \langle a \rangle \mid = \mid a \mid .$$

Lause 2.3.2. *Jos ryhmän kertaluku on alkuluku, niin ryhmä on syklinen.*

Todistus. Olkoon $(G, *)$ ryhmä ja $\mid G \mid = p$, missä p on alkuluku. Nyt Lagrangen lauseen 1.4.5 mukaan aliryhmän kertaluku jakaa ryhmän kertaluvun, jolloin ryhmän G ainoat aliryhmät ovat $\{e\}$ ja G.
Olkoon $a \in G$ ja $a \neq e$. Nyt $\langle a \rangle$ on ryhmän G aliryhmä ja siten Lagrangen lauseen mukaan $\mid \langle a \rangle \mid \mid \mid G \mid$ eli $ord(a) \mid p$. Koska p on alkuluku ja toisaalta $ord(a) > 1$, niin $ord(a) = p$. Näin ollen alkio a generoi koko ryhmän $(G, *)$ eli $\langle a \rangle = G$ eli ryhmä G on syklinen. □

Lause 2.3.3. *Olkoon G ryhmä ja g jokin sen alkio. Alkion g kertaluku on pienin positiivinen kokonaisluku n, jolla pätee $g^n = e$. Jos tällaista kertalukua ei löydy, kertaluku on ääretön.*

Todistus. Oletetaan, että ehto $g^n = e$ pätee positiivisella kokonaisluvulla n ja että n on lisäksi pienin tällainen luku. Lauseen 2.1.3 nojalla tiedetään, että alkion g virittämän aliryhmän alkiot ovat $e, g, g^2, \ldots, g^{n-1}$. Alkion g kertaluku on siis korkeintaan n. Lisäksi täytyy osoittaa, että mitkään edellä luetelluista alkioista eivät ole samoja.
Tehdään nyt vastaoletus, että $g^m = g^k$ joillain kokonaisluvuilla m ja k, joille on voimassa $0 \leq k < m \leq n - 1$. Nyt huomataan, että

$$g^{m-k} = g^m(g^k)^{-1} = g^m(g^m)^{-1} = e,$$

mutta $0 < m - k < n$. Tämä on ristiriita, sillä n on pienin ehdon $g^n = e$ toteuttava positiivinen kokonaisluku. Joten voidaan todeta, että mitkään alkion g virittämän aliryhmä alkioista $e, g, g^2, \ldots, g^{n-1}$ eivät ole samoja. Näin ollen alkion g kertaluku on n.
Tarkastellaan nyt tilannetta, jossa ei ole olemassa positiivista kokonaislukua m, jolle pätisi $g^m = e$.
Tehdään vastaoletus, että alkion g kertaluku on äärellinen. Tällöin myös $\langle g \rangle$ on äärellinen ja $g^k \in \langle g \rangle$ kaikilla $k \in \mathbb{Z}$. Eli nyt täytyisi päteä $g^{k_1} = g^{k_2}$ joillakin $k_1, k_2 \in \mathbb{Z}$, ja $k_1 > k_2$. Nyt $g^{k_1 - k_2} = e$ ja toisaalta taas $k_1 - k_2$ on positiivinen kokonaisluku. Tämä on ristiriita, joten kertaluku on ääretön.

□

Edellä olevaan lauseeseen liittyen huomioidaan, että jos ryhmän laskutoimitusta merkitään yhteenlaskuna, on kertaluku pienin positiivinen kokonaisluku n, jolle pätee $ng = e$.

Lause 2.3.4. *Olkoon G ryhmä ja alkio $g \in G$. Jos $g^m = e$, niin alkion g kertaluku jakaa luvun m.*

Todistus. Oletetaan, että alkion g kertaluku on n ja $g^m = e$. Kokonaislukujen jakoalgoritmin mukaan on olemassa kokonaisluvut q ja r, joille pätee $m = qn + r$ ja $0 \leq r < n$. Osoitetaan, että $r = 0$, jolloin saadaan $m = qn$.
Huomataan, että

$$g^r = g^{m-qn} = g^m g^{-qn} = e(g^n)^{-q} = e.$$

Nyt on siis löydetty luku $r \geq 0$, joka on pienempi kuin n ja jolle on voimassa $g^r = e$. Nyt kuitenkin edellä olevan lauseen 2.3.3 nojalla kertaluku n on pienin positiivinen kokonaisluku, jolle pätee $g^n = e$. Voidaan siis todeta, että $r = 0$. Tästa seuraa edelleen, että $m = qn + 0 = qn$, joten alkion g kertaluku n jakaa luvun m. □

Lause 2.3.5. *Olkoon a kertalukua n oleva alkio ja $d \mid n$, $d > 0$. Tällöin alkion a^d kertaluku on $\frac{n}{d}$.*

Todistus. Nyt $\mid a \mid = n$ eli $a^n = e$.
Lauseen 2.1.3 kohdan i) perusteella saadaan $a^k = e$, jos ja vain jos $n \mid k$ eli $\mid a \mid \mid k$.

Nyt $(a^d)^{\frac{n}{d}} = a^n = e$, josta edelleen lauseen 2.1.3 perusteella saadaan $\mid a^d \mid \mid \frac{n}{d}$.
Olkoon nyt $\mid a^d \mid = k$ eli $(a^d)^k = e$. Saadaan $a^{dk} = e$, jolloin lauseen 2.1.3 mukaan saadaan $\mid a \mid \mid dk$ eli $n \mid dk$.
Koska $d \mid n$ ja $n \mid dk$, niin saadaan $\frac{n}{d} \mid k$.
Erityisesti siis $\frac{n}{d} \mid \mid a^d \mid$.
Koska $\mid a^d \mid \mid \frac{n}{d}$ ja $\frac{n}{d} \mid \mid a^d \mid$, niin tulee olla $\mid a \mid = \frac{n}{d}$. □

Lause 2.3.6. *Syklisen ryhmän tekijäryhmä on aina syklinen.*

Todistus. Olkoon G syklinen ryhmä, jonka virittää alkio g ja olkoon N ryhmän G normaali aliryhmä.

Osoitetaan, että jokainen tekijäryhmän G/N alkio on muotoa $(gN)^k$, missä $k \in \mathbb{Z}$. Olkoon nyt $h \in G$. Koska G on syklinen ryhmä, niin saadaan $h = g^k$, jollakin $k \in \mathbb{Z}$. Nyt tekijäryhmän G/N mielivaltainen alkio hN voidaan esittää muodossa

$$hN = g^k N,$$

jollakin $k \in \mathbb{Z}$. Nyt lauseen 1.6.2 nojalla pätee $g^k N = (gN)^k$, joten saadaan

$$hN = g^k N = (gN)^k.$$

Tekijäryhmä G/N on siis alkion gN virittämä, koska jokainen ryhmän alkio voidaan esittää sen potenssina $(gN)^k$.
Yhden alkion virittämä ryhmä on aina syklinen, joten tekijäryhmä on syklinen. □

3 Syklisen ryhmän isomorfisuus

Sykliset ryhmät muistuttavat rakenteeltaan hyvin paljon toisiaan, sillä jokaisen alkiot ovat yhden virittäjäalkion potensseja. Ja näitä potensseja kerrotaan keskenään yhteenlaskemalla niiden eksponentit. Ryhmän ominaisuuksien kannalta symbolilla, joilla laskutoimitusta tai virittäjäalkiota merkitään, ei ole mitään merkitystä. Ainoa rakenteellinen eroavaisuus syklisten ryhmien välillä onkin alkioiden lukumäärä.
Seuraavissa lauseissa käydään läpi syklisten ryhmien isomorfisuutta niin äärettömässä kuin äärellisessäkin tapauksessa.

3.1 Ääretön syklinen ryhmä

Lause 3.1.1. *Jos* $(G, \cdot)$ *on syklinen ryhmä ja* $(G, \cdot) \cong (H, *)$*, niin* $(H, *)$ *on syklinen ryhmä.*

Todistus. Olkoon $G = \langle a \rangle$ ja $f : G \to H$ isomorfismi. Todistetaan, että $H = \langle f(a) \rangle$.
Nyt $\langle f(a) \rangle \subseteq H$, joten riittää osoittaa, että $H \subseteq \langle f(a) \rangle$.
Olkoon nyt $a' \in H$ mielivaltainen. Silloin $f^{-1}(a') \in G$. Siis $f^{-1}(a') = a^k$, jollakin $k \in \mathbb{Z}$. Eli $a' = f(a^k)$. Koska f on homomorfismi, niin $a' = f(a)^k$ eli $a' \in \langle f(a) \rangle$. Näin ollen $H \subseteq \langle f(a) \rangle$.
Siis $H = \langle f(a) \rangle$. □

Lauseesta 3.1.1 seuraa, että jos $(G, \cdot)$ on syklinen ryhmä ja $(H, *)$ ei ole syklinen ryhmä, niin myöskään isomorfisuus ryhmien välillä ei toteudu eli $(G, \cdot) \ncong (H, *)$.

Lause 3.1.2. *Jokainen ääretön syklinen ryhmä on isomorfinen ryhmän* $(\mathbb{Z}, +)$ *kanssa.*

Todistus. Olkoon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku on ääretön. Nyt

siis

$$G = \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}$$

ja kaikki alkion g potenssit poikkeavat toisistaan.

Määritellään kuvaus

$$f : \mathbb{Z} \to G,$$

siten, että

$$f(k) = g^k.$$

Kuvaus on homomorfismi, sillä

$$f(k+m) = g^{k+m} = g^k g^m = f(k)f(m)$$

kaikilla $k, m \in \mathbb{Z}$.

Osoitetaan seuraavaksi, että f on bijektio.

Osoitetaan ensin, että kuvaus f on injektio. Oletetaan, että $f(k) = f(m)$ joillakin $k, m \in \mathbb{Z}$. Siis $g^k = g^m$. Kuitenkin kaikki alkion g potenssit poikkeavat toisistaan, joten täytyy olla $k = m$. Tästä seuraa, että kuvaus f on injektio. Koska jokainen ryhmän G alkio on muotoa g^k jollakin $k \in \mathbb{Z}$, on kuvaus f myös surjektio.

Näin ollen kuvaus f on bijektiivinen homomorfismi eli kuvaus f on isomorfinen. □

3.2 Äärellinen syklinen ryhmä

Lause 3.2.1. *Jokainen äärellinen syklinen ryhmä, jonka kertaluku on n, on isomorfinen ryhmän $(\mathbb{Z}_n, +)$ kanssa.*

Todistus. Olkoon $G =< g >$ syklinen ryhmä, jonka kertaluku on n. Nyt siis

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

jossa kaikki alkion g potenssit poikkeavat toisistaan.

Jotta voidaan todistaa, että $(G, \cdot) \cong (\mathbb{Z}_n, +)$, tulee osoittaa, että joukkojen

G ja $\mathbb{Z}_n$ välille voidaan esittää kuvaus, joka on bijektiivinen homomorfismi. Olkoon nyt kuvaus $f : \mathbb{Z}_n \to G$ määritelty ehdolla

$$f([k]_n) = g^k.$$

Koska ehto on määritelty jäännösluokan edustajan avulla, tulee varmistaa, että edustajan valinta ei vaikuta kuvauksen arvoon.
Oletetaan nyt, että $[k]_n = [m]_n$. Nyt $k = m + an$ jollakin $a \in \mathbb{Z}$. Koska alkion g kertaluku on n, niin saadaan

$$g^k = g^{m+an} = g^m g^{an} = g^m (g^n)^a = g^m e^a = g^m.$$

Jäännösluokan edustajan valinta ei siis vaikuta kuvauksen arvoon, joten kuvaus on näin ollen hyvin määritelty.
Nyt

$$f([k]_n + [m]_n) = f([k+m]_n) = g^{k+m} = g^k g^m = f([k]_n) f([m]_n)$$

kaikilla $k, m \in \mathbb{Z}$. Näin ollen kuvaus on homomorfismi.
Osoitetaan vielä, että kuvaus f on bijektio. Aloitetaan injektiivisyydestä. Oletetaan, että $f([k]_n) = f([m]_n)$ joillakin $[k]_n, [m]_n \in \mathbb{Z}_n$. Tällöin $g^k = g^m$ eli $g^{k-m} = e$. Koska alkion g kertaluku on n, niin luku $k - m$ on jokin luvun n monikerta. Eli n jakaa luvun $k - m$ eli $k \equiv m (mod\ n)$. Tämä tarkoittaa, että $[k]_n = [m]_n$. Näin ollen kuvaus f on siis injektio.
Lisäksi jokainen ryhmän G alkio on muotoa g^k, jollakin $k \in \{0, 1, \ldots, n-1\}$, joten kuvaus on myös surjektio.
Kuvaus $f : \mathbb{Z}_n \to G$ on siis bijektiivinen. Näin ollen ryhmät G ja $\mathbb{Z}_n$ ovat isomorfiset. □

Lause 3.2.2. *Samaa kertalukua olevat sykliset ryhmät ovat isomorfiset.*

Todistus. Olkoot $(G, \cdot)$ ja $(H, *)$ äärettömät sykliset ryhmät. Nyt lauseen 3.1.2 mukaan jokainen ääretön syklinen ryhmä on isomorfinen ryhmän $(\mathbb{Z}, +)$

kanssa. Eli nyt $(G, \cdot) \cong (\mathbb{Z}, +)$ ja toisaalta $(\mathbb{Z}, +) \cong (H, *)$. Tästä seuraa, että myös $(G, \cdot) \cong (H, *)$. Näin ollen voidaan todeta kertaluvuiltaan äärettömien syklisten ryhmien olevan isomorfisia keskenään.

Olkoon sitten $(G, *)$ ja $(H, \cdot)$ kertalukua n olevat äärelliset sykliset ryhmät. Nyt lauseen 3.2.1 mukaan jokainen kertalukua n oleva äärellinen syklinen ryhmä on isomorfinen ryhmän $(\mathbb{Z}_n, +)$ kanssa. Nyt siis $(G, *) \cong (\mathbb{Z}_n, +)$ ja toisaalta $(\mathbb{Z}_n, +) \cong (H, \cdot)$. Tästä saadaan edelleen $(G, *) \cong (H, \cdot)$ eli voidaan todeta, että samaa kertalukua olevat sykliset ryhmät ovat isomorfiset. $\square$

4 Syklisen ryhmän aliryhmä

Syklisen ryhmän rakenne voidaan määrittää tarkasti. Tässä luvussa syvennytään tutkimaan sylkisen ryhmän aliryhmää ja osoitetaan, että myös syklisen ryhmän aliryhmät voidaan luetella selkeästi niin äärettömässä, kuin äärellisessäkin tapauksessa.

4.1 Syklisen ryhmän aliryhmistä

Lause 4.1.1. *Syklisen ryhmän jokainen aliryhmä on syklinen.*

Todistus. Olkoon G syklinen ryhmä, jonka generaattorina on alkio a. Eli $G = \langle a \rangle$.
Oletetaan, että e on ryhmän neutraalialkio. Olkoon nyt H ryhmän G aliryhmä. Jos aliryhmä $H = \{e\}$, niin H on alkion e generoima syklinen aliryhmä, jolloin väite pätee.
Oletetaan seuraavaksi, että aliryhmässä H on muitakin alkioita kuin neutraalialkio e. Koska H on syklisen ryhmän G osajoukko, niin sen alkiot ovat muotoa a^k, missä $k \in \mathbb{Z}$. Valitaan aliryhmän H alkioista sellainen alkio, jonka potenssi k on pienin mahdollinen positiivinen kokonaisluku. Tullaan osoittamaan, että $H = \langle a^k \rangle$.
Koska nyt $a^k \in H$ ja $\langle a^k \rangle$ on kaikkein pienin ryhmän H aliryhmä, joka sisältää alkion a^k, niin voidaan todeta, että $\langle a^k \rangle \subseteq H$.
Osoitetaan seuraavaksi, että $H \subseteq \langle a^k \rangle$.
Olkoon $h \in H$. Nyt on olemassa sellainen $n \in \mathbb{Z}$, jolle pätee $h = a^n$. Jakoalgoritmin avulla voidaan kirjoittaa $n = qk + r$, missä $q, r \in \mathbb{Z}$ ja $0 \leq r < k$. Tullaan osoittamaan, että $r = 0$, jolloin saadaan $n = qk$, josta edelleen saadaan $h = a^n = a^{qk} = (a^k)^q \in \langle a^k \rangle$. Huomataan, että

$$a^r = a^{n-qk} = a^n a^{-qk} = h(a^k)^{-q}.$$

Koska $h \in H$ ja $(a^k)^{-q} \in H$, niin $a^r \in H$. Koska nyt k on pienin positiivinen kokonaisluku, jolle pätee $a^k \in H$, niin täytyy olla $r = 0$ eli $a^r = a^0 = e \in H$. Näin ollen

$$h = a^n = (a^k)^q \in \langle a^k \rangle,$$

joten nyt

$$H \subseteq \langle a^k \rangle.$$

Koska $\langle a^k \rangle \subseteq H$ ja $H \subseteq \langle a^k \rangle$, niin voidaan todeta, että $H = \langle a^k \rangle$ eli aliryhmä H on syklinen. □

Lause 4.1.2. *Olkoon G syklinen ryhmä. Silloin ryhmän G jokainen aliryhmä on normaali aliryhmä.*

Todistus. Lauseessa 2.2.2 osoitettiin, että jokainen syklinen ryhmä on aina Abelin ryhmä. Ja lauseen 1.5.2 mukaan Abelin ryhmän jokainen aliryhmä on normaali aliryhmä.
Näiden lauseiden nojalla väite on tosi. □

4.2 Äärettömän syklisen ryhmän aliryhmä

Lause 4.2.1. *Äärettömän syklisen ryhmän $C_\infty = \langle c \rangle$ aliryhmät ovat ryhmät*

$$\langle c^n \rangle, n = 0, 1, 2, \ldots$$

Mitkään näistä aliryhmistä eivät ole samoja.

Todistus. Ryhmällä C_∞ on joka tapauksessa edellä mainitut ryhmät $\langle c^n \rangle$ aliryhminä. Osoitetaan, että muita aliryhmiä ei ole.
Oletetaan, että H on ryhmän C_∞ aliryhmä. Jos $H = \{e\}$, niin $H = \langle c^0 \rangle$.
Jos $H \neq \{e\}$, niin H sisältää jonkin alkion c^n, missä $n > 0$. Valitaan nyt pienin tällainen n. Osoitetaan, että $H = \langle c^n \rangle$.
Jos $a \in H$, niin täytyy osoittaa, että $a \in \langle c^n \rangle$.

Nyt a on muotoa c^m, missä $m \in \mathbb{Z}$. Tällöin kokonaislukujen jakoalgoritmin mukaan $m = kn + r$, missä $0 \leqslant r < n$. Nyt saadaan

$$c^r = c^{m-kn} = c^m(c^n)^{-k} \in H.$$

Luvun n minimaalisuuden nojalla saadaan, että $r = 0$.
Täten $m = kn + r = kn$ ja

$$c^0 = e = c^m(c^n)^{-k}$$

eli

$$c^m = (c^n)^k.$$

Saadaan, että

$$a = c^m = (c^n)^k \in \langle c^n \rangle.$$

Näin on saatu tulos $H \subseteq \langle c^n \rangle$. Käänteinen relaatio $\langle c^n \rangle \subseteq H$ seuraa suoraan siitä, että $c^n \in H$.
Näin ollen $H = \langle c^n \rangle$.
Koska c^n on ryhmään $\langle c^n \rangle$ kuuluva alin positiivinen alkion c potenssi, niin saadaan, että jos

$$\langle c^n \rangle = \langle c^{n'} \rangle, \qquad n, n' > 0$$

niin välttämättä

$$n = n'.$$

Näin ollen mitkään ryhmistä $\langle c^n \rangle, n = 0, 1, 2, \ldots$ eivät ole keskenään samoja.
□

Tarkastellaan seuraavaksi tapausta, jossa äärettömän syklisen ryhmän laskutoimitusta merkitään yhteenlaskuna.

Lause 4.2.2. *Äärettömän syklisen ryhmän* $(\mathbb{Z}, +)$ *aliryhmät ovat muotoa* $n\mathbb{Z}$*, missä* $n \in \mathbb{N}$*.*

Todistus. Lauseen 4.2.1 nojalla aliryhmät ovat nyt muotoa $\langle nc \rangle$, missä n on luonnollinen luku. Näin ollen ryhmän $\mathbb{Z}$ aliryhmät ovat

$$\langle n \cdot 1 \rangle = \langle n \rangle = n\mathbb{Z}.$$

Negatiivisia generaattoreita ei tarvitse ottaa huomioon, sillä kaikilla $n \in \mathbb{Z}$ pätee $\langle n \rangle = \langle -n \rangle$. □

4.3 Äärellisen syklisen ryhmän aliryhmä

Lause 4.3.1. *Olkoon* $G = \langle g \rangle$ *syklinen ryhmä, jonka kertaluku on* $n \in \mathbb{N}$*. Kaikilla* $m \in \mathbb{Z}$ *pätee*

$$\langle g^m \rangle = \langle g^d \rangle,$$

missä

$$d = syt(n, m).$$

Todistus. Oletetaan, että $m \in \mathbb{Z}$ ja $d = syt(n, m)$.
Todistetaan ensin, että $\langle g^m \rangle \subseteq \langle g^d \rangle$.
On olemassa kokonaisluku k, jolle pätee $m = kd$. Nyt siis $g^m = (g^d)^k$, josta nähdään, että $g^m \in \langle g^d \rangle$ eli $\langle g^m \rangle \subseteq \langle g^d \rangle$.
Todistetaan seuraavaksi, että $\langle g^d \rangle \subseteq \langle g^m \rangle$.
Nyt $d = syt(n, m)$, jolloin on olemassa kokonaisluvut a ja b, joille pätee $d = an + bm$. Nähdään, että

$$g^d = g^{an+bm} = g^{an} g^{bm} = (g^n)^a (g^m)^b = e^a (g^m)^b = (g^m)^b.$$

Näin ollen $g^d \in \langle g^m \rangle$ eli $\langle g^d \rangle \subseteq \langle g^m \rangle$.
Näin ollen $\langle g^m \rangle = \langle g^d \rangle$. □

Lause 4.3.2. *Olkoon G alkion g generoima äärellinen syklinen ryhmä, jonka kertaluku on $n \in \mathbb{N}$. Tällöin alkio g^m generoi ryhmän G syklisen aliryhmän H, jonka kertaluku on $n/syt(n,m)$ kaikilla $m \in \mathbb{Z}$.*

Todistus. Oletetaan, että $m \in \mathbb{Z}$ ja merkitään $d = syt(n,m)$.
Lauseen 4.1.1 mukaan voidaan todeta, että alkio g^m generoi jonkin syklisen aliryhmän H.
Osoitetaan seuraavaksi, että aliryhmän H kertaluku on $n/syt(n,m)$ eli aliryhmässä H on $n/syt(n,m)$ alkiota.
Nyt on olemassa sellainen $a \in \mathbb{Z}_+$, että $n = ad$. Lauseen 4.3.1 nojalla alkioiden g^m ja g^d generoimat aliryhmät ovat samat, joten näiden alkioiden kertaluvut ovat myös samat. Riittää siis osoittaa, että alkion g^d kertaluku on $n/d = a$.
Nyt huomataan, että $(g^d)^a = g^n = e$. Lisäksi nähdään, että millään luku a pienemmällä positiivisella eksponentilla ei saada neutraalialkiota. Sillä jos b on positiivinen kokonaisluku, jolle pätee $b < a$, niin $0 < db < n$, jolloin $(g^d)^b = g^{db} \neq e$. Näin ollen a on pienin positiivinen luku, jolle pätee $(g^d)^a = e$.
Lauseen 2.3.3 nojalla luku $a = n/syt(n,m)$ on alkion g^d kertaluku. □

Esimerkki 4.3.3. *Tarkastellaan syklistä ryhmää $\mathbb{Z}_{12}$. Ryhmän kertaluku on 12 ja eräs sen generoija on $[1]_{12}$.*
Edellisen lauseen nojalla alkio $[3]_{12} = 3 \cdot [1]_{12}$ generoi syklisen aliryhmän, jonka kertaluku on $12/syt(12,3) = 12/3 = 4$. Aliryhmä on

$$\langle [3]_{12} \rangle = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}.$$

Koska nyt $syt(12,8) = 4$, niin alkio $[8]_{12}$ generoi syklisen aliryhmän, jonka kertaluku on $12/4 = 3$. Aliryhmä on siis

$$\langle [8]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}.$$

Alkion $[5]_{12}$ kertaluku on puolestaan $12/syt(12,5) = 12/1 = 12$ eli alkion

$[5]_{12}$ *generoima aliryhmä on koko ryhmä* $\mathbb{Z}_{12}$,

$$\langle [5]_{12} \rangle = \mathbb{Z}_{12}.$$

Lause 4.3.4. *Äärellisen syklisen ryhmän aliryhmien kertaluvut jakavat koko ryhmän kertaluvun.*

Todistus. Olkoon $G = \langle g \rangle$ kertalukua n oleva äärellinen syklinen ryhmä. Lauseen 4.1.1 mukaan syklisen ryhmän jokainen aliryhmä on syklinen, jolloin nyt ryhmän G jokainen aliryhmä on muotoa $\langle g^m \rangle$, kun $m \in \mathbb{N}$. Lauseen 4.3.2 mukaan aliryhmän $\langle g^m \rangle$ kertaluku on $n/syt(n, m)$. Näin ollen aliryhmän kertaluku jakaa ryhmän G kertaluvun. □

Myös seuraava lause seuraa suoraan lauseesta 4.3.2.

Lause 4.3.5. *Kertalukua n olevan syklisen ryhmän $G = \langle g \rangle$ generaattoreita ovat tarkalleen ne ryhmän alkiot g^m, missä $syt(m, n) = 1$.*

Todistus. Alkio g^m generoi ryhmän G, jos ja vain jos alkion kertaluku on n. Lauseesta 4.3.2 seuraa nyt, että alkio g^m generoi ryhmän G täsmälleen silloin, kun $syt(m, n) = 1$. □

Lause 4.3.6. *Kertalukua n olevalla syklisellä ryhmällä on yksikäsitteinen kertalukua d oleva aliryhmä, kun kertaluku d jakaa kertaluvun n. Lisäksi tämä aliryhmä on syklinen.*

Todistus. Olkoon $G = \langle a \rangle$. Jos nyt ryhmän G kertaluku $n = cd$, niin lauseen 2.3.5 perusteella alkion a^c kertaluku on $n/c = cd/c = d$. Joten $\langle a^c \rangle$ on aliryhmä, jonka kertaluku on d.
Todistetaan seuraavaksi aliryhmän yksikäsitteisyys.
Lauseen 4.1.1 mukaan jokainen syklisen ryhmän aliryhmä on syklinen. Olkoon nyt $\langle x \rangle$ kertalukua d oleva ryhmän G aliryhmä.
Olkoon $x = a^m$. Lauseen 2.1.3 nojalla $e = x^d = a^{md}$, jos ja vain jos $n \mid md$. Saadaan $md = nk$ jollakin $k \in \mathbb{Z}_+$. Näin ollen $x = a^m = (a^{n/d})^k = (a^c)^k$,

joten $\langle x \rangle \leq \langle a^c \rangle$.
Koska molemmilla aliryhmillä $\langle x \rangle$ ja $\langle a^c \rangle$ on sama kertaluku d, niin tästä seuraa, että $\langle x \rangle = \langle a^c \rangle$ eli aliryhmä on yksikäsitteinen. □

Lopuksi todistetaan lause, jonka avulla voidaan löytää ja luetella kaikki äärellisen syklisen ryhmän aliryhmät.

Lause 4.3.7. *Olkoon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku on $n \in \mathbb{N}$. Ryhmän G aliryhmät ovat ryhmät $\langle g^d \rangle$, missä d on luvun n positiivinen tekijä. Eri tekijöitä vastaavat aliryhmät poikkeavat toisistaan.*

Todistus. Lauseen 4.1.1 perusteella jokainen ryhmän G aliryhmä on muotoa $\langle g^m \rangle$, missä $m \in \mathbb{Z}_+$. Nyt lauseen 4.3.1 mukaan $\langle g^m \rangle = \langle g^d \rangle$ kaikilla $m \in \mathbb{Z}$, missä $d = syt(n, m)$. Näin ollen kaikki aliryhmät saadaan tutkimalla ryhmän G kertaluvun n tekijöitä.
Jos nyt d on luvun n tekijä, niin silloin $syt(n, d) = d$. Lauseen 4.3.2 nojalla aliryhmän $\langle g^d \rangle$ kertaluku on $n/syt(n, d) = n/d$. Nyt huomataan, että luvun n eri tekijöitä vastaavat aliryhmät ovat eri kokoisia, joten niiden kaikkien täytyy poiketa toisistaan. □

Tiedetään, että jokainen muotoa $\langle g^m \rangle$ oleva ryhmä on äärellisen syklisen ryhmän $G = \langle g \rangle$ aliryhmä. Osa näistä aliryhmistä on samoja keskenään. Nyt edellisen lauseen nojalla kaikki aliryhmät löydetään tarkastelemalla ryhmän G kertaluvun tekijöitä. Seuraavassa esimerkissä luetellaan jo aiemmin esillä olleen ryhmän $\mathbb{Z}_{12}$ aliryhmät.

Esimerkki 4.3.8. *Etsitään ryhmän $\mathbb{Z}_{12}$ aliryhmät.*
Nyt ryhmän kertaluvun 12 positiiviset tekijät ovat $1, 2, 3, 4, 6$ ja 12, joten edellisen lauseen mukaan toisistaan poikkeavia aliryhmiä on kuusi. Ne ovat
$\langle 1 \cdot [1]_{12} \rangle = \langle [1]_{12} \rangle = \mathbb{Z}_{12}$,
$\langle 2 \cdot [1]_{12} \rangle = \langle [2]_{12} \rangle = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}$,
$\langle 3 \cdot [1]_{12} \rangle = \langle [3]_{12} \rangle = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$,

$\langle 4 \cdot [1]_{12} \rangle = \langle [4]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}$,
$\langle 6 \cdot [1]_{12} \rangle = \langle [6]_{12} \rangle = \{[0]_{12}, [6]_{12}\}$,
$\langle 12 \cdot [1]_{12} \rangle = \langle [12]_{12} \rangle = \{[0]_{12}\}$.

Nyt edellä olevan esimerkin aliryhmän $\langle k \cdot [1]_{12} \rangle$ kertaluku on jokaisessa tapauksessa $12/k$. Tämän avulla on helppo tarkistaa, että aliryhmissä on oikea määrä alkioita.
Nyt esimerkiksi luku 8 ei ole ryhmän G kertaluvun tekijä, joten alkion $8 \cdot [1]_{12} = [8]_{12}$ generoimaa aliryhmää ei tarvinnut ottaa huomioon. Nyt esimerkin 4.3.3 mukaan $\langle [8]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}$, joka on siis sama aliryhmä, kuin alkion $[4]_{12}$ generoima aliryhmä. Tämä tulos saadaan myös lauseen 4.3.1 nojalla, sillä nyt $syt(12, 8) = 4$, joten alkioiden $[4]_{12}$ ja $[8]_{12}$ generoimat aliryhmät ovat samat.

Viitteet

[1] Dummit David S., Foote Richard M.: *Abstract Algebra*. Prentice-Hall, New Jersey (1991).

[2] Fraleigh John B.: *A First Course in Abstract Algebra*, 6th Edition. Addison-Wesley (1999).

[3] Herstein Israel N.: *Abstract Algebra*, 3rd Edition. Prentice-Hall, New Jersey (1990).

[4] Häsä Jokke, Rämö Johanna: *Johdatus Abstraktiin Algebraan*, 2.painos. Gaudeamus (2013).

[5] Metsänkylä Tauno, Näätänen Marjatta: *Algebra*, 2.painos. Yliopistopaino, Jyväskylä (2009).

[6] Rotman Joseph J.: *Advanced Modern Algebra*. Prentice-Hall, New Jersey (2002).

[7] Rotman Joseph J.: *A First Course in Abstract Algebra*, 3rd Edition. Prentice-Hall, Upper Saddle River, New Jersey (2006).

[8] Snaith Victor P.: *Groups, Rings and Galois Theory*. World Scientific (1998).

[9] Stahl Saul: *Introductory Modern Algebra: A Historical Approach*. Wiley Interscience (1996).