Sylowin lauseet äärellisten ryhmien luokittelussa

Jenna Johansson

21. marraskuuta 2018

Pro gradu -tutkielma

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Syksy 2018

Merkintöjä:

$\mathbb{N}$	Luonnollisten lukujen joukko $\{1, 2, \ldots\}$
$\mathbb{Z}$	Kokonaislukujen joukko $\{\ldots, -1, 0, 1, 2, \ldots\}$
$\mathbb{Z}_n$	Additiivinen ryhmä $\{0, 1, 2, \ldots, n-1\}$
$G_1 \oplus G_2 \oplus \cdots \oplus G_n$	Ryhmien $G_1, G_2, \ldots, G_n$ suora summa
$G_1 \otimes G_2 \otimes \cdots \otimes G_n$	Ryhmien $G_1, G_2, \ldots, G_n$ karteesinen tulo
(a, b)	Lukujen a ja b suurin yhteinen tekijä
$-a$	Alkion $a \in G$ käänteisalkio additiivisessa ryhmässä G
a^{-1}	Alkion $a \in G$ käänteisalkio ryhmässä G
$\langle a \rangle$	Additiivisen ryhmän G alkion $a \in G$ virittämä syklinen ryhmä $\{ka : k \in \mathbb{Z}\} \subset G$
$\langle a \rangle$	Ryhmän G alkion $a \in G$ virittämä syklinen ryhmä $\{a^k : k \in \mathbb{Z}\} \subset G$
$\lvert a \rvert$	Additiivisen ryhmän alkion a kertaluku $\min\{k \in \mathbb{N} : ka = 0\}$
$\lvert a \rvert$	Alkion a kertaluku $\min\{k \in \mathbb{N} : a^k = e\}$
$A + B$	Ryhmien $A, B \subset G$ summa $\{a + b : a \in A \text{ ja } b \in B\}$
AB	Ryhmien $A, B \subset G$ tulo $\{ab : a \in A \text{ ja } b \in B\}$
$\lvert G \rvert$	Ryhmän G kertaluku (eli ryhmän G alkioiden lukumäärä)
$[G : H]$	Ryhmän G aliryhmän H indeksi eli aliryhmän H oikeiden sivuluokkien lukumäärä ryhmässä G
$(a_1 a_2 a_3 \cdots a_k)$	Joukon $\{1, 2, \ldots, n\}$ alkioiden $a_1, a_2, a_3, \ldots, a_k$ sykli symmetrisessä ryhmässä S_n, missä $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{k-1} \mapsto a_k$ ja $a_k \mapsto a_1$

Tiivistelmä: Jenna Johansson, *Sylowin lauseet äärellisten ryhmien luokittelussa*, matematiikan pro gradu -tutkielma, 50 sivua, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, syksy 2018.

Tässä tutkielmassa luokitellaan äärelliset ryhmät isomorfiaa vaille kertalukuun 15 asti. Lisäksi tutkielma tarjoaa menetelmiä, joita soveltamalla äärellisten ryhmien luokittelua olisi mahdollista jatkaa myös suurempien kertalukujen tapauksessa. Äärellisten ryhmien luokittelussa keskiöön nousevat Sylowin lauseet, joiden avulla voidaan analysoida äärellisten ryhmien rakenteita.

Lagrangen lauseen mukaan äärellisen ryhmän aliryhmän kertaluku jakaa ryhmän kertaluvun. Sen käänteinen tulos ei yleisesti päde, mutta Sylowin ensimmäisessä lauseessa käänteinen saadaan pätemään sellaisille alkuluvun p potensseille p^k, jotka jakavat ryhmän kertaluvun. Tällöin on siis olemassa äärellisen ryhmän aliryhmä, jonka kertaluku on p^k. Jos tämä kertaluku p^k on suurin sellainen alkuluvun p potenssi, joka jakaa ryhmän kertaluvun, aliryhmää sanotaan Sylowin p-aliryhmäksi. Tällöin voidaan muotoilla Sylowin toinen lause, jonka mukaan äärellisen ryhmän Sylowin p-aliryhmät konjugoivat keskenään. Edelleen voidaan osoittaa, että tällaiset Sylowin p-aliryhmät ovat keskenään isomorfisia. Sylowin kolmas lause antaa puolestaan ehtoja näiden Sylowin p-aliryhmien lukumäärälle. Sen mukaan Sylowin p-aliryhmien lukumäärä jakaa ryhmän kertaluvun ja voidaan kirjoittaa muodossa $1 + pk$ jollekin $k = 0, 1, 2, \ldots$.

Tutkielmassa luokitellaan ensin kaikki äärelliset Abelin ryhmät. Kyseiset ryhmät voidaan luokitella ilman Sylowin lauseiden apua, mutta niiden rakenteet noudattavat kuitenkin Sylowin lauseita. Tämän jälkeen siirrytään Sylowin lauseisiin, joita soveltaen päädytään luokittelemaan yleisesti äärellisiä ryhmiä. Lopuksi kootaan ja viimeistellään äärellisten ryhmien luokittelu isomorfiaa vaille kertalukuun 15 asti.

Sisältö

1. Johdanto 1
2. Esitiedot 3
3. Äärellisten Abelin ryhmien luokittelu 6
4. Esitietoja Sylowin lauseiden todistamiseksi 13
5. Sylowin lauseet 22
6. Apuryhmät 28
7. Äärellisten ryhmien luokittelusta 39
7.1. Äärellisten ryhmien luokittelun viimeistelyä 43
Viitteet 50

1. Johdanto

Äärellisten ryhmien teorian ehkäpä perimmäisin tulos on *Lagrangen lause*. Se asettaa rajoitteita äärellisten ryhmien aliryhmille. Lauseen mukaan

äärellisen ryhmän G aliryhmän K kertaluku jakaa ryhmän G kertaluvun.

Lisäksi *Lagrangen lauseen seurauksena* saadaan, että äärellisen ryhmän G alkion a kertaluku jakaa ryhmän G kertaluvun. Lagrangen lauseen käänteinen tulos ei kuitenkaan yleisesti päde. Jos luku k siis jakaa ryhmän G kertaluvun, tästä ei välttämättä seuraa, että ryhmällä G olisi k-kertalukuinen aliryhmä. *Sylowin ensimmäisessä lauseessa* käänteinen saadaan kuitenkin pätemään tietyin ehdoin, kuten myös viitteessä [5, s. 92] todetaan. Nimittäin

jokaiselle alkuluvun p potenssille p^k, joka jakaa äärellisen ryhmän G kertaluvun, on olemassa ryhmän G aliryhmä H, jonka kertaluku on p^k.

Lisäksi Sylowin ensimmäisen lauseen seurauksena saadaan, että alkuluvun p jakaessa äärellisen ryhmän G kertaluvun, on olemassa alkio $a \in G$, jonka kertaluku on p. Tätä kutsutaan *Cauchyn lauseeksi* ja se on käänteinen tulos edellä mainitulle Lagrangen lauseen seuraukselle, kun rajoitetaan tarkastelu alkulukuihin.

Äärellisten Abelin ryhmien luokittelussa isomorfiaa vaille päätulokseksi muodostuu *Äärellisten Abelin ryhmien peruslause*. Sen mukaan jokainen äärellinen Abelin ryhmä G voidaan esittää sen syklisten aliryhmien suorana summana, joiden kertaluvut ovat alkuluvun potensseja. Lisäksi Lagrangen lauseen sovelluksena saadaan, että näiden syklisten aliryhmien kertaluvut jakavat ryhmän G kertaluvun. Äärellisille Abelin ryhmille saadaan siis pätemään myös Sylowin ensimmäinen lause.

Sylowin p-aliryhmä on äärellisen ryhmän G maksimaalinen p-aliryhmä eli aliryhmä, jonka kertaluku on alkuluvun p suurin sellainen potenssi p^n, joka jakaa ryhmän G kertaluvun. Sylowin lauseisiin ja niiden todistuksiin liittyy olennaisesti näiden Sylowin p-aliryhmien olemassaolo sekä konjugoinnin käsite. Merkintä $x^{-1}Kx$ tarkoittaa, että ryhmää K konjugoidaan alkiolla x. *Sylowin toisen lauseen* mukaan

äärellisen ryhmän G Sylowin p-aliryhmät konjugoivat keskenään.

Tällöin voidaan osoittaa, että kyseiset aliryhmät ovat keskenään isomorfisia. Sylowin kolmas lause antaa puolestaan ehtoja näiden Sylowin p-aliryhmien lukumäärälle. Sen mukaan

äärellisen ryhmän G Sylowin p-aliryhmien lukumäärä jakaa ryhmän G kertaluvun ja voidaan esittää muodossa $1 + pk$ jollekin $k = 0, 1, 2, \ldots$.

Kuten ehkä voidaan jo tässä vaiheessa havaita, edellä kuvatut Sylowin lauseet kertovat paljon äärellisten ryhmien rakenteesta. Ne ovat tunnetusti tehokkaita työkaluja äärellisten ryhmien rakenteiden analysoinnissa ja luovat perustan äärellisten ryhmien luokitteluun isomorfiaa vaille.

Ennen vuotta 1870 ryhmäteoria koostui vain kahdenlaisten ryhmien tutkimuksesta - permutaatioryhmien S_n ja geometristen transformaatioryhmien kuten diedriryhmien D_n [13]. Suurimpia tutkimuksen alla olevia ongelmia olivat permutaatioryhmien rakenteiden määrittäminen tiettyjen oletusten, kuten transitiivisuuden, vallitessa sekä äärellisulotteisten jatkuvien transformaatioryhmien [4, s. 17] rakenteiden määrittäminen. Vuoden 1870 jälkeen käsite *ryhmä* kuitenkin kehittyi abstraktimmaksi useiden

vaiheiden kautta ja johti uudenlaiseen ongelmaan. Haluttiin nimittäin keksiä keino sille, miten pystyttäisiin tutkimaan abstraktien ryhmien rakennetta ilman niiden esittämistä permutaatioiden tai transformaatioiden avulla ja vasta sen jälkeen liittää nämä abstraktit ryhmät permutaatio- tai transformaatioryhmiin. Tavoitteena oli siis löytää yleisiä teorioita liittyen abstraktien ryhmien rakenteeseen sekä määrittää kaikki äärellisen kertaluvun ryhmät. Vuonna 1870 saksalainen matemaatikko Leopold Kronecker todisti artikkelissaan [9] *Äärellisten Abelin ryhmien peruslauseen* ja vuonna 1872 norjalainen matemaatikko Ludwig Sylow esitteli artikkelissaan [12] äärellisten ryhmien rakenteeseen liittyviä tuloksia, muun muassa *Sylowin lauseet*. Nämä ovat olleet ja ovat edelleen keskeisessä osassa äärellisten ryhmien luokittelussa isomorfiaa vaille kuten tämänkin tutkielman aikana tullaan huomaamaan. Tarkempia yksityiskohtia ryhmäteorian alun historiasta löytyy viitteestä [13, ss. 137–159].

Tämän tutkielman pääasiallisena tarkoituksena on luokitella kaikki äärelliset ryhmät isomorfiaa vaille kertalukuun 15 asti. Tutkielma antaa kuitenkin tarvittavia työkaluja ja menetelmiä, joiden avulla äärellisten ryhmien luokittelua olisi mahdollista jatkaa myös suurempien kertalukujen tapauksessa. Välttämättömät esitiedot käsitellään kappaleessa 2, jonka jälkeen siirrytään ensin luokittelemaan kaikki äärelliset Abelin ryhmät isomorfiaa vaille. Tämä tehdään kappaleessa 3. Kun halutaan luokitella ei-Abelisia äärellisiä ryhmiä isomorfiaa vaille, Sylowin lauseet ovat keskeisessä roolissa. Ennen kuin voidaan kappaleessa 5 esitellä itse Sylowin lauseet, käydään kappaleessa 4 läpi tarvittavia esitietoja Sylowin lauseiden todistusta ajatellen. Sylowin lauseiden todistuksien jälkeen ollaan miltei valmiita aloittamaan äärellisten ryhmien luokittelu. Ennen sitä kappaleessa 6 esitellään kuitenkin vielä sellaisia apuryhmiä, jotka ovat tärkeässä osassa, jotta saadaan täydellisesti luokiteltua äärelliset ryhmät kertalukuun 15 asti. Tämän jälkeen ollaan valmiita luokittelemaan kappaleessa 7 kaikki äärelliset ryhmät isomorfiaa vaille kertalukuun 15 asti.

Hyvät esitiedot abstraktin algebran alkeista ovat hyödyksi tämän tutkielman lukijalle ja ne voi tarvittaessa kerrata esimerkiksi lähteestä [6], johon tutkielma myös suurilta osin pohjautuu. Muita merkittäviä tutkielmassa käytettyjä lähteitä ovat [7], [5] ja [1].

2. Esitiedot

Tämä kappale sisältää välttämättömiä esitietoja, joiden avulla äärellisten ryhmien luokittelu isomorfiaa vaille on mahdollista. Määritelmät ja lauseet eivät välttämättä riipu toisistaan, vaan ne on esitetty luettelomaisesti tukemaan äärellisten ryhmien luokittelua. Esitiedot pohjautuvat lähteeseen [6]. Lisäksi lukijalta edellytetään hyvät esitiedot abstraktin algebran alkeista; ryhmäteoriasta, laskutoimituksista ja homomorfismeista sekä modulaariaritmetiikasta.

Lemma 2.1. *Olkoon G additiivinen ryhmä ja alkio $a \in G$.*

(1) *Jos alkion a kertaluku $|a| = h < \infty$, niin $ka = 0$, jos ja vain jos $h|k$.*
(2) *Jos alkion a kertaluku $|a| = td < \infty$, missä $d > 0$, niin $|ta| = d$.*

Määritelmä 2.2. Olkoot $G_1, G_2, \ldots, G_k$ additiivisia Abelin ryhmiä. Määritellään laskutoimitus joukossa

$$G_1 \oplus G_2 \oplus \cdots \oplus G_k = \{(a_1, \ldots, a_k) : a_i \in G_i \text{ kaikilla } i = 1, \ldots, k\}$$

seuraavasti:

$$(a_1, a_2, \ldots, a_k) + (b_1, b_2, \ldots, b_k) = (a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k)$$

missä $a_i, b_i \in G_i$ kaikilla $i = 1, \ldots, k$.

Voidaan osoittaa, että $G_1 \oplus G_2 \oplus \cdots \oplus G_k$ on ryhmä: Jos e_i on ryhmän G_i neutraalialkio kullakin $i = 1, \ldots, k$, niin $(e_1, e_2, \ldots, e_k)$ on ryhmän $G_1 \oplus G_2 \oplus \cdots \oplus G_k$ neutraalialkio ja $(-a_1, -a_2, \ldots, -a_k)$ on alkion $(a_1, a_2, \ldots, a_k)$ käänteisalkio.

Lemma 2.3. *Olkoot M ja N additiivisen ryhmän G normaaleja aliryhmiä siten, että $M \cap N = \{0\}$. Jos $m \in M$ ja $n \in N$, niin $m + n = n + m$.*

Todistus. Olkoon $m \in M$ ja $n \in N$. Koska M on normaali aliryhmä, kaikille sen alkioille $m \in M$ pätee $-n + m + n \in M$. Tällöin, kun lisätään vasemmalle puolelle alkio $-m \in M$, seuraa, että $-m - n + m + n = -m + (-n + m + n) \in M$. Vastaavasti ryhmän N normaaliudesta seuraa, että $-m - n + m \in N$, jolloin lisättäessä oikealle puolelle alkio $n \in N$, saadaan $-m - n + m + n = (-m - n + m) + n \in N$. Nyt siis tiedetään, että alkio $-m - n + m + n \in M \cap N = \{0\}$. Lisäämällä yhtälön $-m - n + m + n = 0$ molemmille puolille vasemmalle $n + m$ saavutetaan väite eli $m + n = n + m$. □

Lemma 2.3 on tarpeellinen seuraavan lemman todistuksessa.

Lemma 2.4. *Olkoot $N_1, \ldots, N_k$ additiivisen ryhmän G normaaleja aliryhmiä siten, että jokainen ryhmän G alkio a voidaan kirjoittaa yksikäsitteisesti mudossa*

$$a_1 + a_2 + \cdots + a_k,$$

missä $a_i \in N_i$. Tällöin

$$G \cong N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

Yksikäsitteisyydellä tarkoitetaan tässä, että jos $a_1 + \cdots + a_k = b_1 + \cdots + b_k$, missä $a_i, b_i \in N_i$, niin $a_i = b_i$ kullakin i.

Todistus. Olkoon $f : N_1 \oplus \cdots \oplus N_k \to G$ kuvaus $f(a_1, \ldots, a_k) = a_1 + \cdots + a_k$. Oletuksen mukaan jokainen ryhmän G alkio voidaan kirjoittaa muodossa $a_1 + \cdots + a_k$, missä $a_i \in N_i$ kaikilla $i = 1, \ldots, k$, jolloin kuvaus f on siis surjektio. Lisäksi kuvaus f on injektio, sillä jos $f(a_1, \ldots, a_k) = f(b_1, \ldots, b_k)$, niin $a_1 + \cdots + a_k = b_1 + \cdots + b_k$ ja yksikäsitteisyyden nojalla $a_i = b_i$ kaikilla $i = 1, \ldots, k$. Täytyy vielä osoittaa, että kuvaus f on homomorfismi. Jos $a \in N_i \cap N_j$, missä $i, j = 1, \ldots, k$ ja $i \neq j$, niin alkio a voidaan kirjoittaa normaalien aliryhmien $N_1, \ldots, N_k$ alkioiden summana kahdella eri tavalla:

$$0 + \cdots + 0 + \underbrace{a}_{i.\text{ alkio}} + 0 + \cdots + 0 = 0 + \cdots + 0 + \underbrace{a}_{j.\text{ alkio}} + 0 + \cdots + 0.$$

Yksikäsitteisyyden nojalla jokaisen ryhmän N_i summattavan täytyy olla yhtäsuuria, joten $a = 0$ ja $N_i \cap N_j = \{0\}$. Näin ollen, koska N_i on ryhmän G normaali aliryhmä kaikilla $i = 1, \ldots, k$, Lemman 2.3 nojalla tiedetään, että $a_i + b_j = b_j + a_i$ kaikilla $a_i \in N_i$ ja $b_j \in N_j$, missä $i \neq j$. Kun käytetään tätä tietoa toistuvasti saadaan:

$$\begin{aligned} f[(a_1, \ldots, a_k) + (b_1, \ldots, b_k)] &= f(a_1 + b_1, \ldots, a_k + b_k) \\ &= (a_1 + b_1) + (a_2 + b_2) + (a_3 + b_3) + \cdots + (a_k + b_k) \\ &= (a_1 + a_2) + (b_1 + b_2) + (a_3 + b_3) + \cdots + (a_k + b_k) \\ &= \cdots \\ &= (a_1 + a_2 + \cdots + a_k) + (b_1 + b_2 + \cdots + b_k) \\ &= f(a_1, \ldots, a_k) + f(b_1, \ldots, b_k). \end{aligned}$$

Kuvaus f saatiin siis osoitettua isomorfismiksi eli $G \cong N_1 \oplus N_2 \oplus \cdots \oplus N_k$. □

Lemma 2.5. *Olkoon M ja N additiivisen ryhmän G normaaleja aliryhmiä. Jos $G = M + N$ ja $M \cap N = \{0\}$, niin*

$$G \cong M \oplus N.$$

Todistus. Jokainen ryhmän G alkio voidaan kirjoittaa muodossa $m+n$, missä $m \in M$ ja $n \in N$. Oletetaan, että alkiolla $m + n \in G$ on toinen vastaava esitystapa eli $m + n = m' + n'$, missä $m, m' \in M$ ja $n, n' \in N$. Muokataan yhtälöä

$$m + n = m' + n'$$

lisäämällä ensin yhtälön molemmille puolille vasemmalle $-m'$. Yhtälö saa tällöin muodon

$$-m' + m + n = -m' + m' + n'.$$

Päädytään yhtälöön

$$-m' + m + n = n',$$

joten jatketaan lisäämällä molemmille puolille oikealle $-n$, jolloin päästään muotoon:

$$-m' + m + n - n = n' - n.$$

Tällöin siis pätee

$$-m' + m = n' - n.$$

Mutta $-m' + m \in M$ ja $n' - n \in N$ ja $M \cap N = \{0\}$, joten täytyy päteä $-m' + m = 0$ eli $m = m'$ ja vastaavasti $n = n'$. Siispä jokainen ryhmän G alkio voidaan kirjoittaa yksikäsitteisesti muodossa $m + n$. Tällöin, koska aliryhmät M ja N ovat normaaleja, Lemman 2.4 nojalla $G \cong M \oplus N$. □

Lemma 2.6. *Olkoon G Abelin ryhmä ja p alkuluku. Tällöin*

$$G(p) = \{a \in G : |a| = p^n \text{ jollekin } n \geq 0\}$$

on ryhmän G aliryhmä.

Todistus. Oletuksen nojalla G on ryhmä, joten sen täytyy sisältää vähintään neutraalialkion $0 \in G$. Tällöin, koska $|0| = 1 = p^0$, niin pätee $0 \in G(p)$. Siispä $G(p) \neq \emptyset$. Olkoon $a \in G(p)$. Tällöin pätee $|a| = p^n$ jollekin $n \geq 0$ ja siis $p^n a = 0$. Tarkistetaan, että alkion a käänteisalkio $-a$ kuuluu myös joukkoon $G(p)$. Lemman 2.1 nojalla tiedetään, että alkiolle a on $ka = 0$, kun $p^n | k$. Käänteisalkiolle $-a$ voidaan tällöin kirjoittaa $k(-a) = -(ka) = 0$. Siispä pätee

$$|a| = \min\{k : ka = 0\} = \min\{k : k(-a) = 0\} = |-a|,$$

jolloin $|-a| = p^n$ ja $-a \in G(p)$. Tarkistetaan, että laskutoimitus on suljettu operaatio. Olkoon nyt $b \in G(p)$, jolle alkion a tavoin pätee $|b| = p^m$ jollekin $m \geq 0$ eli $p^m b = 0$. Voidaan kirjoittaa

$$p^{m+n}(a+b) = p^n p^m (a+b) = p^m(p^n a) + p^n(p^m b) = 0,$$

jolloin Lemman 2.1 nojalla kertaluvun $|a+b|$ täytyy jakaa luku p^{m+n}. Koska p on alkuluku saadaan siis, että kertaluku on muotoa $|a+b| = p^t$ ja pätee $a+b \in G(p)$. Näin ollen $G(p)$ on ryhmän G aliryhmä ja erityisesti sen normaali aliryhmä, sillä koska G on Abelin ryhmä, aliryhmälle $G(p)$ pätee

$$G(p) + a = \{g + a : g \in G(p)\} = \{a + g : g \in G(p)\} = a + G(p)$$

kaikilla $a \in G$. □

Esimerkki 2.7. Jos $G = \mathbb{Z}_{12}$, niin $G(2)$ on joukko alkioita, joiden kertaluvut ovat $2^0, 2^1, 2^2, \ldots$. Siispä $G(2) = \{0, 3, 6, 9\}$, sillä $|0| = 2^0, |3| = 2^2, |6| = 2^1$ ja $|9| = 2^2$. Vastaavasti $G(3) = \{0, 4, 8\}$. Jos $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3$, niin $G(3) = G$, sillä jokaiselle nollasta eroavalle alkiolle $a \in G(3)$ kertaluku $|a| = 3$. Tarkastellaan esimerkiksi alkiota $(1, 2) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Tämän alkion kertaluku on $|(1,2)| = 3$, sillä

$$(1,2) + (1,2) + (1,2) = (3,6) = ([0]_3, [0]_3).$$

3. Äärellisten Abelin ryhmien luokittelu

Tämä kappale sisältää kaikkien äärellisten Abelin ryhmien luokittelun. Luokittelu perustuu todistukseen, että jokainen äärellinen Abelin ryhmä G voidaan esittää sen syklisten aliryhmien suorana summana. Kyseinen tulos on esitetty Lauseena 3.9 ja se on kappaleen 3 päätulos. Lause tunnetaan myös nimellä *Äärellisten Abelin ryhmien peruslause.*
Ensimmäisenä askeleena osoitetaan, että äärellinen Abelin ryhmä G voidaan esittää aliryhmiensä $G(p_i)$ suorana summana, missä p_i:t ovat eri alkulukuja, jotka jakavat ryhmän G kertaluvun yksikäsitteisesti. Tämän osoittamiseksi tarvitaan avuksi seuraava lemma:

Lemma 3.1. *Olkoon G Abelin ryhmä ja $a \in G\backslash\{0\}$ alkio, jonka kertaluku on $|a| < \infty$. Olkoot lisäksi kertaluvun $|a|$ alkutekijät $p_1, \ldots, p_t$. Tällöin*

$$a = a_1 + a_2 + \cdots + a_t,$$

missä $a_i \in G(p_i)$ kullakin $i \in \{1, 2, \ldots, k\}$.

Todistus. Käytetään todistukseen induktiota. Jos kertaluku $|a|$ on jaollinen ainoastaan alkuluvulla p_1, niin alkion a kertaluku on alkuluvun p_1 potenssi eli $|a| = p_1^{r_1}$, missä $r_1 \in \mathbb{N}$. Tällöin $a \in G(p_1)$. Lemma on siis näillä oletuksilla tosi. Tehdään induktio-oletus, että lemma on tosi kaikille alkioille $a \in G$, joiden kertaluku on jaollinen enintään $k-1$ kappaleella eri alkulukuja. Oletetaan nyt, että $|a|$ on jaollinen alkuluvuilla $p_1, \ldots, p_k$, missä $p_i \neq p_j$, kun $i \neq j$. Nyt siis $|a| = p_1^{r_1} \cdots p_k^{r_k}$, missä $r_i \in \mathbb{N}$ kaikilla $i \in \{1, \ldots, k\}$. Olkoon $m = p_2^{r_2} \cdots p_k^{r_k}$ ja $n = p_1^{r_1}$, jolloin $|a| = mn$. Nyt $(m, n) = 1$ ja näin ollen on Bezout'n lemman [6, Theorem 1.2] nojalla olemassa $u, v \in \mathbb{Z}$ siten, että $1 = mu + nv$. Voidaan kirjoittaa alkio $a \in G$ siis muodossa

$$a = 1a = (mu + nv)a = mua + nva.$$

Nyt, koska kertaluku $|a| = nm$, missä $n = p_1^{r_1}$, niin Lemman 2.1 nojalla $|ma| = n = p_1^{r_1}$. Siispä $ma \in G(p_1)$, jolloin myös kaikille $u \in \mathbb{Z}$ pätee $mua \in G(p_1)$, sillä Lemman 2.6 nojalla $G(p_1)$ on aliryhmä. Käytetään nyt hyödyksi tietoa, että alkion ma kertaluku on $|ma| = n$, jolloin

$$p_2^{r_2} \cdots p_k^{r_k}(nva) = m(nva) = (mn)va = v(mna) = v0 = 0.$$

Näin ollen Lemman 2.1 nojalla kertaluku $|nva|$ jakaa luvun $m = p_2^{r_2} \cdots p_k^{r_k}$. Tällöin induktio-oletuksen nojalla $nva = a_2 + a_3 + \cdots + a_k$, missä $a_i \in G(p_i)$. Asetetaan $mua = a_1$.

Yllä tehdyt laskut kokoamalla nähdään, että

$$a = mua + nva = a_1 + a_2 + \cdots + a_k,$$

missä $a_i \in G(p_i)$ kaikilla $i = 1, 2, \ldots, k$. □

Esimerkki 3.2. Olkoon $G = \mathbb{Z}_{12}$ ja $[10]_{12} \in G$. Alkion $[10]_{12}$ kertaluku voidaan esittää alkutekijöiden avulla:

$$\left|[10]_{12}\right| = 6 = 2 \times 3.$$

Toisaalta

$$[6]_{12} + [4]_{12} = [10]_{12},$$

missä $6 \in G(2)$ ja $4 \in G(3)$.

Lause 3.3. *Olkoon G äärellinen Abelin ryhmä. Tällöin*

$$G \cong G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_t),$$

missä $p_1, \ldots, p_t$ ovat ryhmän G kertaluvun $|G|$ kaikki alkutekijät ja $p_i \neq p_j$ kaikilla $i \neq j$.

Todistus. Jos $a \in G$, niin sen kertaluku $|a|$ jakaa ryhmän G kertaluvun $|G|$ Lagrangen lauseen [6, Theorem 8.5] nojalla. Tällöin Lemman 3.1 nojalla

$$a = a_1 + \cdots + a_t, \tag{3.1}$$

missä $a_i \in G(p_i)$. Lisäksi $a_i = 0$, jos alkion a kertaluku $|a|$ ei ole jaollinen alkuluvulla p_i. Osoitetaan, että alkion a esitystapa (3.1) on yksikäsitteinen. Oletetaan, että

$$a_1 + \cdots + a_t = b_1 + \cdots + b_t$$

joillain $a_i, b_i \in G(p_i)$, missä $i = 1, \ldots, t$. Koska G on Abelin ryhmä, niin

$$a_1 - b_1 = (b_2 - a_2) + (b_3 - a_3) + \cdots + (b_t - a_t).$$

Jokaiselle $i \in \{1, 2, \ldots, t\}$ on $b_i - a_i \in G(p_i)$ ja näin ollen alkiolla $b_i - a_i$ on kertaluku $|b_i - a_i| = p_i^{r_i}$, missä $r_i \in \mathbb{N}$. Jos $m = p_2^{r_2} \cdots p_t^{r_t}$, niin $m(b_i - a_i) = 0$ kaikille $i \in \{2, 3, \ldots, t\}$ Lemman 2.1 nojalla. Näin ollen

$$m(a_1 - b_1) = m(b_2 - a_2) + \cdots + m(b_t - a_t) = 0 + \cdots + 0 = 0.$$

Tällöin siis kertaluvun $|a_1 - b_1|$ täytyy jakaa luku m Lemman 2.1 nojalla. Mutta koska $a_1 - b_1 \in G(p_1)$, sen kertaluvun täytyy olla jokin alkuluvun p_1 potenssi $p_1^{r_1}$. Ainoa luku $p_1^{r_1}$, joka jakaa luvun $m = p_2^{r_2} \cdots p_t^{r_t}$, on $p_1^0 = 1$. Tällöin $a_1 - b_1 = 0$ ja siis $a_1 = b_1$. Sama päättely voidaan toistaa myös kaikille $i = 2, \ldots, t$ ja näin osoittaa, että $a_i = b_i$ kaikille $i = 1, 2, \ldots, t$. Tämä osoittaa, että jokainen ryhmän G alkio voidaan esittää yksikäsitteisesti muodossa $a_1 + \cdots + a_t$, missä $a_i \in G(p_i)$ ja Lemman 2.4 nojalla $G \cong G(p_1) \oplus \cdots \oplus G(p_t)$. □

Esimerkki 3.4. Olkoon $G = \mathbb{Z}_{30}$. Ryhmän G kertaluku on $30 = 2 \times 3 \times 5$, jolloin Lauseen 3.3 nojalla pätee

$$\mathbb{Z}_{30} \cong G(2) \oplus G(3) \oplus G(5).$$

Tarkastellaan esimerkiksi alkiota $14 \in \mathbb{Z}_{30}$. Kertaluku $|[14]_{30}| = 15$ jakaa ryhmän $\mathbb{Z}_{30}$ kertaluvun $|\mathbb{Z}_{30}| = 30$. Lisäksi kertaluku $|[14]_{30}| = 15$ on jaollinen alkuluvuilla 3 ja 5, mutta ei alkuluvulla 2, joten alkio $[14]_{30} \in \mathbb{Z}_{30}$ voidaan esittää muodossa $[14]_{30} = [4]_{30} + [24]_{30} + [0]_{30}$, missä $[4]_{30} \in G(3)$ ja $[24]_{30} \in G(5)$, kuten Lemmassa 3.1. Samanlainen päättely voidaan toistaa kaikille alkioille $a \in \mathbb{Z}_{30}$ eli alkiot voidaan kirjoittaa muodossa $a = a_1 + a_2 + a_3$, missä $a_1 \in G(2)$, $a_2 \in G(3)$ ja $a_3 \in G(5)$, kunhan alkuluvut 2, 3 ja 5 jakavat kertaluvun $|a|$. Jos jaollisuus ei toteudu, korvataan vastaava summattava a_j nollalla.

Määritelmä 3.5. Olkoon $p \in \mathbb{N}$ alkuluku. Ryhmä, jonka jokaisen alkion kertaluku on muotoa p^r, missä $r \in \{0, 1, \ldots\}$, on *p-ryhmä*.

Edellisen määritelmän nojalla tiedetään nyt siis, että jos G on Abelin ryhmä, niin tällöin jokainen ryhmä $G(p)$, missä p on alkuluku, on p-ryhmä.

Määritelmä 3.6. Olkoon G p-ryhmä, missä p on alkuluku. Alkio $a \in G$ on *maksimaalinen*, jos sen kertaluku toteuttaa epäyhtälön $|a| \geq |b|$ kaikille $b \in G$.

Lemma 3.7. *Olkoon G p-ryhmä. Jos $a \in G$ on maksimaalinen alkio, jonka kertaluku on $|a| = p^n$, niin $p^n b = 0$ kaikilla $b \in G$.*

Todistus. Alkion $a \in G$ kertaluku on $|a| = p^n$ ja alkion $b \in G$ kertaluku on $|b| = p^j$, missä $j \leq n$ maksimaalisuuden perusteella. Voidaan siis kirjoittaa alkion a kertaluku muodossa $p^n = p^{n-j}p^j$, jolloin

$$p^n b = p^{n-j}(p^j b) = 0.$$

□

Seuraavaksi tavoitteena on osoittaa, että jokainen äärellinen Abelin p-ryhmä on syklisten ryhmien suora summa. Tätä varten tarvitsee kuitenkin ensin todistaa, että jokaisella äärellisellä Abelin p-ryhmällä on syklinen suora summattava.

Lemma 3.8. *Olkoon G äärellinen Abelin p-ryhmä ja $a \in G$ sen maksimaalinen alkio. Tällöin on olemassa ryhmän G aliryhmä K siten, että $G \cong \langle a \rangle \oplus K$ ja $|K| < |G|$.*

Todistus. Tarkastellaan sellaisia ryhmän G aliryhmiä H, joille pätee

$$\langle a \rangle \cap H = \{0\}. \tag{3.2}$$

On olemassa vähintään yksi tällainen aliryhmä, sillä jos $H = \{0\}$, niin ehto (3.2) on voimassa. Lisäksi, koska ryhmä G on äärellinen, täytyy olla olemassa myös inkluusion suhteen suurin aliryhmä K, jolle pätee $\langle a \rangle \cap K = \{0\}$. Toisin sanoen, jos H on ryhmän G aliryhmä ja $K \subsetneq H$, niin $\langle a \rangle \cap H \neq \{0\}$. Lemman 2.5 nojalla riittää osoittaa, että $G = \langle a \rangle + K$, jolloin $G \cong \langle a \rangle \oplus K$. Todistetaan tämä antiteesillä:

$$\text{on olemassa ryhmän } G \text{ alkio } b \neq 0 \text{ siten, että } b \notin \langle a \rangle + K.$$

Olkoon $j > 0$ pienin mahdollinen luonnollinen luku, jolle pätee $p^j b \in \langle a \rangle + K$. Tällainen j on olemassa, sillä G on p-ryhmä, jolloin Lemman 3.7 nojalla, valitsemalla $j = n$, saadaan $p^n b = 0 = 0 + 0 \in \langle a \rangle + K$, kun $|a| = p^n$. Näin ollen

$$c = p^{j-1} b \notin \langle a \rangle + K \tag{3.3}$$

ja $pc = p^j b \in \langle a \rangle + K$, jolloin voidaan kirjoittaa

$$pc = ta + k, \text{ missä } t \in \mathbb{Z} \text{ ja } k \in K. \tag{3.4}$$

Jos alkiolla a on kertaluku $|a| = p^n$, niin $p^n c = 0$, koska alkio a on maksimaalinen. Seurauksena yhtälöstä (3.4) saadaan, että

$$p^{n-1}ta + p^{n-1}k = p^{n-1}(ta + k) = p^{n-1}(pc) = p^n c = 0.$$

Tällöin $p^{n-1}ta = -p^{n-1}k \in \langle a \rangle \cap K = \{0\}$ ja $p^{n-1}ta = 0$. Lemma 2.1 osoittaa, että kertaluvun $|a| = p^n$ täytyy siis jakaa luku $p^{n-1}t$, jolloin myös alkuluku p jakaa luvun $t \in \mathbb{Z}$ eli $t = pm$ jollakin $m \in \mathbb{Z}$. Näin ollen on voimassa yhtäsuuruus $pc = ta + k = pma + k$, josta toisin muotoilemalla saadaan yhtäsuuruus $k = pc - pma = p(c - ma)$. Olkoon

$$d = c - ma. \tag{3.5}$$

Tällöin $pd = p(c - ma) = k \in K$, mutta $d \notin K$. Nimittäin, jos näin ei olisi ja pätisi $d \in K$, niin voitaisiin kirjoittaa $c - ma = k' \in K$. Tämä aiheuttaisi ristiriidan ehdon (3.3) kanssa, sillä olisi voimassa $c = ma + k' \in \langle a \rangle + K$.

Tiedetään, että

$$H = \{x + rd : x \in K, r \in \mathbb{Z}\}$$

on ryhmän G aliryhmä, sillä $H \subset G$, missä $H \neq \emptyset$, ja lisäksi H on suljettu ryhmän G laskutoimituksen suhteen. Koska pätee $d = 0 + 1d \in H$ ja $d \notin K$, täytyy aliryhmän H olla aidosti suurempi kuin aliryhmän K eli $K \subsetneq H$. Ryhmä K on inkluusion suhteen suurin aliryhmä, jolle ehto (3.2) pätee, joten täytyy päteä $\langle a \rangle \cap H \neq \{0\}$. Olkoon $w \in \langle a \rangle \cap H$ nollasta poikkeava alkio. Tällöin

$$w = sa = k_1 + rd, \text{ missä } k_1 \in K \text{ ja } r, s \in \mathbb{Z}. \tag{3.6}$$

Luku $r \in \mathbb{Z}$ ei ole jaollinen alkuluvulla p, sillä jos pätisi $r = py$ jollakin $y \in \mathbb{Z}$, niin koska $pd \in K$ päädyttäisiin ristiriitaan:

$$0 \neq w = sa = k_1 + ypd \in \langle a \rangle \cap K = \{0\}.$$

Tästä seuraa, että $(p, r) = 1$, jolloin Bezout'n lemman nojalla on olemassa luvut $u, v \in \mathbb{Z}$ siten, että $pu + rv = 1$. Käyttäen tätä tietoa ja ehtoja (3.4), (3.5) ja (3.6) päädytään seuraavaan päättelyketjuun:

$$\begin{aligned} c = 1c = (pu + rv)c &= u(pc) + v(rc) \\ &= u(ta + k) + v(r(d + ma)) \\ &= u(ta + k) + v(rd + rma) \\ &= u(ta + k) + v(sa - k_1 + rma) \\ &= (ut + vs + rmv)a + (uk - vk_1) \in \langle a \rangle + K. \end{aligned}$$

Tämä on ristiriidassa ehdon (3.3) kanssa, jolloin haluttu yhtäsuuruus $G = \langle a \rangle + K$ on voimassa ja Lemman 2.5 nojalla $G \cong \langle a \rangle \oplus K$. Lisäksi, koska K on inkluusion suhteen suurin sellainen aliryhmä, jolle pätee $\langle a \rangle \cap K = \{0\}$, niin syklisen ryhmän $\langle a \rangle$ virittäjäalkiolle $a \in G$ pätee $\{a\} \cap K = \emptyset$. Siispä $|K| < |G|$. □

Lause 3.9. *(Äärellisten Abelin ryhmien peruslause) Olkoon G äärellinen Abelin ryhmä. Tällöin*

$$G \cong K_1 \oplus K_2 \oplus \cdots \oplus K_l,$$

joillain syklisillä ryhmillä K_i, joiden kertaluvut ovat muotoa $|K_i| = p_i^{r_i}$, missä p_i on alkuluku ja $r_i \in \mathbb{N}$ kaikilla $i = 1, 2, \ldots, l$. Lisäksi kertaluvut $|K_i| = p_i^{r_i}$ jakavat ryhmän G kertaluvun.

Todistus. Lauseen 3.3 nojalla ryhmä G on isomorfinen aliryhmiensä $G(q_i)$ suoran summan kanssa eli

$$G \cong G(q_1) \oplus \cdots \oplus G(q_t),$$

missä $q_1, \ldots, q_t$ ovat kertaluvun $|G|$ kaikki alkutekijät ja $q_i \neq q_j$ kaikilla $i \neq j$. Jokainen $G(q_i)$ on Abelin q_i-ryhmä, joten riittää osoittaa, että jokainen äärellinen Abelin q_i-ryhmä H on sellaisten syklisten aliryhmiensä K_i suora summa, joiden kertaluvut ovat muotoa $|K_i| = q_i^{r_i}$, missä $i = 1, 2, \ldots, l$. Todistetaan tämä induktiolla käyttämällä ryhmän H kertalukua.

Tarkastellaan ensin tapausta, missä $|H| = 2$. Kun kertaluku $|H|$ on 2 ja alkio $h \in H$ ei ole neutraalialkio, niin syklisen aliryhmän $\langle h \rangle$ kertaluku on $|\langle h \rangle| > 1$. Koska aliryhmän $\langle h \rangle$ kertaluvun täytyy jakaa kertaluku $|H| = 2$ ja 2 on alkuluku, niin täytyy olla $|\langle h \rangle| = 2$. Siispä $\langle h \rangle = H$ ja H on syklinen ryhmä, jonka kertaluku on 2. Näin ollen väite on tosi perusaskeleessa.

Oletetaan nyt, että väite on tosi kaikille Abelin q_i-ryhmille, joiden kertaluku on aidosti pienempi kuin kertaluku $|H|$ ja olkoon maksimaalisen alkion $a \in H$ kertaluku

$|a| = {q_i}^r$. Tällöin Lemman 3.8 nojalla $H \cong \langle a \rangle \oplus K$ ja $|K| < |H|$. Lisäksi, koska K on ryhmän H aliryhmä, K on q_i-ryhmä. Induktio-oletuksen nojalla tiedetään, että ryhmä K on isomorfinen syklisten aliryhmiensä suoran summan kanssa eli $K \cong K_1 \oplus \cdots \oplus K_l$, missä $|K_i| = q_i^{r_i}$ kaikille $i = 1, 2, \ldots, l$. Tällöin, koska ryhmä $\langle a \rangle$ on syklinen ja $|a| = {q_i}^r$, väite pätee myös ryhmälle $H = \langle a \rangle \oplus K$ ja induktioaskel on todistettu.

Lagrangen lauseen sovelluksena saadaan, että ryhmän $K_1 \oplus K_2 \oplus \cdots \oplus K_l$ aliryhmän $\{e\} \oplus \cdots \oplus \{e\} \oplus K_i \oplus \{e\} \oplus \cdots \oplus \{e\}$ kertaluku

$$|\{e\} \oplus \cdots \oplus \{e\} \oplus K_i \oplus \{e\} \oplus \cdots \oplus \{e\}| = |K_i| = p_i^{r_i}$$

jakaa isomorfian nojalla ryhmän G kertaluvun. □

Suoran summan määritelmän nojalla tiedetään, että jos äärellinen ryhmä G voidaan esittää syklisten ryhmien $\mathbb{Z}_m$ ja $\mathbb{Z}_k$ suorana summana, eli $G = \mathbb{Z}_m \oplus \mathbb{Z}_k$ joillakin $m, k \in \mathbb{N}$, niin ryhmän G kertaluku on $|G| = mk$. Tämä yleistyy muotoon, missä ryhmän G kertaluvuksi saadaan $|G| = n_1 n_2 \cdots n_k$, jos äärellinen ryhmä G voidaan esittää syklisten ryhmien $\mathbb{Z}_{n_1}, \mathbb{Z}_{n_2}, \ldots \mathbb{Z}_{n_k}$ suorana summana, eli $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Edelleen, Lauseen 3.9 syklisten ryhmien K_i kertaluvut suhtautuvat äärellisen ryhmän G kertalukuun samalla tavalla.

Esimerkki 3.10. Luku 36 voidaan kirjoittaa alkulukujen potenssien tulona neljällä eri tavalla:

$$36 = 2 \times 2 \times 3 \times 3 = 2 \times 2 \times 3^2 = 2^2 \times 3 \times 3 = 2^2 \times 3^2.$$

Tällöin Lauseesta 3.9 seuraa, että jokainen Abelin ryhmä G, jonka kertaluku on $|G| = 36$, on isomorfinen ryhmän $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ tai ryhmän $\mathbb{Z}_4 \oplus \mathbb{Z}_9$ kanssa, sillä edellämainittujen ryhmien komponenttien kertaluvut voidaan esittää alkulukujen potensseina seuraavasti: $|\mathbb{Z}_2| = 2^1, |\mathbb{Z}_3| = 3^1, |\mathbb{Z}_4| = 2^2$ ja $|\mathbb{Z}_9| = 3^2$. Ryhmän G kertaluku voidaan siis esittää näiden kertalukujen tulona, kuten esimerkin alussa todettiin. Lisäksi nämä ryhmät eivät ole isomorfisia keskenään, joten jokainen kertaluvun 36 Abelin ryhmä on isomorfinen jonkin mainitun ryhmän kanssa.

Edellisessä esimerkissä ryhmä $\mathbb{Z}_{36}$, jonka kertaluku on myös 36, jätettiin kokonaan mainitsematta. Tämä johtuu siitä, että ryhmä $\mathbb{Z}_{36}$ on isomorfinen ryhmän $\mathbb{Z}_4 \oplus \mathbb{Z}_9$ kanssa. Tämä väite perustuu seuraavaksi todistettavaan lemmaan.

Lemma 3.11. *Ryhmät $\mathbb{Z}_m \oplus \mathbb{Z}_k$ ja $\mathbb{Z}_{mk}$ ovat keskenään isomorfisia, jos ja vain jos $(m, k) = 1$.*

Todistus. Oletetaan aluksi, että $(m, k) = 1$. Koska ryhmän $\mathbb{Z}_m \oplus \mathbb{Z}_k$ kertaluku on $|\mathbb{Z}_m \oplus \mathbb{Z}_k| = mk$, niin kyseisen ryhmän syklisyyden osoittamiseksi riittää todistaa, että pätee $|(1,1)| = mk$. Alkion $(1,1) \in \mathbb{Z}_m \oplus \mathbb{Z}_k$ kertaluku $|(1,1)| = t$ on pienin mahdollinen luku $t \in \mathbb{N}$, jolle pätee $(0,0) = t(1,1) = (t,t)$. Näin ollen $t \equiv 0 \pmod{m}$ ja $t \equiv 0 \pmod{k}$, jolloin $m|t$ ja $k|t$. Mutta koska on $(m, k) = 1$, niin pätee $mk|t$, jolloin edelleen $mk \leq t$. Näin ollen, koska $mk(1,1) = (mk, mk) = (0,0)$ ja t on pienin mahdollinen luonnollinen luku, jolle tämä pätee, täytyy olla $mk = t = |(1,1)|$. Alkion $(1,1)$ virittämä aliryhmä on syklisen ryhmän $\mathbb{Z}_m \oplus \mathbb{Z}_k$ aliryhmä ja koska $|\mathbb{Z}_m \oplus \mathbb{Z}_k| = mk$, niin $\mathbb{Z}_m \oplus \mathbb{Z}_k$ on alkion $(1,1)$ virittämä aliryhmä ja näin isomorfinen ryhmän $\mathbb{Z}_{mk}$ kanssa.

Todistetaan seuraavaksi implikaatio vasemmalta oikealle. Tehdään vastaoletus, että $(m, k) = d \neq 1$. Tällöin lukujen m ja k pienimmälle yhteiselle jaettavalle $t = mk/d$

pätee $t < mk$. Olkoon $(a, b) \in \mathbb{Z}_m \oplus \mathbb{Z}_k$. Tällöin saadaan $t(a, b) = (0, 0)$, mutta koska $t < mk = |\mathbb{Z}_m \oplus \mathbb{Z}_k|$, niin mikään ryhmän $\mathbb{Z}_m \oplus \mathbb{Z}_k$ alkioista ei voi virittää koko ryhmää. Päädytään siis ristiriitaan, sillä kyseinen ryhmä ei voi olla syklinen eikä siten isomorfinen syklisen ryhmän $\mathbb{Z}_{mk}$ kanssa. Täytyy siis olla $(m, k) = 1$. □

Havainnollistetaan vielä esimerkin avulla, että edellisen lemman tulos ei päde, jos $(m, k) \neq 1$.

Esimerkki 3.12. Tarkastellaan ryhmää $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, jolloin suurin yhteinen tekijä on $(m, k) = (2, 2) \neq 1$. Kyseinen ryhmä ei kuitenkaan ole alkion $(1, 1)$ virittämä, sillä $\langle(1, 1)\rangle = \{(0, 0), (1, 1)\}$. Tällöin se ei myöskään ole isomorfinen syklisen ryhmän $\mathbb{Z}_4$ kanssa.

Lause 3.13. *Olkoon luku $r = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, missä $p_1, \ldots, p_t$ ovat alkulukuja, $p_i \neq p_j$ kaikille $i \neq j$ ja $n_1, \ldots, n_t \in \mathbb{N}$. Tällöin*

$$\mathbb{Z}_r \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}.$$

Todistus. Väite on tosi, kun $r = 2$. Tehdään induktio-oletus, että väite on tosi kaikille ryhmille $\mathbb{Z}_r$, joiden kertaluku $|\mathbb{Z}_r| < n$. Olkoon nyt $m = p_1^{n_1}$ ja $k = p_2^{n_2} \cdots p_t^{n_t}$, jolloin $(m, k) = 1$. Siispä, koska induktio-oletuksen mukaan $\mathbb{Z}_k \cong \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$ ja $r = mk$, niin Lemman 3.11 nojalla

$$\mathbb{Z}_r \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_k \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}.$$

□

Aikaisemmin osoitimme, että jokainen äärellinen Abelin ryhmä voidaan esittää sellaisten syklisten ryhmien suorana summana, joiden kertaluvut ovat alkulukujen potensseja. Yhdistämällä Lauseet 3.9 ja 3.13 saadaan vaihtoehtoinen tapa esittää äärelliset Abelin ryhmät syklisten ryhmien suorana summana. Ennen kuin muotoillaan kyseinen esitystapa lauseeksi, tarkastellaan havainnollistavaa esimerkkiä.

Esimerkki 3.14. Tarkastellaan ryhmää

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}.$$

Järjestetään nyt syklisten ryhmien kertaluvut alkutekijöidensä mukaan pienimmästä suurimpaan siten, että jokainen alkutekijä saa oman rivinsä:

$$\begin{array}{cccc} 2 & 2 & 2^2 & 2^3 \\ & 3 & 3 & 3 \\ & & 5 & 5^2 \end{array}$$

Järjestetään sykliset ryhmät nyt uudestaan suoraksi summaksi edellisen taulukon sarakkeiden perusteella. Tämä on mahdollista, sillä voidaan määritellä isomorfinen kuvaus $f : K \oplus H \to H \oplus K$, $f(k + h) = h + k$, jolloin induktiivisesti saadaan järjestettyä myös äärellinen määrä ryhmiä halutulla tavalla. Nyt siis pätee

$$G \cong \mathbb{Z}_2 \oplus \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_3}_{\mathbb{Z}_6} \oplus \underbrace{\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5}_{\mathbb{Z}_{60}} \oplus \underbrace{\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}}_{\mathbb{Z}_{600}}.$$

Edelleen, Lauseen 3.13 nojalla päädytään siis lopputulokseen:

$$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{600}.$$

Seuraavan lauseen todistus perustuu Esimerkissä 3.14 esiteltyyn tekniikkaan. Esimerkki yleistyy siis tapaukseen, missä äärellinen Abelin ryhmä G voidaan esittää syklisten ryhmien $M_1, M_2, \ldots, M_t$ suorana summana siten, että syklisten ryhmien kertaluvuille pätee seuraavassa lauseessa muotoiltu jaollisuus. Näitä syklisiä ryhmiä on tällöin itse asiassa lukumäärällisesti vähemmän kuin syklisiä ryhmiä $K_1, K_2, \ldots, K_l$ Lauseessa 3.9.

Lause 3.15. *Olkoon G äärellinen Abelin ryhmä. Tällöin pätee*

$$G \cong M_1 \oplus M_2 \oplus \ldots \oplus M_t,$$

joillain syklisillä ryhmillä M_j, joiden kertaluvuille $|M_j| = m_j$ on $m_{j-1}|m_j$ ja $m_j \in \mathbb{N}$ kaikilla j.

Todistuksen idea. Lauseen 3.9 nojalla äärellinen Abelin ryhmä voidaan esitää sellaisten syklisten ryhmien $K_1, \ldots, K_l$ suorana summana, joiden kertaluvut ovat muotoa $|K_i| = {p_i}^{r_i}$, missä p_i on alkuluku kaikilla $i = 1, 2, \ldots, l$, eli $G \cong K_1 \oplus K_2 \oplus \cdots \oplus K_l$. Järjestetään nyt näiden syklisten ryhmien kertaluvut alkutekijöidensä mukaan pienimmästä suurimpaan siten, että jokainen alkutekijä saa oman rivinsä. Tällöin esimerkiksi kaikkien sellaisten syklisten ryhmien kertaluvut, joiden alkutekijä on p_1, järjestetään ensin riviin oikealta vasemmalle suurimmasta potenssista aloittaen seuraavasti:

$${p_1}^{r_{1_1}} \quad {p_1}^{r_{1_2}} \quad {p_1}^{r_{1_3}} \quad \cdots \quad {p_1}^{r_{1_t}},$$

missä siis ${p_1}^{r_{1_1}} \leq {p_1}^{r_{1_2}} \leq \ldots \leq {p_1}^{r_{1_t}}$. Kun kaikki syklisten ryhmien kertalukujen alkutekijät on löydetty, järjestetään saadut rivit alkutekijänsä mukaan suuruusjärjestykseen ylhäältä alas pienimmästä alkuluvusta aloittaen. Tällöin saadaan siis seuraava taulukko

$$\begin{array}{ccccc} {p_1}^{r_{1_1}} & {p_1}^{r_{1_2}} & {p_1}^{r_{1_3}} & \cdots & {p_1}^{r_{1_t}} \\ {p_2}^{r_{2_1}} & {p_2}^{r_{2_2}} & {p_2}^{r_{2_3}} & \cdots & {p_2}^{r_{2_t}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ {p_k}^{r_{k_1}} & {p_k}^{r_{k_2}} & {p_k}^{r_{k_3}} & \cdots & {p_k}^{r_{k_t}} \end{array}$$

missä $p_1 < p_2 < \ldots < p_k$. Kun ei ole enää mahdollista löytää syklistä ryhmää K_i, jonka kertaluku voidaan esittää tietyn alkutekijän potenssina, täydennetään merkinnällisistä syistä loput rivin soluista tällöin ykkösiksi. Tämä voidaan tehdä, sillä ryhmälle G pätee $G \cong G \oplus \mathbb{Z}_1$.

Järjestämällä sykliset ryhmät K_i uudestaan suoraksi summaksi taulukon sarakkeiden perusteella vasemmalta oikealle ja kokoamalla ne sarakkeittain yhteen saadaan Lauseen 3.13 nojalla esitys

$$G \cong K_1 \oplus K_2 \oplus \cdots \oplus K_l \cong M_1 \oplus M_2 \oplus \cdots \oplus M_t.$$

Lisäksi, koska kertalukutaulukko täytettiin oikealta vasemmalle, tiedetään, että vasemmalta oikealle siirryttäessä seuraava sarake tulee sisältämään vähintään yhden saman alkutekijän kuin aikaisempi sarake. Toisin sanoen, koska pätee

$$|M_{j-1}| = \prod_{i=1}^{k} {p_i}^{r_{i_{j-1}}} \quad \text{ja} \quad \prod_{i=1}^{k} {p_i}^{r_{i_j}} = |M_j|$$

sekä $r_{i_{j-1}} \leq r_{i_j}$, niin kertaluvulla $|M_j| = m_j$ on aina vähintään yksi sama alkutekijä kuin kertaluvulla $|M_{j-1}| = m_{j-1}$ ja tällöin pätee $m_{j-1}|m_j$ kaikilla $j = 1, 2, \ldots, t$.

4. Esitietoja Sylowin lauseiden todistamiseksi

Sylowin lauseista puhuttaessa siirrytään käyttämään ryhmistä multiplikatiivista esitystapaa. Kappaleessa 2 esitiedot on kirjoitettu ryhmien additiivisuutta hyödyntämällä, mutta ne pätevät kuitenkin myös vaihdettaessa multiplikatiiviseen merkintätapaan. Alle on listattu nämä esitiedot multiplikatiivisin merkinnöin ilman todistuksia. Todistukset seuraavat analogisesti additiivisista vastaavista. Muistutuksena lukijalle, merkinnällä e tarkoitetaan multiplikatiivisen ryhmän neutraalialkiota ja merkinnällä x^{-1} käänteisalkiota.

Lemma 4.1. *Olkoon G ryhmä ja alkio $a \in G$.*

(1) *Jos alkion a kertaluku $|a| = h < \infty$, niin $a^k = e$, jos ja vain jos $h|k$.*
(2) *Jos alkion a kertaluku $|a| = td < \infty$, missä $d \geq 1$, niin $|a^t| = d$.*

Määritelmä 4.2. Olkoot $G_1, G_2, \ldots, G_k$ ryhmiä. Määritellään laskutoimitus joukossa

$$G_1 \otimes G_2 \otimes \cdots \otimes G_k = \{(a_1, \ldots, a_k) : a_i \in G_i \text{ kaikilla } i \in \mathbb{N}\}$$

seuraavasti:

$$(a_1, a_2, \ldots, a_k)(b_1, b_2, \ldots, b_k) = (a_1 b_1, a_2 b_2, \ldots, a_k b_k)$$

missä $a_i, b_i \in G_i$ kaikilla $i = 1, \ldots, k$.

Lemma 4.3. *Olkoot M ja N ryhmän G normaaleja aliryhmiä siten, että $M \cap N = \langle e \rangle$. Jos $m \in M$ ja $n \in N$, niin $mn = nm$.*

Lemma 4.4. *Olkoot $N_1, \ldots, N_k$ ryhmän G normaaleja aliryhmiä siten, että jokainen ryhmän G alkio a voidaan kirjoittaa yksikäsitteisesti muodossa*

$$a_1 a_2 \cdots a_k,$$

missä $a_i \in N_i$ kullakin $i = 1, 2, \ldots, k$. Tällöin

$$G \cong N_1 \otimes N_2 \otimes \cdots \otimes N_k.$$

Lemma 4.5. *Olkoon M ja N ryhmän G normaaleja aliryhmiä. Jos $G = MN$ ja $M \cap N = \langle e \rangle$, niin*

$$G \cong M \otimes N.$$

Sylowin lauseiden todistukset riippuvat vahvasti konjugoinnin käsitteestä. Ennen sen tarkasteluun ottamista muotoillaan vielä eräs tarpeellinen lemma.

Lemma 4.6. *Olkoon N ryhmän G normaali aliryhmä ja T tekijäryhmän G/N aliryhmä. Tällöin on olemassa ryhmän G aliryhmä H siten, että pätee $N \subset H$ ja $T = H/N$.*

Todistus. Olkoon $H = \{a \in G : Na \in T\}$. Osoitetaan ensin, että H on ryhmän G aliryhmä. Joukko H sisältää ainakin neutraalialkion e, sillä pätee $Ne = N \in T$. Siispä on $H \neq \emptyset$. Alkioille $a, b \in H$ pätee $N(ab) = (Na)(Nb) \in T$, koska T on ryhmä, ja siten on alkio $ab \in H$. Tekijäryhmän perusominaisuuksista saadaan, että pätee $Na^{-1} = (Na)^{-1} \in T$. Tästä seuraa, että alkio $a^{-1} \in H$. Siispä H on ryhmän G aliryhmä. Lisäksi, jos $a \in N$, niin saadaan $Na = N \in T$. Siispä pätee $N \subset H$. Osoitetaan vielä, että pätee $T = H/N$. Olkoon nyt $A \in T$. Koska T on tekijäryhmän G/N aliryhmä, niin voidaan kirjoittaa $A = Na$ jollekin $a \in G$. Koska $H/N = \{Na : a \in H\}$, niin toisen inkluution todistamiseksi riittää osoittaa, että pätee $a \in H$.

Ryhmän H määrittelystä saadaan, että koska $Na = A \in T$, niin $a \in H$. Tällöin siis $T \subset H/N$. Olkoon nyt $Na \in H/N$, missä siis $a \in H$. Ryhmän H määrittelyn nojalla pätee $Na \in T$. Siispä $H/N \subset T$. □

Määritelmä 4.7. Olkoon G ryhmä ja alkiot $a, b \in G$. Alkio a on alkion b *konjugaatti*, jos on olemassa alkio $x \in G$ siten, että $b = x^{-1}ax$.

Lause 4.8. *Konjugointi on ekvivalenssirelaatio joukossa G.*

Todistus. Olkoon alkiot $a, b, c \in G$.

(1) Refleksiivisyys: Alkio a on itsensä konjugaatti, sillä $a = eae = e^{-1}ae$
(2) Symmetrisyys: Jos alkio a on alkion b konjugaatti, niin pätee $b = x^{-1}ax$ jollekin $x \in G$. Yhtälöä vasemmalta ja oikealta kertomalla saadaan
$$(x^{-1})^{-1}bx^{-1} = xbx^{-1} = xx^{-1}axx^{-1} = a,$$
jolloin siis myös alkio b on alkion a konjugaatti.
(3) Transitiivisuus: Jos alkio a on alkion b konjugaatti ja alkio b alkion c konjugaatti, niin voidaan kirjoittaa $b = x^{-1}ax$ ja $c = y^{-1}by$ joillekin $x, y \in G$. Sijoittamalla alkion b yhtälö alkion c yhtälöön saadaan
$$c = y^{-1}(x^{-1}ax)y = (y^{-1}x^{-1})a(xy) = (xy)^{-1}a(xy).$$
Tällöin siis alkio a on alkion c konjugaatti.

Konjugointi siis toteuttaa ekvivalenssirelaation ehdot. □

Määritelmä 4.9. Olkoon $a \in G$. Joukkoa
$$\begin{aligned} T(a) &= \{b \in G : b = x^{-1}ax \text{ jollakin } x \in G\} \\ &= \{b \in G : a = xbx^{-1} \text{ jollakin } x \in G\} \\ &= \{b \in G : ax = xb \text{ jollakin } x \in G\} \subset G \end{aligned}$$
sanotaan alkion a *konjugaattiluokaksi*.

Konjugaattiluokat ovat aina joko erilliset tai samat ja ryhmä voidaan esittää sen erillisten konjugaattiluokkien yhdisteenä. Havainnollistetaan tätä seuraavalla esimerkillä.

Esimerkki 4.10. Tarkastellaan kolmion symmetriaryhmästä S_3 alkion (12) konjugaattiluokkaa. Alkion (12) konjugaattiluokka koostuu määritelmän mukaan kaikista alkioista $x^{-1}(12)x$, missä $x \in S_3$. Tällöin esimerkiksi alkiot
$$(23)^{-1}(12)(23) = (13) \quad \text{ja} \quad (132)^{-1}(12)(132) = (123)(12)(132) = (23)$$
kuuluvat alkion (12) konjugaattiluokkaan. Käymällä läpi kaikki alkiot $x \in S_3$, saadaan alkion (12) konjugaattiluokaksi osoitettua joukko $\{(12), (13), (23)\}$. Samankaltaisilla laskutoimituksilla voidaan osoittaa, että ryhmällä S_3 on olemassa kolme erillistä konjugaattiluokkaa; $\{(1)\}, \{(12), (13), (23)\}$ ja $\{(123), (132)\}$. Lisäksi nähdään, että kolmion symmetriaryhmä voidaan kirjoittaa sen erillisten konjugaattiluokkien yhdisteenä $S_3 = \{(1)\} \cup \{(12), (13), (23)\} \cup \{(123), (132)\}$.

Edellisestä esimerkistä voidaan havaita, että erillisten konjugaattiluokkien koko vaihtelee eli ne sisältävät eri määrän alkioita. Huomattavaa kuitenkin on, että jokaisen erillisen konjugaattiluokan alkioiden lukumäärä jakaa ryhmän S_3 kertaluvun

$|S_3| = 3! = 6$. Tämä pätee myös yleisesti ja se osoitetaan myöhemmin Lauseessa 4.13. Jotta on mahdollista osoittaa edellä mainittu jaollisuus ja todeta jotakin konjugaattiluokan koosta eli konjugaattiluokan alkioiden lukumäärästä, tarvitaan avuksi keskittäjää.

Määritelmä 4.11. Olkoon G ryhmä. Alkion $a \in G$ *keskittäjä* on joukko

$$C(a) = \{g \in G : ga = ag\}.$$

Lause 4.12. *Olkoon G ryhmä. Tällöin alkion $a \in G$ keskittäjä $C(a)$ on ryhmän G aliryhmä.*

Todistus. Keskittäjä $C(a)$ sisältää vähintään neutraalialkion e, sillä $ea = ae$, joten $C(a) \neq \emptyset$. Tarkistetaan, että alkion $g \in C(a)$ käänteisalkio kuuluu myös joukkoon $C(a)$. Koska $g \in C(a)$, niin pätee $ga = ag$. Kertomalla yhtälöä sekä vasemmalta, että oikealta alkiolla g^{-1} saadaan $g^{-1}gag^{-1} = g^{-1}agg^{-1}$ ja edelleen $ag^{-1} = g^{-1}a$. Siispä $g^{-1} \in C(a)$. Tarkistetaan vielä, että laskutoimitus on suljettu operaatio. Olkoon $g, h \in C(a)$ eli pätee $ga = ag$ ja $ha = ah$. Tällöin voidaan kirjoittaa

$$(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh).$$

Tästä seuraa, että $gh \in C(a)$. Keskittäjä $C(a)$ on siis aliryhmä. □

Lause 4.13. *Olkoon G äärellinen ryhmä ja $a \in G$. Alkion a konjugaattiluokan $T(a)$ alkioiden lukumäärä $\#T(a)$ on aliryhmän $C(a) \subset G$ indeksi $[G : C(a)]$ eli keskittäjän $C(a)$ oikeiden sivuluokkien lukumäärä. Lisäksi luku $\#T(a)$ jakaa kertaluvun $|G|$.*

Todistus. Käytetään tässä todistuksessa keskittäjästä $C(a)$ merkintää C ja konjugaattiluokasta $T(a)$ merkintää T. Olkoon S ryhmän G aliryhmän C erillisten oikeiden sivuluokkien joukko ja T alkion $a \in G$ konjugaattiluokka. Määritellään kuvaus $f : S \to T$, $f(Cx) = x^{-1}ax$. Jos saadaan osoitettua, että kuvaus f on hyvin määritelty bijektio, niin tiedetään, että joukoissa S ja T on sama määrä alkioita. Toisaalta joukon S alkioiden lukumäärä on keskittäjän C oikeiden sivuluokkien lukumäärä eli $[G : C]$ ja joukon T alkioiden lukumäärä on alkion a eri konjugaattien lukumäärä. Tämä todistaa lauseen ensimmäisen osan. Lisäksi luku $\#T = [G : C]$ jakaa kertaluvun $|G|$ Lagrangen lauseen nojalla.

(1) Osoitetaan ensin, että kuvaus f on hyvin määritelty eli, että jokaiseen lähtöjoukon alkioon on liitetty täsmälleen yksi kuvajoukon alkio. Koska konjugoinnille pätee symmetrisyys, niin $f(Cx) \in T$ kun $x \in G$. Olkoon nyt $x, y \in G$ siten, että $Cx = Cy$. Tällöin pätee $Cxy^{-1} = C$. Tästä seuraa, että $xy^{-1} \in C$, sillä C on ryhmä. Koska siis pätee $xy^{-1} \in C$, niin keskittäjän määritelmästä saadaan yhtäsuuruus $(xy^{-1})a = a(xy^{-1})$. Kerrotaan saatua yhtälöä vasemmalta seuraavasti:

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

Nyt siis $a = (xy^{-1})^{-1}a(xy^{-1}) = yx^{-1}axy^{-1}$. Kerrotaan saatua yhtälöä vasemmalta alkiolla y^{-1} ja oikealta alkiolla y, jolloin saadaan:

$$y^{-1}ay = y^{-1}yx^{-1}axy^{-1}y = x^{-1}ax.$$

Nyt kuvauksen f määritelmästä seuraa $f(Cy) = f(Cx)$ eli kuvaus f on hyvin määritelty.

(2) Kun edetään kohdan (1) todistus vastakkaiseen suuntaan, saadaan osoitettua kuvauksen f injektiivisyys. Olkoon $f(Cx) = f(Cy)$. Tällöin kuvauksen f määrittelystä saadaan $y^{-1}ay = x^{-1}ax$. Kertomalla yhtälöä vasemmalta alkiolla y ja oikealta alkiolla y^{-1} saadaan, että

$$a = yx^{-1}axy^{-1} = (y^{-1})^{-1}x^{-1}axy^{-1} = (xy^{-1})^{-1}a(xy^{-1}).$$

Kerrotaan saatua yhtälöä vasemmalta alkiolla xy^{-1}, jolloin saadaan

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

Ryhmän C määrittelyn nojalla siis $xy^{-1} \in C$. Oikealta kertominen tuottaa $x \in Cy$, jolloin alkiolle x pätee $x = cy$ jollakin $c \in C$. Kertomalla saadun yhtälön molempia puolia vasemmalta ryhmällä C saadaan

$$Cx = C(cy) = (Cc)y. \tag{4.1}$$

Osoitetaan nyt, että yhtäsuuruus $Cc = C$ pätee kaikilla $c \in C$. Olkoon ensin $g \in Cc$. Tällöin alkiolle g pätee $g = hc$ jollakin $h \in C$. Koska C on ryhmä, laskutoimitus on suljettu operaatio eli $g = hc \in C$ ja $Cc \subset C$. Toisen suunnan osoittamiseksi olkoon nyt $g \in C$. Voidaan kirjoittaa $g = gc^{-1}c = (gc^{-1})c$, missä $gc^{-1} \in C$. Tällöin pätee $gc^{-1}c \in Cc$ eli $C \subset Cc$. Siispä saatiin osoitettua yhtäsuuruus $Cc = C$. Edellisen yhtäsuuruuden ja yhtälön (4.1) nojalla saadaan osoitettua, että pätee $Cx = Cy$. Tästä seuraa, että kuvaus f on injektio.

(3) Olkoon alkio $b \in T$ jokin alkion a konjugaatti, jolloin on olemassa $x \in G$ siten, että $b = x^{-1}ax$. Tämä on oikean sivuluokan Cx kuva eli kuvaus f on surjektio.

Kohdat (1), (2) ja (3) yhdistämällä nähdään, että kuvaus f on hyvin määritelty bijektio joukolta S joukolle T ja väite on todistettu. □

Luokkayhtälöistä

Olkoon G äärellinen ryhmä ja $T_1, T_2, \ldots, T_t$ ryhmän G konjugaattiluokat, joille on $T_i \cap T_j = \emptyset$ kaikilla $i \neq j$. Kuten aiemmin todettiin, tällöin pätee

$$G = T_1 \cup T_2 \cup \cdots \cup T_t.$$

Koska konjugaattiluokat ovat erillisiä eli ne eivät sisällä samoja alkioita, on mahdollista kirjoittaa ryhmän G kertaluku sen konjugaattiluokkien kertalukujen avulla seuraavasti:

$$|G| = |T_1 \cup T_2 \cup \cdots \cup T_t| = |T_1| + |T_2| + \cdots + |T_t|, \tag{4.2}$$

missä $|T_i|$ on konjugaattiluokan T_i alkioiden lukumäärä. Tätä esitystä on mahdollista jalostaa edelleen, kun valitaan jokaisesta konjugaattiluokasta T_i jokin alkio a_i. Tällöin luokka T_i sisältää kaikki alkion a_i konjugaatit ja Lauseen 4.13 nojalla saadaan

$$|G| = [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_t)]. \tag{4.3}$$

Molempia ryhmän G kertaluvulle $|G|$ saatuja esityksiä kutsutaan luokkayhtälöiksi ja ne ovat tarpeellisia Sylowin lauseiden todistuksissa.

Esimerkki 4.14. Esimerkissä 4.10 löydettiin kolmion symmetriaryhmälle S_3 kolme erillistä konjugaattiluokkaa

$$T_1 = \{(1)\}, \quad T_2 = \{(12), (13), (23)\}, \quad T_3 = \{(123), (132)\},$$

joiden alkioiden lukumäärät ovat $1, 3$ ja 2. Tällöin ryhmän S_3 kertaluku luokkayhtälön (4.2) avulla esitettynä on

$$|S_3| = 1 + 3 + 2 = 6.$$

Valitaan jokaisesta konjugaattiluokasta seuraavat edustajat: $(1) \in T_1$, $(12) \in T_2$ ja $(123) \in T_3$. Tarkastellaan ensin edustajaa (123). Keskittäjä $C((123))$ koostuu niistä alkioista $x \in S_3$, joille pätee $x(123) = (123)x$. Siispä alkion (123) keskittäjäksi saadaan

$$C((123)) = \{(1), (123), (132)\}.$$

Kyseisen keskittäjän oikeat sivuluokat saadaan ratkaisemalla ne joukot, jotka ovat muotoa $C((123))x = \{(1)x, (123)x, (132)x\}$, missä $x \in S_3$. Jos alkio x itse kuuluu keskittäjään $C((123))$ eli $x \in C((123))$, niin tällöin oikeaksi sivuluokaksi saadaan joukko $C((123))x = C((123))$, sillä keskittäjä on ryhmänä suljettu laskutoimituksen suhteen. Täytyy vielä tarkastella erikseen tapaukset, missä alkio x on (12), (13) tai (23). Jos on $x = (12)$, niin saadaan

$$C((123))(12) = \{(1)(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\}.$$

Vastaavasti myös tapauksissa $x = (13)$ ja $x = (23)$ oikea sivuluokka muodostuu samaksi eli joukoksi $\{(12), (13), (23)\}$. Näin ollen keskittäjällä $C((123))$ on siis kaksi oikeaa sivuluokkaa:

$$\{(1), (123), (132)\} \quad \text{ja} \quad \{(12), (13), (23)\}.$$

Näin ollen indeksiksi saadaan $[S_3 : C((123))] = 2$. Voidaan tarkistaa, että näin tosiaan on, sillä Lagrangen lausetta soveltaen indeksiksi saadaan

$$[S_3 : C((123))] = \frac{|S_3|}{|C((123))|} = \frac{6}{3} = 2.$$

Lisäksi pätee $[S_3 : C((123))] = |T_3| = 2$.

Samankaltaisilla laskutoimituksilla saadaan, että keskittäjän $C((12))$ oikeita sivuluokkia on kolme ja keskittäjän $C((1))$ oikeita sivuluokkia vain yksi. Tällöin ryhmän S_3 kertaluku luokkayhtälön (4.3) avulla esitettynä on

$$|S_3| = [S_3 : C((1))] + [S_3 : C((12))] + [S_3 : C((123))] = 1 + 3 + 2 = 6.$$

Keskuksen avulla saadaan kolmas esitys luokkayhtälölle.

Määritelmä 4.15. Ryhmän G keskus on joukko

$$Z(G) = \{c \in G : cx = xc \quad \text{kaikilla} \quad x \in G\}.$$

Pidetään tunnettuna, että keskus $Z(G)$ on ryhmän G aliryhmä ja erityisesti sen normaali aliryhmä. Lisäksi keskus $Z(G)$ on Abelin ryhmä.

Lemma 4.16. *Keskus $Z(G)$ on kaikkien sellaisten ryhmän G konjugaattiluokkien yhdiste, jotka sisältävät ainoastaan yhden alkion.*

Todistus. Olkoon $c \in Z(G)$. Kun kerrotaan keskuksen määritelmän yhtälöä $cx = xc$ molemmilta puolilta vasemmalta alkiolla x^{-1} saadaan yhtäsuuruus $x^{-1}cx = c$ kaikilla $x \in G$. Tämä tarkoittaa, että alkiolla $c \in Z(G)$ ei ole muita konjugaatteja kuin se itse. Inkluusio pätee myös toiseen suuntaan. Olkoon nimittäin $c \in G$ sellainen alkio, että sen konjugaattiluokka on $T(c) = \{c\}$. Kertomalla yhtälön $x^{-1}cx = c$ molempia puolia vasemmalta alkiolla $x \in G$ päädytään keskuksen määritelmän ehtoon $cx = xc$. □

Nyt voidaan kirjoittaa luokkayhtälö muotoon

$$|G| = |Z(G)| + |T_1| + |T_2| + \cdots + |T_r|, \tag{4.4}$$

missä ryhmän G erilliset konjugaattiluokat $T_1, T_2, \ldots, T_r$ sisältävät enemmän kuin yhden alkion ja kertaluku $|T_i|$ jakaa kertaluvun $|G|$ kaikilla $i = 1, 2, \ldots, r$.

Lemma 4.17. *(Abelin ryhmien Cauchyn lause) Olkoon G äärellinen Abelin ryhmä. Jos alkuluku p jakaa ryhmän G kertaluvun $|G|$, niin on olemassa alkio $a \in G$, jonka kertaluku on $|a| = p$.*

Todistus. Todistetaan väite ryhmän G kertalukuun perustuvalla induktiotodistuksella. Osoitetaan ensin, että väite on tosi, kun kertaluku $|G| = 2$. Tällöin kertaluvun $|G| = 2$ jakava alkuluku on $p = 2$. Tiedetään, että alkion $a \in G \setminus \{e\}$ kertaluku jakaa äärellisen ryhmän G kertaluvun $|G| = 2$, joten alkion a kertaluvun täytyy olla $|a| = 2$.

Oletetaan, että väite pätee kaikille Abelin ryhmille, joiden kertaluku on aidosti pienempi kuin n. Osoitetaan nyt, että väite on tosi, kun kertaluku $|G| = n$. Olkoon alkio $a \in G \setminus \{e\}$. Alkion a kertaluku voidaan kirjoittaa muodossa $|a| = qt$, missä q on alkuluku ja $t \in \mathbb{N}$. Tällöin Lauseen 4.1 nojalla alkion $b = a^t$ kertaluku on $|b| = |a^t| = q$. Jos $q = p$, niin väite on todistettu.

Täytyy vielä todistaa tapaus, missä $q \neq p$. Olkoon $N = \langle b \rangle$ ryhmän G syklinen aliryhmä. Koska ryhmä N on alkion b virittämä, sen kertaluku on sama kuin alkion b kertaluku eli $|N| = q$. Lisäksi ryhmä N on normaali, sillä G on Abelin ryhmä. Tekijäryhmän G/N kertaluku on ryhmän N erillisten oikeiden sivuluokkien määrä eli indeksi $[G : N]$. Siispä Lagrangen lauseen nojalla indeksiksi saadaan $[G : N] = |G|/|N|$. Tekijäryhmän kertaluvulle pätee siis $|G/N| = |G|/|N| = n/q < n$. Ryhmän G kertaluku $|G|$ on jaollinen alkuluvulla p ja se voidaan kirjoittaa muodossa $|G| = |N||G/N| = q|G/N|$. Oletettiin, että on $q \neq p$, joten koska alkuluku p ei voi jakaa alkulukua q ja kertaluku $|G|$ on jaollinen alkuluvulla p, täytyy tekijäryhmän kertaluvun $|G/N|$ olla jaollinen alkuluvulla p. Induktio-oletuksen nojalla väite on tosi tekijäryhmälle G/N. Siispä on olemassa alkio $Nc \in G/N$, jonka kertaluku on $|Nc| = p$. Näin ollen, koska N on ryhmän G normaali aliryhmä, pätee $Nc^p = (Nc)^p = Ne$ ja siksi $c^p \in N$. Koska ryhmän N kertaluku $|N| = q$ on alkuluku, niin kertaluvun $|c^p|$ täytyy jakaa alkuluku q. Täytyy siis olla $|c^p| = q$ ja tällöin pätee $c^{pq} = (c^p)^q = e^q = e$.

Edellisen nojalla ja Lausetta 4.1 hyödyntämällä tiedetään, että kertaluvun $|c|$ täytyy jakaa luku pq. Tällöin ainoat vaihtoehdot alkion c kertaluvuksi ovat $1, q, p$ tai pq, joista kaksi 1 ja q voidaan rajata pois. Nimittäin, jos alkion $c = e$ kertaluku olisi $|c| = 1$, niin alkion Nc kertaluku olisi $|Nc| = |N| = 1 \neq p$. Alkion c kertaluku ei voi myöskään olla $|c| = q$, sillä tällöin voitaisiin kirjoittaa $(Nc)^q = Nc^q = Ne$ ja kertaluku $|Nc| = p$ jakaisi alkuluvun q. Ainoat mahdollisuudet alkion c kertaluvuksi ovat siis $|c| = p$ tai $|c| = pq$. Jälkimmäisen pätiessä on olemassa alkio $c^q \in G$, jolla Lauseen 4.1 nojalla on kertaluku $|c^q| = p$. Näin ollen molemmissa tapauksissa ryhmä G sisältää p-kertalukuisen alkion ja väite on induktion nojalla todistettu kaikille äärellisille Abelin ryhmille. □

Ylle on saatu kerättyä kaikki tarvittavat esitiedot Sylowin ensimmäisen lauseen todistamista varten. Toisen ja kolmannen Sylowin lauseen todistamiseen tarvittavat elementit ovat hyvin samankaltaisia aiempien esitietojen kanssa, mutta konjugoinnin käsitettä täytyy jalostaa koskemaan alkioiden sijasta aliryhmiä.

Määritelmä 4.18. Olkoon H ryhmän G aliryhmä. Olkoot lisäksi A ja B mitkä tahansa kaksi ryhmän G aliryhmää. Ryhmä A on ryhmän B *H-konjugaatti*, jos on olemassa alkio $x \in H$ siten, että $B = x^{-1}Ax = \{x^{-1}ax : a \in A\}$.

Lause 4.19. *Olkoon H ryhmän G aliryhmä. Tällöin H-konjugointi on ekvivalenssirelaatio joukossa $\{A : A \subset G$ aliryhmä$\}$.*

Todistus. Todistus seuraa suoraan Lauseen 4.8 todistusta varioimalla. Täydellisyyden vuoksi käydään kuitenkin yksityiskohdat läpi. Olkoon $A, B, C \subset G$ ryhmiä.

(1) Refleksiivisyys: Ryhmä A on itsensä H-konjugaatti, sillä $A = eAe = e^{-1}Ae$ ja $e \in H$.

(2) Symmetrisyys: Jos ryhmä A on ryhmän B H-konjugaatti, niin tällöin pätee $B = x^{-1}Ax$ jollekin $x \in H$. Yhtälöä vasemmalta ja oikealta kertomalla saadaan
$$(x^{-1})^{-1}Bx^{-1} = xBx^{-1} = xx^{-1}Axx^{-1} = A,$$
missä $x^{-1} \in H$, jolloin siis myös ryhmä B on ryhmän A H-konjugaatti.

(3) Transitiivisuus: Jos ryhmä A on ryhmän B H-konjugaatti ja ryhmä B ryhmän C H-konjugaatti, niin voidaan kirjoittaa $B = x^{-1}Ax$ ja $C = y^{-1}By$ joillekin $x, y \in H$. Sijoittamalla ryhmän B yhtälö ryhmän C yhtälöön saadaan
$$C = y^{-1}(x^{-1}Ax)y = (y^{-1}x^{-1})A(xy) = (xy)^{-1}A(xy),$$
missä $xy \in H$. Tällöin siis ryhmä A on ryhmän C H-konjugaatti.

H-konjugointi siis toteuttaa ekvivalenssirelaation ehdot. □

Määritelmä 4.20. Olkoon A ryhmän G aliryhmä. Ryhmän A *normalisoija* on joukko
$$\begin{aligned} N(A) &= \{g \in G : g^{-1}Ag = A\} \\ &= \{g \in G : Ag = gA\} \\ &= \{g \in G : A = gAg^{-1}\}. \end{aligned}$$

Lause 4.21. *Olkoon A ryhmän G aliryhmä. Tällöin normalisoija $N(A)$ on ryhmän G aliryhmä ja A on ryhmän $N(A)$ normaali aliryhmä.*

Todistus. Osoitetaan ensin, että $N(A)$ on ryhmän G aliryhmä. Koska pätee $eA = Ae$, niin normalisoija sisältää ainakin neutraalialkion eli $e \in N(A)$ ja on siten epätyhjä. Jos on $g, h \in N(A)$, niin tällöin pätee
$$(gh)A = g(hA) = g(Ah) = (gA)h = (Ag)h = A(gh).$$
Siispä $gh \in N(A)$ ja siten normalisoija on suljettu laskutoimituksen suhteen. Kertomalla yhtälön $gA = Ag$ molemmat puolet sekä vasemmalta että oikealta alkiolla g^{-1} päädytään yhtäsuuruuteen $Ag^{-1} = g^{-1}A$, jolloin siis on $g^{-1} \in N(A)$. Näin on saatu osoitettua, että $N(A)$ on ryhmän G aliryhmä.

Osoitetaan seuraavaksi, että A on ryhmän $N(A)$ normaali aliryhmä. Olkoon tätä varten $a \in A$. Tällöin voidaan kirjoittaa $a^{-1}Aa = A$. Tämä vastaa normalisoijan määritelmän ehtoa, jolloin siis saadaan $A \subset N(A)$. Lisäksi normalisoijan määritelmästä seuraa, että $Ag = gA$ kaikilla $g \in N(A)$, joten A on ryhmän $N(A)$ normaali aliryhmä. □

Muotoillaan seuraavaksi lause, joka merkintöjä muuttamalla voidaan rinnastaa Lauseeseen 4.13. Korvataan Lauseessa 4.13 ja sen todistuksessa ryhmä G ryhmällä H, alkio a ryhmällä A ja keskittäjä C ryhmällä $H \cap N(A)$. Näin seuraava lause antaa hyödyllistä tietoa H-konjugaattiluokkien alkioiden lukumäärästä ja niihin liittyvästä jaollisuusominaisuudesta.

Lause 4.22. *Olkoot H ja A äärellisen ryhmän G aliryhmiä. Ryhmän A H-konjugaattien lukumäärä on indeksi $[H : H \cap N(A)]$, joka jakaa kertaluvun $|H|$.*

Todistus. Merkintöjä muuttamalla todistus noudattaa suoraan Lauseen 4.13 todistusta. Käytetään ryhmän A H-konjugaattiluokkien joukosta merkintää $T_H(A)$ ja sen alkioiden lukumäärästä merkintää $\#T_H(A)$. Olkoon $S_H(A)$ ryhmän H aliryhmän $H \cap N(A)$ oikeiden sivuluokkien joukko ryhmässä H. Määritellään kuvaus

$$f : S_H(A) \to T_H(A), \quad f((H \cap N(A))x) = x^{-1}Ax.$$

Jos saadaan osoitettua, että kuvaus f on hyvin määritelty bijektio, niin tiedetään, että joukoissa $S_H(A)$ ja $T_H(A)$ on sama määrä alkioita. Toisaalta joukon $S_H(A)$ alkioiden lukumäärä on indeksi $[H : H \cap N(A)]$ ja joukon $T_H(A)$ alkioiden lukumäärä on ryhmän A H-konjugaattien lukumäärä. Näin saadaan osoitettua lauseen ensimmäinen osa. Lisäksi, Lagrangen lauseen nojalla luku $\#T_H(A) = [H : H \cap N(A)]$ jakaa kertaluvun $|H|$. Korvaamalla Lauseen 4.13 todistuksen kohdista (1), (2) ja (3) ryhmä G ryhmällä H, alkio a ryhmällä A ja keskittäjä C ryhmällä $H \cap N(A)$, saadaan osoitettua, että kuvaus f on hyvin määritelty, injektiivinen ja surjektiivinen eli hyvin määritelty bijektio ja lause on näin todistettu.

Osoitetaan, että kuvaus f on hyvin määritelty. Määritelmän nojalla pätee

$$f((H \cap N(A))x) = x^{-1}Ax \in T_H(A),$$

kun $x \in H$. Olkoon nyt $x, y \in H$ siten, että $(H \cap N(A))x = (H \cap N(A))y$. Tällöin pätee

$$(H \cap N(A))xy^{-1} = H \cap N(A).$$

Tästä seuraa, että $xy^{-1} \in H \cap N(A)$, sillä $H \cap N(A)$ on ryhmä. Koska siis pätee $xy^{-1} \in H \cap N(A)$, niin normalisoijan määritelmästä saadaan yhtäsuuruus

$$(xy^{-1})A = A(xy^{-1}).$$

Kerrotaan saatu yhtälö vasemmalta seuraavasti:

$$(xy^{-1})^{-1}(xy^{-1})A = (xy^{-1})^{-1}A(xy^{-1}).$$

Nyt siis $A = (xy^{-1})^{-1}A(xy^{-1}) = yx^{-1}Axy^{-1}$. Kerrotaan saatu yhtälö vasemmalta alkiolla y^{-1} ja oikealta alkiolla y, jolloin saadaan:

$$y^{-1}Ay = y^{-1}yx^{-1}Axy^{-1}y = x^{-1}Ax.$$

Nyt kuvauksen f määritelmästä seuraa

$$f((H \cap N(A))y) = f((H \cap N(A))x)$$

eli kuvaus f on hyvin määritelty.

Käydään esimerkin vuoksi vielä surjektiivisuuden kohdalla yksityiskohdat läpi. Olkoon alkio $B \in T_H(A)$ jokin ryhmän A H-konjugaatti, jolloin on olemassa $x \in H$ siten, että $B = x^{-1}Ax$. Tämä on oikean sivuluokan $(H \cap N(A))x$ kuva eli kuvaus f on surjektio. □

Määritelmä 4.23. Olkoon G äärellinen ryhmä ja p alkuluku. Jos ryhmän G aliryhmällä K on kertaluku $|K| = p^n$ ja luku p^n on suurin alkuluvun p potenssi, joka jakaa kertaluvun $|G|$, niin ryhmää K sanotaan *Sylowin p-ryhmäksi.*

Esimerkki 4.24. Tarkastellaan symmetristä ryhmää S_4. Ryhmän S_4 kertaluku on $|S_4| = 4! = 24 = 2^3 \times 3$. Huomataan, että $2^3 = 8$ on suurin alkuluvun 2 potenssi, joka jakaa kertaluvun $|S_4|$. Tällöin kaikki ryhmän S_4 aliryhmät, joiden kertaluku on 8, ovat Sylowin 2-ryhmiä. Ryhmä

$$\{(1), (13), (24), (1234), (1432), (13)(24), (12)(34), (14)(32)\}$$

on esimerkki tällaisesta 8-kertalukuisesta aliryhmästä. Vastaavasti, kaikki ryhmän S_4 aliryhmät, joiden kertaluku on 3, ovat Sylowin 3-ryhmiä.

Lemma 4.25. *Olkoon K äärellisen ryhmän G Sylowin p-aliryhmä. Jos alkion $x \in G$ kertaluku on muotoa $|x| = p^r$, missä $r \in \mathbb{N}$, ja pätee $x^{-1}Kx = K$, niin $x \in K$.*

Todistus. Koska Lauseen 4.21 nojalla K on ryhmän $N(K)$ normaali aliryhmä, on mahdollista määritellä tekijäryhmä $N(K)/K$. Oletuksen nojalla alkiolle $x \in G$ pätee $x^{-1}Kx = K$, joten $x \in N(K)$. Lisäksi, koska alkion x kertaluku on muotoa $|x| = p^r$, niin myös sivuluokan $Kx \in N(K)/K$ kertaluku on muotoa $|Kx| = p^m$. Tämä saadaan osoitettua Lemman 4.1 avulla, sillä sen nojalla yhtäsuuruusketjusta

$$(Kx)^{p^r} = Kx^{p^r} = Ke$$

seuraa, että kertaluku $|x| = p^r$ on jaollinen kertaluvulla $|Kx|$. Siispä alkio Kx virittää ryhmän $N(K)/K$ syklisen aliryhmän $T = \langle Kx \rangle$, jonka kertaluku on myös muotoa $|T| = p^m$. Lemman 4.6 nojalla pätee $T = H/K$, missä H on ryhmän $N(K)$ aliryhmä ja siten myös ryhmän G aliryhmä ja $K \subset H$. Koska K on Sylowin p-ryhmä, sen kertaluku on muotoa $|K| = p^n$.

Nyt siis sekä ryhmän K että ryhmän T kertaluvut ovat alkuluvun p potensseja, ja koska Lagrangen lauseen nojalla on

$$|H| = |K||T| = p^n p^m = p^{n+m},$$

nähdään myös kertaluvun $|H|$ olevan alkuluvun p potenssi. Mutta nyt, koska K on ryhmän G Sylowin p-aliryhmä, määritelmän 4.23 nojalla kertaluku $|K| = p^n$ on suurin alkuluvun p potenssi, joka jakaa kertaluvun $|G|$. Samanaikaisesti tiedetään, että pätee $K \subset H$, joten täytyy olla $K = H$ ja tällöin aliryhmälle T pätee

$$T = H/K = K/K = \{Ke\}.$$

Siispä ryhmän T virittämän alkion Kx täytyy itseasiassa olla sivuluokka Ke ja tästä yhtäsuuruudesta $Kx = Ke$ seuraa, että pätee $x \in K$. □

5. Sylowin lauseet

Kappaleessa 3 luokiteltiin kaikki äärelliset Abelin ryhmät. Sellaisten äärellisten ryhmien luokittelu, jotka eivät ole Abelin ryhmiä, on huomattavasti vaikeampaa. Jotta myös näiden ei-Abelisten ryhmien luokittelu olisi mahdollista, tarvitaan avuksi Sylowin lauseita. Huomattavaa on, että Sylowin lauseiden todistukset eivät juurikaan kerro tavasta, jolla itse Sylowin lauseita käytetään ryhmien analysointiin. Tässä kappaleessa siis lukijan on syytä kiinnittää erityistä huomiota itse Sylowin lauseisiin ja ymmärtää niiden käyttötarkoitus.

Lause 5.1. *(Sylowin ensimmäinen lause). Olkoon G äärellinen ryhmä ja p alkuluku. Jos luku p^k jakaa kertaluvun $|G|$ jollakin $k \in \mathbb{N}$, niin on olemassa ryhmän G aliryhmä H, jonka kertaluku on $|H| = p^k$.*

Todistus. Todistetaan väite tekemällä induktio ryhmän G kertaluvun suhteen. Väite on tosi, jos kertaluku $|G| = 1$, sillä tällöin ainut alkuluvun p potenssi, joka jakaa kertaluvun $|G|$ on p^0. Lisäksi aliryhmä, jonka kertaluku on p^0, on ryhmä G itse. Olkoon nyt kertaluku $|G| > 1$. Oletetaan, että väite on tosi kaikille ryhmille, joiden kertaluku on aidosti pienempi kuin ryhmän G kertaluku. Luokkayhtälöt 4.3 ja 4.4 yhdistämällä voidaan kirjoittaa kertaluku $|G|$ muodossa

$$\begin{aligned} |G| &= |Z(G)| + |T_1| + |T_2| + \cdots + |T_r| \\ &= |Z(G)| + [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_r)], \end{aligned}$$

missä $[G : C(a_i)] > 1$ jokaisella $i = 1, 2, \ldots, r$. Koska keskus $Z(G)$ sisältää aina neutraalialkion e, niin keskuksen kertaluvulle pätee $|Z(G)| \geq 1$. Lisäksi keskittäjän kertaluvulle pätee $|C(a_i)| < |G|$ kaikilla $i = 1, 2, \ldots, r$, sillä muuten Lagrangen lauseen nojalla olisi $[G : C(a_i)] = |G|/|C(a_i)| = 1$, jolloin keskittäjä $C(a_i)$ olisi koko ryhmä G.

Oletetaan nyt, että on olemassa $j \in \{1, 2, \ldots, r\}$ siten, että indeksi $[G : C(a_j)]$ ei ole jaollinen alkuluvulla p. Näin ollen, koska oletuksen nojalla luku p^k jakaa ryhmän G kertaluvun, joka voidaan kirjoittaa Lagrangen lauseen nojalla muodossa

$$|G| = |C(a_j)|[G : C(a_j)],$$

niin luvun p^k täytyy jakaa myös kertaluku $|C(a_j)|$. Aiemmin todettiin, että pätee $|C(a_i)| < |G|$, joten induktio-oletuksen nojalla keskittäjällä $C(a_i) \subset G$ on aliryhmä H, jonka kertaluku on $|H| = p^k$. Siispä H on myös ryhmän G aliryhmä eli on olemassa ryhmän G aliryhmä, jonka kertaluku on p^k.

Oletetaan seuraavaksi, että alkuluku p jakaa indeksin $[G : C(a_i)]$ kaikilla $i = 1, 2, \ldots, r$. Oletuksen nojalla kertaluku $|G|$ on myös jaollinen alkuluvulla p. Edelleen kirjoittamalla

$$|G| - \sum_{i=1}^{r} [G : C(a_i)] = |Z(G)|$$

nähdään, että myös kertaluku $|Z(G)|$ on jaollinen alkuluvulla p. Keskus $Z(G)$ on Abelin ryhmä, joten Lemman 4.17 nojalla on olemassa alkio $c \in Z(G)$, jonka kertaluku on $|c| = p$. Olkoon nyt N alkion c virittämä syklinen ryhmä. Tällöin ryhmän $N = \langle c \rangle$ kertaluku on $|N| = p$. Lisäksi N on keskuksen $Z(G)$ aliryhmänä ryhmän G normaali aliryhmä, sillä $c^t x = x c^t$ kaikilla $x \in G$ ja kaikilla $t \in \{1, 2, \ldots p\}$. Tekijäryhmä on

ryhmästä G ja sen normaalista aliryhmästä N konstruoitu uusi ryhmä, joten edellisen seurauksena saadaan tekijäryhmä G/N, jonka kertaluvulle pätee

$$|G/N| = |G|/|N| = |G|/p < |G|$$

ja se on jaollinen luvulla p^{k-1}. Induktio-oletuksen nojalla ryhmällä G/N on aliryhmä T, jonka kertaluku on $|T| = p^{k-1}$. Kokoamalla edelliset päättelyt ja käyttämällä Lausetta 4.6 havaitaan, että on olemassa ryhmän G aliryhmä H siten, että pätee $N \subseteq H$ ja $T = H/N$. Lagrangen lausetta kahdesti soveltaen saadaan tällöin

$$|H| = |N|[H : N] = |N|\frac{|H|}{|N|} = |N||H/N| = |N||T| = pp^{k-1} = p^k.$$

Siispä on olemassa ryhmän G aliryhmä H, jonka kertaluku on p^k. □

Esimerkki 5.2. Tarkastellaan ryhmää $\mathbb{Z}_{60}$. Tällöin Lauseen 3.13 nojalla, koska $60 = 2^2 \times 3 \times 5$, niin pätee $\mathbb{Z}_{60} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. Lisäksi nähdään, että ryhmän $\mathbb{Z}_{60}$ kertaluku $|\mathbb{Z}_{60}| = 60$ on jaollinen esimerkiksi alkuluvun 2 toisella potenssilla 2^2. Siispä myös kertaluku $|\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5| = 60$ on jaollinen luvulla 2^2. Sylowin ensimmäisen lauseen nojalla täytyisi siis olla olemassa ryhmän $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ aliryhmä, jonka kertaluku on 2^2. Ryhmä $\mathbb{Z}_{2^2} \oplus \{e\} \oplus \{e\}$ on tällainen aliryhmä.

Esimerkki 5.3. Symmetrisen ryhmän S_6 kertaluku on

$$|S_6| = 6! = 720 = 2^4 \times 3^2 \times 5.$$

Valitaan alkuluvuksi ensin $p = 2$. Tällöin luvut $p^1 = 2, p^2 = 4, p^3 = 8$ ja $p^4 = 16$ jakavat kertaluvun $|S_6|$, joten Sylowin ensimmäisen lauseen nojalla ryhmällä S_6 on aliryhmät, joiden kertaluvut ovat $2, 4, 8$ ja 16. Tämä ei kuitenkaan tarkoita, etteikö saman kertaluvun aliryhmiä voisi olla useampia. Esimerkiksi ryhmät

$$\{(1), (12)\}, \quad \{(1), (12)(34)\} \quad \text{ja} \quad \{(1), (12)(34)(56)\}$$

ovat ryhmän S_6 aliryhmiä, joiden kaikkien kertaluku on 2. Vastaavasti, kun alkuluku on $p = 3$, niin Sylowin ensimmäisen lauseen nojalla ryhmällä S_6 on aliryhmät, joiden kertaluvut ovat 3 ja 9. Lisäksi alkuluvun ollessa $p = 5$, ryhmällä S_6 on vähintään yksi aliryhmä, jonka kertaluku on 5.

Seuraus 5.4. *(Cauchyn lause). Olkoon G äärellinen ryhmä. Jos alkuluku p jakaa kertaluvun $|G|$, niin on olemassa alkio $a \in G$, jonka kertaluku on $|a| = p$.*

Todistus. Olkoon p alkuluku, joka jakaa äärellisen ryhmän G kertaluvun $|G|$. Tällöin Sylowin ensimmäisen lauseen 5.1 nojalla on olemassa ryhmän G aliryhmä K, jonka kertaluku on $|K| = p$. Koska alkion $a \in K \setminus \{e\}$ virittämän syklisen aliryhmän $\langle a \rangle \subset K$ kertaluku jakaa alkuluvun p ja $|\langle a \rangle| \neq 1$, niin sen kertaluvun täytyy olla $|\langle a \rangle| = p$. Koko ryhmä K on siis alkion a virittämä ja on siis olemassa alkio $a \in G$, jonka kertaluku on $|a| = p$. □

Sylowin toinen lause osoittaa, että jokainen ryhmän G Sylowin p-aliryhmä voidaan muodostaa toisen ryhmän G Sylowin p-aliryhmän avulla. Jotta päästään käsiksi tapaan, jolla Sylowin p-aliryhmä on mahdollista muodostaa toista Sylowin p-aliryhmää apuna käyttäen, täytyy ottaa tarkasteluun seuraavat lemmat. Lisäksi Sylowin toista lausetta ja näitä lemmoja hyödyntäen voidaan osoittaa, että mitkä tahansa kaksi ryhmän G Sylowin p-aliryhmää ovat keskenään isomorfisia.

Lemma 5.5. *Olkoon G ryhmä ja $x \in G$. Tällöin kuvaus $f : G \to G$, $f(a) = x^{-1}ax$ on isomorfismi.*

Todistus. Osoitetaan ensin, että kuvaus f on homomorfismi. Olkoon $a, b \in G$. Tällöin pätee

$$f(a)f(b) = (x^{-1}ax)(x^{-1}bx) = x^{-1}a(xx^{-1})bx = x^{-1}abx = f(ab).$$

Osoitetaan vielä, että kuvaus f on bijektio. Olkoon $g \in G$ maalijoukon alkio. Tällöin alkion $xgx^{-1} \in G$ kuva on

$$f(xgx^{-1}) = x^{-1}(xgx^{-1})x = (x^{-1}x)g(x^{-1}x) = ege = g.$$

Siispä kuvaus f on surjektio. Olkoon nyt $f(a) = f(b)$ joillakin $a, b \in G$. Tällöin pätee $x^{-1}ax = x^{-1}bx$. Kertomalla yhtälön molemmat puolet vasemmalta alkiolla x ja oikealta alkiolla x^{-1} saadaan $a = b$ eli kuvaus f on injektio. Näin ollen kuvaus f on homomorfismi ja bijektio eli isomorfismi. □

Lemma 5.6. *Olkoon G ryhmä, K sen aliryhmä ja $x \in G$. Tällöin $x^{-1}Kx$ on ryhmän G aliryhmä, joka on isomorfinen aliryhmän K kanssa.*

Todistus. Tiedetään, että K on ryhmän G aliryhmä ja $x \in G$. Olkoon nyt $f : G \to G$, $f(k) = x^{-1}kx$ kuvaus, joka kuvaa aliryhmän K joukoksi

$$f(K) = x^{-1}Kx = \{x^{-1}kx : k \in K\}.$$

Koska Lemman 5.5 nojalla kuvaus f on isomorfismi, niin myös $x^{-1}Kx$ on ryhmän G aliryhmä ja aliryhmät K ja $x^{-1}Kx$ ovat keskenään isomorfisia. □

Edellisessä Lemmassa todistettiin, että ryhmän G aliryhmät K ja $x^{-1}Kx$ ovat keskenään isomorfisia. Tällöin tiedetään, että kyseisten aliryhmien kertalukujen täytyy olla yhtäsuuret eli $|K| = |x^{-1}Kx|$. Nyt jos K on ryhmän G Sylowin p-aliryhmä eli kertaluku $|K| = p^n$ on suurin alkuluvun p potenssi, joka jakaa ryhmän G kertaluvun, niin myös kertaluku $|x^{-1}Kx| = p^n$ on suurin tälläinen alkuluvun p potenssi eli $x^{-1}Kx$ on Sylowin p-aliryhmä. Nyt ollaan valmiita osoittamaan, että jokainen Sylowin p-aliryhmä voidaan muodostaa edellä kuvatulla tavalla. Muotoillaan kuitenkin sitä ennen avuksi vielä yksi lemma.

Lemma 5.7. *Olkoon K ja P ryhmän G aliryhmiä. Tällöin ryhmän K kaikkien G-konjugaattien joukko $S = \{K_1, K_2, \ldots, K_t\}$ on eräiden P-konjugaattiluokkien yhdiste.*

Todistus. Merkitään $K_1 = K$. Koska ekvivalenssirelaatio muodostaa osituksen [10, s. 46], riittää todistaa, että ryhmän K_i P-konjugaattiluokka sisältää ainoastaan joukon S alkioita kullakin $i = 1, 2, \ldots, t$. Jokainen K_i on ryhmän K_1 G-konjugaatti. Koska konjugoinnille pätee transitiivisuus, jokainen ryhmän K_i G-konjugaatti on myös ryhmän K_1 G-konjugaatti. Toisin sanoen, jokainen ryhmän K_i G-konjugaatti on jokin K_j. Tällöin, koska $P \subset G$ on aliryhmä, niin myös jokainen ryhmän K_i P-konjugaatti on jokin K_j. □

Lause 5.8. *(Sylowin toinen lause). Olkoon p alkuluku. Olkoon lisäksi P ja K ryhmän G Sylowin p-aliryhmiä. Tällöin on olemassa alkio $x \in G$ siten, että $P = x^{-1}Kx$.*

Todistus. Olkoon Sylowin p-aliryhmän K kertaluku $|K| = p^n$. Tällöin ryhmän G kertaluku voidaan kirjoittaa muodossa $|G| = p^n m$ ja $p \nmid m$. Koska K on Sylowin p-aliryhmä, Lemman 4.22 nojalla sen G-konjugaattien lukumäärä on

$$t = [G : G \cap N(K)] = [G : N(K)].$$

Indeksi t ei ole jaollinen alkuluvulla p, sillä Lagrangen lauseen nojalla voidaan kirjoittaa

$$p^n m = |G| = |N(K)|[G : N(K)] = |N(K)|t,$$

missä kertaluku $|N(K)|$ on jaollinen luvulla p^n, koska K on sen aliryhmä. Täytyy osoittaa, että Sylowin p-aliryhmä P on ryhmän K G-konjugaatti eli yksi konjugaateista K_i, missä $i = 1, 2, \ldots, t$. Tehdään tämä P-konjugointia käyttäen.

Lemman 5.7 nojalla ryhmän K kaikkien G-konjugaattien joukko $S = \{K_1, K_2, \ldots, K_t\}$ on eräiden P-konjugaattiluokkien yhdiste. Jokaisessa tällaisessa P-konjugaattiluokassa aliryhmien lukumäärä on jokin alkuluvun p potenssi, sillä Lauseen 4.22 nojalla sellaisten aliryhmien lukumäärä, jotka ovat ryhmän K_i P-konjugaatteja on indeksi

$$[P : P \cap N(K_i)]$$

ja Lagrangen lauseen nojalla tämä jakaa kertaluvun $|P| = p^n$. Tällöin siis joukon S alkioiden lukumäärä t on alkuluvun p potenssien summa

$$p^{n_1} + p^{n_2} + \cdots + p^{n_r},$$

missä $n_j = 0, 1, 2, \ldots$ kaikilla j ja jokainen alkuluvun p potenssi on yhden P-konjugaattiluokan aliryhmien lukumäärä. Aiemmin todettiin, että luku t ei ole jaollinen alkuluvulla p, joten ainakin yhden alkuluvun p potenssin täytyy olla $p^0 = 1$. Tällöin siis jokin yksiö $\{K_i\}$ muodostaa ryhmän K P-konjugaattiluokan, jolloin erityisesti pätee

$$x^{-1} K_i x = K_i$$

kaikilla $x \in P$. Lisäksi jokaisella $x \in P$ on olemassa luku r siten, että kertaluvulle pätee $|x| = p^r$, sillä P on Sylowin p-aliryhmä. Lemmasta 4.25 saadaan tässä tapauksessa, että $x \in K_i$ ja $P \subset K_i$. Koska molemmat ryhmät P ja K_i ovat Sylowin p-aliryhmiä, niillä on sama kertaluku. Siispä pätee $P = K_i$. □

Sylowin toisen lauseen 5.8 ja Lemman 5.6 nojalla pystytään osoittamaan, että mitkä tahansa kaksi ryhmän G Sylowin p-aliryhmää ovat keskenään isomorfisia. Nimittäin, jos P ja K ovat ryhmän G Sylowin p-aliryhmiä, niin Sylowin toisen lauseen nojalla voidaan kirjoittaa $P = x^{-1} K x$ jollekin $x \in G$. Lemmasta 5.6 saadaan, että ryhmät $x^{-1} K x$ ja K ovat keskenään isomorfisia.

Seuraus 5.9. *Olkoon G äärellinen ryhmä ja K sen Sylowin p-aliryhmä jollekin alkuluvulle p. Tällöin K on ryhmän G normaali aliryhmä, jos ja vain jos K on ryhmän G ainoa Sylowin p-aliryhmä.*

Todistus. Aiemmin todettiin, että jos K on Sylowin p-aliryhmä, niin myös $x^{-1} K x$ on Sylowin p-aliryhmä kaikille $x \in G$. Jos K on ryhmän G ainut Sylowin p-aliryhmä, niin tällöin pätee $x^{-1} K x = K$ kaikille $x \in G$. Kertomalla yhtälön molemmat puolet vasemmalta alkiolla x saadaan yhtälö $Kx = xK$ eli K on ryhmän G normaali aliryhmä. Implikaatio pätee myös toiseen suuntaan. Oletetaan nyt, että K on ryhmän G normaali aliryhmä. Olkoon lisäksi P mikä tahansa ryhmän G Sylowin p-aliryhmä. Tällöin

Sylowin toisen lauseen 5.8 nojalla, on olemassa alkio $x \in G$ siten, että $P = x^{-1}Kx$. Nyt, koska K on normaali, pätee

$$P = x^{-1}Kx = K(x^{-1}x) = Ke = K.$$

Siispä K on ryhmän G ainut Sylowin p-aliryhmä. □

Lause 5.10. *(Sylowin kolmas lause). Olkoon G äärellinen ryhmä. Ryhmän G Sylowin p-aliryhmien lukumäärä t jakaa kertaluvun $|G|$ ja voidaan esittää muodossa $t = 1+pk$ jollekin $k = 0, 1, 2, \ldots$.*

Todistus. Olkoon $S = \{K_1, K_2, \ldots, K_t\}$ kaikkien ryhmän G Sylowin p-aliryhmien joukko. Sylowin toisen lauseen 5.8 nojalla joukon S alkiot ovat täsmälleen ryhmän K_1 eri G-konjugaatit. Lemman 4.22 nojalla ryhmän K_1 eri G-konjugaattien lukumäärä on

$$t = [G : G \cap N(K_1)] = [G : N(K_1)]$$

eli Sylowin toista lausetta käyttämällä myös ryhmän G Sylowin p-aliryhmien lukumäärä on $t = [G : N(K_1)]$. Lagrangen lauseen seurauksena tämä indeksi jakaa ryhmän G kertaluvun $|G|$.

Olkoon P joukon S ryhmä K_1. Ryhmän K_1 ainut P-konjugaatti on se itse, sillä $x^{-1}K_1x = K_1$ kaikilla $x \in K_1$. Osoitetaan vielä, että jos R on K_1-konjugaattiluokka siten, että $K_1 \notin R$, niin joukossa R on p^r alkiota jollakin $r \geq 1$. Tehdään vastaoletus, että on olemassa P-konjugaattiluokka $R = \{K_j\}$, missä $j = 2, 3, \ldots, t$. Tällöin erityisesti pätee $x^{-1}K_jx = K_j$ kaikilla $x \in K_1$. Ristiriitaa varten riittää todistaa, että pätee $K_1 = K_j$. Jokaisella $x \in K_1$ on olemassa luku r siten, että kertaluvulle pätee $|x| = p^r$, sillä K_1 on Sylowin p-aliryhmä. Lemmasta 4.25 saadaan tässä tapauksessa, että $x \in K_j$ ja siten erityisesti $K_1 \subset K_j$. Koska molemmat ryhmät K_1 ja K_j ovat Sylowin p-aliryhmiä, niillä on sama kertaluku. Siispä pätee $K_1 = K_j$. Näin ollen ainut P-konjugaattiluokka, joka sisältää vain yhden alkion, on $\{K_1\} = \{P\}$.

Lemman 5.7 nojalla joukko S on eri P-konjugaattiluokkien yhdiste, joista jokainen sisältää jonkin alkuluvun p potenssin verran aliryhmiä K_i. Edellä osoitettiin, että vain yksi P-konjugaattiluokista on yksiö, nimittäin $\{P\}$, jolloin kyseisen konjugaattiluokan alkioiden lukumäärä on $p^0 = 1$. Lisäksi osoitettiin, että muiden P-konjugaattiluokien aliryhmien lukumäärä on jokin alkuluvun p positiivinen potenssi eli p^{r_j}, missä $r_j > 0$. Tällöin Sylowin p-aliryhmien lukumäärä eli indeksi $t = [G : N(K_1)]$ on muotoa

$$t = 1 + p^{r_1} + \ldots + p^{r_k},$$

joka edelleen voidaan kirjoittaa muodossa $t = 1 + kp$, jollekin $k = 0, 1, 2, \ldots$. □

Lemma 5.11. *Olkoon H ja K ryhmän G aliryhmiä. Merkitään*

$$HK = \{hk \in G : h \in H \quad ja \quad k \in K\}.$$

Jos on $H \cap K = \langle e \rangle$, niin tällöin pätee $|HK| = |H||K|$.

Todistus. Tarkastellaan yhtälöä $hk = h_1k_1$. Kertomalla yhtälön molemmat puolet vasemmalta alkiolla ${h_1}^{-1} \in H$ ja oikealta alkiolla $k^{-1} \in K$ saadaan yhtälö

$${h_1}^{-1}hkk^{-1} = {h_1}^{-1}h_1k_1k^{-1},$$

jolloin edelleen

$${h_1}^{-1}h = k_1k^{-1}.$$

Nyt siis $g = {h_1}^{-1}h \in H$ ja $g = k_1k^{-1} \in K$ eli $g \in H \cap K$. Mutta koska oletuksen nojalla $H \cap K = \{e\}$, niin täytyy olla $g = e$ eli pätee $h = h_1$ ja $k = k_1$. Siispä jokainen ryhmän HK alkio voidaan kirjoittaa yksikäsitteisesti muodossa hk, missä $h \in H$ ja $k \in K$ ja pätee $|HK| = |H||K|$. □

Lause 5.12. *Olkoon G ryhmä ja sen kertaluku $|G| = pq$, missä p ja q ovat alkulukuja siten, että pätee $p > q$. Jos alkuluku q ei jaa lukua $p-1$, niin ryhmä G on isomorfinen ryhmän $\mathbb{Z}_{pq}$ kanssa.*

Todistus. Olkoon $\{M_1, M_2, \ldots, M_t\}$ ryhmän G Sylowin p-aliryhmien joukko. Sylowin kolmannen lauseen 5.10 nojalla ryhmän G Sylowin p-aliryhmien lukumäärän t täytyy jakaa kertaluku $|G| = pq$. Tällöin siis luvun t täytyy olla $1, p, q$ tai pq. Toisaalta luvulle t pätee $t = 1 + pk$ jollekin $k = 0, 1, 2, \ldots$.

Osoitetaan seuraavaksi, että Sylowin p-aliryhmien lukumäärä t ei voi olla q, p eikä pq. Koska oletuksen nojalla pätee $p > q$, niin alkulukua q ei voi kirjoittaa muodossa $q = 1 + pk$. Lisäksi molemmista yhtälöistä $p = 1 + pk$ ja $pq = 1 + pk$ seuraisi, että $p|1$. Tämä on mahdotonta, joten täytyy päteä $t = 1$. Siispä on olemassa täsmälleen yksi Sylowin p-aliryhmä H, jonka kertaluku on $|H| = p$, koska $|G| = pq$. Seurauksen 5.9 nojalla Sylowin p-aliryhmä H on normaali.

Olkoon nyt $\{N_1, N_2, \ldots, N_s\}$ ryhmän G Sylowin q-aliryhmien joukko. Vastaavasti Sylowin kolmannen lauseen 5.10 nojalla ryhmän G Sylowin q-aliryhmien lukumäärän s täytyy jakaa kertaluku $|G| = pq$. Lisäksi luvulle s pätee $s = 1 + qk$ jollekin $k = 0, 1, 2, \ldots$.

Osoitetaan, että Sylowin q-aliryhmien lukumäärä s ei voi olla p, q eikä pq. Koska oletuksen nojalla $q \nmid (p-1)$, ei voi olla $p = 1 + qk$. Lisäksi molemmista yhtälöistä $q = 1+qk$ ja $pq = 1+qk$ seuraisi, että $q|1$. Tämä ei ole mahdollista, joten on olemassa täsmälleen yksi Sylowin q-aliryhmä K, jonka kertaluku on $|K| = q$. Jälleen seurauksen 5.9 nojalla tämä Sylowin q-aliryhmä K on normaali.

Tarkastellaan ryhmää $H \cap K$. Koska ryhmä $H \cap K$ on sekä ryhmän H että ryhmän K aliryhmä, sen kertaluvun täytyy Lagrangen lauseen nojalla jakaa molemmat kertaluvut $|H| = p$ ja $|K| = q$. Ainoa luku, joka jakaa sekä alkuluvun p että alkuluvun q on 1, jolloin välttämättä $|H \cap K| = 1$. Siispä täytyy päteä $H \cap K = \langle e \rangle$. Lemman 5.11 nojalla voidaan kirjoittaa

$$|G| = pq = |H||K| = |HK|,$$

jolloin on $G = HK$. Tällöin Lemman 4.5 nojalla pätee $G \cong H \otimes K$. Mutta nyt, koska ryhmien H ja K kertaluvut ovat alkulukuja, kyseiset ryhmät ovat syklisiä ja pätee $H \cong \mathbb{Z}_p$ ja $K \cong \mathbb{Z}_q$. Tällöin Lemmasta 3.11 seuraa, että

$$G \cong H \otimes K \cong \mathbb{Z}_p \otimes \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

□

Esimerkki 5.13. Tarkastellaan ryhmää G, jonka kertaluku on $15 = 5 \times 3$. Valitsemalla $p = 5$ ja $q = 3$ pätee $p > q$ ja $q \nmid (p-1)$. Siispä Lauseen 5.12 nojalla pätee $G \cong \mathbb{Z}_{15}$. Erityisesti kaikki ryhmät, joiden kertaluku on 15, ovat isomorfisia ryhmän $\mathbb{Z}_{15}$ kanssa.

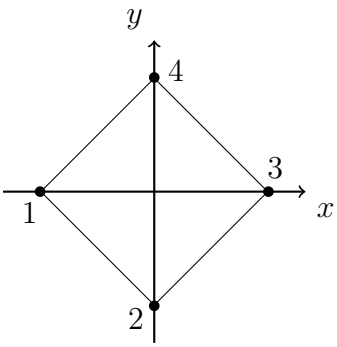
6. Apuryhmät

Tässä luvussa esitellään sellaisia ryhmiä, joita tarvitaan avuksi joidenkin äärellisten ryhmien täydellisessä luokittelussa isomorfiaa vaille. Esitellään lisäksi näihin apuryhmiin liittyviä tarpeellisia tuloksia.

Otetaan ensimmäiseksi tarkasteluun diedriryhmät. Ne ovat merkittävässä roolissa, kun luokitellaan $2p$-kertalukuisia ryhmiä, missä p on alkuluku.

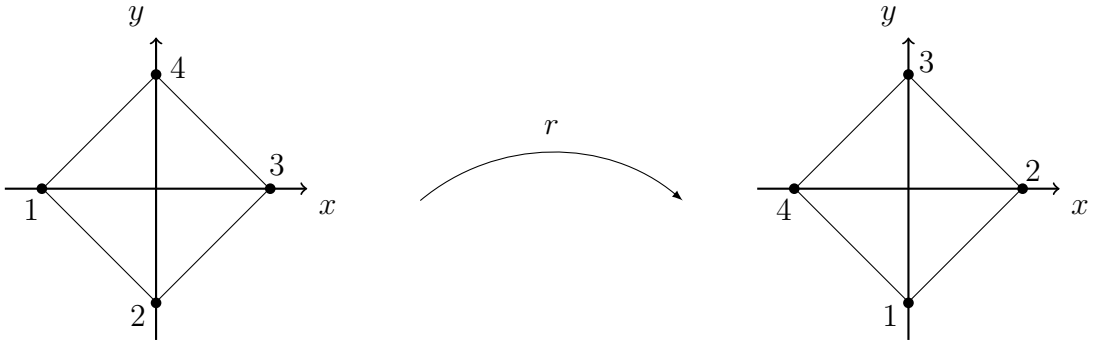
Määritelmä 6.1. *Diedriryhmä* D_n on säännöllisen n-sivuisen monikulmion symmetriaryhmä, missä $n \geq 3$. Toisin sanoen jokainen diedriryhmän alkio on sellainen tason vastapäiväinen kierto r, x-akselin suhteinen peilaus d tai niiden yhdiste, joka kuvaa säännöllisen monikulmion takaisin itselleen, kun sen keskipiste on origossa ja yksi kärki negatiivisella x-akselilla.

Havainnollistetaan diedriryhmiä ja niiden ominaisuuksia esimerkin kautta. Tarkastellaan säännöllistä nelikulmiota, jolloin $n = 4$. Sijoitetaan nelikulmio siten, että sen keskipiste on origossa ja yksi kärki negatiivisella x-akselilla kuten Kuvassa 1.



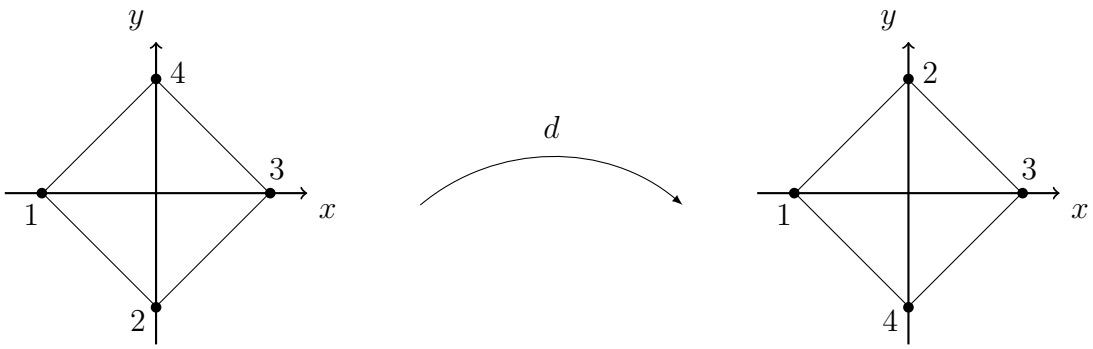
Kuva 1. Säännöllisen nelikulmion asemointi koordinaattiakselistolla.

Tason vastapäiväinen kierto r kiertää nelikulmiota $360/n = 360/4 = 90$ astetta origon ympäri, kuten Kuvassa 2. Edelleen r^2 kiertää nelikulmiota 180 astetta ja r^3 270 astetta vastapäivään origon ympäri. Kierron r kertaluku on $|r| = n = 4$, sillä r^4 kiertää nelikulmiota 360 astetta ja palauttaa sen alkuperäiseen asemaansa. Kierrot säilyttävät symmetrian ja kuuluvat näin diedriryhmään D_4.



Kuva 2. Säännöllisen nelikulmion vastapäiväinen kierto, r.

Vastaavasti x-akselin suhteinen peilaus d säilyttää symmetrian ja kuuluu diedriryhmään D_4. Peilaus muuttaa nelikulmion kärjet käänteiseen järjestykseen, kuten on havinnollistettu Kuvassa 3, ja d^2 palauttaa sen aina alkuperäiseen asemaansa, jolloin peilauksen kertaluku on siis $|d| = 2$.



KUVA 3. Säännöllisen nelikulmion x-akselin suhteinen peilaus, d.

Säännöllinen nelikulmio säilyttää symmetriansa myös kierron ja peilauksen yhdisteellä. Peilaus d muuttaa nelikulmion kärjet käänteiseen järjestykseen jonka jälkeen kierto r kiertää nelikulmiota vastapäivään origon ympäri. Siispä säännöllisen nelikulmion symmetriaryhmä eli diedriryhmä D_4 muodostuu seuraavanlaiseksi:

$$D_4 = \{e = r^0, r, r^2, r^3, d = r^0 d, rd, r^2 d, r^3 d\}.$$

Nähdään, että ryhmän kertaluvuksi muodostuu $|D_4| = 2n = 2 \times 4 = 8$. Havaitaan lisäksi, että operaatiolla drd saadaan kierrettyä nelikulmiota 270 astetta vastapäivään, jolloin siis pätee $drd = r^3$. Koska kierron kertaluku on $|r| = 4$, voidaan kirjoittaa $drd = r^3 = r^{-1}$. Kertomalla oikealta peilauksella d saadaan yhtälö $dr = r^{-1}d$.

Yllä olevat havainnot voidaan yleistää mille tahansa säännölliselle monikulmiolle. Muotoillaan ne lauseeksi, mutta jätetään todistus kuitenkin edellisen esimerkin varaan.

Lause 6.2. *Olkoon D_n diedriryhmä, $n \geq 3$, r tason kierto $360/n$ astetta vastapäivään ja d peilaus x-akselin suhteen. Tällöin ryhmän D_n kertaluku on $|D_n| = 2n$. Lisäksi ryhmä D_n on alkioiden r ja d virittämä siten, että pätee $|r| = n, |d| = 2$ ja $dr = r^{-1}d$.*

Ennen kuin voidaan osoittaa, että Lauseen 6.2 ehdot määräävät diedriryhmän yksikäsitteisesti, tarvitaan avuksi seuraava lemma.

Lemma 6.3. *Olkoon ryhmä G alkioiden a ja b virittämä siten, että pätee*

$$|a| = n \geq 3, \quad |b| = 2 \quad ja \quad ba = a^{-1}b. \tag{6.1}$$

Tällöin pätee $b^j a^i = a^{(-1)^j i} b^j$, missä $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$.

Todistus. Tiedetään, että pätee $ba = a^{-1}b$ eli $bab^{-1} = a^{-1}$, jolloin kaikille $i \in \mathbb{Z}$ pätee $ba^i b^{-1} = a^{-i}$. Koska $b^2 = e$, niin saadaan $b^j a^i b^{-j} = a^{(-1)^j i}$ ja edelleen pätee $b^j a^i = a^{(-1)^j i} b^j$. □

Lause 6.4. *Olkoon G alkioiden a ja b virittämä ryhmä, jolle pätee ehdot (6.1). Tällöin on olemassa isomorfismi*

$$f : D_n \to G,$$

joka kuvaa kierron r alkioksi a ja peilauksen d alkioksi b.

Todistus. Havaitaan aluksi, että koska voidaan kirjoittaa $aa^{n-1} = e$ ja $bb = e$, niin pätee $a^{-1} = a^{n-1}$ ja $b^{-1} = b$. Tällöin, koska ryhmä G on alkioiden a ja b virittämä, jokainen alkio $x \in G$ voidaan kirjoittaa äärellisenä tulona, jonka jokainen tekijä on joko a tai b. Edelleen Lemman 6.3 nojalla jokainen äärellinen tulo, jonka jokainen tekijä on joko a tai b, voidaan kirjoittaa muodossa $a^i b^j$. Koska alkion a kertaluku on $|a| = n$ ja alkion b kertaluku $|b| = 2$, saadaan tulo $a^i b^j$ sievennettyä muotoon, missä i toteuttaa ehdon $0 \leq i \leq n-1$ ja j toteuttaa ehdon $0 \leq j \leq 1$. Siispä jokainen ryhmän G alkio voidaan kirjoittaa muodossa

$$a^i b^j, \quad \text{missä} \quad i \in \{0, 1, \ldots, n-1\} \quad \text{ja} \quad j \in \{0, 1\}.$$

Osoitetaan, että alkioiden a ja b virittämän ryhmän G kertaluku on $|G| = 2n$. Ryhmä $\langle a \rangle$ on ryhmän G aliryhmä, jonka kertaluku on $|\langle a \rangle| = n$. Vastaavasti ryhmä $\langle b \rangle$ on ryhmän G aliryhmä, jonka kertaluku on $|\langle b \rangle| = 2$. Edellä osoitettiin, että jokainen ryhmän G alkio voidaan kirjoittaa muodossa $a^i b^j$, missä $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$ ja lisäksi oletuksen nojalla $ba = a^{-1}b$. Siispä, jos pätee $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$, niin voidaan kirjoittaa $a^i b^j \langle a \rangle = b^j \langle a \rangle$ eli aliryhmällä $\langle a \rangle$ on ryhmässä G täsmälleen kaksi vasenta sivuluokkaa; $e\langle a \rangle$ ja $b\langle a \rangle$. Tällöin pätee $[G : \langle a \rangle] = 2$ ja Lagrangen lauseen nojalla ryhmän G kertaluvuksi saadaan

$$|G| = [G : \langle a \rangle] |\langle a \rangle| = 2n.$$

Jos taas pätee $\langle a \rangle \cap \langle b \rangle \neq \langle e \rangle$, niin täytyy olla $b \in \langle a \rangle$. Tällöin alkio a virittää koko ryhmän G eli $G = \langle a \rangle$ ja edelleen ryhmä G on siis syklisenä Abelinen. Siispä pätee $ab = ba$, jolloin yhdistämällä tämä oletuksen $ba = a^{-1}b$ kanssa saadaan $ab = a^{-1}b$. Edelleen kertomalla kyseisen yhtälön molempia puolia oikealta alkiolla b^{-1} saadaan $a = a^{-1}$ eli alkion a kertaluku on $|a| = 2$. Päädytään ristiriitaan, sillä oletuksen nojalla $|a| \geq 3$. Täytyy siis olla $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$, jolloin saatiin pätemään $|G| = 2n$.

Osoitetaan, että kuvaus $f : D_n \to G$ on hyvin määritelty. Koska ryhmän G kertaluku on $|G| = 2n$ ja aiemman perusteella sen kaikki alkiot voidaan esittää muodossa $a^i b^j$, niin kyseiset alkiot ovat kaikki eri alkioita, kun $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$. Vastaavasti diedriryhmän D_n alkiot $r^i d^j$ ovat kaikki eri alkioita kyseisten rajoitteiden vallitessa. Siispä aina kun $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$ voidaan määritellä $f(r^i d^j) = a^i b^j$. Näin muodostuva kuvaus $f : D_n \to G$ on hyvin määritelty.

Osoitetaan, että kuvaus

$$f : D_n \to G, f(r^i d^j) = a^i b^j$$

on homomorfismi. Olkoon $r^i d^j, r^{i'} d^{j'} \in D_n$. Lemman 6.3 nojalla pätee $b^j a^{i'} = a^{(-1)^j i'} b^j$. Tällöin voidaan kirjoittaa

$$\begin{aligned} f(r^i d^j) f(r^{i'} d^{j'}) &= a^i b^j a^{i'} b^{j'} \\ &= a^i a^{(-1)^j i'} b^j b^{j'} \\ &= a^{i+(-1)^j i'} b^{j+j'}. \end{aligned} \tag{6.2}$$

Merkitään nyt $k = i + (-1)^j i'$ ja $m = j + j'$. Nämä voidaan esittää muodossa $k = nt + i$ ja $m = 2s + j$ joillakin $t, s \in \mathbb{Z}$, missä $0 \leq i \leq n-1$ ja $0 \leq j \leq 1$. Tällöin, koska

alkion a kertaluku on $|a| = n$ ja alkion b kertaluku $|b| = 2$, pätee siis

$$a^{i+(-1)^j i'} b^{j+j'} = a^k b^m = a^i b^j.$$

Edellistä vastaava päättely on voimassa myös ryhmässä D_n. Voidaan siis käyttää kuvauksen f määritelmää ja saadaan

$$a^{i+(-1)^j i'} b^{j+j'} = a^i b^j = f(r^i d^j) = f(r^{i+(-1)^j i'} d^{j+j'}). \tag{6.3}$$

Edelleen Lemman 6.3 nojalla voidaan kirjoittaa

$$\begin{aligned} f(r^{i+(-1)^j i'} d^{j+j'}) &= f(r^i r^{(-1)^j i'} d^j d^{j'}) \\ &= f((r^i d^j)(r^{i'} d^{j'})). \end{aligned} \tag{6.4}$$

Kohtien (6.2), (6.3) ja (6.4) nojalla pätee siis

$$f(r^i d^j) f(r^{i'} d^{j'}) = f((r^i d^j)(r^{i'} d^{j'}))$$

eli kuvaus $f : D_n \to G$ on homomorfismi.

Osoitetaan vielä kuvauksen $f : D_n \to G$ isomorfisuus. Aiemmin todettiin, että koska pätee $|G| = 2n$, niin muotoa $a^i b^j$ olevat alkiot ovat kaikki eri alkioita, kun $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$. Vastaava pätee diedriryhmän D_n muotoa $r^i d^j$ oleville alkioille. Siispä kuvaus f on injektio. Lisäksi aiemmin todettiin, että jokainen ryhmän G alkio voidaan kirjoittaa muodossa $a^i b^j$, missä $i \in \{0, 1, ..., n-1\}$ ja $j \in \{0, 1\}$. Vastaava pätee myös diedriryhmän D_n alkioille. Kuvaus f on siis myös surjektio. Injektiivisyydestä ja surjektiivisuudesta seuraa bijektiivisyys. Tällöin kuvaus $f : D_n \to G$ on sekä bijektio että homomorfismi eli isomorfismi. □

Esimerkki 6.5. Muotoillaan diedriryhmän D_4 laskutaulu hyödyntäen Lauseen 6.2 ominaisuuksia. Lasketaan muutamia tuloja esimerkiksi. Koska kierron r kertaluku on $|r| = 4$ saadaan

$$(r^2)(r^2 d) = r^4 d = ed = d.$$

Vastaavasti, koska peilauksen d kertaluku on $|d| = 2$ voidaan kirjoittaa

$$(r^3 d)d = r^3 e = r^3.$$

Seuraavissa laskutoimituksissa hyödynnetään tietoa $dr = r^{-1}d$. Pidetään lisäksi mielessä, että pätee $r^3 = r^{-1}$ ja että peilauksen kertaluku on $|d| = 2$ ja kierron $|r| = 4$. Saadaan siis

$$(rd)(r^2 d) = rdrrd = rr^{-1}drd = rr^{-1}r^{-1}dd = r^3 e = r^3$$

Vastaavasti saadaan

$$(r^3 d)(r^2 d) = r^3 drrd = r^3 r^{-1} drd = r^3 r^{-1} r^{-1} dd = re = r.$$

Laskutaulukko muodostuu seuraavanlaiseksi:

	e	r	r^2	r^3	d	rd	r^2d	r^3d
e	e	r	r^2	r^3	d	rd	r^2d	r^3d
r	r	r^2	r^3	e	rd	r^2d	r^3d	d
r^2	r^2	r^3	e	r	r^2d	r^3d	d	rd
r^3	r^3	e	r	r^2	r^3d	d	rd	r^2d
d	d	r^3d	r^2d	rd	e	r^3	r^2	r
rd	rd	d	r^3d	r^2d	r	e	r^3	r^2
r^2d	r^2d	rd	d	r^3d	r^2	r	e	r^3
r^3d	r^3d	r^2d	rd	d	r^3	r^2	r	e

Huomautus 6.6. Diedriryhmä D_n ei ole syklinen. Tämä voidaan nähdä esimerkiksi diedriryhmän D_4 tapauksessa sen laskutaulukosta Esimerkissä 6.5, mutta tulos siis pätee myös yleisesti. Tämän vuoksi diedriryhmä D_n ei ole isomorfinen syklisen ryhmän $\mathbb{Z}_{2n}$ kanssa.

Lemma 6.7. *Olkoon N ryhmän G aliryhmä ja $[G : N] = 2$ sen indeksi. Tällöin aliryhmä N on normaali.*

Todistus. Tarkastellaan ensin tapausta, missä $a \in N$. Tällöin pätee $aN = N = Na$ ja ryhmän N normaalius seuraa määritelmästä.

Olkoon nyt $a \notin N$. Tällöin $aN \neq N$, ja koska ryhmällä N on vain kaksi vasenta sivuluokkaa, joista toinen on ryhmä itse, täytyy päteä $aN = G \setminus N$. Vastaavasti ryhmällä N on vain kaksi oikeaa sivuluokkaa, joista toinen on ryhmä itse, joten on $Na = G \setminus N$. Siispä sivuluokat ovat välttämättä samat ja saadaan $aN = G \setminus N = Na$ eli ryhmä N on määritelmän nojalla normaali. □

Lause 6.8. *Olkoon G ryhmä, jonka kertaluku on muotoa $|G| = 2p$, missä $p > 2$ on alkuluku. Tällöin ryhmä G on isomorfinen joko syklisen ryhmän $\mathbb{Z}_{2p}$ tai diedriryhmän D_p kanssa.*

Todistus. Cauchyn lauseen 5.4 nojalla ryhmä G sisältää alkiot a ja b, joiden kertaluvuille pätee $|a| = p$ ja $|b| = 2$, sillä ryhmän G kertaluku on jaollinen alkuluvuilla 2 ja p. Olkoon $N = \langle a \rangle$ syklinen ryhmä. Koska ryhmän G kertaluku on $|G| = 2p$, niin Lagrangen lauseen nojalla indeksi $[G : N] = 2$ ja edelleen Lemman 6.7 nojalla aliryhmä N on normaali. Koska alkion b kertaluku on $|b| = 2$, niin $b = b^{-1}$, josta seuraa ryhmän N normaaliuden nojalla $bab = bab^{-1} \in N$. Koska ryhmä $N = \langle a \rangle$ on syklinen, niin voidaan kirjoittaa $bab = a^t$, jollakin t. Edelleen saadaan

$$a^{t^2} = (a^t)^t = (bab)(bab) \cdots (bab).$$

Kun sovelletaan vielä tietoa $b^2 = e$ kahteen eri otteeseen saadaan

$$(bab)(bab) \cdots (bab) = ba^t b = b(bab)b = a.$$

Siispä, koska $a^{t^2} = a$, niin Lemman 4.1 nojalla alkuluvun p täytyy jakaa luku $t^2 - 1 = (t-1)(t+1)$. Tällöin edelleen alkuluvun p täytyy jakaa joko luku $(t-1)$ tai luku $(t+1)$.

Tarkastellaan ensin tapausta $p|(t-1)$. Tällöin pätee $bab = a^t = a$. Kun kerrotaan yhtälöä molemmilta puolilta alkiolla b saadaan $ba = ab$. Tästä seuraa, että

$$(ab)^{|a||b|} = (a^{|a|}b^{|a|})^{|b|} = (eb^{|a|})^{|b|} = (b^{|b|})^{|a|} = e^{|a|} = e.$$

Edelleen, koska $(ab)^{|a||b|} = e$, niin alkion ab kertaluvun $|ab|$ täytyy jakaa luku $|a||b|$. Alkioiden a ja b kertaluvut ovat alkulukuja, joten alkion ab kertaluku on $2, p$ tai $2p$.

Osoitetaan, että kertaluku $|ab|$ ei voi olla 2 eikä p. Tiedetään, että alkion a kertaluku on $|a| = p$ ja alkion b kertaluku $|b| = 2$, jolloin siis pätee $a^p = e \neq b^{-1}$. Siispä saadaan $a^p b \neq e$. Alkion ab kertaluku ei voi olla $|ab| = 2$, sillä voidaan kirjoittaa

$$(ab)^2 = abab = abba = a^2 \neq e.$$

Osoitetaan vastaavasti, että alkion ab kertaluku ei voi olla $|ab| = p$. Tehdään vastaoletus, että alkion ab kertaluku on $p = 2m+1$ jollakin $m \in \mathbb{N}$. Tällöin edellisen kohdan nojalla voidaan kirjoittaa

$$(ab)^p = (ab)^{2m}ab = a^{2m}ab = a^{2m+1}b = a^p b,$$

jolloin pätee $(ab)^p = a^p b \neq e$. Alkion ab kertaluku ei siis voi olla p. Edellisen nojalla alkion ab kertaluvun täytyy olla

$$|ab| = |a||b| = p2 = |G|.$$

Siispä ryhmä G on syklinen ja isomorfinen ryhmän $\mathbb{Z}_{2p}$ kanssa.

Tarkastellaan seuraavaksi tapausta $p|(t+1)$. Tällöin pätee $bab = bab^{-1} = a^t = a^{-1}$. Siispä kertomalla yhtälön molempia puolia oikealta alkiolla b, saadaan $ba = a^{-1}b$. Lisäksi tiedetään, että alkion a kertaluku on $|a| = p$ ja alkion b kertaluku $|b| = 2$. Tällöin Lauseen 6.4 nojalla on olemassa homomorfismi

$$f : D_n \to G, f(r^i d^j) = a^i b^j,$$

joka kuvaa kierron r alkioksi a ja peilauksen d alkioksi b.

Osoitetaan seuraavaksi kuvauksen f isomorfisuus. Olkoon $K = \langle b \rangle$ ryhmän G aliryhmä. Koska aliryhmien K ja N kertaluvut ovat $|K| = 2$ ja $|N| = p$, missä alkuluku p on pariton, niin Lagrangen lauseen nojalla pätee $N \cap K = \langle e \rangle$. Edelleen Lemman 5.11 nojalla pätee $G = NK$. Siispä jokainen ryhmän G alkio voidaan esittää muodossa $a^i b^j$ eli kuvaus f on surjektio. Lisäksi diedriryhmällä D_p ja ryhmällä G on sama kertaluku, joten kuvauksen f täytyy olla injektio. Näin ollen kuvaus f on siis bijektio ja homomorfismi eli isomorfismi. □

Esimerkki 6.9. Lauseen 6.8 avulla pystytään luokittelemaan kaikki äärelliset ryhmät, joiden kertaluku on muotoa $2p$, missä p on pariton alkuluku. Tällaisia ryhmiä ovat siis esimerkiksi ryhmät, joiden kertaluku on $6, 10, 14, 22, 26, 34, 38, 46, 58, 62, \ldots$. Jos tarkastellaan esimerkiksi ryhmää H_1, jonka kertaluku on $|H_1| = 34 = 2 \times 17$, niin Lauseen 6.8 nojalla ryhmä H_1 on isomorfinen joko syklisen ryhmän $\mathbb{Z}_{34}$ tai diedriryhmän D_{17} kanssa. Vastaavasti, jos tarkastellaan ryhmää H_2, jonka kertaluku on $|H_2| = 62 = 2 \times 31$, on se isomorfinen joko syklisen ryhmän $\mathbb{Z}_{62}$ tai diedriryhmän D_{31} kanssa.

Lauseen 6.8 avulla saadaan myös isomorfiat ryhmille, joiden kertaluku on $6 = 2 \times 3$. Voidaan kuitenkin osoittaa, että diedriryhmä D_3 on isomorfinen symmetrisen ryhmän S_3 kanssa. Siispä ryhmät, joiden kertaluku on 6, ovat isomorfisia joko syklisen ryhmän $\mathbb{Z}_6$ tai symmetrisen ryhmän S_3 kanssa. Kyseinen tulos voidaan todistaa laskutaulukoiden avulla perehtymättä Sylowin lauseiden teoriaan. Yhdenmukaisuuden vuoksi, käytetään kuitenkin 6-kertalukuisten ryhmienkin tapauksessa isomorfioita $\mathbb{Z}_6$ ja D_3. Todistetaan joka tapauksessa ryhmien S_3 ja D_3 isomorfisuus.

Lause 6.10. *Symmetrinen ryhmä S_3 on isomorfinen diedriryhmän D_3 kanssa.*

Todistus. Tiedetään, että diedriryhmä D_3 on alkioiden r ja d virittämä siten, että pätee $|r| = 3$, $|d| = 2$ ja $dr = r^{-1}d$. Lisäksi ryhmän D_3 kertaluku on $|D_3| = 2 \times 3$. Valitaan symmetrisestä ryhmästä S_3 alkiot $r' = (123)$ ja $d' = (12)$. Yksikäsitteisyyden nojalla riittää osoittaa, että alkiot r' ja d' toteuttavat Lauseen 6.2 ehdot, kun $n = 3$. Tarkastellaan ensin alkioiden r' ja d' kertalukuja. Tällöin saadaan $|d'| = |(12)| = 2$ ja $|r'| = |(123)| = 3$. Lisäksi pätee

$$d'r' = (12)(123) = (321)(12) = (r')^{-1}d'$$

ja ryhmän S_3 kertaluku on muotoa $|S_3| = 6 = 2 \times 3$. Ryhmän S_3 kaikki alkiot saadaan muodostettua alkioiden $r' = (123)$ ja $d' = (12)$ avulla:

$$S_3 = \{(1), (123), (123)(123) = (132), (12), (123)(12) = (13), (123)(123)(12) = (23)\}.$$

Ryhmä S_3 toteuttaa siis Lauseen 6.2 ehdot ja on näin isomorfinen ryhmän D_3 kanssa. □

Esitellään seuraavaksi kvaternioryhmä Q, joka on määritelty perustuen lähteeseen [1]. Kyseistä ryhmää tarvitaan kertaluvun 8 ryhmiä luokiteltaessa.

Määritelmä 6.11. *Kvaternioryhmä* on alkioiden a ja b virittämä ryhmä Q siten, että pätee $a^4 = e, a^2 = b^2$ ja $ba = a^3b$.

Määritelmän 6.11 ehdot määräävät ryhmän Q laskutaulukon. Vaihtoehtoisesti kvaternioryhmä voidaan esittää kompleksiarvoisten matriisien avulla eli voidaan määritellä

$$Q = \{\pm I, \pm A, \pm B, \pm C\},$$

missä $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ ja $C = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$. Tällöin laskutaulukko voidaan muodostaa matriisien kertolaskua hyödyntämällä, jonka voi tarvittaessa kerrata esimerkiksi lähteestä [2]. Tässä kvaternioryhmän mallissa siis pätee $e = I, a = A$ ja $b = B$. Alkio C saadaan ilmaistua esimerkiksi muodossa $C = BA$.

Kerrataan seuraavaksi parillisten permutaatioiden määritelmä, jotta alternoivien ryhmien määritteleminen olisi mahdollista. Tämä on tarpeellista, sillä esimerkiksi alternoiva ryhmä A_4 on keskeisessä roolissa, jotta voidaan täydellisesti luokitella 12-kertalukuiset ryhmät isomorfiaa vaille. Kertaluvun 12 ryhmien luokittelua varten muotoillaan lisäksi eräs lemma.

Määritelmä 6.12. Permutaatio $\tau \in S_n$ on *parillinen*, jos se voidaan esittää parillisella määrällä 2-syklien tuloja. Toisin sanoen, jos alkio $\tau \in S_n$ voidaan esittää muodossa $\tau = (a_1a_2)(a_3a_4)\cdots(a_{k-1}a_k)$, missä 2-syklejä (a_ia_j) on parillinen määrä.

Määritelmä 6.13. Symmetrisen ryhmän S_n parillisten permutaatioden joukkoa A_n, missä $n \geq 2$, kutsutaan *alternoivaksi ryhmäksi*.

Huomautus 6.14. Alternoivan ryhmän A_n indeksi ryhmässä S_n on $[S_n : A_n] = 2$, jolloin se on Lemman 6.7 nojalla ryhmän S_n normaali aliryhmä. Lisäksi kertaluvulle pätee $|A_n| = |S_n|/2 = n!/2$.

Esimerkki 6.15. Otetaan tarkasteluun alternoiva ryhmä $A_4 \subset S_4$. Ryhmä S_4 koostuu seuraavista permutaatioista:

$$\begin{aligned} S_4 = \{&(1), (12), (13), (14), (23), (24), (34), \\ &(12)(34), (13)(24), (14)(23), \\ &(123), (124), (132), (134), (142), (143), (234), (243), \\ &(1234), (1243), (1324), (1342), (1423), (1432)\}. \end{aligned}$$

Näistä alkioista 2-syklien tulot ovat selvästi parillisia permutaatioita ja neutraalialkio (1) voidaan esittää parillisena permutaationa $(a_1a_2)(a_1a_2) = (1)$. Lisäksi myös 3-syklit voidaan esittää parillisella määrällä 2-syklien tuloja, sillä voidaan kirjoittaa $(a_1a_2a_3) = (a_1a_2)(a_2a_3)$. Sen sijaan 2-syklit ja 4-syklit ovat parittomia permutaatioita. Siispä, koska alternoiva ryhmä koostuu symmetrisen ryhmän parillisista permutaatioista, näyttää ryhmä A_4 seuraavalta:

$$\begin{aligned} A_4 = \{&(1), (12)(34), (13)(24), (14)(23), \\ &(123), (124), (132), (134), (142), (143), (234), (243)\}. \end{aligned}$$

Nähdään, että ryhmän A_4 kertaluvulle pätee siis $|A_4| = 4!/2 = 12$, kuten edellä huomautettiin.

Tarkastellaan seuraavaksi ryhmän A_4 alkioiden kertalukuja. Havaitaan, että alkioiden $(12)(34), (13)(24)$ ja $(14)(23)$ 2-syklit ovat erillisiä. Koska 2-syklin kertaluku on aina 2, niin kyseisten alkoiden 2-syklien pienin yhteinen jaettava on 2, jolloin myös näiden alkioiden kertaluku on 2. Lisäksi tiedetään, että 3-syklin kertaluku on syklin pituus, joten alkioiden $(123), (124), (132), (134), (142), (143), (234)$ ja (243) kertaluku on 3. Erityisesti siis ryhmä A_4 ei sisällä alkiota, jonka kertaluku on 6. Tätä tietoa tarvitaan myöhemmin 12-kertalukuisten ryhmien luokittelussa.

Seuraavan lauseen todistuksen ideat ovat oleellisesti viitteestä [3, s. 144]. Yksityiskohtien laatimiseen on kuitenkin myös itse kontribuoitu.

Lause 6.16. *Olkoon G ei-Abelinen ryhmä, jonka kertaluku on $|G| = 12$. Oletetaan, että sen Sylowin 3-aliryhmien lukumäärä on $t = 4$. Tällöin ryhmä G on isomorfinen alternoivan ryhmän A_4 kanssa.*

Todistus. Olkoon $P = \{K_1, K_2, K_3, K_4\}$ Sylowin 3-aliryhmien joukko. Olkoon lisäksi $x \in G$ ja $j = 1, 2, 3, 4$. Lemman 5.6 nojalla xK_jx^{-1} on ryhmän G aliryhmä ja isomorfinen ryhmän K_j kanssa. Siispä xK_jx^{-1} on jokin Sylowin 3-aliryhmistä eli pätee $xK_jx^{-1} = K_i$ jollakin $1 \leq i \leq 4$. Voidaan siis määritellä kuvaus

$$\tau_x : P \to P, \tau_x(K_j) = xK_jx^{-1}.$$

Osoitetaan, että τ_x on injektio. Oletetaan tätä varten, että joillekin $K_i, K_j \in P$ pätee $\tau_x(K_i) = \tau_x(K_j)$. Tällöin voidaan kirjoittaa

$$xK_ix^{-1} = xK_jx^{-1}.$$

Kertomalla yhtälön molempia puolia oikealta alkiolla x ja vasemmalta alkiolla x^{-1} saadaan $K_i = K_j$ eli kuvaus τ_x on injektio. Tästä seuraa, että kuvaus τ_x on bijektio, sillä pätee $|P| = 4$. Näin ollen x tuottaa symmetrisen ryhmän $\mathrm{Sym}(P)$ alkion τ_x, mutta kyseinen symmetrinen ryhmä on itse asiassa S_4. Voidaan muodostaa siis kuvaus $f : G \to S_4$ asettamalla $f(x) = \tau_x$.

Osoitetaan, että kuvaus $f : G \to S_4$ on homomorfismi. Olkoon $x, y \in G$. Olkoon lisäksi $K \in P$ eli $K = K_j$ jollekin $1 \leq j \leq 4$. Voidaan kirjoittaa

$$\begin{aligned}[f(xy)](K) &= \tau_{xy}(K) = (xy)K(xy)^{-1} = x(yKy^{-1})x^{-1} \\ &= \tau_x(yKy^{-1}) = \tau_x(\tau_y(K)) = [\tau_x\tau_y](K) = [f(x)f(y)](K).\end{aligned}$$

Siispä kuvaus $f : G \to S_4$ on homomorfismi.

Osoitetaan kuvaus $f : G \to S_4$ injektioksi. Olkoon tätä varten $x \in G$ kuvauksen f ytimessä, eli $f(x) = (1)$. Tällöin siis erityisesti pätee $K_j = xK_jx^{-1}$ jokaisella $1 \leq j \leq 4$, sillä kyseessä on identtinen permutaatio. Normalisoijan määritelmän 4.20 nojalla tästä seuraa, että x kuuluu ryhmän K_j normalisoijaan $N(K_j)$.

Osoitetaan seuraavaksi, että pätee $K_j = N(K_j)$ kullakin $1 \leq j \leq 4$. Olkoon siis $1 \leq j \leq 4$. Sylowin toisesta lauseesta 5.8 ja Lemmasta 5.6 seuraa, että ryhmän K_j G-konjugaattiluokkia on neljä kappaletta, jotka ovat täsmälleen Sylowin 3-aliryhmät. Lauseesta 4.22 valinnalla $H = G$ ja $A = K_j$ seuraa, että

$$4 = [G : N(K_j)] = |G|/|N(K_j)| = 12/|N(K_j)|.$$

Tällöin edelleen pätee $|N(K_j)| = 3$. Koska ryhmä K_j sisältyy normalisoijaan $N(K_j)$ ja pätee $|K_j| = 3$, niin $K_j = N(K_j)$.

Nyt ollaan siis saatu osoitettua, että x kuuluu ryhmään $N(K_j) = K_j$ kullakin $1 \leq j \leq 4$ eli erityisesti x kuuluu kaikkiin Sylowin 3-aliryhmiin. Koska $K_i \cap K_j$ on sekä ryhmän K_i että ryhmän K_j aliryhmä, niin Lagrangen lauseesta seuraa, että leikkaus on joko $\langle e \rangle$ tai pätee $K_i = K_j$. Jälkimmäinen ei kuitenkaan ole mahdollinen, joten pätee $K_i \cap K_j = \langle e \rangle$ kaikille $i \neq j$. Toisin sanoen $x = e$ on neutraalialkio.

Saatiin osoitettua, että jos $f(x) = (1)$ niin $x = e$. Siispä, koska kuvaus f on homomorfismi, niin se on myös injektio ja edelleen isomorfismi kuvajoukolleen. Näin ollen $f(G)$ on symmetrisen ryhmän S_4 aliryhmä, jossa on 12 alkiota. Riittää vielä osoittaa, että kyseinen aliryhmä on A_4. Ryhmä G sisältää 8 alkiota, joiden kertaluku on 3, sillä pätee $K_i \cap K_j = \langle e \rangle$ ja jokainen neljästä aliryhmästä K_i sisältää neuraalialkion lisäksi kaksi 3-kertalukuista alkiota. Koska kuvaus f on isomorfismi, niin ryhmä $f(G)$ - joka on symmetrisen ryhmän S_4 12-alkioinen aliryhmä - sisältää täsmälleen 8 alkiota, joiden kertaluku on 3. Toisaalta, kuten Esimerkissä 6.15 havaitaan, symmetrinen ryhmä S_4 sisältää täsmälleen 8 alkiota, joiden kertaluku on 3. Lisäksi havaitaan, että sen aliryhmä A_4 sisältää kaikki nämä 8 3-kertalukuista alkiota. Siten leikkaus $f(G) \cap A_4$, joka on aliryhmien leikkauksena ryhmän A_4 aliryhmä, sisältää vähintään 8 ja korkeintaan 12 alkiota. Lagrangen lauseesta seuraa, että kertaluvun $|f(G) \cap A_4|$ täytyy jakaa kertaluku $|A_4| = 12$. Siispä täytyy olla $|f(G) \cap A_4| = 12$, jolloin välttämättä ryhmä $f(G)$ on isomorfinen ryhmän A_4 kanssa. □

Todistetaan vielä erään 12-kertalukuisen, ei-Abelisen ryhmän olemassaolo.

Lause 6.17. *Olkoon $a = ((123), 2), b = ((12), 1) \in S_3 \otimes \mathbb{Z}_4$. Tällöin on olemassa alkioiden a ja b virittämä ei-Abelinen ryhmä T, siten että pätee $|a| = 6$, $b^2 = a^3$ ja $ba = a^{-1}b$.*

Todistus. Tiedetään, että alkion $(123) \in S_3$ kertaluku on $|(123)| = 3$ ja alkion $2 \in \mathbb{Z}_4$ kertaluku $|2| = 2$. Koska lukujen 2 ja 3 pienin yhteinen jaettava on 6, alkion a kertaluvulle pätee $|a| = |((123), 2)| = 6$. Lisäksi voidaan kirjoittaa

$$b^2 = ((12), 1)^2 = ((1), 2) \quad \text{ja} \quad a^3 = ((123), 2)^3 = ((1), 2)$$

eli $b^2 = a^3$. Osoitetaan vielä, että $ba = a^{-1}b$. Nyt siis pätee

$$ba = ((12), 1)((123), 2) = ((23), 3).$$

Voidaan myös kirjoittaa

$$a^{-1}b = ((123), 2)^{-1}((12), 1) = ((321), 2)((12), 1) = ((23), 3).$$

Saadaan siis $ba = a^{-1}b$.

Osoitetaan, että

$$T = \{((1), 0), ((123), 2), ((132), 0), ((1), 2), ((123), 0), ((132), 2),$$
$$((12), 1), ((13), 3), ((23), 1), ((12), 3), ((13), 1), ((23), 3)\}$$

on ryhmän $S_3 \otimes \mathbb{Z}_4$ ei-Abelinen aliryhmä. Selvästi $T \neq \emptyset$ ja $T \subset S_3 \otimes \mathbb{Z}_4$. Riittää osoittaa, että T on suljettu ryhmän $S_3 \otimes \mathbb{Z}_4$ laskutoimituksen suhteen. Muotoillaan ryhmän T laskutaulukko:

	$((1),0)$	$((123),2)$	$((132),0)$	$((1),2)$	$((123),0)$	$((132),2)$	$((12),1)$	$((13),3)$	$((23),1)$	$((12),3)$	$((13),1)$	$((23),3)$
$((1),0)$	$((1),0)$	$((123),2)$	$((132),0)$	$((1),2)$	$((123),0)$	$((132),2)$	$((12),1)$	$((13),3)$	$((23),1)$	$((12),3)$	$((13),1)$	$((23),3)$
$((123),2)$	$((123),2)$	$((132),0)$	$((1),2)$	$((123),0)$	$((132),2)$	$((1),0)$	$((13),3)$	$((23),1)$	$((12),3)$	$((13),1)$	$((23),3)$	$((12),1)$
$((132),0)$	$((132),0)$	$((1),2)$	$((123),0)$	$((132),2)$	$((1),0)$	$((123),2)$	$((23),1)$	$((12),3)$	$((13),1)$	$((23),3)$	$((12),1)$	$((13),3)$
$((1),2)$	$((1),2)$	$((123),0)$	$((132),2)$	$((1),0)$	$((123),2)$	$((132),0)$	$((12),3)$	$((13),1)$	$((23),3)$	$((12),1)$	$((13),3)$	$((23),1)$
$((123),0)$	$((123),0)$	$((132),2)$	$((1),0)$	$((123),2)$	$((132),0)$	$((1),2)$	$((13),1)$	$((23),3)$	$((12),1)$	$((13),3)$	$((23),1)$	$((12),3)$
$((132),2)$	$((132),2)$	$((1),0)$	$((123),2)$	$((132),0)$	$((1),2)$	$((123),0)$	$((23),3)$	$((12),1)$	$((13),3)$	$((23),1)$	$((12),3)$	$((13),1)$
$((12),1)$	$((12),1)$	$((23),3)$	$((13),1)$	$((12),3)$	$((23),1)$	$((13),3)$	$((1),2)$	$((132),0)$	$((123),2)$	$((1),0)$	$((132),2)$	$((123),0)$
$((13),3)$	$((13),3)$	$((12),1)$	$((23),3)$	$((13),1)$	$((12),3)$	$((23),1)$	$((123),0)$	$((1),2)$	$((132),0)$	$((123),2)$	$((1),0)$	$((132),2)$
$((23),1)$	$((23),1)$	$((13),3)$	$((12),1)$	$((23),3)$	$((13),1)$	$((12),3)$	$((132),2)$	$((123),0)$	$((1),2)$	$((132),0)$	$((123),2)$	$((1),0)$
$((12),3)$	$((12),3)$	$((23),1)$	$((13),3)$	$((12),1)$	$((23),3)$	$((13),1)$	$((1),0)$	$((132),2)$	$((123),0)$	$((1),2)$	$((132),0)$	$((123),2)$
$((13),1)$	$((13),1)$	$((12),3)$	$((23),1)$	$((13),3)$	$((12),1)$	$((23),3)$	$((123),2)$	$((1),0)$	$((132),2)$	$((123),0)$	$((1),2)$	$((132),0)$
$((23),3)$	$((23),3)$	$((13),1)$	$((12),3)$	$((23),1)$	$((13),3)$	$((12),1)$	$((132),0)$	$((123),2)$	$((1),0)$	$((132),2)$	$((123),0)$	$((1),2)$

Laskutaulukosta nähdään, että ryhmä T on suljettu ryhmän $S_3 \otimes \mathbb{Z}_4$ laskutoimituksen suhteen. Havaitaan vielä, että ryhmä T ei ole Abelinen, sillä pätee

$$ab = ((123), 2)((12), 1) = ((13), 3) \neq ((23), 3) = ((12), 1)((123), 2) = ba.$$

□

Lause 6.18. *Mikä tahansa ryhmä G, joka on alkioiden a ja b virittämä siten, että pätee $|a| = 6, a^3 = b^2$ ja $ba = a^{-1}b$ on isomorfinen ryhmän T kanssa.*

Todistus. Hyödynnetään alkioiden a ja b ominaisuuksia ryhmän G laskutaulukon muodostamiseksi. Lasketaan muutamia tuloja esimerkiksi. Koska alkion a kertaluku on $|a| = 6$ saadaan

$$(a^5)(a^2b) = a^7b = ab.$$

Seuraavissa laskutoimituksissa hyödynnetään tietoja $ba = a^{-1}b$ ja $b^2 = a^3$. Pidetään myös mielessä, että pätee $a^{-1} = a^5$. Saadaan siis

$$(b)(a^4) = a^{-1}ba^3 = a^{-2}ba^2 = a^{-3}ba = a^{-4}b = a^2b$$

ja

$$(ab)(ab) = aa^{-1}bb = b^2 = a^3.$$

Lisäksi saadaan

$$(a^5b)(a^4b) = a^5a^{-4}bb = aa^3 = a^4.$$

Ryhmän laskutaulukoksi muodostuu

	e	a	a^2	a^3	a^4	a^5	b	ab	a^2b	a^3b	a^4b	a^5b
e	e	a	a^2	a^3	a^4	a^5	b	ab	a^2b	a^3b	a^4b	a^5b
a	a	a^2	a^3	a^4	a^5	e	ab	a^2b	a^3b	a^4b	a^5b	b
a^2	a^2	a^3	a^4	a^5	e	a	a^2b	a^3b	a^4b	a^5b	b	ab
a^3	a^3	a^4	a^5	e	a	a^2	a^3b	a^4b	a^5b	b	ab	a^2b
a^4	a^4	a^5	e	a	a^2	a^3	a^4b	a^5b	b	ab	a^2b	a^3b
a^5	a^5	e	a	a^2	a^3	a^4	a^5b	b	ab	a^2b	a^3b	a^4b
b	b	a^5b	a^4b	a^3b	a^2b	ab	a^3	a^2	a	e	a^5	a^4
ab	ab	b	a^5b	a^4b	a^3b	a^2b	a^4	a^3	a^2	a	e	a^5
a^2b	a^2b	ab	b	a^5b	a^4b	a^3b	a^5	a^4	a^3	a^2	a	e
a^3b	a^3b	a^2b	ab	b	a^5b	a^4b	e	a^5	a^4	a^3	a^2	a
a^4b	a^4b	a^3b	a^2b	ab	b	a^5b	a	e	a^5	a^4	a^3	a^2
a^5b	a^5b	a^4b	a^3b	a^2b	ab	b	a^2	a	e	a^5	a^4	a^3

Kun valitaan alkio a vastaamaan ryhmän T alkiota $((123), 2)$ ja alkio b ryhmän T alkiota $((12), 1)$, niin ryhmän G laskutaulukko vastaa ryhmän T laskutaulukkoa, joka on näkyvissä Lauseen 6.17 todistuksen yhteydessä. Ryhmä G on siis isomorfinen ryhmän T kanssa.

Osoitetaan vielä esimerkinomaisesti eräät laskutaulukoiden vastinalkiot samoiksi. Tarkastellaan tuloa $(a^3b)(a^5b)$. Koska pätee $ba = a^{-1}b$ ja $b^2 = a^3$, niin voidaan kirjoittaa

$$(a^3b)(a^5b) = a^3a^{-5}bb = a^{-2}b^2 = a^{-2}a^3 = a.$$

Laskutaulukoita vertaamalla voidaan löytää alkiota a^3b vastaava alkio $((12), 3)$, alkiota a^5b vastaava alkio $((23), 3)$ ja alkiota a vastaava alkio $((123), 2)$. Laskutaulukosta nähdään, että näille ryhmän T alkioille pätee edellistä vastaava tulo:

$$((12), 3)((23), 3) = ((123), 2).$$

□

7. Äärellisten ryhmien luokittelusta

Kappaleessa 3 luokiteltiin kaikki äärelliset Abelin ryhmät isomorfiaa vaille. Kappaleessa 5 käytiin puolestaan läpi Sylowin lauseet, jotta myös ei-Abelisten ryhmien luokittelu olisi mahdollista. Edellisissä kappaleissa luotuja työkaluja ollaan nyt valmiita käyttämään, jotta voidaan tässä kappaleessa luokitella kaikki äärelliset ryhmät kertalukuun 15 asti.

Seuraava lause on perusalgebraa ja se on tullut tutkielman aikana useasti esille todistuksineen, vaikka sitä ei erityisesti olekaan korostettu. Kyseinen lause on kuitenkin merkittävässä roolissa, kun luokitellaan äärellisiä alkulukukertalukuisia ryhmiä isomorfiaa vaille. Tämän vuoksi sen muotoilu tässä vaiheessa on vielä perusteltua.

Lause 7.1. *Olkoon p alkuluku. Jos ryhmän G kertaluku on $|G| = p$, niin ryhmä G on syklinen ja isomorfinen ryhmän $\mathbb{Z}_p$ kanssa.*

Todistus. Olkoon ryhmän G kertaluku $|G| = p$ ja alkio $a \in G \setminus \{e\}$. Tällöin ryhmän G syklisen aliryhmän $\langle a \rangle$ kertaluvulle pätee $|\langle a \rangle| > 1$. Lagrangen lauseen nojalla ryhmän $\langle a \rangle$ kertaluvun täytyy jakaa ryhmän G kertaluku p. Koska p on alkuluku, niin täytyy päteä $|\langle a \rangle| = p$. Siispä alkio $a \in G$ virittää koko ryhmän G, jolloin G on syklinen ryhmä ja sen kertaluku on $|G| = p$. Tällöin siis ryhmä G on isomorfinen ryhmän $\mathbb{Z}_p$ kanssa. □

Käydään seuraavaksi läpi joitakin hyödyllisiä yksityiskohtia p-ryhmistä, jotka ovat olennaisessa osassa äärellisten ryhmien luokittelussa isomorfiaa vaille. Tässä vaiheessa on hyvä palauttaa mieleen keskuksen määritelmä 4.15; ryhmän G keskus on siis joukko $Z(G) = \{c \in G : cx = xc \text{ kaikilla } x \in G\}$. Lisäksi pidetään mielessä, että keskus $Z(G)$ on ryhmän G normaali aliryhmä ja jopa Abelin ryhmä. Siispä, jos pätee $G = Z(G)$, niin myös G on Abelin ryhmä.

Lause 7.2. *Olkoon G ryhmä, jonka kertaluku on muotoa $|G| = p^n$, missä p on alkuluku ja $n \geq 1$. Tällöin ryhmän G keskus $Z(G)$ sisältää useamman kuin yhden alkion. Erityisesti pätee $|Z(G)| = p^k$, missä $1 \leq k \leq n$.*

Todistus. Lagrangen lauseen nojalla tiedetään, että $|Z(G)| = p^k$, missä $0 \leq k \leq n$. Täytyy vielä osoittaa, että $k \geq 1$ eli että $|Z(G)| \geq p$. Luokkayhtälön (4.4) nojalla voidaan kirjoittaa keskuksen kertaluku muodossa

$$|Z(G)| = |G| - |T_1| - |T_2| - \cdots - |T_r|,$$

missä $T_1, T_2, \ldots$ ja T_r ovat siis ryhmän G erilliset konjugaattiluokat, joiden kertaluvut $|T_i| > 1$ jakavat kertaluvun $|G|$ kaikilla $i = 1, 2, \ldots, r$. Koska ryhmän G kertaluku on $|G| = p^n$, niin kyseinen kertaluku on jaollinen ainoastaan luvulla 1 ja alkuluvun p potensseilla p^m, missä $1 \leq m \leq n$. Siispä kertaluku $|T_i| > 1$ on jaollinen alkuluvulla p kaikilla $i = 1, 2, \ldots, r$. Ryhmän G kertaluku on myös jaollinen alkuluvulla p, joten seuraa, että kertaluku $|Z(G)| = |G| - |T_1| - |T_2| - \cdots |T_r|$ on jaollinen alkuluvulla p ja pätee $|Z(G)| \geq p$. □

Määritelmä 7.3. Olkoon $G \neq \langle e \rangle$ ryhmä. Ryhmä G on *yksinkertainen*, jos sen ainoat normaalit aliryhmät ovat $\langle e \rangle$ ja G.

Lemma 7.4. *Ryhmä G on yksinkertainen Abelin ryhmä, jos ja vain jos se on isomorfinen additiivisen ryhmän $\mathbb{Z}_p$ kanssa jollakin alkuluvulla p.*

Todistus. Osoitetaan ensin, että jos ryhmä G on isomorfinen ryhmän $\mathbb{Z}_p$ kanssa jollakin alkuluvulla p, niin G on yksinkertainen Abelin ryhmä. Ryhmän G Abelisuus seuraa ryhmän $\mathbb{Z}_p$ vaihdannaisuudesta, sillä isomorfismi säilyttää vaihdannaisuuden. Isomorfisuudesta seuraa, että ryhmän G kertaluku on $|G| = p$. Tällöin edelleen Lagrangen lauseen nojalla minkä tahansa aliryhmän H kertaluvun täytyy jakaa kertaluku $|G| = p$. Siispä pätee $|H| = 1$ tai $|H| = p$, jolloin on $H = \langle e \rangle$ tai $H = G$. Näin ollen ryhmä G on yksinkertainen ja edelleen saadaan, että G on yksinkertainen Abelin ryhmä.

Osoitetaan seuraavaksi väite toiseen suuntaan. Olkoon nyt G yksinkertainen Abelin ryhmä. Koska jokainen Abelin ryhmän aliryhmä on normaali, ryhmällä G ei ole muita aliryhmiä kuin $\langle e \rangle$ ja G. Tästä seuraa, että jos $a \neq e$ on jokin ryhmän G alkio, niin alkio a virittää koko ryhmän G. Toisin sanoen $G = \langle a \rangle$. Koska jokainen ääretön syklinen ryhmä on isomorfinen ryhmän $\mathbb{Z}$ kanssa ja ryhmällä $\mathbb{Z}$ on useita aitoja aliryhmiä, ryhmän $G = \langle a \rangle$ täytyy olla äärellinen eli pätee $|G| = n = |\langle a \rangle|$. Osoitetaan, että kertaluvun n täytyy olla alkuluku. Jos n ei olisi alkuluku eli se voitaisiin kirjoittaa muodossa $n = td$, missä $1 < d < n$, niin tällöin $\langle a^t \rangle$ olisi ryhmän G normaali aliryhmä, jonka kertaluvulle pätisi $|\langle a^t \rangle| = d$ Lemman 4.1 nojalla. Tämä ei ole mahdollista, sillä oletuksen nojalla ryhmä G on yksinkertainen. Siispä G on syklinen p-kertalukuinen ryhmä ja isomorfinen ryhmän $\mathbb{Z}_p$ kanssa. □

Seuraus 7.5. *Olkoon p alkuluku ja $n > 1$. Tällöin ei ole olemassa yksinkertaista ryhmää G, jonka kertaluku on $|G| = p^n$.*

Todistus. Olkoon G ryhmä, jonka kertaluku on $|G| = p^n$. Osoitetaan, että ryhmä G ei ole yksinkertainen. Aiemmin todettiin, että keskus $Z(G)$ on ryhmän G normaali aliryhmä. Jos on $Z(G) \neq G$, niin Lauseesta 7.2 seuraa, että ryhmällä G on aito normaali aliryhmä, jolloin ryhmä G ei voi olla yksinkertainen. Aiemmin todettiin, että jos $Z(G) = G$, niin G on Abelin ryhmä. Koska ryhmän G kertaluku $|G| = p^n$, missä $n > 1$, ei ole alkuluku, niin ryhmä G ei voi olla isomorfinen ryhmän $\mathbb{Z}_q$ kanssa millään alkuluvulla q. Tällöin Lemmasta 7.4 saadaan, että ryhmä G ei ole yksinkertainen. □

Lemma 7.6. *Olkoon G sellainen ryhmä, että tekijäryhmä $G/Z(G)$ on syklinen. Tällöin G on Abelin ryhmä.*

Todistus. Koska $G/Z(G)$ on syklinen, on olemassa alkio $Z(G)g$, joka virittää kyseisen ryhmän eli $G/Z(G) = \langle Z(G)g \rangle$. Erityisesti jokainen ryhmän $G/Z(G)$ sivuluokka on muotoa $(Z(G)g)^k = Z(G)g^k$ jollekin $k \in \mathbb{Z}$. Olkoon $a, b \in G$. Koska voidaan kirjoittaa $a = ea$, niin pätee $a \in Z(G)a$. Lisäksi pätee $Z(G)a = Z(G)g^i$ jollekin $i \in \mathbb{Z}$. Voidaan siis esittää alkio a muodossa $a = c_1 g^i$, missä $c_1 \in Z(G)$. Vastaavasti on $b = c_2 g^j$, missä $c_2 \in Z(G)$ ja $j \in \mathbb{Z}$. Nyt koska pätee yhtäsuuruus

$$g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$$

ja lisäksi alkiot $c_1, c_2 \in Z(G)$ kommutoivat keskuksen määritelmän nojalla kaikkien ryhmän G alkioiden kanssa, niin voidaan kirjoittaa

$$ab = (c_1 g^i)(c_2 g^j) = c_1 c_2 g^i g^j = c_2 c_1 g^j g^i = (c_2 g^j)(c_1 g^i) = ba.$$

Siispä G on Abelin ryhmä. □

Seuraus 7.7. *Olkoon G ryhmä ja p alkuluku. Jos ryhmän G kertaluku on muotoa $|G| = p^2$, niin G on Abelin ryhmä ja isomorfinen ryhmän $\mathbb{Z}_{p^2}$ tai ryhmän $\mathbb{Z}_p \otimes \mathbb{Z}_p$ kanssa.*

Todistus. Lagrangen lauseen ja Lauseen 7.2 nojalla keskuksen $Z(G)$ kertaluku on $|Z(G)| = p$ tai $|Z(G)| = p^2$. Oletetaan ensin, että $|Z(G)| = p^2$. Tällöin pätee $Z(G) = G$, josta seuraa, että G on Abelin ryhmä. Oletetaan seuraavaksi, että $|Z(G)| = p$. Tekijäryhmän $G/Z(G)$ kertaluku on indeksi $[G : Z(G)]$, jolloin Lagrangen lauseesta saadaan

$$|G/Z(G)| = [G : Z(G)] = |G|/|Z(G)| = p^2/p = p.$$

Tällöin Lauseesta 7.1 seuraa, että tekijäryhmä $G/Z(G)$ on syklinen. Edelleen Lemman 7.6 avulla saadaan osoitettua, että G on Abelin ryhmä. Lopulta Äärellisten Abelin ryhmien peruslauseen 3.9 nojalla ryhmä G on isomorfinen ryhmän $\mathbb{Z}_{p^2}$ tai ryhmän $\mathbb{Z}_p \otimes \mathbb{Z}_p$ kanssa. □

Esimerkki 7.8. Seurauksen 7.7 nojalla jokainen ryhmä G, jonka kertaluvulle pätee $|G| = 9 = 3^2$, on isomorfinen ryhmän $\mathbb{Z}_9$ tai ryhmän $\mathbb{Z}_3 \otimes \mathbb{Z}_3$ kanssa. Ehkä tunnetuin esimerkki, johon seurausta voidaan soveltaa, on 4-kertalukuiset ryhmät. Ryhmät, joiden kertaluku on siis $4 = 2^2$, ovat Seurauksen 7.7 nojalla isomorfisia ryhmän $\mathbb{Z}_4$ tai ryhmän $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ kanssa. Tunnetusti ryhmät $\mathbb{Z}_4$ ja $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ eivät ole isomorfisia keskenään. Vastaavasti seurausta voidaan soveltaa myös isommille kertaluvuille. Jos ryhmän G kertaluku on $|G| = 841 = 29^2$, niin ryhmä G on isomorfinen ryhmän $\mathbb{Z}_{841}$ tai ryhmän $\mathbb{Z}_{29} \otimes \mathbb{Z}_{29}$ kanssa.

Lauseessa 5.12 osoitettiin, että pq-kertalukuiset ryhmät, missä p ja q ovat alkulukuja tietyin ehdoin, ovat isomorfisia ryhmän $\mathbb{Z}_{pq}$ kanssa. Jalostetaan kyseistä lausetta edelleen koskemaan ryhmiä, joiden kertaluku on p^2q.

Lause 7.9. *Olkoon p ja q eri alkulukuja siten, että alkuluku p ei jaa lukua $q-1$ eikä alkuluku q lukua p^2-1. Jos ryhmän G kertaluku on $|G| = p^2q$, niin tällöin ryhmä G on isomorfinen ryhmän $\mathbb{Z}_{p^2q}$ tai ryhmän $\mathbb{Z}_p \otimes \mathbb{Z}_p \otimes \mathbb{Z}_q$ kanssa.*

Todistus. Sylowin kolmannen lauseen 5.10 nojalla tiedetään, että ryhmän G Sylowin p-aliryhmien lukumäärä t on muotoa $t = 1 + pk$ jollekin $k = 0, 1, 2, \ldots$ ja t jakaa ryhmän G kertaluvun $|G|$. Koska ryhmän G kertaluku on $|G| = p^2q$, se on jaollinen luvuilla $1, p, p^2, q, pq$ ja p^2q. Sylowin p-aliryhmien lukumäärä voitiin kirjoittaa muodossa $t = 1+pk$, joten yhtölöistä $p = 1+pk$, $p^2 = 1+pk$, $pq = 1+pk$ ja $p^2q = 1+pk$ päädytään ristiriitaan $p|1$. Ainoat vaihtoehdot ovat siis $t = 1$ tai $t = q$. Kuitenkin oletuksen nojalla alkuluku p ei jaa lukua $q-1$, joten ei voi olla $t = q$. Siispä on olemassa ainoastaan yksi Sylowin p-aliryhmä H, joka on normaali Seurauksen 5.9 nojalla.

Vastaavasti Sylowin kolmannesta lauseesta saadaan, että ryhmän G Sylowin q-aliryhmien lukumäärä s on muotoa $s = 1 + qk$ jollekin $k = 0, 1, 2, \ldots$ ja s jakaa kertaluvun $|G| = p^2q$. Yhtälöistä $q = 1 + qk$, $pq = 1 + qk$ ja $p^2q = 1 + qk$ päädytään ristiriitaan $q|1$, jolloin ainoat vaihtoehdot ovat $s = 1$, $s = p$ tai $s = p^2$. Mutta oletuksen nojalla alkuluku q ei jaa lukua $p^2 - 1 = (p + 1)(p - 1)$, joten ei voi olla $s = p$ eikä $s = p^2$. Siispä on olemassa ainoastaan yksi Sylowin q-ryhmä K, joka on normaali.

Ryhmä $H \cap K$ on sekä ryhmän H että ryhmän K aliryhmä. Tällöin kertaluvun $|H \cap K|$ täytyy jakaa molemmat kertaluvut $|H| = p^2$ ja $|K| = q$ Lagrangen lauseen

nojalla, jolloin välttämättä $|H \cap K| = 1$ ja $H \cap K = \langle e \rangle$. Lemmasta 5.11 saadaan, että $|G| = p^2q = |H||K| = |HK|$ eli $G = HK$. Tällöin Lemman 4.5 nojalla pätee $G \cong H \otimes K$. Nyt Seurauksesta 7.7 saadaan, että ryhmä H on isomorfinen joko ryhmän $\mathbb{Z}_{p^2}$ tai ryhmän $\mathbb{Z}_p \otimes \mathbb{Z}_p$ kanssa. Lisäksi ryhmä K on isomorfinen ryhmän $\mathbb{Z}_q$ kanssa Lauseen 7.1 nojalla. Nyt siis pätee

$$G = H \otimes K \cong \mathbb{Z}_{p^2} \otimes \mathbb{Z}_q \quad \text{tai} \quad G = H \otimes K \cong \mathbb{Z}_p \otimes \mathbb{Z}_p \otimes \mathbb{Z}_q.$$

Yhdistämällä edelliset havainnot saadaan Lemman 3.11 avulla ryhmälle G kaksi vaihtoehtoista isomorfismia

$$G \cong \mathbb{Z}_{p^2} \otimes \mathbb{Z}_q \cong \mathbb{Z}_{p^2q} \quad \text{tai} \quad G \cong \mathbb{Z}_p \otimes \mathbb{Z}_p \otimes \mathbb{Z}_q.$$

□

Esimerkki 7.10. Olkoon G ryhmä, jonka kertaluku on $|G| = 99$. Kyseinen kertaluku voidaan kirjoittaa muodossa $|G| = 99 = 9 \times 11 = 3^2 \times 11$. Lisäksi alkuluku 3 ei jaa lukua $11 - 1 = 10$ eikä alkuluku 11 lukua $3^2 - 1 = 8$. Siispä merkitsemällä $p = 3$ ja $q = 11$ havaitaan Lauseen 7.9 oletuksien olevan voimassa, jolloin ryhmä G on kyseisen lauseen nojalla isomorfinen joko ryhmän $\mathbb{Z}_{99}$ tai ryhmän $\mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_{11}$ kanssa.

Lemma 7.11. *Olkoon G ryhmä, jonka kertaluku on $|G| = 12$. Tällöin ryhmä G ei ole yksinkertainen.*

Todistus. Koska ryhmän G kertaluku on $|G| = 12 = 2^2 \times 3$, niin Sylowin 2-aliryhmien kertaluku on 4 ja Sylowin 3-aliryhmien kertaluku 3. Sylowin kolmannen lauseen 5.10 nojalla Sylowin 2-aliryhmien lukumäärä jakaa kertaluvun $|G|$ ja on muotoa $1 + 2k$ jollakin $k = 0, 1, 2, \ldots$. Siispä Sylowin 2-aliryhmien lukumäärä on joko 1 tai 3. Vastaavasti Sylowin kolmannen lauseen nojalla Sylowin 3-aliryhmien lukumäärä jakaa kertaluvun $|G|$ ja on muotoa $1 + 3k$ jollakin $k = 0, 1, 2, \ldots$. Sylowin 3-aliryhmien lukumäärä on siis joko 1 tai 4.

Jos Sylowin 3-aliryhmien lukumäärä on 1, niin Seurauksesta 5.9 saadaan, että tämä ainoa Sylowin 3-aliryhmä on normaali.

Oletetaan nyt, että Sylowin 3-aliryhmien lukumäärä on 4. Kaikkien ryhmän G Sylowin 3-aliryhmien K_1, K_2, K_3 ja K_4 kertaluku on 3. Lisäksi tiedetään, että $K_i \cap K_j$ on sekä ryhmän K_i että ryhmän K_j aliryhmä. Siispä Lagrangen lauseen nojalla leikkaus on joko $\langle e \rangle$ tai pätee $K_i = K_j$. Jälkimmäinen ei ole mahdollinen, joten pätee $K_i \cap K_j = \langle e \rangle$, kun $i \neq j$. Siispä jokainen Sylowin 3-aliryhmä K_i sisältää kaksi alkiota, virittäjäalkion ja sen käänteisalkion, joiden kertaluku on 3 ja jotka eivät sisälly muihin Sylowin 3-aliryhmiin. Näin ollen ryhmä G sisältää $4 \times 2 = 8$ alkiota, joiden kertaluku on 3 ja $|G| - 8 = 12 - 8 = 4$ alkiota, joiden kertaluku ei ole 3. Mikä tahansa ryhmän G Sylowin 2-aliryhmä sisältää $2^2 = 4$ alkiota, joten kyseiset alkiot muodostavat loput ryhmän G alkioista. On siis olemassa ainoastaan yksi 4-kertalukuinen Sylowin 2-aliryhmä, jolloin se Seurauksen 5.9 nojalla on normaali.

Molemmissa tapauksissa ryhmällä G on aito normaali aliryhmä, jolloin ryhmä G ei voi olla yksinkertainen. □

Edellisessä lemmassa osoitettiin Sylowin kolmannen lauseen 5.10 ja Seurauksen 5.9 avulla, että 12-kertalukuinen ryhmä ei ole yksinkertainen. Samaisia työkaluja käyttämällä voidaan useassa tapauksessa osoittaa aidon normaalin aliryhmän olemassaolo

eli se, että ryhmä ei ole yksinkertainen. Tarkastellaan vielä toista havainnollistavaa esimerkkiä.

Esimerkki 7.12. Olkoon G ryhmä, jonka kertaluku on $63 = 3^2 \times 7$. Tällöin jokaisen Sylowin 7-aliryhmän kertaluku on 7. Lisäksi Sylowin kolmannen lauseen nojalla 5.10 näiden aliryhmien lukumäärä jakaa kertaluvun $|G| = 63$ ja on muotoa $1+7k$, jollakin $k = 0, 1, 2, \ldots$. Luku 63 on jaollinen luvuilla $1, 3, 7, 9, 21$ ja 63, joista ainoastaa luku 1 voidaan esittää muodossa $1 + 7k$, kun valitaan $k = 0$. Ryhmällä G on siis ainoastaan yksi Sylowin 7-aliryhmä, joka Seurauksen 5.9 nojalla on normaali. Näin ollen ryhmällä G on aito normaali aliryhmä eli se ei voi olla yksinkertainen. Toisin sanoen, ei ole olemassa yksinkertaista ryhmää, jonka kertaluku on 63.

Seuraus 7.13. *Olkoon p ja q eri alkulukuja. Tällöin ei ole olemassa yksinkertaista ryhmää G, jonka kertaluku on $|G| = p^2q$.*

Todistus. Olkoon G ryhmä, jonka kertaluku on $|G| = p^2q$. Jos alkuluku p ei jaa lukua $(q-1)$ eikä alkuluku q lukua (p^2-1), niin Lauseen 7.9 todistuksessa osoitettiin, että tällöin ryhmällä G on normaali Sylowin aliryhmä eikä G näin ole yksinkertainen. Oletetaan seuraavaksi, että pätee sekä $q|(p^2-1)$ että $p|(q-1)$. Koska alkuluku p jakaa luvun $(q-1)$, niin seurauksena saadaan epäyhtälö $p \leq q-1$, joka on yhtäpitävä epäyhtälön $q \geq p+1$ kanssa. Lisäksi havaitaan, että voidaan kirjoittaa

$$p^2 - 1 = (p-1)(p+1),$$

joten alkuluvun q täytyy jakaa joko luku $(p-1)$ tai $(p+1)$. Aiemmin todettiin, että pätee $q \geq p+1$ eli ainakin $q \nmid (p-1)$. Jos taas alkuluku q jakaisi luvun $(p+1)$, pätisi $q \leq p+1$. Koska aiemmin todettiin, että $q \geq p+1$, täytyy siis olla $q = p+1$. Ainoat alkuluvut, jotka toteuttavat tämän yhtäsuuruuden ovat $p = 2$ ja $q = 3$, sillä luku 2 on ainoa parillinen alkuluku. Lemmasta 7.11 puolestaan saadaan, että ei ole olemassa yksinkertaista ryhmää, jonka kertaluku on $2^2 \times 3 = 12$. □

7.1. **Äärellisten ryhmien luokittelun viimeistelyä.** Viimeistellään ja kootaan yhteen seuraavaksi äärellisten ryhmien luokittelu kertalukuun 15 asti. Jatkossa symbolilla G_k merkitään ryhmää, jonka kertaluku on k.

Lauseen 7.1 avulla saadaan luokiteltua kaikki alkulukukertalukuiset ryhmät. Oletetaan, että G_p on ryhmä, jonka kertaluvulle pätee $|G_p| = p$. Tällöin Lauseen 7.1 nojalla, koska kertaluku $|G_p| = p$ on alkuluku, ryhmä G_p on syklinen ja isomorfinen ryhmän $\mathbb{Z}_p$ kanssa. Siispä tarkastellessa äärellisiä ryhmiä kertalukuun 15 asti, voidaan todeta ryhmien $G_2, G_3, G_5, G_7, G_{11}$ ja G_{13} olevan syklisiä ja isomorfisia ryhmien $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}$ ja $\mathbb{Z}_{13}$ kanssa tässä järjestyksessä.

Lause 7.14. *Olkoon G_4 ryhmä, jonka kertaluku on $|G_4| = 4$. Tällöin ryhmä G_4 on isomorfinen joko ryhmän $\mathbb{Z}_4$ tai ryhmän $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ kanssa.*

Todistus. Ryhmän G_4 kertaluvulle pätee $|G_4| = 4 = 2^2$. Koska 2 on alkuluku, niin Seurauksen 7.7 nojalla ryhmä G_4 on Abelin ryhmä ja edelleen isomorfinen joko syklisen ryhmän $\mathbb{Z}_4$ tai ryhmän $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ kanssa. □

Aiemmin todettiin, että Lauseen 6.8 avulla saadaan isomorfiat äärellisille ryhmille, joiden kertaluku on 6. Muotoillaan tämä kuitenkin vielä lauseeksi.

Lause 7.15. *Olkoon G_6 ryhmä, jonka kertaluku on $|G_6| = 6$. Tällöin ryhmä G_6 on isomorfinen joko ryhmän $\mathbb{Z}_6$ tai ryhmän D_3 kanssa.*

Todistus. Koska ryhmän G_6 kertaluvulle pätee $|G_6| = 6 = 2 \times 3$, missä 3 on pariton alkuluku, Lauseesta 6.8 seuraa, että ryhmä G_6 on tällöin isomorfinen joko syklisen ryhmän $\mathbb{Z}_6$ tai diedriryhmän D_3 kanssa. □

Jotta voidaan täydellisesti luokitella kaikki kertaluvun 8 ryhmät, tarvitaan avuksi Äärellisten Abelin ryhmien peruslausetta 3.9, Lemmaa 6.7 sekä Lemmaa 5.5. Lisäksi pidetään mielessä kvaternioryhmän Q määritelmä.

Lause 7.16. *Olkoon G_8 ryhmä, jonka kertaluku on $|G_8| = 8$. Tällöin ryhmä G_8 on isomorfinen joko ryhmän $\mathbb{Z}_8$, ryhmän $\mathbb{Z}_4 \otimes \mathbb{Z}_2$, ryhmän $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$, diedriryhmän D_4 tai kvaternioryhmän Q kanssa.*

Todistus. Jos ryhmä G_8 on Abelin ryhmä, niin Äärellisten Abelin ryhmien peruslauseen 3.9 nojalla se on isomorfinen ryhmän $\mathbb{Z}_8$, ryhmän $\mathbb{Z}_4 \otimes \mathbb{Z}_2$ tai ryhmän $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ kanssa.

Oletetaan seuraavaksi, että ryhmä G_8 ei ole Abelin ryhmä. Lagrangen lauseesta seuraa, että alkiolla $a \in G_8 \setminus \{e\}$ täytyy olla kertaluku $2, 4$ tai 8. Jos pätisi $|a| = 8$, niin alkio a virittäisi koko ryhmän G_8, jolloin se olisi syklinen ja Abelin ryhmä. Siispä ei-Abelinen ryhmä G_8 ei voi sisältää alkiota, jonka kertaluku on 8. Kaikkien ryhmän G_8 alkioiden kertaluku ei voi myöskään olla 2, sillä muuten pätisi

$$ab = (bb)ab(aa) = b(ba)(ba)a = ba,$$

jolloin G_8 olisi Abelin ryhmä. Täytyy siis olla olemassa alkio $a \in G_8 \setminus \{e\}$, jonka kertaluku on $|a| = 4$. Olkoon b sellainen ryhmän G_8 alkio, että $b \notin \langle a \rangle = \{e, a, a^2, a^3\}$. Koska alkion a kertaluvulle pätee $|a| = 4$ ja yhtälöstä $a^i = a^j b$ saadaan vasemmalta alkiolla a^{-j} molempia puolia kertomalla yhtälö $b = a^{i-j} \in \langle a \rangle$, joka on ristiriidassa alkion b valinnan kanssa, muodostuu ryhmä G_8 seuraavanlaiseksi:

$$G_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Aliryhmän $\langle a \rangle$ kertaluku on $|\langle a \rangle| = 4$, jolloin siis indeksiksi muodostuu

$$[G_8 : \langle a \rangle] = |G|/|\langle a \rangle| = 8/4 = 2.$$

Tällöin Lemman 6.7 nojalla aliryhmä $\langle a \rangle$ on normaali. Lemman 5.5 nojalla $a \mapsto x^{-1}ax$ on isomorfismi, joten se säilyttää alkioiden kertaluvut. Tällöin siis pätee $|a| = |bab^{-1}|$ ja lisäksi ryhmän $\langle a \rangle$ normaaliudesta seuraa, että $bab^{-1} \in \langle a \rangle$. Koska alkion e kertaluku on $|e| = 1$ ja alkion a^2 kertaluku $|a^2| = 2$, pätee joko $bab^{-1} = a$ tai $bab^{-1} = a^3$. Yhtälö $bab^{-1} = a$ johtaa kuitenkin ristiriitaan, sillä siitä seuraisi $ba = ab$, jolloin ryhmä G_8 olisi Abelin ryhmä. Täytyy siis olla $bab^{-1} = a^3 = a^{-1}$ ja edelleen molemmin puolin oikealta alkiolla b kerrottaessa saadaan $ba = a^{-1}b$. Tämän tieto on hyödyllinen kootessa ryhmän G_8 laskutaulukkoa. Saadaan muodostettua esimerkiksi laskutoimitukset

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

Laskutaulukko näyttää siis tähän mennessä seuraavalta:

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab				
ab	ab	b	a^3b	a^2b				
a^2b	a^2b	ab	b	a^3b				
a^3b	a^3b	a^2b	ab	b				

Jotta voidaan täydellisesti täydentää ryhmän G_8 laskutaulukko täytyy selvittää laskutoimitus b^2. Jos pätisi yhtälö $b^2 = a^i b$, niin edelleen saataisiin $b = a^i \in \langle a \rangle$, joka on ristiriidassa oletuksen $b \notin \langle a \rangle$ kanssa. Siispä alkio b^2 on e, a, a^2 tai a^3. Jos pätisi $b^2 = a$, niin tästä seuraisi yhtäsuuruusketju $ab = b^2b = bb^2 = ba$, jolloin siis ryhmä G_8 olisi Abelin ryhmä. Vastaavasti yhtälöstä $b^2 = a^3 = a^{-1}$ seuraisi yhtäsuuruusketju $a^{-1}b = b^2b = bb^2 = ba^{-1}$, jolloin yhtälön molempia puolia sekä vasemmalta että oikealta alkiolla a kertomalla saataisiin $ba = aa^{-1}ba = aba^{-1}a = ab$. Tästä edelleen seuraisi ryhmän G_8 Abelisuus. Siispä täytyy päteä joko $b^2 = e$ tai $b^2 = a^2$. Molemmat vaihtoehdot tuottavat erilaiset ryhmän G_8 laskutaulukot.

Tarkastellaan ensin tapausta, jossa $b^2 = e$ ja täydennetään ryhmän G_8 laskutaulukko.

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Kun valitaan alkio a vastaamaan diedriryhmän D_4 vastapäiväistä kiertoa r ja alkio b peilausta d x-akselin suhteen, niin ryhmän G_8 laskutaulukko vastaa diedriryhmän D_4 laskutaulukkoa, jonka voi nähdä Esimerkistä 6.5. Ryhmä G_8 on siis isomorfinen ryhmän D_4 kanssa.

Jos taas valitaan $b^2 = a^2$, niin ryhmän G_8 laskutaulukko näyttää seuraavalta:

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	a^3b	b	ab	a^2b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	ab	a^2b	a^3b	b
b	b	ab	a^2b	a^3b	a^2	a^3	e	a
ab	ab	a^2b	a^3b	b	a	a^2	a^3	e
a^2b	a^2b	ab	b	a^3b	e	a	a^2	a^3
a^3b	a^3b	b	ab	a^2b	a^3	e	a	a^2

Kvaternioryhmän laskutaulukko taas näyttää seuraavalta:

	I	A	$-I$	$-A$	B	C	$-B$	$-C$
I	I	A	$-I$	$-A$	B	C	$-B$	$-C$
A	A	$-I$	$-A$	I	$-C$	B	C	$-B$
$-I$	$-I$	$-A$	I	A	$-B$	$-C$	B	C
$-A$	$-A$	I	A	$-I$	C	$-B$	$-C$	B
B	B	C	$-B$	$-C$	$-I$	$-A$	I	A
C	C	$-B$	$-C$	B	A	$-I$	$-A$	I
$-B$	$-B$	C	B	$-C$	I	A	$-I$	$-A$
$-C$	$-C$	B	C	$-B$	$-A$	I	A	$-I$

Osoitetaan esimerkinomaisesti eräät laskutaulukoiden vastinalkiot samoiksi. Tarkastellaan tuloa $(a^2b)(a^2b)$. Koska oletuksen nojalla on $a^2 = b^2$ voidaan kirjoittaa

$$(a^2b)(a^2b) = b^2bb^2b = b^2b^2b^2 = a^2a^2a^2 = a^2.$$

Laskutaulukoita vertaamalla voidaan löytää alkiota a^2b vastaava alkio $-B$ ja alkiota a^2 vastaava alkio $-I$. Osoitetaan, että näille kvaternioryhmän alkioille pätee edellistä vastaava tulo:

$$(-B)(-B) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I.$$

Ryhmän G_8 ja kvaternioryhmän Q laskutaulukoita vertailemalla nähdään ryhmien olevan isomorfisia keskenään. Tällöin on siis olemassa alkiota A vastaava alkio a ja alkiota B vastaava alkio b siten, että ryhmälle G_8 pätee myös Määritelmän 6.11 yhteydessä mainitut kvaternioryhmän ominaisuudet $a^4 = e$, $a^2 = b^2$ sekä $ba = a^3b$. □

Lause 7.17. *Olkoon G_9 ryhmä, jonka kertaluvulle pätee $|G_9| = 9$. Tällöin ryhmä G_9 on isomorfinen joko ryhmän $\mathbb{Z}_9$ tai ryhmän $\mathbb{Z}_3 \otimes \mathbb{Z}_3$ kanssa.*

Todistus. Ryhmän G_9 kertaluku voidaan kirjoittaa muodossa $|G_9| = 9 = 3^2$. Koska 3 on alkuluku, niin Seurauksen 7.7 nojalla ryhmä G_9 on Abelin ryhmä ja isomorfinen joko ryhmän $\mathbb{Z}_9$ tai ryhmän $\mathbb{Z}_3 \otimes \mathbb{Z}_3$ kanssa. □

Lause 7.18. *Olkoon G_{10} ryhmä, jonka kertaluku on $|G_{10}| = 10$. Tällöin ryhmä G_{10} on isomorfinen joko ryhmän $\mathbb{Z}_{10}$ tai diedriryhmän D_5 kanssa.*

Todistus. Ryhmän G_{10} kertaluvulle pätee $|G_{10}| = 10 = 2 \times 5$, missä 5 on pariton alkuluku. Tällöin Lauseen 6.8 nojalla ryhmä G_{10} on isomorfinen joko ryhmän $\mathbb{Z}_{10}$ tai diedriryhmän D_5 kanssa. □

Äärellisten Abelin ryhmien peruslauseella saadaan luokiteltua kertaluvun 12 äärelliset Abelin ryhmät. Ei-Abelisia 12-kertalukuisia ryhmiä varten pidetään mielessä diedriryhmä D_6, alternoivien ryhmien käsite ja Lemmassa 6.17 esitelty ryhmä T, jonka kertaluku on myös $|T| = 12$. Osoitetaan lisäksi, että nämä 12-kertalukuiset ei-Abeliset ryhmät eivät ole keskenään isomorfisia. Lauseen 7.20 todistus nojautuu osin lähteeseen [7].

Lemma 7.19. *Mitkään ryhmistä D_6, A_4 ja T eivät ole keskenään isomorfisia.*

Todistus. Ryhmät D_6 ja A_4 eivät ole keskenään isomorfisia, sillä alkion $r \in D_6$ kertaluku on $|r| = 6$, mutta kuten Esimerkissä 6.15 huomautettiin, ryhmä $A_4 \subset S_4$ ei sisällä alkiota, jonka kertaluku on 6.

Vastaavasti voidaan osoittaa, että A_4 ei ole isomorfinen ryhmän T kanssa. Tiedetään nimittäin, että alkion $(123) \in S_3$ kertaluku on $|(123)| = 3$ ja alkion $2 \in \mathbb{Z}_4$ kertaluku $|2| = 2$. Koska lukujen 2 ja 3 pienin yhteinen jaettava on 6, alkion $a = ((123), 2) \in T$ kertaluku on $|a| = |((123), 2)| = 6$, mutta ryhmä A_4 ei sisällä 6-kertalukuista alkiota.

Osoitetaan vielä, että ryhmät D_6 ja T eivät myöskään voi olla keskenään isomorfisia. Tiedetään, että alkion $(12) \in S_3$ kertaluku on $|(12)| = 2$ ja alkion $1 \in \mathbb{Z}_4$ kertaluku $|1| = 4$. Koska lukujen 2 ja 4 pienin yhteinen jaettava on 4, alkion $b = ((12), 1) \in T$ kertaluku on $|b| = |((12), 1)| = 4$. Ryhmä D_6 ei sen sijaan sisällä 4-kertalukuista alkiota. Sen alkioiden kertaluvut ovat $|e| = 1, |r| = 6, |r^2| = 3, |r^3| = 2, |r^4| = 3, |r^5| = 6$ ja $|r^i d| = 2$ kaikille $i \in \{0, 1, \ldots, 5\}$, sillä pätee $(r^i d)^2 = r^i d r^i d = r^i r^{-i} dd = d^2 = e$. □

Lause 7.20. *Olkoon G_{12} ryhmä, jonka kertaluku on $|G_{12}| = 12$. Tällöin ryhmä G_{12} on isomorfinen ryhmän $\mathbb{Z}_{12}$, ryhmän $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3$, alternoivan ryhmän A_4, diedriryhmän D_6 tai ryhmän T kanssa.*

Todistus. Oletetaan ensin, että ryhmä G_{12} on Abelin ryhmä. Tällöin Äärellisten Abelin ryhmien peruslauseen 3.9 nojalla ryhmä G_{12} on isomorfinen ryhmän $\mathbb{Z}_{12}$ tai ryhmän $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3$ kanssa. Sivuhuomautuksena on hyvä pistää merkille, että tämä Lause 7.20 ei sisällä ryhmän G_{12} isomorfioita $\mathbb{Z}_3 \otimes \mathbb{Z}_4$ ja $\mathbb{Z}_2 \otimes \mathbb{Z}_6$. Tämä johtuu siitä, että Lemman 3.11 nojalla pätee

$$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \otimes \mathbb{Z}_4 \quad \text{ja} \quad \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_6.$$

Oletetaan nyt, että ryhmä G_{12} ei ole Abelin ryhmä. Sen kertaluku voidaan kirjoittaa muodossa $|G_{12}| = 12 = 2^2 \times 3$. Olkoon lisäksi $S_t = \{K_1, K_2, \ldots, K_t\}$ ryhmän G_{12} Sylowin 3-aliryhmien joukko. Sylowin kolmannen lauseen 5.10 nojalla Sylowin 3-aliryhmien lukumäärän t täytyy jakaa kertaluku $|G_{12}| = 12 = 2^2 \times 3$. Toisaalta luvulle t pätee $t = 1 + 3k$ jollekin $k = 0, 1, 2, \ldots$. Siispä Sylowin 3-aliryhmien lukumäärä on joko $t = 1$ tai $t = 4$.

Tarkastellaan aluksi tapausta $t = 4$. Tällöin Lauseen 6.16 nojalla ryhmä G_{12} on isomorfinen alternoivan ryhmän A_4 kanssa.

Otetaan seuraavaksi tarkasteluun tapaus $t = 1$. Tällöin K_1 on ryhmän G_{12} ainoa Sylowin 3-aliryhmä ja Seurauksen 5.9 nojalla ryhmän G_{12} normaali aliryhmä. Siispä ryhmä G_{12} sisältää ainoastaan 2 alkiota, joiden kertaluku on 3. Jos $c \in G$ on toinen näistä alkioista, niin sen konjugaattien kertaluku on 3, jolloin konjugaattiluokan

$$T(c) = \{g \in G_{12} : g = x^{-1}cx \quad \text{jollakin} \quad x \in G_{12}\}$$

alkioiden lukumäärä on joko 1 tai 2. Siispä edelleen Lauseen 4.13 nojalla pätee joko $[G_{12} : C(c)] = 1$ tai $[G_{12} : C(c)] = 2$ ja Lagrangen lauseen nojalla keskittäjän $C(c)$ kertaluku on joko $|C(c)| = 12$ tai $|C(c)| = 6$. Tällöin molemmissa tapauksissa on Seurauksen 5.4 nojalla olemassa alkio $d \in C(c)$, jonka kertaluvulle pätee $|d| = 2$. Koska alkiot c ja d kommutoivat keskenään ja kertaluvut ovat $|c| = 3$ ja $|d| = 2$, voidaan kirjoittaa

$$(cd)^{3k} = c^{3k} d^{3k} = d^{3k} = e,$$

jos ja vain jos $2|3k$ eli $2|k$. Toisaalta voidaan kirjoittaa

$$(cd)^{2k} = c^{2k} d^{2k} = c^{2k} = e,$$

jos ja vain jos $3|2k$ eli $3|k$. Tällainen lukujen 2 ja 3 pienin yhteinen jaettava on $k = 6$, joten alkion cd kertaluvulle pätee $|cd| = 6$.

Olkoon nyt $a = cd$. Tällöin Lagrangen lauseen nojalla

$$[G_{12} : \langle a \rangle] = |G|/|\langle a \rangle| = 12/6 = 2$$

eli ryhmä $\langle a \rangle$ on Lemman 6.7 nojalla ryhmän G_{12} normaali aliryhmä ja tekijäryhmän $G_{12}/\langle a \rangle$ kertaluku on ryhmän $\langle a \rangle$ erillisten oikeiden sivuluokkien lukumäärä eli $|G_{12}/\langle a \rangle| = [G_{12} : \langle a \rangle] = 2$. Tällöin on siis olemassa alkio $b \in G_{12}$ siten, että pätee $b \notin \langle a \rangle$, $b \neq e$ ja $b^2 \in \langle a \rangle$. Jos nimittäin olisi $b^2 \notin \langle a \rangle$, niin erillisten oikeiden sivuluokkien $\langle a \rangle e$ ja $\langle a \rangle b$ lisäksi olisi olemassa kolmas erillinen oikea sivuluokka $\langle a \rangle b^2$. Lisäksi ryhmän $\langle a \rangle$ normaaliuden nojalla pätee $ba = a^i b$ jollekin $i \in \{0, 1, \ldots, 5\}$ eli $bab^{-1} \in \langle a \rangle$. Osoitetaan, että ainoa vaihtoehto on $bab^{-1} = a^5$. Jos olisi $bab^{-1} = e$, niin kertomalla yhtälön molempia puolia ensin oikealta alkiolla b ja sitten vasemmalta alkiolla b^{-1} päädyttäisiin yhtäsuuruuteen $a = e$, joka ei ole mahdollinen. Yhtäsuuruus $bab^{-1} = a$ taas johtaisi ryhmän G_{12} Abelisuuteen. Vaihtoehdot $bab^{-1} = a^2$ ja $bab^{-1} = a^4$ eivät myöskään ole mahdollisia, sillä molemmista seuraa, että alkion bab^{-1} kertaluku on $|bab^{-1}| = 3$. Tällöin edelleen pätisi $bab^{-1}bab^{-1}bab^{-1} = ba^3b^{-1} = e$, joka ei ole mahdollista, sillä alkion a kertaluku on $|a| = 6$. Vastaavasti yhtäsuuruudesta $bab^{-1} = a^3$ seuraa, että alkion bab^{-1} kertaluku on $|bab^{-1}| = 2$, jolloin yhtälö $bab^{-1}bab^{-1} = ba^2b^{-1} = e$ tuottaa ristiriidan, sillä alkion a kertaluku on $|a| = 6$. Siispä koska G_{12} ei ole Abelin ryhmä ja alkion a kertaluku on $|a| = 6$, täytyy pätеä $bab^{-1} = a^5 = a^{-1}$. Tällöin kertomalla saadun yhtälön molempia puolia oikealta alkiolla b, saadaan $ba = a^{-1}b$.

Tarkastellaan nyt alkiota $b^2 \in \langle a \rangle$. Alkiolle b^2 pätee $b^2 = a^i$ jollekin $i \in \{0, 1, \ldots, 5\}$. Alkiolle b^2 ei voi kuitenkaan päteä $b^2 = a$ tai $b^2 = a^5 = a^{-1}$, sillä molemmista seuraa, että alkion b kertaluku olisi $|b| = 12$, jolloin ryhmä G_{12} olisi Abelinen. Myös vaihtoehdot $b^2 = a^2$ tai $b^2 = a^4$ johtavat ristiriitaan, sillä molemmista seuraa, että alkion b kertaluku olisi $|b| = 6$. Kertomalla yhtälön $b^2 = a^2$ molempia puolia oikealta alkiolla b saadaan $a^2b = b^3$. Tällöin täytyisi päteä $|b^3| = |a^2b| = 2$ eli $a^2ba^2b = a^2a^{-1}bab = a^2a^{-1}a^{-1}bb = bb = e$, joka ei ole mahdollista, sillä saatiin $|b| = 6$. Vastaavasti kertomalla yhtälön $b^2 = a^4$ molempia puolia oikealta alkiolla saadaan $a^4b = b^3$. Tällöin täytyisi päteä $|b^3| = |a^4b| = 2$ eli $a^4ba^4b = a^4a^{-4}bb = bb = e$, joka ei ole mahdollista, sillä saatiin $|b| = 6$ Siispä ainoat vaihtoehdot ovat $b^2 = e$ ja $b^2 = a^3$. Päädytään siis kahteen lopputulemaan:

(1) joko pätee $|a| = 6, b^2 = e$ ja $ba = a^{-1}b$, jolloin G_{12} on Lauseen 6.4 nojalla isomorfinen ryhmän D_6 kanssa.
(2) tai pätee $|a| = 6, b^2 = a^3$ ja $ba = a^{-1}b$, jolloin G_{12} on Lauseen 6.18 nojalla isomorfinen ryhmän T kanssa.

□

Lause 7.21. *Olkoon G_{14} ryhmä, jonka kertaluvulle pätee $|G_{14}| = 14$. Tällöin ryhmä G_{14} on isomorfinen joko ryhmän $\mathbb{Z}_{14}$ tai diedriryhmän D_7 kanssa.*

Todistus. Ryhmän G_{14} kertaluku voidaan kirjoittaa muodossa $|G_{14}| = 14 = 2 \times 7$, missä 7 on pariton alkuluku. Siispä Lauseen 6.8 nojalla ryhmä G_{14} on isomorfinen joko ryhmän $\mathbb{Z}_{14}$ tai diedriryhmän D_7 kanssa. □

Lause 7.22. *Olkoon G_{15} ryhmä, jonka kertaluvulle pätee $|G_{15}| = 15$. Tällöin ryhmä G_{15} on isomorfinen ryhmän $\mathbb{Z}_{15}$ kanssa.*

Todistus. Ryhmän G_{15} kertaluvulle pätee $|G_{15}| = 15 = 3 \times 5$, missä 3 ja 5 ovat alkulukuja siten, että pätee $5 > 3$ ja alkuluku 3 ei jaa lukua $5 - 1 = 4$. Tällöin Seurauksen 5.12 nojalla ryhmä G_{15} on isomorfinen ryhmän $\mathbb{Z}_{15}$ kanssa. □

Nyt ollaan saatu luokiteltua isomorfiaa vaille kaikki äärelliset ryhmät kertalukuun 15 asti. Kertaluvun 16 ryhmiä on 14 erilaista [14, s. 20]. Niiden läpikäyminen on tekninen ja pitkä todistus, vaikka apuna voidaankin käyttää tämän tutkielman aikana luotuja työkaluja. Kyseinen todistus vaatisi myös uusien ryhmien esittelyä. Lisäksi esimerkiksi 64-kertalukuisia ryhmiä on 294 [11, s. 617] ja 128-kertalukuisia ryhmiä 2358 [8, s. 138]. Kun ylitetään kertaluku 15, ryhmien luokittelu käy siis huomattavasti työläämmäksi eivätkä tutkielman aikana luodut tulokset ole yksinään riittäviä siihen. Ne muodostavat silti perustan äärellisten ryhmien luokittelulle.

Viitteet

[1] Artin, Michael, *Algebra*. Prentice-Hall, Inc. Upper Saddle River, New Jersey. 1991.

[2] Axler, Sheldon Jay, *Linear algebra done right*. Springer. 1999.

[3] Dummit, David S. & Foote, Richard M., *Abstract Algebra*. John Wiley & Sons, Inc. Third Edition, 2004.

[4] Eisenhart, Luther P., *Continuous Groups of Transformations*. Princeton University Press. 1933.

[5] Gilbert, William J., *Modern Algebra with Applications*. John Wiley & Sons, Inc. 1976.

[6] Hungerford, Thomas W., *Abstract Algebra: An Introduction*. Brooks/Cole, Cengage Learning. Third Edition, 2013.

[7] Hungerford, Thomas W., *Algebra*. Springer-Verlag New York Inc. 1974.

[8] James, Rodney & Newman, M.F. & O'Brien, E.A. *The Groups of Order 128*. Journal of Algebra, Vol. 129, pp. 136–158, 1990.

[9] Kronecker, Leopold, *Auseinandersetzung einiger Eigenschaften der Klassenzahl idealer komplexer Zahlen*. Monatshefte der Berliner Akademie, pp. 881–889, 1870.

[10] Metsänkylä, Tauno & Näätänen, Marjatta, *Algebra*. Limes ry. 2. korjattu painos. 2005.

[11] Miller, G.A., *Determination of All the Groups of Order 64*. American Journal of Mathematics, Vol. 52, pp. 617–634, 1930.

[12] Sylow, M.L., *Théorèmes sur les groupes de substitutions*. Mathematische Annalen, Vol. 5, pp. 584–594, 1872.

[13] van der Waerden, B.L., *A History of Algebra*. Springer-Verlag, Berlin. 1985.

[14] Wild, Marcel, *The Groups of Order Sixteen Made Easy*. The American Mathematical Monthly, Vol. 112, pp. 20–31, 2005.