TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Aleksi Heiskanen

Sylowin lauseet äärellisten ryhmien teoriassa

Luonnontieteiden tiedekunta
Matematiikka
Marraskuu 2017

Tampereen yliopisto
Luonnontieteiden tiedekunta
HEISKANEN, ALEKSI: Sylowin lauseet äärellisten ryhmien teoriassa
Pro gradu -tutkielma, 101 s.
Matematiikka
Marraskuu 2017

Tiivistelmä

Tutkielmassa perehdytään äärellisten ryhmien teoriaan erityisesti Sylowin lauseiden näkökulmasta. Sylowin lauseet täsmentävät äärellisten ryhmien rakennetta ja ovat perustavaa laatua oleva tulos äärellisten ryhmien luokittelun taustalla. Niiden avulla voidaan hahmottaa, minkälaisia tietyn kertaluvun omaavat äärelliset ryhmät ovat. Sylowin lauseet kertovat, että alkuluvulla p jaollista kertalukua olevat ryhmät sisältävät kaikki Lagrangen lauseen perusteella mahdolliset p-aliryhmät. Toisaalta niiden mukaan kaikki ryhmän Sylowin p-aliryhmät ovat konjugaatteja keskenään. Jos ryhmän kertaluku on muotoa $p^r m$, missä p on alkuluku, p ja m ovat keskenään jaottomia, ja r ja m ovat positiivisia kokonaislukuja, niin lauseiden perusteella ryhmän Sylowin p-aliryhmien lukumäärä jakaa luvun m ja on luvun m kanssa kongruentti modulo p.

Äärellisten ryhmien teoriaan tullaan johdattelemaan tuomalla aluksi esiin joukkoopillisia perusmääritelmiä, kuten relaatio ja kuvaus. Määritellään ryhmä ja tutkielmassa keskeisessä osassa olevan kertaluvun käsite. Tutustutaan permutaatioryhmiin ja käydään läpi aliryhmän, syklisen ryhmän, normaalin aliryhmän ja yksinkertaisen ryhmän käsitteet. Todistetaan myös alternoivan ryhmän yksinkertaisuus. Kohdistetaan tarkastelu edelleen kuvauksiin, joita ovat ryhmien väliset isomorfiat, ja todistetaan kolme isomorfialausetta.

Tutkielman keskiössä ovat ryhmätoiminnat, joiden avulla tullaan todistamaan Sylowin lauseet. Määritellään erityisen hyödyllinen ryhmän toiminta, konjugaatio, jota käytetään Sylowin lauseiden todistukseen ja sen avulla määritellään joukon normalisoijan ja keskittäjän käsitteet. Todistetaan lisäksi Cauchyn lause ja määritellään p-ryhmän ja Sylowin p-aliryhmän käsitteet.

Sylowin lauseiden hyödyllisyyttä tutkitaan tarkastelemalla äärellisten ryhmien yksinkertaisuutta. Osoitetaan, että ryhmät kertaluvuilla 1–100 eivät ole yksinkertaisia tai ovat vaihdannaisia kertalukua 60 lukuun ottamatta. Todistetaan myös, että alternoiva ryhmä A_5 on isomorfiaa vaille ainoa ryhmä, jonka kertaluku 60. Edelleen Sylowin lauseita käytetään ryhmien luokittelussa. Tullaan luokittelemaan isomorfiaa vaille erilaiset ryhmät kertaluvuilla 1–10 ja osoittamaan, että kertaluvun pqr omaava ryhmä, missä p, q ja r ovat eri alkulukuja, on syklinen alkuluvuille asetetuin tietyin jaollisuusehdoin.

Sisältö

Johdanto

Äärellisten ryhmien teoria on abstraktin algebran osa-alue, joka tarkastelee äärellisiä ryhmiä eli sellaisia ryhmiä, joilla on äärellinen määrä alkioita. Ryhmät ovat algebrallisia struktuureita, jonka muodostavat joukko ja joukossa määritelty laskutoimitus. Sylowin lauseet täsmentävät äärellisten ryhmien rakennetta ja auttavat luokittelemaan äärellisiä ryhmiä isomorfian perusteella. Äärellisten ryhmien esityksiin erikoistunut matemaatikko Geoffrey Robinson onkin sanonut, että ryhmäteoreetikolle Sylowin lauseet ovat perustyöväline, joita käytetään melkein ajattelematta, aivan kuin ne olisivat osa hengitystä (ks. [2, s. 1]).

Sylowin lauseita on kokonaisuudessaan kolme. Ensimmäisen mukaan jokaisella alkuluvulla p jaollisella ryhmällä on olemassa kaikki Lagrangen lauseen perusteella mahdolliset p-aliryhmät. Toisen Sylowin lauseen nojalla ryhmän Sylowin p-aliryhmät muodostavat täsmälleen yhden konjugaattiluokan. Ryhmän Sylowin p-aliryhmä on kyseisen ryhmän maksimaalinen p-aliryhmä. Kolmas lause määrittää puolestaan käyttöön hyödyllisen kongruenssin, joka auttaa täsmentämään sitä, kuinka monta Sylowin p-aliryhmää äärellisessä ryhmässä on.

Sylowin lauseet on nimetty norjalaisen matemaatikon Peter Ludvig Mejdell Sylowin mukaan. Hän julkaisi tulokset artikkelissaan *Théorèms sur les groupes de substitution* [20] vuonna 1872. Myöhemmin Sylowin kolmatta lausetta ovat yleistäneet vielä Ferdinand G. Frobenius vuonna 1895 ja Louis Weisner vuonna 1935 (ks. [3]).

Luvussa 1 käydään läpi joukko-opin ja ryhmien peruskäsitteitä, joista tärkeimpiä ovat relaatio, kuvaus, ryhmä ja kertaluku. Lisäksi tässä luvussa osoitetaan joukon laskutoimitukselle yleinen liitäntälaki. Luku 2 käsittelee permutaatioryhmiä, erityisesti sellaista permutaatioryhmää, joka sisältää kaikki joukon permutaatiot eli symmetriaryhmää. Osoitetaan, että jokainen symmetriaryhmän permutaatio voidaan esittää yksikäsitteisesti syklien tulona. Edelleen todistetaan vaihtojen lukumäärän olevan jokaisessa permutaatiossa joko parillinen tai pariton. Luvun 3 sisältö rakentuu aliryhmän, syklisen ryhmän, normaalin aliryhmän ja yksinkertaisen ryhmän käsitteiden ympärille. Tässä luvussa lukijan oletetaan tietävän nämä ryhmäteorian peruskäsitteet, minkä vuoksi monet tulokset esiintyvät ilman todistusta. Tämän luvun päätuloksena voidaan pitää alternoivan ryhmän yksinkertaisuutta tarkastelevaa tulosta. Luvussa 4 osoitetaan yhtä mahtavien ryhmien välisten ominaisuuksien säilyttävän kuvauksen eli isomorfismin avulla Cayleyn lause, jonka mukaan jokainen ryhmä voidaan nähdä permutaatioryhmänä. Lisäksi todistetaan kolme isomorfialausetta.

Tutkielman keskiössä ovat ryhmätoiminnat, sillä niiden avulla todistetaan Sylowin lauseet. Näitä käsitellään luvussa 5. Tässä luvussa esitetään ja todistetaan ryhmätoimintojen luokkayhtälö, joka näyttää erittäin hyödyllisen esitystavan ryhmän toimintaan liittyvälle äärelliselle ja epätyhjälle joukolle, erityisesti siis kyseisen joukon alkioiden lukumäärälle. Ryhmätoimintojen kautta tullaan myös osoittamaan, että äärellisen indeksin omaavan aliryhmän keskiön muodostama tekijäryhmä voidaan

upottaa sellaiseen symmetriaryhmään, jonka joukon kertaluku vastaa tätä indeksiä. Luvussa 6 todistetaan ensin Caychyn lause ja esitetään p-ryhmän käsite. Caychyn lauseen ja ryhmätoimintojen avulla todistetaan Sylowin lauseet ja määritellään yksi tutkielman tärkeimmistä käsitteistä eli Sylowin p-aliryhmä. Lopulta, luku 7 käsittelee Sylowin lauseiden sovelluksia äärellisten yksinkertaisten ryhmien sekä äärellisten ryhmien luokittelun näkökulmasta.

Lukijan oletetaan tuntevan lukuteorian perusteet, eikä siihen liittyviä käsitteitä ja tuloksia esitellä tässä tutkielmassa. Suurin osa tutkielman havainnollistavista esimerkeistä on joko lähdeteosten harjoitustehtäviä tai tekijän itsensä kehittämiä. Lähdeviittauksettomat todistukset ovat tekijän todistamia, eikä niihin näin ollen ole suoraa lähdeviittausta. Tutkielman päälähteinä on käytetty D. S. Malikin, John M. Mordesonin ja M. K. Senin sekä John S. Rosen teoksia *Fundamentals of Abstract Algebra* [11] ja *A Course on Group Theory* [18].

Käytettyjä merkintöjä

Merkintä	**Selitys**
$:=$	Määritellään samaksi kuin
$\square$	Todistus päättyy
$x \in A$	x on joukon A alkio
$A \subseteq B$	Joukko A on joukon B osajoukko
$A \subset B$	Joukko A on joukon B aito osajoukko
$\bigcup \mathcal{A}$	Perheen $\mathcal{A}$ yhdiste, $\bigcup \mathcal{A} = \{ x \mid \exists A \in \mathcal{A}(x \in A) \}$
$\bigcap \mathcal{A}$	Perheen $\mathcal{A} \neq \emptyset$ leikkaus, $\bigcap \mathcal{A} = \{ x \mid \forall A \in \mathcal{A}(x \in A) \}$
(a, b)	Joukkojen a ja b järjestetty pari, $(a, b) = \{\{a\}, \{a, b\}\}$
$A \times B$	Joukkojen A ja B karteesinen tulo, $A \times B = \{(a, b) \mid a \in A, b \in B\}$
$\mathcal{P}(A)$	Joukon A kaikkien osajoukkojen joukko eli potenssijoukko
$\bigtimes \mathcal{A}$	Perheen $\mathcal{A}$ yleinen karteesinen tulo
$f \colon A \to B$	Kuvaus f joukolta A joukkoon B
id_A	Joukon A identtinen kuvaus, $\mathrm{id}_A \colon A \to A, \mathrm{id}_A(x) = x$
$\mathrm{dom}(f)$	Kuvauksen f määrittelyjoukko, $\mathrm{dom}(f) = \{ a \mid \exists b \, (f(a) = b) \}$
$\mathrm{ran}(f)$	Kuvauksen f arvojoukko, $\mathrm{ran}(f) = \{ b \mid \exists a \, (f(a) = b) \}$
$f \restriction A$	Kuvauksen $f \colon A' \to B$ rajoittuma joukkoon $A \subseteq A'$, $f \restriction A = \{ (a, b) \in f \mid a \in A \}$
$f[A]$	Joukon $A \subseteq A'$ kuva kuvauksessa $f \colon A' \to B$, $f[A] = \{f(a) \mid a \in A\}$
$f^{-1}[B]$	Joukon $B \subseteq B'$ alkukuva kuvauksessa $f \colon A \to B'$, $f^{-1}[B] = \{a \in A \mid f(a) \in B\}$
$A \approx B$	Joukot A ja B ovat yhtämahtavat
f^{-1}	Kääntyvän kuvauksen f eli bijektion käänteiskuvaus
$\mathbb{N}$	Luonnollisten lukujen 0,1,2, . . . joukko
$\mathbb{Z}$	Kokonaislukujen . . ., -2,-1,0,1,2, . . . joukko
$\mathbb{Z}_+$	Positiivisten kokonaislukujen 1,2,3, . . . joukko
$\mathbb{R}$	Reaalilukujen joukko
$\mathbb{C}$	Kompleksilukujen joukko
$\lvert G \rvert$	Äärellisen ryhmän G kertaluku eli ryhmän alkioiden lukumäärä
$\mathrm{ord}(g)$	Ryhmän alkion g kertaluku, joka on pienin positiivinen kokonaisluku n, jolle $g^n = e$
$\mathrm{syt}(a, b)$	Lukujen a ja b suurin yhteinen tekijä
$\mathrm{pyj}(a, b)$	Lukujen a ja b pienin yhteinen jaettava
$a \equiv b \pmod{n}$	Luvut a ja b ovat kongruentteja modulo n
$\mathbb{Z}_n$	Jäännösluokkien joukko modulo n

$\mathbb{Z}_n^*$	$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n \mid \text{syt}(a, n) = 1\}$
S_X	Joukon X symmetriaryhmä
I_n	$I_n = \{1, 2, \ldots, n\}$
S_n	Joukon I_n symmetriaryhmä
(1)	Symmetriaryhmän S_n neutraalialkio
$(i_1\ i_2\ \cdots\ i_k)$	Symmetriaryhmän S_n k-sykli
$\epsilon(\alpha)$	Symmetriaryhmän S_n permutaation α merkki
A_n	Alternoiva ryhmä
G, G', H, K, L	Käytettyjä merkintöjä ryhmille
$H \leqslant G$	H on ryhmän G aliryhmä
$H < G$	H on ryhmän G aito aliryhmä
$\langle S \rangle$	Joukon S virittämä aliryhmä
$\langle g \rangle$	Ryhmän alkion g virittämä syklinen ryhmä
D_n	Asteen $n \geq 3$ diedriryhmä
$H_1 H_2 \cdots H_n$	Ryhmän G osajoukkojen $H_1, H_2, \ldots, H_n$ tulo
G/H	Kaikkien aliryhmän H vasempien sivuluokkien joukko, $G/H = \{gH \mid g \in G\}$
$(G : H)$	Aliryhmän H indeksi ryhmässä G, $(G : H) = \lvert G/H \rvert$
$H \trianglelefteq G$	H on ryhmän G normaali aliryhmä
$H \triangleleft G$	H on ryhmän G aito normaali aliryhmä
$G \cong G'$	Ryhmät G ja G' ovat isomorfiset
$\text{Ker}(f)$	Homomorfismin $f\colon G \to G'$ ydin, $\text{Ker}(f) = \{g \in G \mid f(g) = e'\}$
$\text{Im}(f)$	Homomorfismin $f\colon G \to G'$ kuva, $\text{Im}(f) = f[G]$
$\text{Aut}(G)$	Ryhmän G kaikkien automorfismien joukko
$\text{Inn}(G)$	Ryhmän G kaikkien sisäisten automorfismien joukko
$\mathcal{O}_x$	Epätyhjän joukon X alkion x määräämä ryhmän G rata
$\text{Stab}_G(x)$	Alkion $x \in X$ stabilisaattori, $\text{Stab}_G(x) = \{\, g \in G \mid gx = x \,\}$
H_G	Aliryhmän H keskiö ryhmässä G, $H_G = \bigcap_{x \in G} xHx^{-1}$
$\text{Fix}_X(G)$	Ryhmän G kiinnittämä joukon X osajoukko, $\text{Fix}_X(G) = \{x \in X \mid gx = x \text{ kaikilla } g \in G\}$
$Z(G)$	Ryhmän G keskus, $Z(G) = \{\, g \in G \mid xg = gx \text{ kaikilla } x \in G \,\}$
$\mathcal{L}(G)$	Kaikkien ryhmän G epätyhjien osajoukkojen perhe
U^g, x^g	Ryhmän G osajoukon U ja alkion x konjugaatit gUg^{-1} ja gxg^{-1}
$C_l(U), C_l(x)$	Ryhmän G osajoukon U ja alkion x konjugaattiluokat
$C(U), C(x)$	Ryhmän G osajoukon U ja alkion x keskittäjät
$N(U)$	Ryhmän G osajoukon U normalisoija, $N(U) = \{\, g \in G \mid U^g = U \,\}$
P, Q, R	Tyypillisiä merkintöjä Sylowin p-, q- ja r-aliryhmille
$\text{Syl}_p(G)$	Ryhmän G kaikkien Sylowin p-aliryhmien muodostama perhe
n_p	Ryhmän G Sylowin p-aliryhmien lukumäärä

1 Esitietoja

Luvussa 1 tarkoituksena on luoda lukijalle riittävä joukko-opillinen ja ryhmäteoreettinen pohjatieto jatkossa esille tulevien tulosten todistamista varten. Esitetään joukko-opillisia peruslähtökohtia ryhmäteorialle ja määritellään ryhmä sekä tutkielmassa keskiössä olevan kertaluvun käsite. Lähtökohtana joukko-opissa on ZFC:n mukainen aksiomaattinen lähestymistapa. Joukko-opillisesti oleellisimpia määriteltäviä käsitteitä ovat relaatio, ositus, ekivivalenssirelaatio, kuvaus ja karteesinen tulo. Luvun tärkeimpinä tuloksina pidetään lauseita 1.13, 1.21 ja 1.29, joista jälkimmäiseen annetaan myös täsmällinen todistus.

Useisiin esitettyihin tuloksiin ei esitetä tässä luvussa todistuksia, vaan ne sivuutetaan tunnetuiksi oletettuina tuloksina. Tämän luvun rakenne noudattaa pääosin, ja erityisesti alaluvun 1.1 osalta, Scottin teoksen *Group Theory* [19, s. 1–4] rakennetta.

1.1 Joukko-oppia ja tarvittavia peruskäsitteitä

Tarkasti ottaen joukot voidaan määritellä aksiomaattisesti Zermelo-Fraenkelin (mukaan luettuna valinta-aksiooma) joukko-opin eli lyhyesti ZFC:n mukaan (ks. [7, s. 8–12]). Perusajatus on, että joukot määräytyvät alkioistaan. Kaikille joukoille A ja B pätee tällöin, että $A = B$, jos ja vain jos $x \in A \Leftrightarrow x \in B$ kaikilla joukoilla x. Tämän ekstensionaalisuusaksiooman lisäksi on muitakin aksioomia, joita ei tässä kuitenkaan esitetä.

Tässä tutkielmassa käsitellään pääasiassa vain äärellisiä joukkoja, ja myöhemmin samaten äärellisiä ryhmiä. Joukkoa kutsutaan *äärelliseksi*, kun se sisältää äärellisen määrän alkioita.

Määritelmä 1.1. Äärellisen joukon A alkioiden lukumäärää kutsutaan joukon A *kertaluvuksi*, ja sitä merkitään symbolilla $|A|$. Joukon A sanotaan olevan *yksiö*, jos $|A| = 1$.

Huomautus. Yleisesti joukko-opissa puhutaan mieluummin joukkojen mahtavuuksista ja kardinaaleista kuin kertaluvuista. Joukkoa sanotaan äärettömäksi, kun se ei ole äärellinen.

Tunnetuksi oletetaan perinteisen (intuitiivisen) joukko-oppin yhdisteen, leikkauksen ja erotuksen määritelmät. Seuraavaksi esitetään yhdisteen ja leikkauksen yleisemmät versiot. Määritellään lisäksi, mitä tarkoitetaan perheen maksimaalisella alkiolla.

Määritelmä 1.2. Perheen $\mathcal{A}$ *yhdiste* on $\bigcup \mathcal{A} = \{ x \mid \exists A \in \mathcal{A}(x \in A) \}$. Perheen $\mathcal{A}$ *leikkaus* on $\bigcap \mathcal{A} = \{ x \mid \forall A \in \mathcal{A}(x \in A) \}$, kunhan $\mathcal{A} \neq \emptyset$.

Määritelmä 1.3. Joukko M on epätyhjän perheen $\mathcal{A}$ *maksimaalinen alkio*, jos M on sisältyvyyden suhteen maksimaalinen. Toisin sanoen, jos $M \subseteq A \in \mathcal{A}$, niin $M = A$.

Huomautus. Joukko-opillisesti perheet ja alkiot ovat myös joukkoja. Tyypillisesti näitä nimityksiä käytetään vain joukkojen kategorisoimiseksi. Perheiden alkioina ajatellaan olevan joukkoja, jotka sisältävät alkioita. Joukot taas sisältävät alkioita, joiden mahdollisilla alkioiden alkioilla ei ajatella olevan merkitystä.

Huomautus. Täsmällisesti ottaen, muotoa $\{ x \mid p(x) \}$ olevan joukon, eli ns. joukkoabstraktion, esitys on ongelmallinen, mikä voidaan osoittaa Russelin paradoksilla (ks. esim. [14, s. 51–52]). Kaikkien tällaista muotoa olevien joukkojen olemassolo tulisi perustella ZFC:n aksioomien kautta. Tässä tutkielmassa tätä perustelua ei esitetä, mutta lukijan on hyvä tiedostaa kyseinen fakta.

Relaation ja järjestetyn parin käsitteet kulkevat käsi kädessä.

Määritelmä 1.4. Joukkojen a ja b *järjestetty pari* on $(a, b) = \{\{a\}, \{a, b\}\}$. *Relaatio* on joukko järjestettyjä pareja.

Järjestetyn parin määritelmän avulla voidaan osoittaa, että seuraava oleellinen ominaisuus pätee:

Lause 1.5. *$(a, b) = (c, d)$, jos ja vain jos $a = c$ ja $b = d$.*

Todistus. Sivuutetaan. Todistuksen idean voi katsoa lähteestä [11, s. 4]. □

Seuraavaksi esitetään määrittely- ja arvojoukon sekä kentän käsitteet. Määritellään myös yhdistetty relaatio ja käänteisrelaatio sekä relaation rajoittuma ja joukon kuva relaatiossa.

Määritelmä 1.6. Relaation R *määrittelyjoukko* on $\operatorname{dom}(R) = \{ a \mid \exists b \, ((a, b) \in R) \}$, *arvojoukko* on $\operatorname{ran}(R) = \{ b \mid \exists a \, ((a, b) \in R) \}$, ja *kenttä* on $\operatorname{fld}(R) = \operatorname{dom}(R) \cup \operatorname{ran}(R)$.

Määritelmä 1.7. Relaatioiden R ja S *yhdistetty relaatio* on

$$R \circ S = \{ (x, z) \mid \exists y ((x, y) \in S, (y, z) \in R) \}.$$

Relaation R *käänteisrelaatio* on $R^{-1} = \{ (b, a) \mid (a, b) \in R \}$.

Määritelmä 1.8. Relaation R *rajoittuma* joukkoon A on

$$R \upharpoonright A = \{ (a, b) \in R \mid a \in A \}.$$

Joukon A *kuva* relaatiossa R on

$$R[A] = \operatorname{ran}(R \upharpoonright A) = \{ b \mid \exists a \in A ((a, b) \in R) \}.$$

Relaatioiden yhdistäminen on liitännäinen operaatio. Esitetään lisäksi karteesisen tulon ja ekvalenssirelaation määritelmät.

Lause 1.9. *Olkoot R, S ja T relaatioita. Tällöin $R \circ (S \circ T) = (R \circ S) \circ T$.*

Todistus. Ks. [19, s. 2]. □

Määritelmä 1.10. Joukkoa $A \times B = \{(a, b) \mid a \in A, b \in B\}$ kutsutaan joukkojen A ja B *karteesiseksi tuloksi*.

Määritelmä 1.11. Relaatio E on *ekvivalenssirelaatio* joukossa A, jos se on refleksiivinen joukossa A, symmetrinen ja transitiivinen. Jos E on joukon A ekvivalenssirelaatio, niin joukko $[x] = \{y \in A \mid (y, x) \in E\}$ on alkion x määräämä *ekvivalenssiluokka*.

Ekvivalenssirelaation liittyy oleellisesti joukon osituksen eli luokkajaon käsitteeseen. Seuraavaksi näytetään perustavaa laatua oleva tulos, jonka mukaan joukon ekvivalenssiluokat osittavat kyseisen joukon. Jos joukolla A on siis ekvivalenssirelaatio E, niin joukko A voidaan muodostaa relaation E määräämistä erillisistä ekvivalenssiluokista.

Määritelmä 1.12. Olkoon A joukko ja $\mathcal{P}$ perhe, joka koostuu joukon A epätyhjistä osajoukoista. Tällöin perheen $\mathcal{P}$ sanotaan olevan joukon A *ositus* eli *luokkajako*, jos seuraavat ehdot ovat voimassa:

(i) Kaikilla $B, C \in \mathcal{P}$ pätee joko $B = C$ tai $B \cap C = \emptyset$.

(ii) $A = \bigcup \mathcal{P}$.

Lause 1.13. *Olkoon E joukon A ekvivalenssirelaatio. Tällöin ekvivalenssirelaation E määräämät joukon A ekvivalenssiluokat osittavat joukon A. Toisin sanoen, perhe $\mathcal{P} = \{[x] \mid x \in A\}$ on joukon A ositus.*

Todistus. Ks. [7, s. 30]. □

Määritellään nyt yksi tärkeimmistä joukko-opillisista käsitteistä eli kuvaus.

Määritelmä 1.14. Joukko f on *kuvaus* eli *funktio*, jos f on relaatio, joka toteuttaa *funktionaalisuusehdon*:

$$\text{Jos } (x, y) \in f \text{ ja } (x, y') \in f, \text{ niin } y = y'.$$

Huomautus. Kuvaukselle f merkintä $f\colon A \to B$ (eli f on kuvaus joukosta A joukkoon B) tarkoittaa, että $\mathrm{dom}(f) = A$ ja $\mathrm{ran}(f) \subseteq B$. Tällöin $f \subseteq A \times B$. Usein kuvaukselle f merkinnän $(x, y) \in f$ sijasta käytetään merkintää $f(x) = y$. Lisäksi kuvauksen f käänteisrelaatio f^{-1} ei ole välttämättä kuvaus.

Määritelmä 1.15. Olkoon $f\colon A \to B'$ kuvaus ja $B \subseteq B'$. Joukon B *alkukuva*, $f^{-1}[B]$, on joukko, joka koostuu niistä joukon A alkioista, jotka kuvautuvat joukolle B eli

$$f^{-1}[B] := \{a \in A \mid f(a) \in B\}.$$

Merkintä 1.16. Joukon A *identtistä kuvausta* merkitään symbolilla id_A, toisin sanoen $\mathrm{id}_A\colon A \to A, \mathrm{id}_A(x) = x$.

Seuraavassa lauseessa näytetään muutamia relaatioiden ja kuvausten perusominaisuuksia.

Lause 1.17. *Olkoot R ja S relaatioita sekä f, g ja h kuvauksia. Tällöin*

(a) $\mathrm{dom}(R^{-1}) = \mathrm{ran}(R)$ *ja* $\mathrm{ran}(R^{-1}) = \mathrm{dom}(R)$.

(b) $(R^{-1})^{-1} = R$.

(c) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

(d) $f \circ g$ *on kuvaus.*

(e) *Jokaisella* $x \in \mathrm{dom}(f \circ g)$ *pätee* $(f \circ g)(x) = f(g(x))$.

(f) $f \circ (g \circ h) = (f \circ g) \circ h$.

Todistus. Sivuutetaan. Osaan kohdista löytyy todistukset lähteistä [19, s. 3] ja [11, s. 44]. □

Määritellään sitten, mitä tarkoitetaan kuvauksen surjektiivisuudella ja injektiivisyydellä. Bijektio, joka on surjektio ja injektio, on kuvaus, joka muodostaa kahden joukon alkioiden välille yksi-yhteen-vastaavuuden.

Määritelmä 1.18. Olkoon $f\colon A \to B$ kuvaus joukolta A joukkoon B. Kuvaus f on *injektio*, jos kaikilla $x, y \in A$, $x \neq y$, pätee $f(x) \neq f(y)$. Kuvaus f on *surjektio*, jos $\mathrm{ran}(f) = B$. Kuvaus f on *bijektio*, jos se on injektio ja surjektio.

Määritelmä 1.19. Joukot A ja B ovat *yhtämahtavat*, $A \approx B$, jos on olemassa bijektio $f\colon A \to B$.

Huomautus. On helppoa osoittaa, että yhtämahtavuudella on ekvivalenssirelaation ominaisuudet, mutta se ei kuitenkaan ole ekvivalenssirelaatio, koska se ei ole joukko. Kun $A \approx B$, niin usein kirjoitetaan $|A| = |B|$. On välitön seuraus, että äärellisille joukoille A ja B pätee: $|A| = |B|$, jos ja vain jos kyseisillä joukoilla on sama määrä alkioita. Tässä mielessä alussa annettu määritelmä 1.1 äärellisen joukon kertaluvusta on mielekäs.

Määritelmä 1.20. Olkoon $f\colon A \to B$ kuvaus. Kuvauksen f sanotaan olevan *vasemmalta kääntyvä*, jos on olemassa sellainen kuvaus $g\colon B \to A$, että $g \circ f = \mathrm{id}_A$. Kuvaus f on puolestaan *oikealta kääntyvä*, jos on olemassa sellainen kuvaus $h\colon B \to A$, että $f \circ h = \mathrm{id}_B$. Tällaista kuvausta g sanotaan *vasemman puoleiseksi käänteiskuvaukseksi*, ja vastaavasti kuvaus h on *oikean puoleinen käänteiskuvaus*. Kuvaus f on *kääntyvä*, jos se on sekä vasemmalta että oikealta kääntyvä.

Seuraava lause mahdollistaa kuvauksen f käänteiskuvauksen olemassaolon ja yksikäsitteisyyden. Lauseen täsmällinen todistus vaatisi ZFC:n valinta-aksiooman käyttöä, joten todistuksen täsmällinen tarkastelu jätetään lukijalle.

Lause 1.21. *Olkoot A ja B joukkoja, $A \neq \emptyset$, ja $f\colon A \to B$. Tällöin*

(i) f *on injektio, jos ja vain jos* f *on vasemmalta kääntyvä.*

(ii) *f on surjektio, jos ja vain jos f on oikealta kääntyvä.*

(iii) *f on bijektio, jos ja vain jos f on kääntyvä.*

Todistus. Ks. [7, s. 25]. □

Seuraus 1.22. *Olkoon $f\colon A \to B$ kääntyvä kuvaus. Tällöin kuvauksella f on olemassa yksikäsitteinen käänteiskuvaus $f^{-1}\colon B \to A$, jolle $f^{-1} \circ f = \mathrm{id}_A$ ja $f \circ f^{-1} = \mathrm{id}_B$.*

Todistus (vrt. [11, s. 46]). Kääntyvä kuvaus f on bijektio, joka on surjektio ja injektio. Edellisen lauseen nojalla on siis olemassa kuvauksen f vasemman puoleinen käänteiskuvaus g ja oikean puoleinen käänteiskuvaus h. Tällöin $g \circ f = \mathrm{id}_A$ ja $f \circ h = \mathrm{id}_B$. Siis $g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h$. Täten merkitsemällä $g = h := f^{-1}$ väite on todistettu. □

Seurauksen 1.22 nojalla jokaisella bijektiolla on siis olemassa yksikäsitteinen käänteiskuvaus. Seuraavaksi esitetään laskutoimuksen käsite kuvauksen avulla. Lisäksi laskutoimitukselle nimetään liitännäisyys- ja vaihdannaisuusominaisuudet.

Määritelmä 1.23. Joukon A *laskutoimitus* on kuvaus $*\colon A \times A \to A$.

Huomautus. Joukon A laskutoimitukselle kuvauksille tyypillisen merkinnän $*((a, b))$, missä $(a, b) \in A \times A$, sijasta käytetään merkintää $a * b$. Laskutoimituksen hyvin määriteltävyyden tarkistamiseksi osoitetaan, että jokaisella $(a, b) \in A \times A$ on olemassa täsmälleen yksi sellainen $c \in A$, että $x * y = z$. Riittää siis osoittaa, että kaikilla $(a, b), (a', b') \in A \times A$ pätee implikaatio: $(a, b) = (a', b') \Rightarrow a * b = a' * b'$.

Määritelmä 1.24. Joukon A laskutoimitus $*$ on *liitännäinen*, jos

$$(a * b) * c = a * (b * c) \text{ kaikilla } a, b, c \in A.$$

Laskutoimitus on puolestaan *vaihdannainen*, jos

$$a * b = b * a \text{ kaikilla } a, b \in A.$$

Määritelmä 1.25. Olkoon $*$ joukon A laskutoimitus, ja olkoot joukot B ja C joukon A osajoukkoja. Tällöin joukkojen B ja C *tulo* on $B * C = \{b * c \mid b \in B, c \in C\}$.

Näytetään nyt, että liitännäisyyden määritelmästä seuraa itse asiassa yleinen liitännäisyys. Tavoitteena on siis osoittaa, että liitännäisyys yleistyy kolmen alkion tapauksesta n:n alkion tapaukseen. Tätä varten on kuitenkin yleistettävä määritelmän 1.10 karteesinen tulo koskemaan kahden joukon sijasta kokonaista joukkoperhettä, ja järjestetyt parit yleistetään äärellisen pituisiksi jonoiksi. Tarkastellaan indeksöityä joukkoperhettä $\mathcal{A} = \{A_i \mid i \in I\}$, missä I on indeksijoukko.

Määritelmä 1.26. *Indeksöity jono* $(x_i)_{i \in I}$ on kuvaus f, jolle $\mathrm{dom}(f) = I$ ja jokaisella $i \in I$ pätee $f(i) = x_i$.

Indeksöityjen jonojen avulla voidaan määritellä hyvin myös yhdisteitä ja leikkauksia. Olkoon $\mathcal{A} = \{A_i \mid i \in I\}$ indeksöity joukkoperhe, missä I on indeksijoukko. Tarkastellaan indeksöityä jonoa $(A_i)_{i\in I}$. Nyt $\bigcup \mathcal{A} = \bigcup_{i\in I} A_i = \bigcup \operatorname{ran}((A_i)_{i\in I})$. Jos perhe $\mathcal{A}$ on lisäksi epätyhjä, niin $\bigcap \mathcal{A} = \bigcap_{i\in I} A_i = \bigcap \operatorname{ran}((A_i)_{i\in I})$. Nyt voidaan määritellä yleinen karteesinen tulo.

Määritelmä 1.27. Joukkoperheen $\mathcal{A} = \{A_i \mid i \in I\}$ *yleinen karteesinen tulo* on

$$\bigtimes \mathcal{A} = \bigtimes_{i\in I} A_i = \{f \mid f\colon I \to \bigcup \mathcal{A} \text{ ja } f(i) \in A_i \text{ kaikilla } i \in I\} =$$
$$\{(a_i)_{i\in I} \mid \forall i \in I(a_i \in A_i)\}.$$

Merkintä 1.28. Olkoon $I = \{1, 2, \ldots, n\}$ äärellinen indeksijoukko. Tällöin karteesista tuloa $\Pi_{i\in I} A_i$ merkitään termien $A_1, \ldots, A_n$ tulona $A_1 \times A_2 \times \ldots \times A_n$. Joukon $A_1 \times A_2 \times \ldots \times A_n$ alkiota merkitään jonolla $(a_1, a_2, \ldots, a_n)$, missä $a_i \in A_i$ kaikilla $i \in I$. Jos $A_1 = A_2 = \ldots = A_n = A$, niin karteesista tuloa merkitään symbolilla A^n, ja tällöin $a_i \in A$, kun $i \in I$.

Olkoon nyt $*$ joukon A laskutoimitus. Olkoon $f_1\colon A \to \mathcal{P}(A)$, $f_1(a_1) = \{a_1\}$. Määritellään rekursiolla luvun $n \geq 2$ suhteen kuvaus $f_n\colon A^n \to \mathcal{P}(A)$,

$$f_n(a_1, \ldots, a_n) = \bigcup \{f_r(a_1, \ldots, a_r) * f_{n-r}(a_{r+1}, \ldots, a_n) \mid 0 < r < n\}. \tag{1.1}$$

Induktiolla voidaan osoittaa, että $f_n(a_1, \ldots, a_n) \neq \emptyset$, kun $(a_1, \ldots, a_n) \in A^n$. Lisäksi havaitaan, että määritelmän 1.24 nojalla $f_3(a_1, a_2, a_3)$ on yksiö, jos ja vain jos $*$ on liitännäinen laskutoimitus, kun $(a_1, a_2, a_3) \in A^3$. Nyt ollaan valmiita todistamaan yleinen liitäntälaki.

Lause 1.29. *Olkoon $*$ joukon A liitännäinen laskutoimitus ja $(a_1, \ldots, a_n) \in A^n$, missä $n \in \mathbb{Z}_+$. Tällöin $f_n(a_1, \ldots, a_n)$ on yksiö.*

Todistus (vrt. [19, s. 4]). Todistetaan lause induktiolla luvun n suhteen. Väite on selvä, kun $n = 1$ ja $n = 2$. Olkoon $n > 2$. Oletetaan, että väite pätee kaikille lukua n pienemmille luvuille. Olkoon $z \in f_n(a_1, \ldots, a_n)$ ja $z' \in f_n(a_1, \ldots, a_n)$. Tällöin on olemassa sellaiset alkiot $x, y, x', y' \in A$ ($f_n(a_1, \ldots, a_n) \in \mathcal{P}(A) \Rightarrow f_n(a_1, \ldots, a_n) \subseteq A$) ja luonnolliset luvut r ja t, että

$$z = x * y \text{ ja } z' = x' * y', \text{ missä } x \in f_r(a_1, \ldots, a_r), y \in f_{n-r}(a_{r+1}, \ldots, a_n),$$
$$x' \in f_t(a_1, \ldots, a_t), y' \in f_{n-t}(a_{t+1}, \ldots, a_n).$$

Oletetaan ensin, että $r = t$. Nyt induktio-oletuksen nojalla $f_r(a_1, \ldots, a_r) = f_t(a_1, \ldots, a_t)$ ja $f_{n-r}(a_{r+1}, \ldots, a_n) = f_{n-t}(a_{t+1}, \ldots, a_n)$ ovat yksiöitä, joten $x = x'$ ja $y = y'$. Siis $z = x * y = x' * y' = z'$.

Oletetaan sitten, että $r < t$. Induktio-oletuksen perusteella $f_{t-r}(a_{r+1}, \ldots, a_t)$ on yksiö $\{v\}$. Edelleen induktio-oletuksen mukaan myös $f_{n-r}(a_{r+1}, \ldots, a_n)$ ja $f_{n-t}(a_{t+1}, \ldots, a_n)$ ovat yksiöitä $\{y\}$ ja $\{y'\}$. Nyt kuvauksen (1.1) määritelmän nojalla $f_{t-r}(a_{r+1}, \ldots, a_t) * f_{n-t}(a_{t+1}, \ldots, a_n) \subseteq f_{n-r}(a_{r+1}, \ldots, a_n)$ eli $\{v * y'\} \subseteq \{y\}$, joten itse asiassa $\{v * y'\} = \{y\}$ (yksiöön voi sisältyä vain tyhjä joukko tai yksiö

itse, ja aiemmin todettiin, että käsiteltävät joukot muotoa $f_n(a_1, \ldots, a_n)$ ovat epätyhjiä). Siis $y = v * y'$. Vastaavasti induktio-oletuksesta seuraa, että $f_t(a_1, \ldots, a_t)$ ja $f_r(a_1, \ldots, a_r)$ ovat yksiöitä $\{x'\}$ ja $\{x\}$. Edelleen $f_r(a_1, \ldots, a_r) * f_{t-r}(a_{r+1}, \ldots, a_n) \subseteq f_t(a_{r+1}, \ldots, a_t)$ eli $\{x * v\} \subseteq \{x'\}$, joten $\{x * v\} = \{x'\}$. Täten $x' = x * v$. Nyt liitännäisyyden vuoksi

$$z = x * y = x * (v * y') = (x * v) * y' = x' * y' = z'.$$

Täysin symmetrisesti käsitellään tapaus $r > t$. Siis induktiolla ollaan osoitettu, että $f_n(a_1, \ldots, a_n)$ on yksiö. □

Lauseen 1.29 joukon $f_n(a_1, \ldots, a_n)$ yksiötä merkitään symbolilla $a_1 * \cdots * a_n$. Jos laskutoimitus $*$ olisi lisäksi vaihdannainen, voitaisiin osoittaa, ettei tekijöiden $a_1, \ldots, a_n$ keskinäisellä järjestyksellä ole väliä esityksessä $a_1 * \cdots * a_n$.

1.2 Ryhmän määritelmä

Alaluvussa 1.2 esitetään ryhmän määritelmä sekä joitakin ryhmien perusominaisuuksia ilman todistusta.

Määritelmä 1.30. Olkoon $*$ joukon G laskutoimitus. Tällöin järjestetty pari $(G, *)$ on *ryhmä*, jos seuraavat ehdot pätevät:

1. Laskutoimitus $*$ on liitännäinen joukossa G.

2. On olemassa sellainen alkio $e \in G$, että kaikille $g \in G$ pätee

   $$g * e = e * g = g.$$

   Tällaista alkiota e kutsutaan *neutraalialkioksi*.

3. Jokaisella alkiolla $g \in G$ on olemassa sellainen $g^{-1} \in G$, että

   $$g * g^{-1} = g^{-1} * g = e.$$

   Alkiota g^{-1} kutsutaan alkion g *käänteisalkioksi*.

Lisäksi, jos laskutoimitus $*$ on vaihdannainen, sanotaan ryhmän $(G, *)$ olevan *Abelin*[1] *ryhmä*.

Huomautus. Mikäli ryhmän laskutoimitus $*$ on asiayhteyden perusteella tunnettu, käytetään perinteisen ryhmän määritelmän merkinnän $(G, *)$ sijaan ryhmälle yksinkertaisesti merkintää G. Vastaavasti, jos laskutoimituksen $*$ merkitystä ei ole tarpeen erikseen korostaa voidaan alkiota $g_1 * g_2$ merkitä yksinkertaisesti symbolilla $g_1 g_2$, kun $g_1, g_2 \in G$.

[1] Niels Henrik Abel (1802–1829) oli norjalainen matemaatikko, joka todisti, ettei viidennen tai sitä korkeamman asteen yhtälöä voida ratkaista algebrallisesti. Abel mullisti myös elliptisten funktioiden teorian. [11, s. 82]

Jos $(G, *)$ on ryhmä ja $g_1, g_2, \ldots, g_n \in G$ ryhmän alkioita, niin lauseen 1.29 perusteella seuraavassa määritelmässä niiden avulla esitettävä tulo on yksikäsitteinen joukon G alkio. Lauseessa 1.32 esitetään ryhmän perusominaisuuksia.

Määritelmä 1.31. Olkoon $(G, *)$ ryhmä ja H sen äärellinen osajoukko, jonka kertaluku on n. Merkitään $A = \{(a_1, \ldots, a_n) \in H^n \mid a_i \neq a_j, \text{kun } i \neq j\}$. Tarkastellaan kuvausta $f\colon A \to G$,

$$f(a_1, \ldots, a_n) = a_1 * \cdots * a_n.$$

Kuvajoukon $f[A]$ alkioita kutsutaan *joukon* H *tuloiksi*. Jos $f[A]$ on yksiö, niin joukon H tuloa merkitään symbolilla $\prod H$.

Jos $h_1, h_2, \ldots, h_n$ ovat joukon H alkiot, niin joukon G alkiota $h_1 * h_2 * \cdots * h_n$ kutsutaan *alkioiden* $h_1, \ldots, h_n$ *tuloksi*, jota merkitään myös lausekkeella $\prod_{1 \leq i \leq n} h_i$.

Määritellään lisäksi erikseen, että tyhjän joukon tulo on ryhmän G neutraalialkio, eli toisin sanoen $\prod \emptyset = e$.

Huomautus. Määritelmässä 1.31 joukon H tulo on yksikäsitteinen vain, jos $f[A]$ on yksiö. Tällöin merkintä $\prod H$ on mielekäs. On hyvä huomata myös, että vain Abelin ryhmässä *kaikki* tulot ovat määriteltyjä.

Lause 1.32. *Olkoon $(G, *)$ ryhmä. Olkoot $g, x, y, z \in G$ ja $g_1, \ldots, g_n \in G$. Tällöin seuraavat ehdot pätevät.*

(a) *Ryhmän G neutraalialkio ja jokaisen ryhmän G alkion käänteisalkio ovat yksikäsitteisiä.*

(b) $(g^{-1})^{-1} = g$.

(c) *Jos $x * z = y * z$ tai $z * x = z * y$, niin $x = y$.*

(d) *On olemassa sellaiset yksikäsitteiset alkiot $u, v \in G$, että $x * u = y$ ja $v * x = y$.*

(e) $(g_1 * \cdots * g_n)^{-1} = g_n^{-1} * \cdots * g_1^{-1}$.

Todistus. Sivuutetaan. Ks. [11, s. 63] ja [19, s. 7]. □

Määritellään sitten rekursiivisesti ryhmän alkion positiivinen potenssi. Tästä määritelmästä seuraa myös lause 1.34.

Määritelmä 1.33. Olkoon $(G, *)$ ryhmä, $g \in G$ ryhmän alkio ja $n \in \mathbb{N}$. Määritellään

1. $g^0 = e$,

2. $g^{n+1} = g^n * g$.

Edelleen kaikilla $n \in \mathbb{Z}_+$ määritellään

3. $g^{-n} = (g^n)^{-1}$.

Lause 1.34. *Olkoon $(G, *)$ ryhmä, $x, y \in G$ ja $m, n \in \mathbb{Z}$. Tällöin*

(a) $e^n = e$,

(b) $x^n * x^m = x^{n+m} = x^m * x^n$,

(c) $(x^n)^m = x^{nm}$,

(d) $(x * y)^n = x^n * y^n$, *jos* G *on Abelin ryhmä.*

Todistus. Sivuutetaan. Todistus perustuu induktioon ja määritelmään 1.33. Kohta (a) on hyvin yksinkertainen yhden muuttujan induktiotodistus ja kohtien (b) ja (c) todistuksen ideaa voi katsoa lähteestä [19, s. 7–8]. Kohta (d) todistetaan melko suoraviivaisesti induktiolla luvun n suhteen. □

Tehdään nyt ryhmien $G_1, G_2, \ldots, G_n$ karteesisesta tulosta $G_1 \times G_2 \times \cdots \times G_n$ ryhmä määrittelemällä sille sopiva laskutoimitus.

Lause 1.35. *Olkoot* $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ *ryhmiä. Merkitään*

$$G := G_1 \times G_2 \times \cdots \times G_n = \{\, (g_1, g_2, \ldots, g_n) \mid g_i \in G_i, i \in \{1, \ldots, n\} \,\}.$$

Määritellään laskutoimitus $*$ *joukossa* G *asettamalla*

$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \ldots, a_n *_n b_n)$ *aina, kun* $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in G$.

Tällöin $(G, *)$ *on ryhmä.*

Todistus. Suoraviivainen todistus, joka voidaan todistaa suoraan ryhmän määritelmän avulla. Ks. [11, s. 181–183]. □

1.3 Kertaluvun käsite

Tässä alaluvussa määritellään kertaluvun käsite sekä ryhmälle että ryhmän alkiolle. Tämä käsite esiintyy jatkossa hyvin monessa kohtaa tutkielmaa. Ryhmän kertaluvun määritelmä palautuu joukon kertaluvun määritelmään 1.1.

Määritelmä 1.36. Ryhmän $(G, *)$ sanotaan olevan *äärellinen ryhmä*, jos joukossa G on äärellisen monta alkioita. Ryhmä $(G, *)$ on puolestaan *ääretön*, jos se ei ole äärellinen. Äärellisen ryhmän $(G, *)$ *kertaluku* on joukon G alkioiden lukumäärä. Ryhmän G kertalukua merkitään symbolilla $|G|$.

Määritelmä 1.37. Olkoon G ryhmä ja g tämän ryhmän alkio. Jos on olemassa sellainen positiivinen kokonaisluku n, että $g^n = e$, niin pienintä tällaista lukua sanotaan alkion g *kertaluvuksi*. Alkion g kertaluvulle käytetään merkintää $\mathrm{ord}(g)$. Tällöin alkion kertaluvun sanotaan olevan lisäksi *äärellinen*. Jos tällaista positiivista kokonaislukua ei ole olemassa, alkion kertaluku on *ääretön*.

Huomautus. Ryhmän alkion kertaluvun määritelmä on mielekäs, sillä äärelliselle ryhmälle G voidaan osoittaa, että on olemassa sellainen positiivinen kokonaisluku n, että $g^n = e$ kaikilla $g \in G$ (ks. [11, s. 68]). Jos ryhmä G on ääretön, niin on toki mahdollista löytää tällainen positiivinen kokonaisluku. Tässä tapauksessa sellaista kokonaislukua ei kuitenkaan aina löydy.

Seuraava lause 1.38 määrittää ryhmän alkion kertaluvun hyödyllisiä ominaisuuksia. Seuraus 1.39 voidaan johtaa suoraviivaisesti lauseesta 1.38.

Lause 1.38. *Olkoon a sellainen ryhmän G alkio, jolla on äärellinen kertaluku. Merkitään* $\operatorname{ord}(a) = n$. *Tällöin seuraavat ehdot pätevät.*

(i) *Jos $a^m = e$, missä $m \in \mathbb{Z}_+$, niin n jakaa luvun m.*

(ii) *Kaikilla positiivisilla kokonaisluvuilla t pätee, että*

$$\operatorname{ord}(a^t) = \frac{n}{\operatorname{syt}(t, n)}.$$

Todistus. Todistus pohjautuu jakoyhtälöön. Ks. [11, s. 69]. □

Seuraus 1.39. *Olkoon $x^q = e$, missä x on ryhmän G alkio, p on alkuluku, $k \in \mathbb{Z}_+$ ja $q = p^k$. Tällöin $x = e$ tai* $\operatorname{ord}(x) = p^n$ *jollakin kokonaisluvulla n, $1 \leq n \leq k$.*

Todistus. Lauseen 1.38 kohdan (i) perusteella $\operatorname{ord}(x) \mid p^k$, joten $\operatorname{ord}(x) = p^n$, missä $n \in \{0, \ldots, k\}$. Erityisesti, jos $n = 0$, niin $\operatorname{ord}(x) = 1$, jolloin $x = e$. Siis $\operatorname{ord}(x) = p^n$, missä $1 \leq n \leq k$, tai $x = e$. □

2 Permutaatioryhmät

Tässä luvussa käsitellään permaatioryhmiä. Historiallisesti permutaatioryhmät nähdään usein abstraktin ryhmäteorian kulmakivenä (ks. [11, s. 83]), ja ne muodostavatkin tärkeän erikoistyypin ryhmistä. Myöhemmin tullaan nimittäin osoittamaan, että kaikki ryhmät ovat isomorfisia sopivasti määritellyn permutaatioryhmän kanssa. Tämä luku noudattaa suurilta osin kirjan *Fundamentals of Abstract Algebra* [11, s. 83–96] rakennetta, ja osin myös lähteen [4, Conrad] sisältöä.

Luvun päätuloksia ovat lauseet 2.13 ja 2.15, joista ensimmäisen mukaan jokainen symmetriaryhmän permutaatio voidaan esittää yksikäsitteisesti syklien tulona. Jälkimmäinen lause taas sanoo, että kun permutaatio esitetään vaihtojen tulona, niin vaihtojen lukumäärä on joko parillinen tai pariton.

2.1 Permutaatioryhmät, syklit ja symmetriaryhmät

Määritellään ensin, mitä tarkoitetaan permutaatiolla ja permutaatioryhmällä.

Määritelmä 2.1. Olkoon X epätyhjä joukko. Joukon X *permutaatio* on bijektio joukolta X itseensä.

Määritelmä 2.2. Ryhmää $(G, \circ)$ kutsutaan *permutaatioryhmäksi* epätyhjässä joukossa X, jos ryhmän G alkiot ovat joukon X permutaatioita, missä laskutoimitus $\circ$ on kuvausten yhdistäminen.

Määritelmässä 2.2 ryhmä G koostuu siis vain joistakin joukon X permutaatioista. Määritellään seuraavaksi symmetriaryhmä, joka koostuu kaikista joukon X permutaatioista. Määritelmässä 2.3 oletetaan jo symmetriaryhmän neutraalialkion olemassaolo, mikä seuraa heti lauseesta 2.4.

Määritelmä 2.3. Olkoon X epätyhjä joukko ja S_X joukko, joka sisältää kaikki joukon X permutaatiot. Paria $(S_X, \circ)$ kutsutaan joukon X *symmetriaryhmäksi*.

Seuraava lause kertookin, miksi symmetriaryhmää voidaan ylipäätään kutsua ryhmäksi.

Lause 2.4. *Symmetriaryhmä* $(S_X, \circ)$ *on ryhmä.*

Todistus. Sivuutetaan. Todistuksessa käsitellään kuvausten tyypillisiä ominaisuuksia. Ks. [19, s. 9]. □

Huomautus. Symmetriaryhmän S_X, ja jokaisen joukon X permutaatioryhmän, neutraalialkio on tietysti identtinen kuvaus id_X.

Otetaan nyt käyttöön hyödyllinen merkintätapa, jossa symmetriaryhmään S_X liittyvää joukkoa X tarkastellaan luonnollisten lukujen $\mathbb{N}$ äärellisenä osa-joukkona.

Merkintä 2.5. Olkoon $I_n = \{1, 2, \ldots, n\}$, missä $n \in \mathbb{Z}_+$. Tällöin symbolilla S_n merkitään joukon I_n symmetriaryhmää. Symmetriaryhmän S_n neutraalialkiolle käytetään identtisen kuvauksen merkinnän id_{I_n} sijasta merkintää (1). S_n on siis ryhmä, joka koostuu kaikista joukon I_n permutaatioista. Olkoon $\alpha \in S_n$. Tällöin $\alpha = \{(1, \alpha(1)), (2, \alpha(2)), \ldots, (n, \alpha(n))\}$. Usein joukon I_n mielivaltaiselle permutaatiolle $\alpha \in S_n$ käytetään myös seuraavaa kaksirivistä merkintätapaa:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha(1) & \alpha(1) & \alpha(3) & \ldots & \alpha(n) \end{pmatrix}.$$

Jos $\alpha(i) = i$ jollakin $i \in I_n$, niin saraketta $\begin{matrix} i \\ \alpha(i) \end{matrix}$ ei tarvitse merkitä.

Huomautus. Lauseen 2.4 nojalla S_n on ryhmä.

Seuraava lause kertoo kaksi symmetriaryhmän S_n perusominaisuutta.

Lause 2.6.

(i) *Jos $n \geq 3$, niin symmetriaryhmä S_n ei ole vaihdannainen.*

(ii) $|S_n| = n!$.

Todistus. (i) Ks. [11, s. 87]. Olkoon $n \geq 3$. Tarkastellaan symmetriaryhmän S_n seuraavia permutaatioita α ja β:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Nyt

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

jolloin $(\alpha \circ \beta)(1) = 2 \neq 3 = (\beta \circ \alpha)(1)$. Siis $\alpha \circ \beta \neq \beta \circ \alpha$, ja näin ollen S_n ei ole vaihdannainen.

(ii) Symmetriaryhmä S_n koostuu kaikista bijektioista äärelliseltä joukolta I_n itseensä. Olkoon $\alpha \in S_n$ jokin permutaatio eli bijektio $\alpha \colon I_n \to I_n$. Tällöin jokaisella $i \in I_n$ on olemassa sellainen yksikäsitteinen $j \in I_n$, että $(i, j) \in \alpha$. Permutaatio α on siis joukko, joka koostuu järjestetyistä pareista seuraavasti: $\alpha = \{(1, \alpha(1)), (2, \alpha(2)), \ldots, (n, \alpha(n))\}$, missä $\alpha(i) \neq \alpha(j)$, kun $i \neq j$. Lisäksi, permutaation surjektiivisuudesta seuraa, että $I_n = \mathrm{ran}(\alpha) = \{\alpha(1), \ldots, \alpha(n)\}$, missä injektiviisyyden vuoksi $\alpha(1), \ldots, \alpha(n) \in I_n$ ovat eri lukuja. Tästä seuraakin suoraan, että symmetriaryhmän mielivaltaisella permutaatiolla voi olla $n!$ kappaletta erilaisia esityksiä. Siis $|S_n| = n!$. □

Määritellään seuraavaksi syklin ja vaihdon käsitteet. Syklit ovat erittäin käyttökelpoinen merkintätapa symmetriaryhmän permutaatioille.

Määritelmä 2.7. Permutaatio $\alpha \in S_n$ on *k-sykli* ($k > 1$), jos on olemassa sellaiset eri luvut $i_1, \ldots, i_k \in I_n$, että

$$\alpha = \begin{pmatrix} i_1 & i_2 & \ldots & i_{k-1} & i_k \\ i_2 & i_3 & \ldots & i_k & i_1 \end{pmatrix},$$

eli toisin ilmaisten, $\alpha(i_j) = i_{j+1}$ ja $\alpha(i_k) = i_1$, kun $j \in \{1, 2, \ldots, k-1\}$, ja lisäksi $\alpha(j) = j$ aina, kun $j \notin \{i_1, \ldots, i_k\}$. Tällöin merkitään $\alpha = (i_1 \ i_2 \ \cdots \ i_k)$. 2-syklejä kutsutaan *vaihdoiksi* tai *transpositioksi*. k-syklin *pituus* on yksinkertaisesti k.

Symmetriaryhmän permutaatiossa, joka on sykli, luvut siis kuvautuvat syklimäisesti aina toiselta toiselle ($i_1 \mapsto i_2 \mapsto i_3 \ldots i_{k-1} \mapsto i_k \mapsto i_1$), kunnes sykli päättyy, ja alkaa alusta. Vaihto on taas permutaatio $(i_1 \ i_2)$, joka kuvaa kaksi lukua toisikseen, ja jättää muut luvut itsekseen. Määritellään nyt, mitä tarkoitetaan sillä, että kaksi permutaatiota ovat konjugaatteja.

Määritelmä 2.8. Symmetriaryhmän S_n permutaatioita α ja β kutsutaan *konjugaateiksi*, jos on olemassa sellainen $\gamma \in S_n$, että $\gamma \circ \alpha \circ \gamma^{-1} = \beta$.

Seuraava lause näyttää, miten voidaan määrittää minkä tahansa syklin konjugaatti.

Lause 2.9. *Olkoon $\beta = (i_1 \ i_2 \ \cdots \ i_l) \in S_n$ sykli. Tällöin kaikilla $\alpha \in S_n$ pätee, että*

$$\alpha \circ \beta \circ \alpha^{-1} = (\alpha(i_1) \ \alpha(i_2) \ \cdots \ \alpha(i_l)).$$

Todistus (ks. [11, s. 88–89]). Olkoon $\alpha \in S_n$. Ensinnäkin, kuten lauseen 2.6 todistuksessa todettiin $I_n = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$, missä $\alpha(1), \ldots, \alpha(n) \in I_n$ ovat eri alkioita. Olkoon r sellainen kokonaisluku, että $1 \leq r < l$. Tällöin

$$(\alpha \circ \beta \circ \alpha^{-1})(\alpha(i_r)) = \alpha(\beta(\alpha^{-1}(\alpha(i_r)))) = \alpha(\beta(i_r)) = \alpha(i_{r+1}).$$

Vastaavasti saadaan, että $(\alpha \circ \beta \circ \alpha^{-1})(\alpha(i_l)) = \alpha(i_1)$. Olkoon sitten $a \in I_n$ sellainen luku, että $a \neq \alpha(i_j)$ aina, kun $1 \leq j \leq l$. Nyt koska α on bijektio, niin $\alpha^{-1}(a) \neq i_j$ aina, kun $1 \leq j \leq l$, ja lisäksi $\alpha^{-1}(a) \in I_n$. Täten $\beta(\alpha^{-1}(a)) = \alpha^{-1}(a)$. Edelleen

$$(\alpha \circ \beta \circ \alpha^{-1})(a) = \alpha(\beta(\alpha^{-1}(a))) = \alpha(\alpha^{-1}(a)) = a.$$

Siis $\alpha \circ \beta \circ \alpha^{-1} = (\alpha(i_1) \ \alpha(i_2) \ \cdots \ \alpha(i_l))$. □

Voisiko kaikki symmetriaryhmän permutaatiot esittää sykleinä? Intuition mukaan voi, erityisesti syklien tulona, missä tulolla viitataan kuvausten yhdistämiseen. Kyseinen väite ei ole kuitenkaan läheskään triviaali. Ennen kun voidaan alkaa tarkastella kyseistä perustavaa laatua olevaa tulosta, on määriteltävä, mitä tarkoitetaan erillisillä permutaatioilla.

Määritelmä 2.10. Permutaation $\alpha \in S_n$ sanotaan *liikuttavan* lukua $a \in I_n$, jos $\alpha(a) \neq a$. Permutaatio $\alpha \in S_n$ taas *kiinnittää* luvun $a \in I_n$, jos $\alpha(a) = a$.

Määritelmä 2.11. Symmetriaryhmän S_n permutaatioiden α ja β sanotaan olevan *erillisiä*, jos β kiinnittää kaikki ne joukon I_n luvut, joita α liikuttaa. Permutaatiot $\alpha_1, \alpha_2, \ldots, \alpha_k \in S_n$ ovat puolestaan keskenään erillisiä, jos ne ovat pareittain erillisiä. Formaalisti ilmaistuna tämä on yhtäpitävää seuraavan ehdon kanssa:

$$\text{Jos } \alpha_i(a) \neq a, \text{ niin } \alpha_j(a) = a \text{ aina, kun } a \in I_n \text{ ja } i \neq j, \text{ missä } i, j \in \{1, \ldots, k\}.$$

Oletetaan, että symmetriaryhmän permutaatiot $\alpha_1, \alpha_2, \ldots, \alpha_k$ ovat erillisiä. Tällöin jos jokin permutaatioista liikuttaa lukua $a \in I_n$, niin määritelmän 2.11 mukaan kaikki muut permutaatiot kiinnittävät sen. Tästä seuraa myös se, että jos symmetriaryhmän syklit ovat erillisiä, niin niissä ei voi esiintyä samoja lukuja. Toisin sanoen, jos syklit $(a_1 \ldots a_k)$ ja $(b_1 \ldots b_l)$ ovat erillisiä, niin $a_i \neq b_j$ kaikilla $i \in \{1, \ldots, k\}$ ja $j \in \{1, \ldots, l\}$ eli $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$.

Osoitetaan seuraavaksi, että erilliset permutaatiot kommutoivat.

Lause 2.12. *Symmetriaryhmän erillisille permutaatioille $\alpha, \beta \in S_n$ pätee*

$$\alpha \circ \beta = \beta \circ \alpha.$$

Todistus (vrt. [11, s. 89]). Olkoot α ja β ryhmän S_n erillisiä permutaatiota. Olkoon $a \in I_n$. Oletetaan, että permutaatio α liikuttaa lukua a eli $\alpha(a) \neq a$. Tällöin koska α ja β ovat erillisiä, niin permutaatio β kiinnittää luvun a eli $\beta(a) = a$. Merkitään $b = \alpha(a)$. Tällöin $(\alpha \circ \beta)(a) = \alpha(\beta(a)) = \alpha(a) = b$, ja $(\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(b)$. Jos olisi $\alpha(b) = b$, niin $\alpha(b) = b = \alpha(a)$, jolloin permutaation α injektiivisyydestä seuraa $a = b$. Mutta silloinhan $\alpha(a) = b = a$, mikä on ristiriidassa aiemmin oletetun kanssa. Siis $\alpha(b) \neq b$, joten $\beta(b) = b$, sillä α ja β ovat erillisiä. Silloin $(\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(b) = b$, joten $(\alpha \circ \beta)(a) = (\beta \circ \alpha)(a)$.

Oletetaan toisaalta, että permutaatio α kiinnittää luvun a eli $\alpha(a) = a$. Tällöin $(\alpha \circ \beta)(a) = a = (\beta \circ \alpha)(a)$, jos $\beta(a) = a$. Oletetaan siis, että $\beta(a) \neq a$. Merkitään $c = \beta(a)$. Jos olisi $\beta(c) = c$, niin $\beta(a) = c = \beta(c)$, joten $a = c$. Siis $\beta(a) = c = a$, mikä on ristiriita. Täten $\beta(c) \neq c$, jolloin $\alpha(c) = c$. Tästä seuraa, että $(\alpha \circ \beta)(a) = \alpha(\beta(a)) = \alpha(c) = c = \beta(a) = \beta(\alpha(a)) = (\beta \circ \alpha)(a)$.

Ollaan siis osoitettu, että $(\alpha \circ \beta)(a) = (\beta \circ \alpha)(a)$ kaikilla $a \in I_n$. Siis $\alpha \circ \beta = \beta \circ \alpha$. □

Lauseesta 2.12 seuraa, että jos $\alpha_1 \circ \cdots \circ \alpha_k$ on erillisten symmetriaryhmän permutaatioiden tulo, niin se voidaan esittää permutaatioiden $\alpha_1, \ldots, \alpha_k$ keskinäisen järjestyksen suhteen missä tahansa muodossa. Todistetaan nyt tämän aliluvun päätulos, jonka mukaan jokainen symmetriaryhmän permutaatio voidaan esittää yksikäsitteisesti erillisten syklien tulona.

Lause 2.13. *Jokainen symmetriaryhmän $S_n (n \geq 2)$ permutaatio voidaan esittää järjestystä vaille yksikäsitteisesti erillisten syklien tulona.*

Todistus (vrt. [11, s. 89–90]). Määritelmän 1.31 mukaan neutraalialkio (1) on tyhjän joukon tulo. Voidaan siis ajatella, että neutraalialkio on tavallaan nollan erillisen syklin tulo. Olkoon $\alpha \in S_n, \alpha \neq (1)$. Todistetaan lause induktiolla luvun n ($n \geq$

2) suhteen. Olkoon $n = 2$. Tällöin $|S_2| = 2$, ja $\alpha = (1\ \ 2)$, joten α on sykli. Lause on siis tosi, kun $n = 2$. Olkoon $n > 2$, ja oletetaan, että väite pätee kaikille symmetriaryhmille S_k, missä $2 \leq k < n$. Toisin sanoen, väite pätee kaikille joukkojen $I \subset I_n (I \subset I_n \Rightarrow |I| < |I_n|)$ permutaatioille. Nyt $\alpha^i(1) \in I_n$ kaikilla $i \in \mathbb{Z}_+$, joten $\{\alpha^i(1) \mid i \in \mathbb{Z}_+\} \subseteq I_n$. Koska I_n on äärellinen, on olemassa sellaiset kokonaisluvut l ja m, $l > m \geq 1$, joille $\alpha^l(1) = \alpha^m(1)$, eli $\alpha^{l-m}(1) = 1$. Merkitään $p = l - m$. Täten $\alpha^p(1) = 1$ jollakin $p > 0$. On siis osoitettu, että on olemassa sellainen positiivinen kokonaisluku p, jolle $\alpha^p(1) = 1$. Olkoon nyt j pienin tällainen kokonaisluku. Olkoon $A = \{1, \alpha(1), \alpha^2(1), \ldots, \alpha^{j-1}(1)\}$, missä kaikki joukon A alkiot ovat eri lukuja, sillä α on kuvaus (jos pätisi $\alpha^a(1) = \alpha^b(1)$ joillakin $a, b \in \{1, \ldots, j-1\}$, niin α ei olisi kuvaus). Olkoon $\tau = (1\ \ \alpha(1)\ \ \alpha^2(1)\ \cdots\ \alpha^{j-1}(1)) \in S_n$ joukon $A \subseteq I_n$ sykli. Merkitään $B = I_n \backslash A$. Jos $B = \emptyset$, niin $I_n = A$, joten α on sykli. Oletetaan siis, että $B \neq \emptyset$. Olkoon $\sigma = \alpha \restriction B$. Jos $\sigma = (1)$, niin $\alpha(a) = a$ kaikilla $a \in B$, joten α on sykli. Oletetaan, että $\sigma \neq (1)$. Nyt induktio-oletuksen nojalla σ on tulo joukon $B \subset I_n$ erillisiä syklejä. Olkoon $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r$ tällainen tulo. Määritellään jokaiselle $i \in \{1, \ldots, r\}$ sellainen kuvaus $\alpha_i \colon I_n \to I_n$, että

$$\alpha_i(a) = \begin{cases} \sigma_i(a), & \text{kun } a \in B \\ a, & \text{kun } a \notin B. \end{cases}$$

Selvästi α_i on permutaatio kaikilla $i \in \{1, \ldots, r\}$. Olkoon $a \in B$. Tällöin $\alpha_i(a) = \sigma_i(a)$ kaikilla $i \in \{1, \ldots, r\}$, joten kaikki permutaatiot α_i , $i \in \{1, \ldots, r\}$, ovat keskenään erillisiä syklejä. Toisaalta $\tau(a) = a$, sillä $a \notin A$. Täten määritelmän 2.11 ehto on aina tosi. Siis permutaatiot $\alpha_1, \ldots, \alpha_r$ ja τ ovat erillisiä syklejä. Lisäksi

$$(\alpha_1 \circ \cdots \circ \alpha_r \circ \tau)(a) = (\sigma_1 \circ \cdots \circ \sigma_r)(\tau(a)) = \sigma(a) = (\alpha \restriction B)(a) = \alpha(a).$$

Oletetaan sitten, että $a \notin B$. Tällöin $\alpha_i(a) = a$ kaikilla $i \in \{1, \ldots, r\}$. Täten permutaatiot $\alpha_1, \ldots, \alpha_r$ ja τ ovat selvästi keskenään erillisiä. Saadaan edelleen, että

$$\begin{aligned}&(\alpha_1 \circ \cdots \circ \alpha_r \circ \tau)(a) = (\tau \circ \alpha_1 \circ \cdots \circ \alpha_r)(a) = \\ &(\tau)((\alpha_1 \circ \cdots \circ \alpha_r)(a)) = \tau(a) = \alpha(a).\end{aligned}$$

Ollaan siis saatu, että $\alpha_1, \alpha_2, \ldots, \alpha_r$ ja τ ovat ryhmän S_n erillisiä syklejä ja $\alpha_1 \circ \cdots \circ \alpha_r \circ \tau = \alpha$. Permutaatio α on näin ollen erillisten syklien tulo.

Yksikäsitteisyyden osoittamiseksi, olkoon

$$\alpha = \alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_r = \beta_1 \circ \beta_2 \circ \cdots \circ \beta_s,$$

jolloin permutaatio $\alpha \in S_n$ on esitetty kahdella eri tavalla erillisten syklien tulona. Osoitetaan, että jokainen α_i, $i \in \{1, \ldots, r\}$, on jokin β_j, $j \in \{1, \ldots, s\}$, ja vastaavasti, että jokainen β_k, $k \in \{1, \ldots, s\}$ on yhtä suuri jonkin syklin β_t, $t \in \{1, \ldots, r\}$, kanssa. Kiinnitetään α_i jollakin $i \in \{1, \ldots, r\}$. Olkoon $\alpha_i = (i_1\ \ i_2\ \cdots\ i_l)$, jolloin permutaatio α liikuttaa lukua i_1. Edelleen koska $\alpha = \beta_1 \circ \cdots \circ \beta_s$, niin jokin sykli β_j, $j \in \{1, \ldots, s\}$, liikuttaa myös lukua i_1. Koska erityisesti syklit ovat erillisiä,

niin tämä β_j on lisäksi yksikäsitteinen. Täten voidaan kirjoittaa syklille β_j esitys: $\beta_j = (i_1 \ c_1 \ c_2 \ \cdots \ c_m)$. Nyt

$$\begin{aligned}
&i_2 = \alpha_i(i_1) = \alpha(i_1) = \beta_j(i_1) = c_2,\\
&i_3 = \alpha_i(i_2) = \alpha(i_2) = \alpha(c_2) = \beta_j(c_2) = c_3,\\
&\ldots\\
&i_l = \alpha_i(i_{l-1}) = \alpha(i_{l-1}) = \alpha(c_{l-1}) = \beta_j(c_{l-1}) = c_l.
\end{aligned}$$

Siis $i_x = c_x$ kaikilla $x \in \{2, \ldots, l\}$. Jos $l < m$, niin $i_1 = \alpha_i(i_l) = \alpha(i_l) = \alpha(c_l) = \beta_j(c_l) = c_{l+1}$. Jos taas $l > m$, niin vastaavasti $i_1 = i_{m+1}$. Molemmissa tapauksissa päädytään näin ollen ristiriitaan. Siis $l = m$. Täten ollaan saatu, että $\alpha_i = \beta_j$. Täysin vastaavalla tavalla voidaan osoittaa, että jokaisella β_k, $k \in \{1, \ldots, s\}$, on olemassa sellainen α_t, $t \in \{1, \ldots, r\}$, että $\beta_k = \alpha_t$. Yksikäsitteisyys on myös näin ollen todistettu. □

Seuraus 2.14. *Olkoon $n \geq 2$. Jokainen symmetriaryhmän S_n permutaatio voidaan esittää vaihtojen tulona.*

Todistus (vrt. [11, s. 90]). Edeltävän lauseen nojalla riittää osoittaa, että jokainen sykli voidaan esittää vaihtojen tulona. Ensinnäkin

$$(1) = (1 \ \ 2) \circ (1 \ \ 2).$$

Olkoon sitten $(i_1 \ i_2 \ \cdots \ i_k)$, $k \geq 2$, symmetriaryhmän S_n sykli, jolloin $\{i_1, \ldots, i_k\} \subseteq I_n$. Olkoon $i_j \in \{i_1, \ldots, i_k\}$. Tällöin

$$\begin{aligned}
&\big((i_1 \ i_2) \circ (i_2 \ i_3) \circ \cdots \circ (i_{k-1} \ i_k)\big)(i_j) =\\
&\big((i_1 \ i_2) \circ \cdots \circ (i_{j-1} \ i_j) \circ (i_j \ i_{j+1}) \circ \cdots \circ (i_{k-1} \ i_k)\big)(i_j) =\\
&\Big((i_1 \ i_2) \circ \cdots \circ (i_{j-1} \ i_j) \circ (i_j \ i_{j+1})\Big)\Big(\big((i_{j+1} \ i_{j+2}) \circ \cdots \circ (i_{k-1} \ i_k)\big)(i_j)\Big) =\\
&\big((i_1 \ i_2) \circ \cdots \circ (i_{j-1} \ i_j) \circ (i_j \ i_{j+1})\big)(i_j) =\\
&\big((i_1 \ i_2) \circ \cdots \circ (i_{j-1} \ i_j)\big)\big((i_j \ i_{j+1})(i_j)\big) =\\
&\big((i_1 \ i_2) \circ \cdots \circ (i_{j-1} \ i_j)\big)(i_{j+1}) = i_{j+1} = (i_1 \ i_2 \ \cdots \ i_j \ i_{j+1} \ \cdots \ i_k)(i_j).
\end{aligned}$$

Siis $(i_1 \ i_2 \ \cdots \ i_k) = (i_1 \ i_2) \circ (i_2 \ i_3) \circ \cdots \circ (i_{k-1} \ i_k)$. □

Esimerkki 2.1 (vrt. [11], tehtävät 17 ja 18, s. 97)**.** Tarkastellaan symmetriaryhmän S_n ($n \geq 2$) syklin α kertalukua $\mathrm{ord}(\alpha)$. Koska S_n on äärellinen, tiedetään, että $\mathrm{ord}(\alpha)$ on äärellinen. Hyvin nopeasti havaitaan, että jos α on k-sykli, niin $\mathrm{ord}(\alpha) = k$. Kyseinen väite pätee sykleille itseasiassa myös kääntäen. Osoitetaan siis, että α on k-sykli, jos ja vain jos $\mathrm{ord}(\alpha) = k$.

Oletetaan ensin, että α on k-sykli. Olkoon $\alpha = (i_1 \ i_2 \ \cdots \ i_k)$. On osoitettava, että k on pienin positiivinen kokonaisluku, jolle pätee $\alpha^k = (1)$. Valitaan $i_j \in \{i_1, \ldots, i_k\}$, jolloin $1 \leq j \leq k$. Nyt

$$\alpha^k(i_j) = \alpha^j(\alpha^{k-j}(i_j)) = \alpha^j(i_k) = \alpha^{j-1}(i_1) = i_j, \text{ joten } \alpha^k = (1).$$

Jos olisi olemassa $m < k$, jolle $\alpha^m = (1)$, niin $i_k = \alpha^m(i_k) = \alpha^{m-1}(i_1) = i_m \neq i_k$, mikä on ristiriita. Siis $\text{ord}(\alpha) = k$.

Jos kääntäen pätee, että $\text{ord}(\alpha) = k$ ja α on sykli, niin α on r-sykli ($r \geq 2$), jolloin edellä osoitetun nojalla $k = \text{ord}(\alpha) = r$. Siis α on k-sykli.

Tarkastellaan sitten symmetriaryhmän S_n ($n \geq 2$) permutaatiota σ. Ensinnäkin lauseen 2.13 mukaan permutaatio σ voidaan esittää erillisten syklien tulona: $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$. Esitetään kätevä tapa määrittää minkä tahansa permutaation kertaluku siitä muodostettujen erillisten syklien kertalukujen avulla. Kun nimittäin tiedetään jokaisen erillisen syklin kertaluku, joka on siis aiemmin osoitetun perusteella syklin pituus, on permutaation kertaluku pienin yhteinen jaettava näistä syklien kertaluvuista. Todistetaan tämä. Merkitään $\text{ord}(\sigma_i) = n_i$ kaikilla $i \in \{1, \ldots, r\}$ ja $d = \text{ord}(\sigma)$. On osoitettava, että $d = \text{pyj}(n_1, \ldots, n_r)$. Osoitetaan ensin, että $n_i \mid d$ kaikilla $i \in \{1, \ldots, r\}$. Tarkastellaan sykliä σ_i, $i \in \{1, \ldots, r\}$. Aiemmin saadun perusteella σ_i on n_i-sykli, joten voidaan olettaa, että $\sigma_i = (i_1 \ i_2 \ \cdots \ i_{n_i})$. Merkitään $A = \{i_1, \ldots, i_{n_1}\}$. Koska syklit $\sigma_1, \ldots, \sigma_r$ ovat erillisiä, niin $\sigma(i_j) = \sigma_i(i_j)$ kaikilla $i_j \in A$. Täten $\sigma_i^d(i_j) = \sigma^d(i_j) = (1)(i_j) = i_j$ kaikilla $i_j \in A$, joten $\sigma_i^d = (1)$. Siis lauseen 1.38 nojalla $n_i \mid d$.

Oletetaan vielä, että $n_i \mid c$ kaikilla $i \in \{1, \ldots, r\}$, missä $c \in \mathbb{Z}_+$. On osoitettava, että tällöin $d \mid c$. Tarkastellaan taas jotakin tiettyä sykliä σ_i, $i \in \{1, \ldots, r\}$. Olkoon $\sigma_i = (i_1 \ i_2 \ \cdots \ i_{n_i})$. Nyt koska $n_i \mid c$, niin $c = mn_i$ jollakin $m \in \mathbb{Z}_+$. Vastaavasti kuin aiemmin, syklien erillisyydestä seuraa

$$\sigma^c(i_j) = \sigma_i^c(i_j) = \sigma^{mn_i}(i_j) = i_j \text{ kaikilla } i_j \in \{i_1, \ldots, i_{n_1}\}.$$

Täten $\sigma^c = (1)$, joten lauseesta 1.38 seuraa, että $d \mid c$. On siis osoitettu, että $\text{ord}(\sigma) = d = \text{pyj}(n_1, \ldots, n_r)$.

2.2 Permutaation merkki ja alternoiva ryhmä

Toisin kuin erillisten syklien tapauksessa, symmetriaryhmän permutaation esitys vaihtojen tulona ei ole yksikäsitteinen. Voidaan kuitenkin osoittaa, että mielivaltainen permutaatio voidaan kirjoittaa joko parillisena tai parittomana lukumääränä vaihdoista, mutta ei yhtä aikaa molempina. Tarkastellaan permutaatiota $\alpha \in S_n$ ja oletetaan, että sillä on kaksi erilaista esitystä vaihtojen tulona: ensimmäisessä esityksessä permutaatioita on r kappaletta, ja toisessa s kappaletta. Jos pystytään osoittamaan, että tällöin r ja s ovat kongruentteja modulo 2, niin luvun r parillisuudesta seuraa luvun s parittomuus ja päinvastoin. Tällöin haluttu väite siis pätisi. Tästä seuraakin nyt esitettävä lause.

Lause 2.15. *Olkoon $\alpha \in S_n$ vaihtojen tulo kahdella eri tavalla:*

$$\alpha = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s.$$

Tällöin $r \equiv s \pmod 2$.

Todistus (vrt. [4, s. 2–3]). Nyt

$$(1) = \alpha \circ \alpha^{-1} = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r \circ \sigma_s \circ \sigma_{s-1} \circ \cdots \circ \sigma_1.$$

Identiteettipermutaatio on siis vaihtojen tulo, missä vaihtojen lukumäärä on $r + s$. Täten riittää osoittaa, että identiteettipermutaatio voidaan esittää vain sellaisten vaihtojen tulona, joita on parillinen lukumäärä. Tällöinhän $r + s$ olisi parillinen, mistä seuraisi $r \equiv s \pmod 2$.

Olkoon symmetriaryhmän S_n identiteettipermutaatio seuraava mielivaltainen vaihtojen tulo:

$$(1) = (a_1 \;\; b_1) \circ (a_2 \;\; b_2) \circ \cdots \circ (a_n \;\; b_n), \tag{2.1}$$

missä $n \geq 1$ ja $a_i \neq b_i$ kaikilla $i \in \{1, \ldots, n\}$. Merkitään $\rho = (a_1 \;\; b_1) \circ \cdots \circ (a_n \;\; b_n)$. Esityksessä (2.1) $n \neq 1$, sillä muuten ρ ei olisi (1). Jos $n = 2$, niin $\rho = (a_1 \;\; b_1) \circ (a_2 \;\; b_2)$, joten (1) on kahden vaihdon tulo. Oletetaan nyt, että $n \geq 3$, ja todistetaan väite induktiolla luvun n suhteen. Oletetaan, että identiteettipermutaatiolla, jolla on vähemmän kuin n vaihtoa tuloesityksessä, on parillinen määrä vaihtoja.

Esityksessä (2.1) on olemassa sellainen vaihto (a_j, b_j), missä $j > 1$, että vaihdot (a_1, b_1) ja (a_j, b_j) ovat epäerillisiä, sillä muuten ρ ei olisi identiteettipermutaatio. Olkoon $i > 1$ pienin joukon $\{2, \ldots, n\}$ luvuista, jolla $(a_1 \;\; b_1)$ ja $(a_i \;\; b_i)$ eivät ole erillisiä. Nyt voidaan olettaa, että $a_1 = a_i$, sillä tämä on vain merkintöjen kiinnittämisestä kiinni (yhtä hyvin voitaisiin olettaa, että $b_1 = b_i$, $a_1 = b_i$ tai $b_1 = a_i$, mutta tällöin tarkastelu jatkuisi täysin vastaavasti). Nyt $(c \;\; d) \circ (a \;\; b) = (a \;\; b) \circ (c \;\; d)$ ja $(b \;\; c) \circ (a \;\; b) = (a \;\; c) \circ (b \;\; c)$ eri luvuilla $a, b, c, d \in I_n$. Näin ollen vaihto $(a_i \;\; b_i)$ voidaan siirtää esityksessä (2.1) vaihdon $(a_1 \;\; b_1)$ viereen:

$$\begin{aligned}&(a_1 \;\; b_1) \circ \cdots \circ (a_n \;\; b_n) = (a_1 \;\; b_1) \circ \cdots \circ (a_i \;\; b_i) \circ \cdots \circ (a_n \;\; b_n) = \\ &(a_1 \;\; b_1) \circ (a_i \;\; b_i) \circ (a'_3 \;\; b'_3) \circ \cdots \circ (a'_{i-1} \;\; b'_{i-1}) \circ (a_{i+1} \;\; b_{i+1}) \circ \cdots \circ (a_n \;\; b_n),\end{aligned}$$

missä $a'_k, b'_k \in \{a_i, b_i \mid i \in I_n\}$ kaikilla $k \in \{3, \ldots, i-1\}$. Täten voidaan hyvin olettaa, että esityksessä (2.1) $a_1 = a_2$.

Jos $b_2 = b_1$, niin $(a_1 \;\; b_1) \circ (a_1 \;\; b_2)$ on identiteettipermutaatio, jolloin ρ on enää $n - 2$ vaihtoa sisältävä tulo. Tällöin induktio-oletuksen nojalla $n - 2$ on parillinen, ja siis n on parillinen.

Jos taas $b_2 \neq b_1$, niin $(a_1 \;\; b_1) \circ (a_1 \;\; b_2) = (a_1 \;\; b_2) \circ (b_1 \;\; b_2)$. Siis $\rho = (a_1 \;\; b_2) \circ (b_1 \;\; b_2) \circ \cdots \circ (a_n \;\; b_n)$. Nyt permutaatio ρ on edelleen n vaihtoa sisältävä tulo, mutta vaihtoja, jotka voivat liikuttaa lukua a_1 on yksi vähemmän, sillä $(b_1 \, b_2)$ ei liikuta lukua a_1 (jos se liikuttaisi, olisi oltava $b_2 = a_1$, mistä seuraisi, että permutaatiossa ρ olisi yksi vaihto vähemmän. Tällöin haluttu tulos seuraisi induktio-oletuksesta). Edelleen jonkin toisen vaihdon kuin $(a_1 \, b_2)$ on liikutettava lukua a_1, sillä muuten ρ ei olisi identiteettipermutaatio. Täten vastaavalla tavalla kuin edellä voidaan olettaa, että seuraavaksi $(a_3 \, b_3)$ liikuttaa lukua a_1, jolloin siis $a_3 = a_1$ ja vaihtojen lukumäärää voidaan vähentää kahdella ja todeta, että väite pätee induktio-oletuksen nojalla tai niiden vaihtojen lukumäärä, jotka voivat liikuttaa lukua a_1, laskee yhdellä.

Jatketaan tätä niin kauan, kunnes voidaan olettaa, että vain $(a_n \; b_n)$ liikuttaa lukua a_1, jolloin $a_n = a_1$. Tällöin $\rho = (a_1 \;\; b_{n-1}) \circ (a_1 \;\; b_n) \circ (b_{n-2} \;\; b_{n-1}) \circ \cdots \circ$

$(b_2 \;\; b_3) \circ (b_1 \;\; b_2)$, missä mikään muu vaihto (vaihdon $(a_1 \;\; b_{n-1})$ lisäksi) kuin $(a_1 \;\; b_n)$ ei enää liikuta lukua a_1. Jos $b_{n-1} = b_n$, niin tulos seuraa induktio-oletuksesta kuten aiemmin. Jos taas $b_{n-1} \neq b_n$, niin $\rho = (a_1 \;\; b_n) \circ (b_{n-1} \;\; b_n) \circ \cdots \circ (b_1 \;\; b_2)$, jolloin mikään permutaatioista, paitsi $(a_1 \;\; b_n)$, ei enää liikuta lukua a_1. Tämä on ristiriita, sillä ρ oli identiteettipermutaatio. On siis oltava lopulta $b_{n-1} = b_n$, ja väite seuraa joka tapauksessa induktio-oletuksesta. Täten induktiolla on osoitettu, että n on parillinen. □

Lauseen 2.15 perusteella voidaan määritellä permutaation merkki. Permutaation parillisuus voidaan edelleen määritellä sen mukaan, onko tuloesityksessä parillinen vai pariton määrä vaihtoja. Näin on mielekästä määritellä, sillä lauseen 2.15 nojalla siitä, että symmetriaryhmän permutaatiolla on parillinen määrä vaihtoja, seuraa, että sen kaikki muut mahdolliset esitykset vaihtojen tuloina sisältävät edelleen parillisen määrän vaihtoja. Vastaavasti käy parittomille permutaatioille.

Määritelmä 2.16. Olkoon $\alpha \in S_n$ permutaatio, jonka tuloesityksessä on r vaihtoa. Tällöin lukua $(-1)^r$ kutsutaan permutaation α *merkiksi*, ja sitä merkitään symbolilla $\epsilon(\alpha)$.

Määritelmä 2.17. Parillisen lukumäärän vaihtoja tuloesityksessään sisältävää permutaatiota $\alpha \in S_n$ kutsutaan *parilliseksi*. Muuten permutaatiota α kutsutaan *parittomaksi*.

Huomautus. Edeltävistä määritelmistä seuraa, että jos $\alpha \in S_n$, niin permutaatio α on parillinen, jos ja vain jos $\epsilon(\alpha) = 1$, ja pariton, jos ja vain jos $\epsilon(\alpha) = -1$.

Lause 2.18. *Olkoot $\alpha, \beta \in S_n$. Tällöin $\epsilon(\alpha \circ \beta) = \epsilon(\alpha)\epsilon(\beta)$.*

Todistus (ks. [4, s. 4]). $\epsilon(\alpha \circ \beta) = (-1)^{r+s} = (-1)^r(-1)^s = \epsilon(\alpha)\epsilon(\beta)$, kun r ja s ovat vaihtojen lukumäärät permutaatioissa α ja β. □

Määritellään seuraavaksi symmetriaryhmän tärkein erikoistapaus eli alternoiva ryhmä.

Määritelmä 2.19. *Alternoiva ryhmä* $(A_n, \circ)$ on pari, missä joukko A_n on symmetriaryhmän S_n osajoukko, joka koostuu kaikista sen parillisista permutaatiosta. Täten voidaan merkitä, että $A_n := \{\alpha \in S_n \mid \epsilon(\alpha) = 1\}$.

Lause 2.20. *Kun $n \geq 2$, niin pari $(A_n, \circ)$ on ryhmä.*

Todistus (vrt. [11, s. 94]). Koska A_n on joukon S_n osajoukko, riittää ryhmän määritelmän nojalla osoittaa, että A_n on suljettu laskutoimituksen $\circ$ suhteen ja että jokaisen alternoivan ryhmän permutaation käänteiskuvaus on alkiona alternoivassa ryhmässä. Ensinnäkin $A_n \neq \emptyset$, sillä $(1) = (1 \;\; 2) \circ (1 \;\; 2)$. Olkoot $\alpha, \beta \in A_n$. Tällöin lauseen 2.18 perusteella $\epsilon(\alpha \circ \beta) = \epsilon(\alpha)\epsilon(\beta) = 1 \cdot 1 = 1$, joten $\alpha \circ \beta \in A_n$. Jos $\tau \in A_n$, niin $1 = \epsilon((1)) = \epsilon(\tau \circ \tau^{-1}) = \epsilon(\tau)\epsilon(\tau^{-1}) = \epsilon(\tau^{-1})$, joten $\tau^{-1} \in A_n$. On siis osoitettu, että $(A_n, \circ)$ on ryhmä. □

Seuraava lause kertoo alternoivan ryhmän perusominaisuuksista.

Lause 2.21.

(i) *Jos $n \geq 3$, niin alternoivan ryhmän A_n jokainen alkio voidaan esittää 3-syklien tulona.*

(ii) $|A_n| = \frac{n!}{2}$.

Todistus. (i) Ks. [11, s. 94]. Olkoon $\alpha \in A_n$. Tällöin $\alpha = \alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_r$, missä α_i on vaihto kaikilla $i \in \{1, \ldots r\}$ ja r on parillinen. Nyt mille tahansa symmetriaryhmän vaihdolle $(a \;\; b)$, missä $1 \notin \{a, b\}$, pätee:

$$(a \;\; b) = (1 \;\; a) \circ (1 \;\; b) \circ (1 \;\; a).$$

Täten

$$\alpha = (1 \;\; i_1) \circ (1 \;\; i_2) \circ \cdots \circ (1 \;\; i_m),$$

missä m on parillinen ja $i_k \in I_n$ kaikilla $k \in \{1, \ldots, m\}$. Koska $(1 \;\; i_1) \circ (1 \;\; i_2) = (1 \;\; i_2 \;\; i_1)$, niin α on todellakin 3-syklien tulo.

(ii) Vrt. [4, s. 7]. Tarkastellaan vaihtoa $\tau = (1 \;\; 2)$. Nyt $A_n\tau = \{\alpha \circ \tau \mid \alpha \in A_n\}$. Olkoon σ symmetriaryhmän S_n permutaatio, jolle $\sigma \notin A_n$. Täten

$$\epsilon(\sigma \circ \tau) = \epsilon(\sigma)\epsilon(\tau) = (-1) \cdot (-1) = 1,$$

joten $\sigma \circ \tau \in A_n$. Merkitään $\rho = \sigma \circ \tau$. Nyt $\sigma = \rho \circ \tau^{-1} = \rho \circ \tau \in A_n\tau$. Symmetriaryhmä voidaan näin ollen esittää kahden sen osajoukkonsa yhdisteenä:

$$S_n = A_n \cup A_n\tau.$$

Nyt $A_n \cap A_n\tau = \emptyset$, sillä jos olisi $\alpha \in A_n \cap A_n\tau$, niin $1 = \epsilon(\alpha) = -1$, mikä on ristiriita. Edelleen kuvaus $f\colon A_n \to A_n\tau$, $f(\alpha) = \alpha \circ \tau$ on selvästi bijektio, joten $|A_n| = |A_n\tau|$. Siis $n! = |S_n| = |A_n| + |A_n\tau| = 2\,|A_n|$. □

3 Lagrangen lause ja normaalit aliryhmät

Luvun 3 tarkoituksena on esitellä sellaisia ryhmäteorian perustuloksia ja -käsitteitä, kuten aliryhmä, diedriryhmä, syklinen ryhmä, sivuluokka, Lagrangen[1] lause, normaali aliryhmä, tekijäryhmä ja yksinkertainen ryhmä. Useat tämän luvun tuloksista, kuten Lagrangen lause, oletetaan tunnetuiksi, eikä niille siten esitetä todistusta. Sen sijaan alternoivan ryhmän A_n yksinkertaisuus, kun $n \geq 5$, tullaan osoittamaan täsmällisesti luvun 2 tietojen perusteella. Tutkielmassa jatkossa useasti käytetty lause 3.27, jota kutsutaan tulokaavaksi, tullaan myös todistamaan. Lukija voi tarvittaessa syventää tämän luvun tietoja teoksen *Fundamentals of Abstract Algebra* [11, s. 99 – 136] pohjalta.

3.1 Aliryhmän määritelmä

Edellisessä luvussa tarkasteltiin symmetriaryhmää, ja erityisesti sen erikoistapausta eli alternoivaa ryhmää, missä A_n on joukon S_n osajoukko. Lauseessa 2.20 osoitettiin, että pari $(A_n, \circ)$ on ryhmä. Onkin mielekästä määritellä tämän perusteella ryhmän aliryhmä seuraavalla luonnollisella tavalla. Lisäksi määritellään triviaalin ryhmän ja aliryhmän käsitteet.

Määritelmä 3.1. Olkoon $(G, *)$ ryhmä ja H joukon G epätyhjä osajoukko. Tällöin paria $(H, *)$ kutsutaan ryhmän $(G, *)$ *aliryhmäksi*, jos $(H, *)$ on ryhmä. Kun H on ryhmän G aliryhmä, merkitään toisinaan lyhyemmin $H \leqslant G$. Jos H on erityisesti ryhmän G aito osajoukko, merkitään $H < G$.

Huomautus. Ryhmän $(G, *)$ ja sen aliryhmän $(H, *)$ laskutoimituksille käytetään tavanomaisesti samaa symbolia $*$, vaikka oikeastaan aliryhmän H laskutoimitus on rajoittuma ryhmän G vastaavasta laskutoimituksesta eli $* \restriction (H \times H)$.

Määritelmä 3.2. Ryhmä G on *triviaali*, jos $G = \{e\}$, ja *epätriviaali*, jos $G \neq \{e\}$. Ryhmän G aliryhmiä $\{e\}$ ja G sanotaan *triviaaleiksi aliryhmiksi*.

Seuraavassa lauseessa esitetään kaksi yhtäpitävää ehtoa ryhmän aliryhmälle. Viimeisintä näistä kutsutaan toisinaan myös aliryhmäkriteeriksi.

Lause 3.3. *Olkoon G ryhmä ja H joukon G epätyhjä osajoukko. Seuraavat kohdat ovat tällöin yhtäpitäviä.*

(i) *H on ryhmän G aliryhmä.*

[1]Joseph Louis Lagrange (1736–1813), syntymänimeltään Giuseppe Lodovico Lagrangia, oli italialais-ranskalainen matemaatikko ja astronomi, joka työskenteli ryhmäteorian lisäksi muun muassa lukuteorian, differentiaaliyhtälöiden, taivaanmekaniikan ja virtausmekaniikan parissa. Vuonna 1770 Lagrange todisti kuuluisan Lagrangen lauseen. [11, s. 139], [22]

(ii) *Seuraavat kolme ehtoa toteutuvat:*
   1. $e \in H$.
   2. Jos $h \in H$*, niin* $h^{-1} \in H$.
   3. Jos $x, y \in H$*, niin* $xy \in H$.

(iii) $xy^{-1} \in H$ *kaikilla* $x, y \in H$.

Todistus. Sivuutetaan. Kohtien (i) ja (ii) yhtäpitävyys seuraa ryhmän määritelmästä. Kohtien (i) ja (iii) yhtäpitävyydelle ks. [11, s. 100]. □

Entä jos tarkastellaankin perhettä, joka koostuu ryhmän G aliryhmistä? Lause 3.4 osoittaa, että tällaisen perheen leikkaus on myös ryhmän G aliryhmä.

Lause 3.4. *Olkoon* G *ryhmä ja* $\mathcal{H}$ *epätyhjä perhe, joka on kokoelma ryhmän* G *aliryhmiä. Tällöin* $\bigcap \mathcal{H}$ *on ryhmän* G *aliryhmä.*

Todistus (vrt. [11, s. 101]). Käytetään aliryhmäkriteeriä. Kaikilla $H \in \mathcal{H}$ pätee, että $e \in H$, sillä jokainen perheen $\mathcal{H}$ alkio on ryhmän G aliryhmä. Täten $e \in \bigcap \mathcal{H}$, joten $\bigcap \mathcal{H} \neq \emptyset$. Olkoot nyt $x, y \in \bigcap \mathcal{H}$. Olkoon $H \in \mathcal{H}$. Tällöin $x, y \in H$. Edelleen aliryhmäkriteerin nojalla $xy^{-1} \in H$, sillä H on ryhmän G aliryhmä. Siis $xy^{-1} \in \bigcap \mathcal{H}$. On siis osoitettu, että $\bigcap \mathcal{H}$ on ryhmän G aliryhmä. □

Määritelmä 3.5. Olkoon G ryhmä ja S joukon G osajoukko. Olkoon

$$\mathcal{A} = \{H \mid H \text{ on ryhmän } G \text{ aliryhmä ja } S \subseteq H\}.$$

Merkitään

$$\langle S \rangle := \bigcap \mathcal{A}.$$

Tällaista ryhmän G aliryhmää $\langle S \rangle$ kutsutaan *joukon* S *virittämäksi aliryhmäksi*. Jos $G = \langle S \rangle$, niin joukkoa S kutsutaan ryhmän G *virittäjäjoukoksi* ja sanotaan, että joukko S virittää ryhmän G. Erityisesti joukon S ollessa äärellinen sanotaan, että sen alkiot virittävät ryhmän G.

Huomautus. Tällä tavoin määritelty pari $(\langle S \rangle, *)$, missä $*$ on ryhmän G laskutoimitus, on ryhmän G aliryhmä lauseen 3.4 nojalla. Jos $S = \emptyset$ tai $S = \{e\}$, niin $\langle S \rangle = \{e\}$. Lisäksi, $\langle G \rangle = G$.

Seuraava lause täsmentää joukon virittämän aliryhmän rakennetta. Sitä ennen todistetaan lauseessa tarpeellinen lemma.

Lemma 3.6. *Olkoon* S *ryhmän* G *epätyhjä osajoukko. Tällöin* $\langle S \rangle$ *on pienin joukon* G *aliryhmä, joka sisältää joukon* S.

Todistus. Olkoon $\mathcal{A} = \{H \mid H \text{ on ryhmän } G \text{ aliryhmä ja } S \subseteq H\}$. On osoitettava, että kaikilla $H \in \mathcal{A}$ pätee $\langle S \rangle \subseteq H$. Olkoon $H \in \mathcal{A}$. Olkoon $h \in \langle S \rangle$. Koska $\langle S \rangle = \bigcap \mathcal{A}$, niin kaikilla $A \in \mathcal{A}$ pätee, että $h \in A$. Nyt erityisesti $H \in \mathcal{A}$, joten $h \in H$. Siis $\langle S \rangle \subseteq H$. □

Lause 3.7. *Olkoon S ryhmän G epätyhjä osajoukko. Tällöin*

$$\langle S\rangle = \{s_1^{e_1}\cdots s_n^{e_n} \mid s_i \in S, e_i \in \{1,-1\}, i \in \{1,\ldots,n\}, n \in \mathbb{Z}_+\}.$$

Todistus (vrt. [11, s. 102]). Merkitään

$$A = \{s_1^{e_1}\cdots s_n^{e_n} \mid s_i \in S, e_i \in \{1,-1\}, i \in \{1,\ldots,n\}, n \in \mathbb{Z}_+\}.$$

Olkoon $\mathcal{A} = \{H \mid H \text{ on ryhmän } G \text{ aliryhmä ja } S \subseteq H\}$. Osoitetaan ensin, että $A \subseteq \langle S\rangle$. Olkoon $s_1^{e_1}\cdots s_n^{e_n} \in A$. Olkoon $H \in \mathcal{A}$ eli H on ryhmän G aliryhmä, jolle $S \subseteq H$. Nyt $s_1, \ldots s_n \in S \subseteq H$, joten koska H on ryhmä, niin $s_1^{e_1}\cdots s_n^{e_n} \in H$. Siis $s_1^{e_1}\cdots s_n^{e_n} \in \bigcap \mathcal{A} = \langle S\rangle$. Siten $A \subseteq \langle S\rangle$.

Osoitetaan sitten, että $\langle S\rangle \subseteq A$. Lemman 3.6 nojalla riittää osoittaa, että A on ryhmän G aliryhmä, joka sisältää joukon S. Kaikilla $s \in S$ pätee, että $s = s^1 \in A$, joten $S \subseteq A$. Olkoot sitten $s_1^{e_1}\cdots s_n^{e_n}, t_1^{f_1}\cdots t_m^{f_m} \in A$. Tällöin

$$(s_1^{e_1}\cdots s_n^{e_n})(t_1^{f_1}\cdots t_m^{f_m})^{-1} = s_1^{e_1}\cdots s_n^{e_n} t_m^{-f_m}\cdots t_1^{-f_1} \in A.$$

Siis aliryhmäkriteerin nojalla A on ryhmän G aliryhmä. Täten $\langle S\rangle \subseteq A$. □

Merkintä 3.8. Kun $g_1, \ldots, g_n$ ovat ryhmän G alkioita, niin joukon $\{g_1, \ldots, g_n\}$ virittämälle aliryhmälle käytetään merkintää $\langle g_1, \ldots, g_n\rangle$ matemaattisesti johdonmukaisemman merkinnän $\langle\{g_1, \ldots, g_n\}\rangle$ sijasta.

Nyt esitettävä tulos seuraa suoraan lauseesta 3.7.

Seuraus 3.9. *Olkoon g ryhmän G alkio. Tällöin $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$.*

Todistus. Ks. [11, s. 102]. □

Tarkastellaan seuraavaksi tärkeää sovellusta kahden alkion muodostaman joukon virittämästä ryhmästä, jota kutsutaan diedriryhmäksi.

Määritelmä 3.10. Ryhmää G kutsutaan asteen $n \geq 3$ *diedriryhmäksi*, jos ryhmän G virittää kaksi sen eri alkioita a ja b niin, että $\operatorname{ord}(a) = n$, $\operatorname{ord}(b) = 2$ ja $ba = a^{-1}b$. Asteen n diedriryhmää merkitään symbolilla D_n.

Huomautus. Diedriryhmän olemassaolo ja yksikäsitteisyys eivät ole triviaaleja faktoja. Kombinatorisen ryhmäteorian avulla voidaan kuitenkin osoittaa, että diedriryhmät ovat olemassa ja yksikäsitteisiä. Luvussa 4 käsitellään konkreettinen esimerkki diedriryhmästä, mikä osoittaa myös sen olemassaolon.

Diedriryhmä on tärkeä esimerkki äärellisestä ja epävaihdannaisesta ryhmästä, jolla on parillinen kertaluku. Osoitetaan, että näin todellakin on.

Lause 3.11. *Olkoon $n \geq 3$. Tällöin diedriryhmän D_n kertaluku on $2n$ ja D_n ei ole Abelin ryhmä.*

Todistus (vrt. [11, s. 167]). Määritelmän mukaan $D_n = \langle a, b\rangle$, missä $\text{ord}(a) = n$, $\text{ord}(b) = 2$ ja $ba = a^{-1}b$. Nyt lauseen 3.7 perusteella

$$D_n = \{s_1^{e_1} \cdots s_n^{e_n} \mid s_i \in \{a, b\}, e_i \in \{1, -1\}, i \in \{1, \ldots, n\}, n \in \mathbb{Z}_+\}.$$

Lisäksi tiedetään, että $b^2 = e$ eli $b = b^{-1}$, $ba = a^{-1}b$ ja $a^n = e$, jolloin $b^{-1}a = ba = a^{-1}b$ ja $b^{-1}a^{-1} = ba^{-1} = a^{-(n-1)}ba^{-n} = ab$ (viimeisin voidaan osoittaa induktiolla). Siis kaikki diedriryhmän alkiot ovat muotoa $a^i b^j$, missä $0 \leq i < n$ ja $0 \leq j < 2$. Edelleen koska $\text{ord}(a) = n$, niin $e, a, a^2, \ldots, a^{n-1}$ ovat eri alkioita, ja myös $b, ab, a^2b, \ldots, a^{n-1}b$ ovat eri alkioita. Oletetaan, että $a^i = a^j b$ joillakin $i, j \in \{1, \ldots, n\}$. Tällöin $b = a^{i-j}$. Jos $i = j$, niin $b = e$, mikä on ristiriita. Jos taas $i \neq j$, niin voidaan merkitä $m = i - j \neq 0$. Silloin kuitenkin $a^m a = ba = a^{-1}b = a^{-1}a^m$, joten $a = a^{-1}$ eli $a^2 = e$, mikä on ristiriita. Näin ollen $a^i \neq a^j b$ kaikilla $i, j \in \{1, \ldots, n\}$, joten

$$\{e, a, a^2, \ldots, a^{n-1}\} \cap \{b, ab, a^2b, \ldots, a^{n-1}b\} = \emptyset$$

Siis $D_n = \{e, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$, joten $|D_n| = 2n$.

Osoitetaan vielä, että D_n ei ole Abelin ryhmä. Jos D_n nimittäin olisi Abelin ryhmä, niin $ab = ba$. Mutta tällöin $ab = ba = a^{-1}b$, joten $a = a^{-1}$, mikä on ristiriita. □

Tarkastellaan seuraavaksi ryhmän aliryhmien tuloa.

Määritelmä 3.12. Olkoot H ja K ryhmän G epätyhjiä osajoukkoja. Joukkojen H ja K *tulo* on joukko

$$HK = \{hk \mid h \in H, k \in K\}.$$

.

Jos $H_1, H_2, \ldots, H_n$ ovat ryhmän G epätyhjiä osajoukkoja, niin näiden joukkojen *tulo* on vastaavasti joukko

$$H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n \mid h_i \in H_i, i = 1, 2, \ldots, n\}.$$

Huomautus. Jos yksiö $\{g\}$ ja H ovat ryhmän G osajoukkoja, niin niiden tuloa merkitään määritelmän 3.12 mukaisen merkinnän $\{g\}H$ sijaan yksinkertaisemmin symbolilla gH. Vastaavasti, jos $\{x\}$ on edelleen ryhmän G yksiö, niin osajoukkojen $\{g\}$, H ja $\{x\}$ tuloa vastaava merkintä on gHx. Yksiöiden $\{g\}$ ja $\{x\}$ tulo on kuitenkin määritelmän mukaisesti yksiö $\{gx\}$, ei alkio gx.

Jos määritelmässä 3.12 H ja K olisivatkin ryhmän G aliryhmiä, niin olisiko tällöin aliryhmien H ja K tulo HK tällöin myös ryhmän G aliryhmä? Näin ei välttämättä ole (ks. esim [11, s. 103]), mutta seuraava lause antaa kaksikin ehtoa sille, milloin HK on ryhmän G aliryhmä.

Lause 3.13. *Olkoot H ja K ryhmän G aliryhmiä. Tällöin aliryhmien H ja K tulo HK on ryhmän G aliryhmä, jos ja vain jos $HK = KH$, jos ja vain jos $HK = \langle H \cup K\rangle$.*

Todistus. Sivuutetaan. Todistus on melko rutiininomainen. Ks. [11, s. 103–104]. □

3.2 Sykliset ryhmät

Nyt esitellään syklisen ryhmän käsite ja siihen liittyvät perustulokset ilman todistusta. Oleellisena tuloksena voidaan pitää lausetta 3.17, joka samaistaa syklisen aliryhmän kertaluvun ja ryhmän alkion kertaluvun käsitteet.

Määritelmä 3.14. Ryhmä G on *syklinen ryhmä*, jos on olemassa sellainen $g \in G$, että

$$G = \langle g \rangle.$$

On helppoa todeta, että jokainen syklinen ryhmä on Abelin ryhmä. Jos nimittäin a ja b ovat syklisen ryhmän $G = \langle g \rangle$ alkioita, niin seurauksen 3.9 perusteella on olemassa sellaiset kokonaisluvut n ja m, että $a = g^n$ ja $b = g^m$. Siis $ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba$.

Lause 3.15. *Jos G on ryhmä ja $g \in G$, niin $\langle g \rangle$ on suppein ryhmän G aliryhmä, jonka alkiona on g.*

Todistus. Ks. [21, s. 28]. □

Seuraava lause täsmentää äärellisen syklisen ryhmän rakennetta. Tämän lauseen todistuksessa tarvitaan jakoyhtälöä (ks. [21, s. 1]) ja käytetään samoja perusteluja kuin kertaluvun määritelmän mielekkyyden perustelussa.

Lause 3.16. *Olkoon $\langle g \rangle$ äärellinen syklinen ryhmä, jonka kertaluku on n. Tällöin $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.*

Todistus. Todistus perustuu seuraukseen 3.9 ja jakoyhtälöön. Ks. [11, s. 111]. □

Lause 3.17. *Olkoon g äärellisen ryhmän G alkio. Tällöin* $\operatorname{ord}(g) = |\langle g \rangle|$.

Todistus. Ks. [21, s. 29–30]. Tulos seuraa myös suoraan edellisestä lauseesta. □

Lauseesta 3.17 seuraakin suoraan tärkeä ehto sille, milloin äärellinen ryhmä on syklinen. Lisäksi voidaan osoittaa, että jokaisen syklisen ryhmän aliryhmä on syklinen (ks. esim. [21, s. 30]).

Seuraus 3.18. *Olkoon G äärellinen ryhmä. Tällöin G on syklinen ryhmä, jos ja vain jos on olemassa sellainen ryhmän G alkio g, että* $\operatorname{ord}(g) = |G|$.

Todistus. Välttämätön ehto ryhmän G syklisyydelle seuraa lauseesta 3.17 ja siitä, että ryhmän G alkion virittämä ryhmä on sen aliryhmä. Riittävä ehto saadaan taas suoraan lauseesta 3.16. □

3.3 Lagrangen lause

Tässä alaluvussa esitetään yksi äärellisen ryhmäteorian perustavaa laatua olevista tuloksista, jota kutsutaan Lagrangen lauseeksi, jonka mukaan äärellisen ryhmän aliryhmän kertaluku jakaa ryhmänsä kertaluvun. Lauseen todistuksessa käytetään sivuluokan käsitettä.

Määritelmä 3.19. Olkoon H ryhmän G aliryhmä ja $g \in G$. Joukkoja

$$gH = \{gh \mid h \in H\} \text{ ja } Hg = \{hg \mid h \in H\}$$

kutsutaan alkion g määräämäksi aliryhmän H *vasemmaksi ja oikeaksi sivuluokaksi*. Kaikkien aliryhmän H vasempien sivuluokkien joukkoa ryhmässä G merkitään symbolilla G/H. Toisin sanoen, $G/H := \{gH \mid g \in G\}$.

Merkintä 3.20. Kun tarkastellaan ryhmää G ja sen aliryhmien H ja K muodostamaa leikkausta $H \cap K$, niin leikkauksen vasempien sivuluokkien joukkoa $G/(H \cap K)$ merkitään lyhyemmin ilman sulkeita joukkona $G/H \cap K$. Näin ollen käsiteltäessä joukkoa $(G/H) \cap K$ sulkeita ei jätetä kirjoittamatta.

Tarkastellaan nyt ryhmää G ja sen aliryhmää H. Määritellään relaatio E asettamalla

$$E = \{(x, y) \in G \times G \mid x = yh \text{ jollain } h \in H\}.$$

Siis $(x, y) \in E$, jos ja vain jos $x = yh$ jollain $h \in H$. On helppoa osoittaa, että näin määriteltynä E on ekvivalenssirelaatio joukossa G. Havaitaan itseasiassa, että ryhmän G alkion g määräämä relaation E ekvivalenssiluokka on aliryhmän H vasen sivuluokka:

$$[g] = \{x \in G \mid (x, g) \in E\} = \{x \in G \mid x = gh \text{ jollain } h \in H\} = \{gh \mid h \in H\} = gH.$$

Silloinhan kaikkien aliryhmän H vasempien sivuluokkien joukko G/H määräytyy vain relaation E kaikista ekvivalenssiluokista, eli $G/H = \{[g] \mid g \in G\}$. Tästä seuraakin nyt esitettävä lause.

Lause 3.21. *Olkoon H ryhmän G aliryhmä. Tällöin seuraavat ehdot ovat voimassa.*

(i) $G = \bigcup G/H = \bigcup_{g \in G} gH$.

(ii) *Kaikilla $x, y \in G$ pätee, että joko $xH = yH$ tai $xH \bigcap yH = \emptyset$.*

(iii) *$xH = yH$, jos ja vain jos $x = yh$ jollakin $h \in H$, jos ja vain jos $y^{-1}x \in H$.*

Todistus. Kuten aiemmin todettiin, niin sivuluokat gH, missä $g \in H$, ovat relaation E ekvivalenssiluokkia ja $G/H = \{[g] \mid g \in G\}$. Täten lauseen 1.13 perusteella G/H on joukon G ositus, mistä seuraa joukon osituksen määritelmän mukaan suoraan kohdat (i) ja (ii). Kohdan (iii) todistus on hyvin suoraviivainen; ks. esim [11, s. 118]. □

Täysin vastaavalla tavalla voitaisiin muodostaa ekvivalenssirelaatio myös oikean sivuluokan kautta. Yleensä kuitenkin käsitellään lähinnä vasempia sivuluokkia, sillä jos g on ryhmän G alkio ja H sen aliryhmä, niin alkion g määräämä vasen ja oikea sivuluokka ovat yhtämahtavat. Seuraava lause paketoikin tämän väitteen.

Lause 3.22. *Olkoon H ryhmän G aliryhmä. Olkoon $\mathcal{R} = \{Hg \mid g \in G\}$ kaikkien aliryhmän H oikeiden sivuluokkien joukko joukossa G. Tällöin*

$$|H| = |gH| = |Hg| \text{ ja } |G/H| = |\mathcal{R}| .$$

Todistus. Lause todistetaan konstruoimalla sopivat bijektiot. Ks. [11, s. 119]. □

Määritelmä 3.23. Olkoon G ryhmä ja H sen aliryhmä. Aliryhmän H vasemmanpuolisten sivuluokkien lukumäärää $|G/H|$ ryhmässä G merkitään symbolilla $(G : H)$. Tätä kutsutaan aliryhmän H *indeksiksi* ryhmässä G.

Aiempien tulosten pohjalta voidaan todistaa Lagrangen lause. Lauseen todistus jätetään tässä kuitenkin lukijalle.

Lause 3.24 (Lagrangen lause)**.** *Olkoon G äärellinen ryhmä ja H ryhmän G aliryhmä. Tällöin aliryhmän H kertaluku jakaa ryhmän G kertaluvun. Erityisesti,*

$$|G| = (G : H)\,|H| .$$

Todistus. Sivuutetaan. Ks. [11, s. 120]. □

Seuraavaksi esitettävän seurauksen 3.25 mukaan ryhmän kertaluku on jaollinen ryhmän minkä tahansa alkion kertaluvulla. Seuraus 3.26 kertoo puolestaan, että kaikki ryhmät, joiden kertaluku on alkuluku, ovat syklisiä. Nämä molemmat seuraavat hyvin suoraviivaisesti Lagrangen lauseesta.

Seuraus 3.25. *Olkoon G äärellinen ryhmä. Tällöin* $\operatorname{ord}(g) \mid |G|$ *aina, kun $g \in G$.*

Todistus. Ks. [11, s. 121]. □

Seuraus 3.26. *Olkoon G ryhmä, jonka kertaluku on alkuluku, ja $g \in G \setminus \{e\}$. Tällöin $G = \langle g \rangle$. G on siis syklinen ryhmä, jonka virittävät kaikki sen alkiot neutraalialkiota lukuun ottamatta.*

Todistus. Ks. [11, s. 121]. □

Tarkastellaan ryhmän G äärellisiä aliryhmiä H ja K. Aiemmin ollaan havaittu, että tulo HK ei ole välttämättä ryhmän G aliryhmä, joten sen kertaluku ei välttämättä jaa ryhmän G kertalukua. Lauseessa 3.27 määritetään kuitenkin tulon HK kertaluvulle hyödyllinen kaava Lagrangen lauseen avulla. Tätä kaavaa kutsutaan sen tärkeyden vuoksi jatkossa lyhyesti tulokaavaksi. Lauseen todistus perustuu hyvin pitkälti samoihin periaatteisiin kuin Lagrangen lauseen todistus.

Lause 3.27 (Tulokaava)**.** *Olkoot H ja K ryhmän G äärellisiä aliryhmiä. Tällöin*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Todistus (vrt. [11, s. 122]). Merkitään $A = H \cap K$. Lauseen 3.4 nojalla A on ryhmän G aliryhmä ja koska $A \subseteq H$, niin A on myös aliryhmän H aliryhmä. Täten Lagrangen lauseen nojalla $|H| = (H : A)\,|A|$. Merkitään $n = (H : A)$. Kaikkien aliryhmän A vasempien sivuluokkien joukossa H/A on siis n eri alkiota. Olkoon $H/A = \{x_1A, x_2A, \ldots, x_nA\}$. Tällöin $H = \bigcup H/A = \bigcup_{i=1}^{n} x_iA$.

Osoitetaan nyt, että $(\bigcup_{i=1}^{n} x_iA)K = \bigcup_{i=1}^{n} x_iK$. Olkoon $x \in (\bigcup_{i=1}^{n} x_iA)K$. Tällöin $x = bk$ joillakin $b \in \bigcup_{i=1}^{n} x_iA$ ja $k \in K$. Edelleen on olemassa sellaiset $x_i \in H, i \in \{1, \ldots, n\}$, ja $a \in A$, että $b = x_ia$. Siis $x = bk = (x_ia)k = x_i(ak)$, missä $ak \in K$, sillä $A \subseteq K$. Täten $x \in \bigcup_{i=1}^{n} x_iK$. Oletetaan toisaalta, että $x \in \bigcup_{i=1}^{n} x_iK$. Silloin $x = x_ik$, missä $x_i \in H$, $i \in \{1, \ldots, n\}$, ja $k \in K$. Nyt $x = x_ik = (x_ie)k$, $e \in A$ ja $x_ie \in \bigcup_{i=1}^{n} x_iA$. Siis $x \in \bigcup_{i=1}^{n} x_iA$. Yhtäsuuruus on näin ollen osoitettu. Tästä seuraakin, että $HK = (\bigcup_{i=1}^{n} x_iA)K = \bigcup_{i=1}^{n} x_iK$.

Osoitetaan sitten, että $x_iK \cap x_jK = \emptyset$ aina, kun $i \neq j$. Oletetaan vastoin tätä väitettä, että $x_iK \cap x_jK \neq \emptyset$ joillakin $i \neq j$. Tällöin lauseen 3.21 nojalla $x_iK = x_jK$, joten $x_i^{-1}x_j \in K$. Koska myös $x_i^{-1}x_j \in H (x_i, x_j \in H)$, niin $x_i^{-1}x_j \in A$, jolloin $x_iA = x_jA$. Mutta tämä on ristiriidassa sen kanssa, että $x_1A, \ldots, x_nA$ ovat eri sivuluokkia. Täten siis $x_iK \cap x_jK = \emptyset$ kaikilla $i \neq j$ eli $x_1K, \ldots, x_nK$ ovat aliryhmän K eri sivuluokkia. Lisäksi lauseen 3.22 mukaan $|K| = |x_iK|$ kaikilla $i = 1, 2, \ldots, n$. Täten

$$|HK| = |x_1K| + \ldots + |x_nK| = \underbrace{|K| + \ldots + |K|}_{n \text{ kertaa}} = n\,|K| = \frac{|H|\,|K|}{|A|} = \frac{|H|\,|K|}{|H \cap K|}.$$

□

Huomautus. Lauseesta 3.27 havaitaan hyvin nopeasti, että se supistuu muotoon

$$|HK| = |H|\,|K|,$$

jos aliryhmillä H ja K ei ole muuta yhteistä alkiota kuin neutraalialkio.

Esimerkki 3.1 (vrt. [19, s. 20] [2])**.** Todistetaan Poincarén lause sen yleisessä muodossa. Olkoon $\mathcal{A}$ äärellinen perhe, joka koostuu ryhmän G aliryhmistä, joilla on äärellinen indeksi. Osoitetaan, että tällöin myös näiden aliryhmien leikkauksen indeksi on äärellinen. Olkoon nyt $\mathcal{A} = \{H_1, \ldots, H_n\}$. Merkitään $\mathcal{R} = \{G/H_i \mid i \in I_n\}$ ja $K = \bigcap \mathcal{A}$. Tarkastellaan kuvausta

$$f : G/K \to \bigtimes \mathcal{R},\ f(xK) = g,$$

missä $g \in \bigtimes \mathcal{R}$ on kuvaus $g : I_n \to \bigcup \mathcal{A}, g(i) = xH_i$. Osoitetaan, että f on näin määriteltynä injektio. Olkoon $f(xK) = f(yK)$, missä $xK, yK \in G/K$. Tällöin on olemassa sellaiset $g, g' \in \bigtimes \mathcal{R}$, että $g = g'$, missä $g(i) = xH_i$ ja $g'(i) = yH_i$ kaikilla $i \in I_n$. Siis $xH_i = yH_i$ kaikilla $i \in I_n$, joten $xK = yK$. Täten f on injektio. Näin ollen

$$(G : K) \leq |\bigtimes \mathcal{R}| = \prod_{1 \leq i \leq n} (G : H_i).$$

Siis $(G : K)$ on äärellinen, sillä indeksit $(G : H_i)$ ovat äärellisiä kaikilla $i \in I_n$.

[2] Scott esittää Poincarén lauseelle pelkän relaation, mutta ei täsmällistä todistusta.

Tarkastellaan nyt kahta syklisiin ryhmiin liittyvää tulosta, joita tullaan hyödyntämään jatkossa. Esitetään ensin näissä tuloksissa tarvittava lukuteoriaan liittyvä lemma. Lukuteorian perustulokset, kuten Eukleiden algoritmin mukainen esitys kahden luvun suurimmalle yhteiselle tekijälle, oletetaan tunnetuksi.

Lemma 3.28. *Olkoot a, b ja c sellaisia kokonaislukuja, että $a \mid c$ ja $b \mid c$. Oletetaan lisäksi, että a ja b ovat keskenään jaottomia. Tällöin $ab \mid c$.*

Todistus. Nyt koska $\text{syt}(a, b) = 1$, niin on olemassa sellaiset $\lambda, \mu \in \mathbb{Z}$, että $1 = \lambda a + \mu b$. Siis $c = c\lambda a + c\mu b$. Koska lisäksi $a \mid c$ ja $b \mid c$, niin $c = k_1 a$ ja $c = k_2 b$ joillakin $k_1, k_2 \in \mathbb{Z}$. Tällöin $c = (k_2 b)\lambda a + (k_1 a)\mu b = (k_2\lambda + k_1\mu)ab$, joten $ab \mid c$. □

Tarkastellaan ryhmää G, jolla on kaksi eri alkioita, joilla on äärelliset kertaluvut. Osoitetaan syklisten ryhmien ominaisuuksien sekä Lagrangen lauseen seurausten avulla, että tällöin näiden kertalukujen keskinäisestä jaottomuudesta ja kahden alkion vaihdannaisuudesta seuraa, että kertalukujen tulo vastaa alkioiden tulon kertalukua.

Lause 3.29. *Olkoon G ryhmä, ja a ja b sen alkioita, joiden äärelliset kertaluvut ovat $\text{ord}(a) = n$ ja $\text{ord}(b) = m$. Oletetaan lisäksi, että $\text{syt}(m, n) = 1$ ja $ab = ba$. Tällöin $\text{ord}(ab) = \text{ord}(a)\,\text{ord}(b)$.*

Todistus (vrt. [18], tehtävä 6, s. 5). Merkitään $\text{ord}(ab) = k$. Ensinnäkin koska a ja b ovat keskenään vaihdannaisia, niin $(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m(b^m)^n = e$. Siis lauseen 1.38 kohdan (i) perusteella $k \mid mn$.

Toisaalta $(ab)^k = e$, joten $a^k = b^{-k} = c \in \langle a\rangle \cap \langle b\rangle$. Nyt $|\langle a\rangle| = \text{ord}(a) = n$ ja $|\langle b\rangle| = \text{ord}(b) = m$ lauseen 3.17 perusteella, joten seurauksen 3.25 nojalla $\text{ord}(c) \mid n$ ja $\text{ord}(c) \mid m$. Täten $\text{ord}(c) \mid \text{syt}(m, n)$. Mutta koska $\text{syt}(m, n) = 1$, niin $\text{ord}(c) = 1$, joten $c = e$. Siis $a^k = e = b^k$, mistä lauseen 1.38 kohdan (i) nojalla $m \mid k$ ja $n \mid k$. Koska edelleen $\text{syt}(m, n) = 1$, niin lemmasta 3.28 seuraa, että $mn \mid k$.

Täten ollaan saatu, että $k \mid mn$ ja $mn \mid k$. Näin ollen $\text{ord}(ab) = k = mn = \text{ord}(a)\,\text{ord}(b)$. □

Tarkastellaan sitten kahden äärellisen syklisen ryhmän karteesista tuloa. Osoitetaan, että tämä karteesinen tulo on myös syklinen ryhmä, kun syklisten ryhmien kertaluvut ovat keskenään jaottomia.

Lause 3.30. *Olkoot G ja H alkioiden g ja h virittämiä äärellisiä syklisiä ryhmiä kertaluvuilla n ja m. Oletetaan, että $\text{syt}(m, n) = 1$. Tällöin $G \times H$ on syklinen ryhmä.*

Todistus (vrt. [17]). Tarkastellaan ryhmän $G \times H$ alkiota (g, h). Nyt

$$(g, e_H)(e_G, h) = (g, h) = (e_G, h)(g, e_H), \text{ord}((g, e_H)) = n \text{ ja } \text{ord}((e_G, h)) = m.$$

Täten lauseen 3.29 nojalla

$$\begin{aligned}\text{ord}((g, h)) &= \text{ord}((g, e_H)(e_G, h)) = \text{ord}((g, e_H))\,\text{ord}((e_G, h)) \\ &= nm = |G|\,|H| = |G \times H|\,.\end{aligned}$$

Siis seurauksen 3.18 nojalla $G \times H$ on syklinen ryhmä. □

Havaitaan, että lauseen 3.30 tulos yleistyy toki koskemaan myös useamman kuin kahden äärellisen syklisen ryhmän karteesista tuloa.

Lause 3.31. *Olkoot $G_1, G_2, \ldots, G_k$ äärellisiä syklisiä ryhmiä, joiden kertaluvut ovat $n_1, n_2, \ldots, n_k$. Oletetaan, että kaikki nämä kertaluvut ovat keskenään jaottomia. Tällöin ryhmien muodostama karteesinen tulo $G_1 \times G_2 \times \cdots \times G_k$ on syklinen ryhmä.*

Todistus. Täsmällinen todistus sivuutetaan. Lause voidaan todistaa vastaavasti edellisen lauseen kanssa. Tulos seuraa induktiivisesti myös edeltävästä lauseesta. □

3.4 Normaalit aliryhmät ja tekijäryhmät

Tässä alaluvussa perehdytään normaalin aliryhmän käsitteeseen, ja muodostetaan sen avulla ryhmän G aliryhmän H kaikkien vasempien sivuluokkien joukosta G/H tekijäryhmä. Normaalit aliryhmät muodostavat aliryhmille erikoistapauksen, jossa niiden vasemmat ja oikeat sivuluokat yhtyvät. Tällöin ei siis tarvitse puhua erikseen oikeista tai vasemmista sivuluokista. Normaali aliryhmä onkin yksi ryhmäteorian keskeisistä käsitteistä.

Määritelmä 3.32. Ryhmän G aliryhmän H sanotaan olevan *normaali*, jos $xH = Hx$ kaikilla $x \in G$. Tällöin merkitään $H \trianglelefteq G$. Jos H on ryhmän G aito normaali aliryhmä, merkitään $H \triangleleft G$.

Kannattaa huomata, että normaalin aliryhmän H määritelmästä ei kuitenkaan seuraa se, että $xh = hx$ kaikilla $h \in H$. Määritelmästä seuraa ennemminkin, että kaikilla $h \in H$ on olemassa sellainen $h' \in H$, että $xh = h'x$. Seuraava lause antaa käyttökelpoisen ehdon aliryhmän normaaliuudelle.

Lause 3.33. *Olkoon H ryhmän G aliryhmä. Tällöin H on ryhmän G normaali aliryhmä, jos ja vain jos $gHg^{-1} \subseteq H$ aina, kun $g \in G$.*

Todistus. Ks. [11, s. 128–129]. □

Edeltävää lausetta käytetään sellaisenaan, kun on osoitettava jonkin aliryhmän normaalius. On hyvä todeta kuitenkin, että aliryhmän normaaliudesta seuraa myös joukkojen gHg^{-1} ja H yhtäsuuruus kaikilla $g \in G$. Tätä varten riittää enää osoittaa osajoukkous toiseen suuntaan: Oletetaan että $H \trianglelefteq G$. Jos $g \in G$ ja $h \in H$, niin on olemassa sellainen $h' \in H$, että $hg = gh'$ ($H \trianglelefteq G$). Täten $h = gh'g^{-1} \in gHg^{-1}$. Siis $H \subseteq gHg^{-1}$, ja näin ollen lauseessa 3.33 osajoukkouden lisäksi pätee myös joukkojen välinen yhtäsuuruus.

On melko suoraviivaista havaita, että jokaisen Abelin ryhmän aliryhmä on normaali.

Lause 3.34. *Jokaisen Abelin ryhmän aliryhmä on normaali.*

Todistus. Olkoon H Abelin ryhmän G aliryhmä. On osoitettava, että $xH = Hx$ aina, kun $x \in G$. Valitaan siis mielivaltainen $x \in G$. Oletetaan ensin, että $a \in xH$. Tällöin $a = xh$ jollakin $h \in H$. Koska G on Abelin ryhmä, niin $a = xh = hx \in Hx$. Siis $xH \subseteq Hx$. Täysin vastaavasti saadaan $Hx \subseteq xH$. Täten $xH = Hx$. □

Tiedetään, että sellaisen perheen leikkaus, joka koostuu ryhmän G aliryhmistä on myös aliryhmä. Osoitetaan nyt, että sama pätee myös normaaleille aliryhmille.

Lause 3.35. *Olkoon $\mathcal{H}$ epätyhjä perhe, joka koostuu ryhmän G normaaleista aliryhmistä. Tällöin $\bigcap \mathcal{H}$ on ryhmän G normaali aliryhmä.*

Todistus. Olkoon $g \in G$. Tarkastellaan joukon $g(\bigcap \mathcal{H})g^{-1}$ alkiota ghg^{-1}, missä $h \in \bigcap \mathcal{H}$. Olkoon $H \in \mathcal{H}$. Tällöin $h \in H$. Tarkastellaan sitten termiä gh. Koska h on alkiona normaalissa aliryhmässä H, niin normaalin aliryhmän määritelmän perusteella on olemassa sellainen $h' \in H$, että $gh = h'g$. Siis $ghg^{-1} = h' \in H$, jolloin $ghg^{-1} \in \bigcap \mathcal{H}$. Näin ollen $g\mathcal{H}g^{-1} \subseteq \bigcap \mathcal{H}$. Lauseen 3.33 nojalla $\bigcap \mathcal{H}$ on ryhmän G normaali aliryhmä. □

Jos ryhmän G ja sen normaalin aliryhmän K välissä on olemassa sellainen ryhmä H, joka on ryhmän G aliryhmä ja jonka aliryhmä on K, niin K on ryhmän H normaali aliryhmä. Tällöin H ei kuitenkaan välttämättä ole ryhmän G normaali aliryhmä.

Lause 3.36. *Olkoon G ryhmä. Oletetaan, että $K \trianglelefteq G$ ja $K \leqslant H \leqslant G$. Tällöin $K \trianglelefteq H$, mutta H ei ole välttämättä ryhmän G normaali aliryhmä.*

Todistus (ks. [18, s. 37 ja 39]). Ensimmäinen väite seuraa suoraan normaalin aliryhmän määritelmästä. Toisen väitteen osoittamiseksi voidaan valita $G = S_3$, $H = \{(1), (1\ \ 2)\}$ ja $K = \{(1)\}$. □

Aiemmin todettiin, että pelkästään kahden aliryhmän tulo ei ole välttämättä aliryhmä. Havaitaan kuitenkin, että toisen aliryhmän normaalius riittää tekemään aliryhmien tulosta aliryhmän. Edelleen jos molemmat aliryhmät ovat normaaleja, niin niiden tulokin on normaali aliryhmä.

Lause 3.37. *Jos $H \leqslant G$ ja $K \trianglelefteq G$, niin $HK \leqslant G$.*

Todistus. Ks. [18, s. 55] □

Lause 3.38. *Olkoot H ja K ryhmän G normaaleja aliryhmiä. Tällöin*

(i) *$HK = KH$ on ryhmän G normaali aliryhmä,*

(ii) *$\langle H \cup K \rangle = HK$.*

Todistus. (i) Vrt. [11, s. 129] ja [18, s. 55–56]. Jos $hk \in HK$, missä $h \in H$ ja $k \in K$, niin $hk \in hK = Kh \subseteq KH (K \trianglelefteq G)$, joten $HK \subseteq KH$. Vastaavasti $KH \subseteq HK$. Siis $HK = KH$.

Edellisen lauseen nojalla $HK \leqslant G$. Olkoot $g \in G$, $h \in H$, $k \in K$. Koska $H \trianglelefteq G$ ja $K \trianglelefteq G$, niin $ghg^{-1} \in H$ ja $gkg^{-1} \in K$. Siis $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$. Täten $HK \trianglelefteq G$.

Kohta (ii) seuraa suoran kohdasta (i) sekä lauseesta 3.13. □

Millä tavalla saataisiin sitten muodostettua ryhmän G aliryhmän H vasempien sivuluokkien joukosta G/H ryhmä? Määritellään joukon G/H laskutoimitus $*$ asettamalla

$$*\colon G/H \times G/H \to G/H, (xH) * (yH) = (xy)H. \tag{3.1}$$

Onko kyseinen laskutoimitus sitten hyvinmääritelty? Ei välttämättä; esimerkiksi symmetriaryhmän S_3 avulla voidaan tehdä vastaesimerkki, joka osoittaa, että laskutoimitus ei ole hyvinmääritelty (ks. [11, s. 130]). Jos taas aliryhmä H on ryhmän G normaali aliryhmä, laskutoimitus $*$ on hyvinmääritelty (ks. [21, s. 37]). Seuraavaksi onkin luonnollista todistaa, että pari $(G/H, *)$ on ryhmä, jota kutsutaan erityisesti tekijäryhmäksi.

Lause 3.39. *Olkoon H ryhmän G normaali aliryhmä. Tällöin $(G/H, *)$ on ryhmä, missä laskutoimitus on määritelty lausekkeen* (3.1) *mukaisesti.*

Todistus. Ks. [11, s. 131]. □

Määritelmä 3.40. Olkoon H ryhmän G normaali aliryhmä. Ryhmää G/H kutsutaan tällöin ryhmän G *tekijäryhmäksi*.

Tarkastellaan ryhmää G ja sen aliryhmää H. Havaitaan, että jos aliryhmän H indeksi on 2, niin H on ryhmän G normaali aliryhmä.

Lause 3.41. *Olkoon H ryhmän G aliryhmä.*

(i) *Oletetaan, että $x^2 \in H$ kaikilla $x \in G$. Tällöin $H \trianglelefteq G$.*

(ii) *Jos $(G : H) = 2$, niin $H \trianglelefteq G$.*

Todistus (vrt. [11, s. 135]). (i). Olkoon $g \in G$ ja $h \in H$. Havaitaan, että

$$ghg^{-1} = ghgh(gh)^{-1}g^{-1} = (gh)^2h^{-1}g^{-2}.$$

Nyt $h^{-1} \in H$ ja oletuksen nojalla $(gh)^2, g^{-2} \in H$. Tästä seuraa, että $ghg^{-1} \in H$, joten $gHg^{-1} \subseteq H$. Siis $H \trianglelefteq G$.

(ii). Olkoon $(G : H) = 2$. Oletetaan, että on olemassa sellainen $x \in G$, että $x^2 \notin H$. Tällöin $x \notin H$, joten $H \neq xH$ ja siis $H \cap xH = \emptyset$. Koska $(G : H) = 2$, niin $G/H = \{H, xH\}$, ja $G = H \cup xH$. Tästä seuraa, että $x^2 \in H \cup xH$. Toisaalta koska $x^2 \notin H$, on oltava $x^2 \in xH$. Siis $x^2 = xh$ jollakin $h \in H$. Mutta silloinhan $x = h \in H$, mikä on ristiriita. Näin ollen $x^2 \in H$ kaikilla $x \in G$. Täten kohdan (i) nojalla $H \trianglelefteq G$. □

3.5 Alternoivan ryhmän A_n yksinkertaisuus

Yksinkertaiset ryhmät ovat ryhmien tärkeä erikoistapaus, jotka auttavat määrittämään tarkemmin ryhmien rakenteita. Erityisesti myöhemmin tullaan havaitsemaan, että yksinkertaiset ryhmät ovat oleellinen osa äärellisten ryhmien kertalukujen luokittelua ja määrittelyä.

Määritelmä 3.42. Epätriviaalin ryhmän G sanotaan olevan *yksinkertainen*, jos sen ainoat normaalit aliryhmät ovat G ja $\{e\}$.

Yksinkertaisimmillaan havaitaan, että Lagrangen lauseen perusteella kaikki ryhmät, joiden kertaluku on alkuluku, ovat yksinkertaisia.

Pyritään seuraavaksi osoittamaan, että alternoiva ryhmä A_n on yksinkertainen, kun $n \geq 5$. Näin saadaan kasattua jo iso joukko yksinkertaisia ryhmiä. Todistetaan ensin, että kaikkien 3-syklien joukko virittää alternoivan ryhmän.

Lause 3.43. *Olkoon $n \geq 3$. Tällöin kaikkien 3-syklien joukko virittää alternoivan ryhmän A_n.*

Todistus (vrt. [11, s. 103]). Olkoon S kaikkien 3-syklien joukko. Jokainen joukon S virittämän aliryhmän $\langle S \rangle$ alkio on selvästi lauseen 3.7 perusteella 3-syklien tulo. Edelleen koska jokainen 3-sykli on parillinen ja A_n on ryhmä, niin selvästi $\langle S \rangle \subseteq A_n$. Toisaalta lauseen 2.21 nojalla $A_n \subseteq \langle S \rangle$. □

Seuraava lemma antaa avaimet alternoivan ryhmän yksinkertaisuuden osoittamiseksi.

Lemma 3.44. *Olkoon H alternoivan ryhmän A_n normaali aliryhmä, kun $n \geq 5$. Jos H sisältää 3-syklin, niin $H = A_n$.*

Todistus (vrt. [11, s. 133]). Oletetaan, että H sisältää 3-syklin $(a \;\; b \;\; c)$. Olkoon $(u \;\; v \;\; w)$ symmetriaryhmän S_n mielivaltainen 3-sykli, jolloin myös $(u \;\; v \;\; w) \in A_n$. Olkoon $\alpha \in S_n$ permutaatio, jolle $\alpha(a) = u, \alpha(b) = v$ ja $\alpha(c) = w$. Oletetaan lisäksi, että α kiinnittää muut luvut. Nythän $(u \;\; v \;\; w) = (\alpha(a) \;\; \alpha(b) \;\; \alpha(c))$, jolloin lauseen 2.9 nojalla $\alpha \circ (a \;\; b \;\; c) \circ \alpha^{-1} = (u \;\; v \;\; w)$. Jos $\alpha \in A_n$, niin lauseen 3.33 mukaan $(u \;\; v \;\; w) = \alpha \circ (a \;\; b \;\; c) \circ \alpha^{-1} \in H$.

Oletetaan sitten, että $\alpha \notin A_n$. Tällöin α on pariton permutaato. Koska $n \geq 5$, niin on olemassa kokonaisluvut $d, f \in I_n$, jotka ovat eri lukuja kuin a, b ja c. Nyt $\epsilon(\alpha \circ (d \;\; f)) = \epsilon(\alpha)\epsilon((d \;\; f)) = -1 \cdot (-1) = 1$, joten $\alpha \circ (d \;\; f) \in A_n$. Edelleen

$$\begin{aligned}(u \;\; v \;\; w) &= \alpha \circ (a \;\; b \;\; c) \circ \alpha^{-1} \\ &= \alpha \circ (a \;\; b \;\; c) \circ (d \;\; f) \circ (d \;\; f)^{-1} \circ \alpha^{-1} \\ &= \alpha \circ (d \;\; f) \circ (a \;\; b \;\; c) \circ (d \;\; f)^{-1} \circ \alpha^{-1} \\ &= (\alpha \circ (d \;\; f)) \circ (a \;\; b \;\; c) \circ (\alpha \circ (d \;\; f))^{-1},\end{aligned}$$

joten lauseen 3.33 perusteella $(u \;\; v \;\; w) \in H$.

Siis H sisältää kaikki 3-syklit. Olkoon S kaikkien 3-syklien joukko, jolloin $S \subseteq H$. Nyt lauseesta 3.43 seuraa, että $\langle S \rangle = A_n$ ja toisaalta lemman 3.6 perusteella $\langle S \rangle \subseteq H$, jolloin $A_n \subseteq H$. Tietysti pätee myös $H \subseteq A_n$, sillä H on alternoivan ryhmän aliryhmä. Siis $H = A_n$. □

Lause 3.45. *A_n on yksinkertainen, kun $n \geq 5$.*

Todistus (vrt. [11, s. 133–134]). Olkoon H alternoivan ryhmän A_n normaali aliryhmä ja $H \neq \{e\}$. Olkoon $\alpha \in H, \alpha \neq e$, permutaatio, joka liikuttaa pienintä mahdollista määrää lukuja. Asetetaan näiden lukujen määräksi m. Koska vaihdot eivät ole parillisia permutaatioita, niin $m \geq 3$. Pyritään osoittamaan, että $m = 3$, jolloin α on 3-sykli ja tulos seuraa suoraan lemmasta 3.44.

Oletetaan, että $m > 3$. Olkoon $\alpha = \alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_k$ erillisten syklien tulo. Oletetaan, että α_i on vaihto kaikilla $i \in \{1, \ldots, k\}$. Koska $m > 3$, on oltava $k \geq 2$. Olkoot $\alpha_1 = (a \;\; b)$ ja $\alpha_2 = (c \;\; d)$. Valitaan $f \in I_n \backslash \{a, b, c, d\}$ ja merkitään $\sigma = (c \;\; d \;\; f)$. Nyt $\sigma \in A_n$ ja H on alternoivan ryhmän normaali aliryhmä, joten lauseen 3.33 nojalla $\sigma \circ \alpha \circ \sigma^{-1} \in H$. Lisäksi $\alpha^{-1} \in H$, jolloin $\alpha' = \alpha^{-1} \circ \sigma \circ \alpha \circ \sigma^{-1} \in H$. Selvästi α' kiinnittää luvut a ja b. Jos on $\alpha(u) = u$, missä $u \in I_n \backslash \{a, b, c, d, f\}$, niin $\alpha'(u) = u$. Koska $\alpha'(f) = c$, niin $\alpha' \neq e$. Näin ollen $\alpha' \in H, \alpha' \neq e$ ja α' liikuttaa vähemmän lukuja kuin α (α' liikuttaa korkeintaan kolmea lukua, kun α liikuttaa vähintään neljää lukua), mikä on ristiriita.

Täten jollakin luvulla $i \in \{1, \ldots, k\}$ α_i on sykli, jonka pituus on vähintään 3. Koska erilliset syklit kommutoivat, voidaan olettaa, että $i = 1$. Olkoon $\alpha_1 = (a \;\; b \;\; c \;\; \cdots)$ sykli, jonka pituus on vähintään 3. Jos $m = 4$, niin $\alpha = \alpha_1$ on sykli, jonka pituus on 4, joten se on pariton permutaatio, mikä on ristiriita. On siis oltava $m \geq 5$, jolloin α liikuttaa vähintään viittä lukua. Olkoot $d, f \in I_n \backslash \{a, b, c\}$ permutaation α liikuttamia lukuja ja $\sigma = (c \;\; d \;\; f)$. Vastaavalla tavalla kuten aiemmin voidaan osoittaa, että tällöin $\alpha' = \alpha^{-1} \circ \sigma \circ \alpha \circ \sigma^{-1} \in H$. Nyt $\alpha'(b) = \alpha^{-1}(d) \neq b$ (sillä $\alpha^{-1}(c) = b$), joten $\alpha' \neq e$. Jos on $\alpha(u) = u$, missä $u \in I_n \backslash \{a, b, c, d, f\}$, niin $\alpha'(u) = u$. Selvästi myös $\alpha'(a) = a$. Näin ollen α' liikuttaa vähemmän lukuja kuin α (α' liikuttaa korkeintaan neljää lukua), mikä on jälleen ristiriita. Siis $m = 3$. □

4 Ryhmähomomorfismit ja isomorfialauseet

Tässä luvussa tullaan käsittelemään ryhmien välisiä kuvauksia, joille annettaan tiettyjä lisäominaisuuksia. Tarkasteltavat kuvaukset voidaan määritellä homomorfismeiksi, jos ne säilyttävät ryhmien laskutoimituksen kuvauksessa. Edelleen homomorfismista saadaan isomorfismi, kun oletetaan kuvauksen bijektiivisyys.

Isomorfian avulla tullaan todistamaan ensin Cayleyn[1] lause, jonka kautta jokainen ryhmä voidaan itse asiassa nähdä permutaatioryhmänä. Edelleen tullaan todistamaan kolme isomorfialausetta, joista erityisesti kahta ensimmäistä tullaan hyödyntämään usein tässä tutkielmassa. Lähteinä tässä luvussa on käytetty kirjoja *A Course on Group Theory* [18, s. 12–60] ja *Fundamentals of Abstract Algebra* [11, s. 140–164].

4.1 Ryhmähomomorfismit ja Cayleyn lause

Eri ryhmillä voi olla algebrallisesti hyvinkin samanlainen rakenne sen suhteen, miten ryhmän alkiot järjestäytyvät niiden laskutoimituksen suhteen. Esimerkiksi ryhmien $H = \{(1), (1\ 3\ 2), (1\ 2\ 3)\}$ (voidaan helposti osoittaa, että H on symmetriaryhmän S_3 normaali aliryhmä) ja $\mathbb{Z}_3$ kertotaulut ovat (alkioiden nimeämistä vaille) täsmälleen samat. Vastaavalla tavalla keskenään yhteydessä ovat myös diedriryhmä D_3 ja symmetriaryhmä S_3. Ne käyttäytyvät laskutoimituksensa suhteen siis identtisesti. Tällaisia rakenteeltaan samanlaisia ryhmiä kutsutaan keskenään isomorfisiksi. Isomorfisuus vaatii selvästi siis ryhmien bijektiivisyyden. Havaitaan, että isomorfisuus vaatii myös, että ryhmien väliset laskutoimitukset säilyvät jonkin kuvauksen avulla. Tällaista kuvausta taas sanotaan homomorfismiksi.

Määritelmä 4.1. Olkoot $G = (G, *)$ ja $G' = (G', *')$ ryhmiä ja $f : G \to G'$ kuvaus. Tällöin kuvausta f kutsutaan *homomorfismiksi* ryhmältä G ryhmälle G', jos kaikilla $x, y \in G$ pätee:

$$f(x * y) = f(x) *' f(y).$$

Kuvausta g, joka on ryhmien G ja G' välinen bijektio ja homomorfismi, kutsutaan *isomorfismiksi*. Tällöin sanotaan, että ryhmät G ja G' ovat *isomorfiset*, ja merkitään $G \cong G'$. Jos halutaan erityisesti täsmentää, että kuvaus g on isomorfismi näiden ryhmien välillä, merkitään $g : G \cong G'$. Isomorfismia ryhmästä G itseensä kutsutaan *automorfismiksi*. Homomorfismia kutsutaan *epimorfismiksi*, jos se on surjektio, ja *monomorfismiksi*, jos se on injektio.

Huomautus. Tässä tutkielmassa G' ei ole ryhmän G kommutaattorialiryhmän merkintä, vaan yksi yleismerkintä ryhmille.

[1] Arthur Cayley (1821–1895) oli englantilainen matemaatikko ja juristi, joka otti ensimmäisenä käyttöön ryhmän käsitteen modernissa mielessä: joukko laskutoimituksen kanssa, joka toteuttaa tietyt lait. Aiemmin ryhmiä oli käsitelty vain permutaatioryhminä. Cayleya pidetäänkin yleisesti abstraktin ryhmäteorian perustajana. [11, s. 180]

Ryhmäteoreettisesti on mahdotonta erotella ryhmiä, jotka ovat isomorfisia, mutta joilla ei ole samoja alkioita. Joissakin lähteissä sanotaankin, että kaksi keskenään isomorfisista ryhmää ovat samaa tyyppiä tai jopa samoja, kun ollaan kiinnostuttu vain ryhmien välisestä isomorfisuudesta. Joukko-opillisesti taas on mielekkäämpää erotella keskenään yhtämahtavia joukkoja.

Kaikki sellaiset symmetriaryhmät ovat isomorfisia keskenään, joiden epätyhjät joukot ovat keskenään yhtämahtavia. Todetaan myös, että jokainen äärellinen syklinen ryhmä, jonka kertaluku on n, on isomorfinen vastaavan kertaluvun omaavan ryhmän $\mathbb{Z}_n$ kanssa.

Lause 4.2. *Jos epätyhjät joukot X ja Y ovat yhtämahtavia, niin $S_X \cong S_Y$.*

Todistus (ks. [18, s. 15–16]). Koska on olemassa bijektio $\varphi : X \to Y$, niin voidaan osoittaa, että kuvaus $f\colon S_X \to S_Y$, $f(\alpha) = \varphi \circ \alpha \circ \varphi^{-1}$ on isomorfismi. □

Lause 4.3. *Jokainen kertalukua n oleva äärellinen syklinen ryhmä on isomorfinen ryhmän $\mathbb{Z}_n$ kanssa.*

Todistus (ks. [11, s. 147]). Olkoon $G = \langle a \rangle$ jollakin $a \in G$. Silloin voidaan osoittaa, että kuvaus $f\colon G \to \mathbb{Z}_n$, $f(a^i) = \bar{i}$ on isomorfismi. Ks. myös [21, s. 42–43]. □

Lauseesta 4.3 seuraakin suoraan, että kaksi syklistä ryhmää, joilla on sama kertaluku, ovat keskenään isomorfiset. Näin ollen isomorfisuuden näkökulmasta onkin olemassa vain yksi syklinen ryhmä, jolla on tietty kertaluku. Edelleen lauseen 3.30 perusteella havaitaan, että, jos m ja n ovat keskenään jaottomia, niin $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Seuraavassa esimerkissä osoitetaan diedriryhmän olemassaolo konstruoimalla konkreettinen ryhmä, joka toteuttaa diedriryhmän määritelmän oletukset.

Esimerkki 4.1. Tarkastellaan seuraavaa joukkoa

$$D = \{R_0, R_1, \ldots, R_{n-1}, S_0, S_1, \ldots, S_{n-1}\},$$

missä $n \geq 3$, ja R_k ja S_k ovat seuraavia kuvauksia:

$$R_k\colon \mathbb{C} \to \mathbb{C},\ R_k(z) = e^{i\frac{2\pi}{n}k} z,$$
$$S_k\colon \mathbb{C} \to \mathbb{C},\ S_k(z) = e^{i\frac{2\pi}{n}k} \overline{z},$$

kun $k \in \mathbb{Z}$. Tällöin havaitaan, että R_k on itse asiassa kierto kompleksitasossa kulman $k\frac{2\pi}{n}$ verran ja S_k on vastaavasti peilaus suuntaan $k\frac{\pi}{n}$ kulkevan suoran suhteen. Osoitetaan, että D on näin määriteltynä symmetriaryhmän $S_{\mathbb{C}}$ aliryhmä. Ensinnäkin havaitaan, että $R_n = R_0$ ja $S_n = S_0$ ja, jos $k > 0$, niin $R_{-k} = R_{n-k}$ ja $S_{-k} = S_{n-k}$. Selvästi $\mathrm{id}_{\mathbb{C}} = R_0 \in D$. Tarkastellaan joukon D kuvauksia R_k ja S_k, missä $k \in \{0, \ldots, n-1\}$. Havaitaan, että $R_k^{-1} = R_{-k} = R_{n-k} \in D$ ja $S_k^{-1} = S_{-k} = S_{n-k} \in D$. Olkoot R_a ja S_b joukon D kuvauksia, missä $a, b \in \{0, \ldots, n-1\}$. Olkoon $z \in \mathbb{C}$. Nyt

$$(R_a \circ S_b)(z) = R_a(S_b(z)) = R_a(e^{i\frac{2\pi}{n}b}\overline{z}) = e^{i\frac{2\pi}{n}a} e^{i\frac{2\pi}{n}b}\overline{z} = e^{i\frac{2\pi}{n}(a+b)}\overline{z} = S_{a+b}(z),$$

joten $R_a \circ S_b = S_{a+b} \in D$. Vastaavasti osoitetaan, että $S_b \circ R_a \in D$. Täten on osoitettu, että $D \leqslant S_{\mathbb{C}}$.

Edelleen havaitaan, että $S_k = R_k \circ S_0$, sillä jos $z \in \mathbb{C}$, niin $(R_k \circ S_0)(z) = R_k(S_0(z)) = R_k(\overline{z}) = e^{i\frac{2\pi}{n}k}\overline{z} = S_k(z)$. Selvästi myös $R_k = (R_1)^k$. Merkitään $R = R_1$ ja $S = S_0$, jolloin

$$D = \{\mathrm{id}_{\mathbb{C}}, R, R^2, \ldots, R^{n-1}, S, R \circ S, R^2 \circ S, \ldots, R^{n-1} \circ S\}.$$

Mutta nythän huomataan, että $\langle R, S\rangle = D$, $\mathrm{ord}(S) = 2$, $\mathrm{ord}(R) = n$ ja $S \circ R = R^{-1} \circ S$. Näin ollen aliryhmä D täyttää diedriryhmän oletukset. Jokainen astetta n oleva diedriryhmä voidaan siis samaistaa tämän säännöllisen n-kulmion symmetriaryhmän kanssa. Täsmällisesti ottaen voidaan osoittaa, että kuvaus

$$f\colon D_n \to D, f(a^i b^j) = R^i \circ S^j (i \in \{0, \ldots, n-1\}, j \in \{0, 1\})$$

on ryhmien D_n ja D välinen isomorfismi eli $f\colon D_n \cong D$.

Aiemmin luvussa 3 todettiin, että kombinatorisen ryhmäteorian avulla voidaan osoittaa diedriryhmän olemassaolo ja yksikäsitteisyys. Täsmällisesti ottaen ryhmän voi aina määritellä relaatioiden avulla, joten on olemassa (homomorfismien suhteen) maksimaalinen ryhmä, jonka virittävät alkiot a ja b ja joka toteuttaa relaatiot $a^n = e$, $b^2 = e$ ja $ba = a^{-1}b$. Voidaankin itse asiassa osoittaa, että jos G on nämä relaatiot toteuttava ryhmä, missä $n \geq 3$, niin on olemassa epimorfismi $D_n \to G$. Tämä epimorfismi on edelleen isomorfismi, jos ryhmät G ja D_n ovat yhtämahtavat. Näin ollen diedriryhmän D_n kanssa samaa kertalukua oleva ryhmä G on sen kanssa isomorfinen, kun ryhmälle G toteutuu nämä määritelmän 3.10 ehtoja $\mathrm{ord}(a) = n$ ja $\mathrm{ord}(b) = 2$ lievemmät relaatiot $a^n = e$ ja $b^n = e$. Tarkemman todistuksen tälle isomorfialle voi katsoa lähteestä [5, s. 1–2].

Määritellään seuraavaksi homomorfismin ydin ja kuva.

Määritelmä 4.4. Olkoot G ja G' ryhmiä ja $f\colon G \to G'$ homomorfismi. Tällöin homomorfismin f *ydin*, $\mathrm{Ker}(f)$, on joukko, joka koostuu niistä ryhmän G alkioista, jotka kuvautuvat ryhmän G' neutraalialkiolle e' eli

$$\mathrm{Ker}(f) := \{g \in G \mid f(g) = e'\},$$

Homomorfismin f *kuva*, $\mathrm{Im}(f)$, on taas yksinkertaisesti joukon G kuva kuvauksessa f eli

$$\mathrm{Im}(f) := f[G] = \{f(g) \mid g \in G\}.$$

Yllä olevassa määritelmässä homomorfismin f kuva on itse asiassa myös sen arvojoukko. Ryhmien välisten homomorfismien arvojoukoille halutaan tässä yhteydessä kuitenkin käyttää omaa merkintäänsä.

Käsitellään seuraavaksi joitakin homomorfismin ja isomorfismin perusominaisuuksia.

Lause 4.5. *Olkoon f homomorfismi ryhmältä G ryhmälle G'. Olkoon $g\colon H \to H'$ isomorfismi. Tällöin seuraavat ehdot ovat voimassa.*

(a) $f(e) = e'$.

(b) $f(g^{-1}) = f(g)^{-1}$ *kaikilla* $g \in G$.

(c) $\mathrm{Ker}(f) \trianglelefteq G$. *Jos* $H \leqslant G$ *, niin* $f[H] \leqslant G'$.

(d) *Jos* $H' \leqslant G'$, *niin* $f^{-1}[H'] \leqslant G$. *Jos* H' *on lisäksi normaali, niin on sen alkukuvakin.*

(e) f *on injektio, jos ja vain jos* $\mathrm{Ker}(f) = \{e\}$.

(f) $g^{-1} \colon H' \to H$ *on isomorfismi.*

(g) $\mathrm{ord}(a) = \mathrm{ord}(g(a))$ *kaikilla* $a \in H$.

Todistus. Kohdat (a), (b) ja (e): ks. [21, s. 33–34]. Kohdat (c), (d), (f) ja (g): ks. [11, s. 141, 143 ja 145]. □

Määritelmä 4.6. Jos on olemassa monomorfismi ryhmästä G ryhmään G', sanotaan, että ryhmä G voidaan *upottaa* ryhmään G'.

Lause 4.7. *Jos* $\varphi \colon G \to G'$ *on monomorfismi, niin* $G \cong \mathrm{Im}(\varphi)$*, ja jokaiselle ryhmän* G *aliryhmälle* H *pätee, että* $H \cong \varphi[H]$. *Ryhmä* G *voidaan lisäksi upottaa ryhmään* G'*, jos ja vain jos* G *on isomorfinen jonkin ryhmän* G' *aliryhmän kanssa.*

Todistus. Lause seuraa melko suoraan edeltävästä lauseesta, mutta esitetään tässä isomorfismiin vaadittavat kuvaukset. Olkoon $\varphi \colon G \to G'$ monomorfismi ja $H \leqslant G$. Lauseen 4.5 perusteella $\mathrm{Im}(\varphi)$ ja $\varphi[H]$ ovat ryhmän G' aliryhmiä. Näin ollen kuvaus $\varphi' \colon G \to \mathrm{Im}(\varphi), \varphi'(x) = \varphi(x)$ on selvästi isomorfismi, joten $G \cong \mathrm{Im}(\varphi)$. Vastaavasti kuvaus $\varphi'' \colon H \to \varphi[H], \varphi''(x) = \varphi(x)$ on selvästi isomorfismi, ja näin ollen $H \cong \varphi[H]$.

Oletetaan sitten, että ryhmä G voidaan upottaa ryhmään G', jolloin on olemassa monomorfismi $f \colon G \to G'$. Jo aiemmin osoitetun nojalla tällöin $G \cong \mathrm{Im}(f)$, missä $\mathrm{Im}(f)$ on ryhmän G' aliryhmä. Oletetaan toisaalta, että G on isomorfinen jonkin $H \leqslant G'$ kanssa. Tällöin on olemassa isomorfismi $g \colon G \to H$, jolloin kuvaus $g' \colon G \to G', g'(x) = g(x)$ on selvästi monomorfismi. □

Tarkastellaan sitten tiettyä mielenkiintoista ryhmän G automorfismia. Kyseisen automorfismin avulla määritellään, mitä tarkoitetaan ryhmän alkioiden välisellä konjugoinnilla. On suhteellisen suoraviivaista osoittaa, että kyseinen kuvaus on todellakin ryhmän G automorfismi (ks. [18, s. 22]).

Määritelmä 4.8. Määritellään kaikille ryhmän G alkioille g sellainen kuvaus $\tau_g \colon G \to G$, että

$$\tau_g(x) = gxg^{-1}.$$

Tällaista alkion g synnyttämää automorfismia kutsutaan ryhmän G *sisäiseksi automorfismiksi*.

Jos $g \in G$, niin alkiota gxg^{-1} kutsutaan ryhmän alkion g määräämäksi *alkion x konjugaatiksi* ryhmässä G. Ilman sisäistä automorfismia voidaan määritellä yleisesti, että alkio $b \in G$ on *alkion $a \in G$ konjugaatti*, jos on olemassa sellainen $c \in G$, että $b = cac^{-1}$.

Merkintä 4.9. Kaikkien ryhmän G automorfismien joukkoa merkitään symbolilla $\mathrm{Aut}(G)$. Symbolilla $\mathrm{Inn}(G)$ tarkoitetaan taas joukkoa kaikista ryhmän G sisäisistä automorfismeista.

Olkoon g ryhmän G alkio. Lauseen 4.7 mukaan sisäinen automorfismi τ_g kuvaa jokaisen ryhmän G aliryhmän H sen kuvalle $\tau_g[H] \leqslant \mathrm{Im}(\tau_g) = G$ niin, että

$$H \cong \tau_g[H] = \{ghg^{-1} \mid h \in H\} = gHg^{-1}.$$

Näin ollen saadaan suoraan seuraava lause.

Lause 4.10. *Jokaiselle $H \leqslant G$ ja $g \in G$ pätee, että gHg^{-1} on ryhmän G aliryhmä, joka on isomorfinen aliryhmän H kanssa.*

Tarkastellaan vielä ryhmän G symmetriaryhmää S_G. Havaitaan, että ryhmältä G saadaan muodostettua sisäisen automorfismin avulla kuvaus τ symmetriaryhmälle S_G, joka on homomorfismi (ks [18, s. 22]):

$$\tau \colon G \to S_G, \tau(g) = \tau_g. \tag{4.1}$$

Edelleen $\mathrm{Im}(\tau) = \{\tau_g \mid g \in G\} = \mathrm{Inn}(G) \leqslant \mathrm{Aut}(G)$, ja myös selvästi $\mathrm{Aut}(G) \leqslant S_G$, joten

$$\mathrm{Inn}(G) \leqslant \mathrm{Aut}(G) \leqslant S_G.$$

On lisäksi osoitettavissa, että kaikkien sisäisten automorfismien ryhmä on myös normaali aliryhmä kaikkien automorfismien ryhmälle:

Lause 4.11. *Kun G on ryhmä, niin* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Todistus. Ks. [11, s. 161] □

Esimerkki 4.2. Kaikkien sisäisten automorfismien ryhmä on siis aliryhmä kaikkien automorfismien ryhmälle. Mutta milloin $\mathrm{Inn}(G)$ on ryhmän $\mathrm{Aut}(G)$ aito aliryhmä, kun G on ryhmä? Onko siis olemassa automorfismia, joka ei ole sisäinen automorfismi? Vastaus tähän ei ole täysin triviaali, joten tarkastellaan kahta eri tapausta.

Havaitaan, että yleisesti Abelin ryhmälle G automorfismi, joka ei ole identtinen kuvaus, ei ole sisäinen automorfismi. Tarkastellaan tällaista automorfismia $f \colon G \to G$. Olkoon $b \in G$. Koska f ei ole identtinen kuvaus, on olemassa sellainen $a \in G$, että $f(a) \neq a$. Tällöin

$$\tau_b(a) = bab^{-1} = bb^{-1}a = a \neq f(a),$$

joten $\tau_b \neq f$. Siis $f \notin \mathrm{Inn}(G)$, ja $\mathrm{Inn}(G) < \mathrm{Aut}(G)$. Konkreettinen esimerkki tällaisesta automorfismista on kuvaus

$$f \colon \mathbb{R}^* \to \mathbb{R}^*, f(x) = x^3,$$

missä ryhmä $\mathbb{R}^*$ on pari $(\mathbb{R} \setminus \{0\}, \cdot)$ eli reaaliluvut nolla pois lukien, varustettuna kertolaskulla.

Entä jos G ei olekaan Abelin ryhmä? Tarkastellaan alternoivaa ryhmää A_4 ja sen kaikkien sisäisten automorfismien ryhmää $\mathrm{Inn}(A_4) = \{\tau_\beta \mid \beta \in A_4\}$, jonka alkiot ovat siis kuvauksia muotoa $\tau_\beta \colon A_4 \to A_4, \tau_\beta(\alpha) = \beta \circ \alpha \circ \beta^{-1}$. Tässä kohtaa lukijan on hyvä huomata, että jokainen alternoivan ryhmän sisäinen automorfismi saadaan symmetriaryhmän sisäisestä automorfismista rajoittamalla, mutta kaikki tällaiset kuvaukset eivät toki ole sisäisiä automorfismeja. Määritellään seuraavaksi esimerkki tällaisesta kuvauksesta.

Tarkastellaan erityisesti vaihdon $(1\ \ 2)$ konjugoimalla kiinnittämää vastaavaa kuvausta

$$\tau_{(1\ \ 2)} \colon A_4 \to A_4, \tau_{(1\ \ 2)}(\alpha) = (1\ \ 2) \circ \alpha \circ (1\ \ 2)^{-1}.$$

Nythän $(1\ \ 2) \notin A_4$. Seuraava taulukko kuitenkin osoittaa, että $\tau_{(1\ \ 2)}$ on bijektiivinen kuvaus (bijektiivisyys voidaan osoittaa lyhyemminkin, mutta jatkotarkastelun kannalta taulukko on tarpeellinen). Taulukossa on esitetty alternoivan ryhmän A_4 permutaatiot sekä niiden kuvat tässä kuvauksessa.

α	$\tau_{(1\ 2)}(\alpha)$
(1)	(1)
$(2\ \ 3\ \ 4)$	$(1\ \ 3\ \ 4)$
$(2\ \ 4\ \ 3)$	$(1\ \ 4\ \ 3)$
$(1\ \ 2) \circ (3\ \ 4)$	$(1\ \ 2) \circ (3\ \ 4)$
$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$
$(1\ \ 2\ \ 4)$	$(1\ \ 4\ \ 2)$
$(1\ \ 3\ \ 2)$	$(1\ \ 2\ \ 3)$
$(1\ \ 3\ \ 4)$	$(2\ \ 3\ \ 4)$
$(1\ \ 3) \circ (2\ \ 4)$	$(1\ \ 4) \circ (2\ \ 3)$
$(1\ \ 4\ \ 2)$	$(1\ \ 2\ \ 4)$
$(1\ \ 4\ \ 3)$	$(2\ \ 4\ \ 3)$
$(1\ \ 4) \circ (2\ \ 3)$	$(1\ \ 3) \circ (2\ \ 4)$

Yllä olevan taulukon oikeellisuuden voi todeta hyödyntämällä lausetta 2.9. On helppoa osoittaa, että $\tau_{(1\ 2)}$ on myös homomorfismi. Täten $\tau_{(1\ \ 2)} \in \mathrm{Aut}(A_4)$. Nyt

$\tau_\alpha(\alpha) = \alpha \circ \alpha \circ \alpha^{-1} = \alpha \neq \tau_{(1\ \ 2)}(\alpha)$ kaikilla $\alpha \in A_4 \setminus \{(1), (1\ \ 2) \circ (3\ \ 4)\}$,
$\tau_{(1\ \ 2)\circ(3\ \ 4)}((1\ \ 3\ \ 4)) = (2\ \ 4\ \ 3) \neq (2\ \ 3\ \ 4) = \tau_{(1\ \ 2)}((1\ \ 3\ \ 4))$ ja
$\tau_{(1)}((2\ \ 3\ \ 4)) = (2\ \ 3\ \ 4) \neq (1\ \ 3\ \ 4) = \tau_{(1\ \ 2)}((2\ \ 3\ \ 4))$.

Näin ollen $\tau_{(1\ \ 2)} \neq \tau_\beta$ kaikilla $\beta \in A_4$. Siis $\tau_{(1\ \ 2)} \notin \mathrm{Inn}(A_4)$. Täten ollaan osoitettu, että on olemassa automorfismi, joka ei ole sisäinen eikä vaihdannainen.

Päätetään tämä alaluku todistamalla Cayleyn lause, jonka mukaan mikä tahansa ryhmä voidaan käsittää permutaatioryhmänä. Olkoon a ryhmän G alkio. Määritellään sellainen kuvaus $f_a \colon G \to G$, että $f_a(b) = ab$. On helppoa osoittaa, että näin

määritelty kuvaus on bijektio. Näin ollen f_a on ryhmän G permutaatio. Olkoon $F(G) = \{f_a \mid a \in G\}$, jolloin $F(G)$ on ryhmän G symmetriaryhmän S_G osajoukko.

Cayleyn lause kertoo täsmällisesti, että jokainen ryhmä G on isomorfinen sellaisen permutaatioryhmän kanssa, joka koostuu sen omista permutaatioista. Osoitetaan, että tällainen ryhmä on $F(G)$.

Lause 4.12 (Cayleyn lause)**.** *Olkoon G ryhmä. Tällöin $F(G)$ on ryhmä ja $G \cong F(G)$.*

Todistus (ks. [11, s. 149]). Osoitetaan ensin, että $F(G)$ on symmetriaryhmän S_G aliryhmä. Ensinnäkin symmetriaryhmän S_G neutraalialkio id_G on alkiona joukossa $F(G)$, sillä $\mathrm{id}_G(a) = a = ea = f_e(a)$ kaikilla $a \in G$. Olkoot $a, b \in G$. Koska $f_a(a^{-1}b) = b$, niin $(f_a)^{-1}(b) = a^{-1}b$. Tällöin $f_{a^{-1}}(b) = a^{-1}b = (f_a)^{-1}(b)$, joten $(f_a)^{-1} = f_{a^{-1}} \in F(G)$. Valitaan joukosta $F(G)$ kaksi permutaatiota f_a ja f_b. Tällöin

$$(f_a \circ f_b)(c) = f_a(f_b(c)) = f_a(bc) = a(bc) = (ab)c = f_{ab}(c)$$

kaikilla $c \in G$, joten $f_a \circ f_b = f_{ab} \in F(G)$. Täten $F(G) \leqslant S_G$. Määritellään sellainen kuvaus $g\colon G \to F(G)$, että $g(a) = f_a$. Olkoot $a, b \in G$. Seuraava ekvivalenssiketju osoittaa, että f on injektiivinen kuvaus:

$$\begin{aligned} a = b \Leftrightarrow ac = bc \text{ kaikilla } c \in G &\Leftrightarrow f_a(c) = f_b(c) \text{ kaikilla } c \in G \\ &\Leftrightarrow f_a = f_b \Leftrightarrow g(a) = g(b). \end{aligned}$$

Lisäksi g on selvästi surjektio. Siis g on bijektio. Edelleen kaikilla $c \in G$ pätee:

$$\begin{aligned} (g(ab))(c) &= f_{ab}(c) = (ab)c = a(bc) = f_a(bc) \\ &= f_a(f_b(c)) = (f_a \circ f_b)(c) = (g(a) \circ (g(b))(c). \end{aligned}$$

Siis $g(ab) = g(a) \circ g(b)$, joten g on homomorfismi. Näin ollen $G \cong F(G)$. □

Itse asiassa lauseen 4.7 mukaan Cayleyn lause siis kertoo, että jokainen ryhmä G voidaan upottaa omaan symmetriaryhmäänsä S_G.

4.2 Isomorfialauseet

Tässä alaluvussa tarkastellaan homomorfismien ja tekijäryhmien välistä suhdetta. Tavoitteena on todistaa kolme isomorfialausetta, joiden avulla voidaan määrittää isomorfioita erilaisten tekijäryhmien välille.

Havaitaan, että ryhmän G mikä tahansa normaali aliryhmä H synnyttää epimorfismin f ryhmästä G tekijäryhmään G/H, missä $\mathrm{Ker}(f) = H$. Määritellään tämä kuvaus.

Määritelmä 4.13. Olkoon $H \trianglelefteq G$. Tällöin kuvausta $\pi\colon G \to G/H$,

$$\pi(g) = gH,$$

kutsutaan *luonnolliseksi homomorfismiksi* (tai *kanoniseksi surjektioksi*) ryhmältä G tekijäryhmälle G/H.

Lause 4.14. *Olkoon $H \trianglelefteq G$. Tällöin luonnollinen homomorfismi π ryhmältä G ryhmälle G/H on epimorfismi, ja* $\operatorname{Ker}(\pi) = H$.

Todistus. Ks. [21, s. 40] □

Nyt voidaan esittää yksi ryhmäteorian perustuloksista, jota kutsutaan *homomorfismien peruslauseeksi* (the fundamental theorem of homomorphisms). Kyseinen lause on tämän luvun kolmesta isomorfialauseesta ensimmäinen. Lause todistetaan ilman konstruoitavan kuvauksen monomorfisuuden perustelua.

Lause 4.15 (Ensimmäinen isomorfialause)**.** *Olkoon $\varphi\colon G \to H$ homomorfismi, ja merkitään $K = \operatorname{Ker}(\varphi)$, jolloin $K \trianglelefteq G$ (lause 4.5). Olkoon π luonnollinen homomorfismi ryhmältä G ryhmälle G/K. Tällöin on olemassa sellainen monomorfismi $\psi\colon G/K \to H$, että $\varphi = \psi \circ \pi$. Erityisesti* $\operatorname{Im}(\varphi) \cong G/\operatorname{Ker}(\varphi)$.

Todistus (ks. [18, s. 45]). Määritellään sellainen kuvaus $\psi\colon G/K \to H$, että

$$\psi(gK) = \varphi(x).$$

Voidaan osoittaa, että ψ on hyvin määritelty kuvaus, joka on monomorfismi. Nyt

$$(\psi \circ \pi)(x) = \psi(xK) = \varphi(x) \text{ kaikilla } x \in G,$$

joten $\varphi = \psi \circ \pi$.

Selvästi $\operatorname{Im}(\varphi) = \operatorname{Im}(\psi)$. Lauseen 4.7 perusteella myös $G/K \cong \operatorname{Im}(\psi)$. Siis $G/K \cong \operatorname{Im}(\varphi)$. □

Ensimmäinen isomorfialause on käytännöllinen, kun tarvitsee todistaa tekijäryhmän G/H isomorfisuus jonkin toisen ryhmän K kanssa. Tällöin täytyy löytää sellainen homomorfismi $f\colon G \to G'$, jolle $\operatorname{Ker}(f) = H$ ja $\operatorname{Im}(f) = K$. Seuraavan lauseen todistuksessa tätä ideaa tullaankin hyödyntämään.

Tarkastellaan nyt epimorfismia ryhmältä G ryhmälle G'. Havaitaan, että tällaisen epimorfismin avulla voidaan synnyttää vaastaavuus kahden perheen välille, jotka koostuvat näiden ryhmien kaikista aliryhmistä; ts. epimorfismin avulla voidaan määritellä bijektio kyseisten perheiden välille. Tällöin siis ryhmän G aliryhmät (jotka sisältävät epimorfismin ytimen) ovat yksi-yhteen-vastaavuudessa ryhmän G' aliryhmien kanssa. Lisäksi havaitaan, että ryhmien G ja G' aliryhmien normaalius säilyy luodun bijektion kautta. Seuraava lause tunnetaankin joissain lähteissä *vastaavuuslauseena* (correspondence theorem) (ks. [11, s. 158]).

Lause 4.16 (Vastaavuuslause)**.** *Olkoon $f\colon G \to G'$ epimorfismi. Olkoon $\mathcal{H}$ perhe, joka koostuu kaikista niistä ryhmän G aliryhmistä, jotka sisältävät ytimen* $\operatorname{Ker}(f)$*, ja olkoon $\mathcal{K}$ perhe ryhmän G' kaikista aliryhmistä. Tällöin on olemassa bijektio $f^*\colon \mathcal{H} \to \mathcal{K}$. Lisäksi jos H ja K ovat perheiden $\mathcal{H}$ ja $\mathcal{K}$ sellaisia joukkoja, että $f^*(H) = K$, niin $H \trianglelefteq G$, jos ja vain jos $K \trianglelefteq G'$. Jos näin on, niin myös $G/H \cong G'/K$.*

Todistus (vrt. [18, s. 48–49]). Määritellään kuvaus $f^* \colon \mathcal{H} \to \mathcal{K}$ niin, että

$$f^*(H) = f[H].$$

Nyt lauseen 4.5 perusteella $f^*(H) = f[H] \in \mathcal{K}$ kaikilla $H \in \mathcal{H}$ ja lisäksi f on kuvaus, joten f^* on hyvinmääritelty. On melko rutiininomaista osoittaa, että f^* on bijektio (ks. [11, s. 158–159] tai [18, s. 49]).

Olkoon $H \in \mathcal{H}$. Valitaan nyt sellainen $K \in \mathcal{K}$, että $f^*(H) = K$. Oletetaan ensin, että $H \trianglelefteq G$. Silloin lauseen 4.5 nojalla $K = f[H] \leqslant G'$. Olkoot $x \in G'$ ja $k \in K$. Koska f on surjektio, niin on olemassa sellaiset $g \in G$ ja $h \in H$, että $x = f(g)$ ja $k = f(h)$. Täten

$$xkx^{-1} = f(g)f(h)f(g)^{-1} = f(ghg^{-1}) \in f[H] = K,$$

sillä $ghg^{-1} \in H$ (H on normaali) ja f on homomorfismi. Siis $K \trianglelefteq G'$.

Oletetaan kääntäen, että $K \trianglelefteq G'$. Olkoon $\pi \colon G' \to G'/K$ luonnollinen homomorfismi. Nyt $\pi \circ f \colon G \to G'/K$ on kahden epimorfismin yhdistettynä kuvauksena epimorfismi. Edelleen

$$\begin{aligned}
\operatorname{Ker}(\pi \circ f) &= \{g \in G \mid \pi(f(g)) = e'K\} = \{g \in G \mid f(g)K = e'K\} \\
&= \{g \in G \mid f(g) \in f[H]\} \\
&= \{g \in G \mid g \in H\} \quad (\operatorname{Ker}(f) \subseteq H) \\
&= H.
\end{aligned}$$

Täten $H \trianglelefteq G$. On siis osoitettu, että $H \trianglelefteq G$, jos ja vain jos $K \trianglelefteq G'$. Nyt ensimmäisen isomorfialauseen nojalla

$$G'/K = \operatorname{Im}(\pi \circ f) \cong G/H.$$

□

Vastaavuuslauseen erikoistapauksena voidaan johtaa toinen isomorfialause. Tämä isomorfialause onkin erityisen tärkeä, sillä sen mukaan jokaisen tekijäryhmän aliryhmä on samanlaista muotoa eli se koostuu vasemmista sivuluokista. Lisäksi sen avulla saadaan tärkeä isomorfia tekijäryhmän G/H ja kahdesta tekijäryhmästä G/K ja H/K muodostetun tekijäryhmän välille (kun $K \trianglelefteq H \trianglelefteq G$).

Lause 4.17 (Toinen isomorfialause)**.** *Olkoon $K \trianglelefteq G$. Tällöin jokainen tekijäryhmän G/K aliryhmä on muotoa H/K, missä $K \leqslant H \leqslant G$. Edelleen, $H \trianglelefteq G$, jos ja vain jos $H/K \trianglelefteq G/K$. Jos näin on, niin $(G/K)/(H/K) \cong G/H$.*

Todistus (vrt. [18, s. 50]). Tarkastellaan luonnollista homomorfismia π ryhmältä G tekijäryhmälle G/K yhtenevyyslauseen epimorfismin f sijasta, jolloin $\operatorname{Ker}(\pi) = K$. Olkoot $\mathcal{H}$ ja $\mathcal{K}$ vastaavat perheet ryhmien G ja G/K aliryhmille. Tällöin vastaavuuslauseen nojalla kuvaus $f^* \colon \mathcal{H} \to \mathcal{K}$, $f^*(H) = \pi[H]$ on bijektio. Jos nyt $H \in \mathcal{H}$ eli $K \leqslant H \leqslant G$, niin

$$f^*(H) = \pi[H] = \{\pi(h) \mid h \in H\} = \{hK \mid h \in H\} = H/K.$$

Koska f^* on surjektio, niin

$$\mathcal{K} = f^*[\mathcal{H}] = \{f^*(H) \mid H \in \mathcal{H}\} = \{H/K \mid K \leqslant H \leqslant G\}.$$

Näin ollen kaikki tekijäryhmän G/K aliryhmät ovat todellakin muotoa H/K, missä $K \leqslant H \leqslant G$. Edelleen, koska osoitettiin, että $f^*(H) = H/K$, niin vastaavuuslauseen perusteella $H \trianglelefteq G$, jos ja vain jos $H/K \trianglelefteq G/K$. Jos näin on, niin vastaavuuslauseesta seuraa myös suoraan, että

$$(G/K)/(H/K) \cong G/H.$$

□

Tarkastellaan vielä viimeistä eli kolmatta isomorfialausetta, jossa kahdesta ryhmän G aliryhmästä, joista toinen on normaali, saadaan muodostettua tekijäryhmät. Näiden tekijäryhmien välinen isomorfisuus tullaan todistamaan.

Lause 4.18 (Kolmas isomorfialause)**.** *Olkoon $H \leqslant G$ ja $K \trianglelefteq G$. Tällöin $H \cap K \trianglelefteq H$, $K \trianglelefteq HK$ ja*

$$H/H \cap K \cong HK/K.$$

Todistus (vrt. [18, s. 56]). Tarkastellaan luonnollista homomorfismia $\pi\colon G \to G/K$. Merkitään $\pi_1 = \pi \restriction H$. Tällöin $\pi_1\colon H \to G/K$ on homomorfismi ja

$$\begin{aligned}\operatorname{Ker}(\pi_1) &= \{h \in H \mid \pi_1(h) = eK\} = \{h \in H \mid \pi(h) = eK\} \\ &= \{h \in H \mid hK = eK\} = \{h \in H \mid h \in K\} = H \cap K.\end{aligned}$$

Täten lauseen 4.5 ja ensimmäisen isomorfialauseen nojalla

$$H \cap K \trianglelefteq H \text{ ja } H/H \cap K \cong \operatorname{Im}(\pi_1).$$

Nyt lauseesta 3.37 seuraa, että $HK \leqslant G$. Koska $HK \leqslant G$, $K \leqslant G$ ja $K \subseteq HK$, niin $K \leqslant HK$. Olkoon $hk \in HK$, missä $h \in H$ ja $k \in K$, ja $k' \in K$. Tällöin

$$(hk)k'(hk)^{-1} = h(kk'k^{-1})h^{-1} \in K,$$

sillä $K \trianglelefteq G$. Siis $K \trianglelefteq HK$. Edelleen jokaiselle $h \in H$, $\pi_1(h) = hK \in HK/K (H \subseteq HK)$, joten $\operatorname{Im}(\pi_1) \subseteq HK/K$. Toisaalta tekijäryhmän HK/K mielivaltainen alkio on muotoa $(hk)K = h(kK) = hK = \pi_1(h) \in \operatorname{Im}(\pi_1)$, missä $h \in H$ ja $k \in K$. Täten $HK/K \subseteq \operatorname{Im}(\pi_1)$. Näin ollen $\operatorname{Im}(\pi_1) = HK/K$, ja lause on todistettu. □

Tarkastellaan vielä lopuksi tiettyä hyödyllistä isomorfiaa, jolla saadaan kahden aliryhmän tulo ja karteesinen tulo osoitettua isomorfisiksi. Osoitetaan, että jos kaksi normaalia aliryhmää sisältävät yhteisenä alkioina vain neutraalialkion, niin kyseinen isomorfia pätee.

Lause 4.19. *Olkoot H ja K ryhmän G normaaleja aliryhmiä, ja $H \cap K = \{e\}$. Tällöin $HK \cong H \times K$.*

Todistus (vrt. [18, s. 33–34 ja s. 59–60]). Tiedetään, että $HK \trianglelefteq G$, sillä $H \trianglelefteq G$ ja $K \trianglelefteq G$. Osoitetaan ensin, että aliryhmien H ja K alkiot ovat vaihdannaisia keskenään. Olkoot $h \in H$ ja $k \in K$. Ensinnäkin aliryhmien normaaliuudesta seuraa, että $kh^{-1}k^{-1} \in H$ ja $hkh^{-1} \in K$. Siis $h(kh^{-1}k^{-1}) \in H$ ja $(hkh^{-1})k^{-1} \in K$, joten $hkh^{-1}k^{-1} \in H \cap K$. Edelleen koska $H \cap K = \{e\}$, niin $hkh^{-1}k^{-1} = e$, jolloin $hk = kh$.

Seuraavaksi havaitaan, että jokainen ryhmän HK alkio on ilmaistavissa yksikäsitteisesti aliryhmien H ja K alkioiden tulona: Oletetaan siis, että $g \in HK$ niin, että $g = hk = h'k'$, missä $h, h' \in H$ ja $k, k' \in K$. Tällöin $(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\}$, joten $h = h'$ ja $k = k'$.

Näin ollen voidaan määritellä sellainen kuvaus $f\colon HK \to H \times K$, että $f(hk) = (h, k)$. Havaitaan, että f on selvästi bijektio. Lisäksi aliryhmien H ja K alkioiden vaihdannaisuudesta seuraa, että f on homomorfismi: Olkoot $h, h' \in H$ ja $k, k' \in K$. Tällöin

$$f(hk)f(h'k') = (h, k)(h', k') = (hh', kk') = f((hh')(kk')) = f((hk)(h'k')).$$

Siis $HK \cong H \times K$. □

5 Ryhmätoiminnat

Ryhmätoiminnat luovat tässä tutkielmassa pohjan Sylowin lauseiden todistamiselle. Ryhmän toiminta on yksinkertaisesti sopivasti määritelty kuvaus, jossa mukana ovat jokin ryhmä ja epätyhjä joukko. Ryhmätoimintojen avulla tullaan määrittelemään useita tutkielman ydinkäsitteitä, joita ovat muun muassa permutaatioesitys, rata, stabilisaattori, keskiö, keskus, konjugaatio, keskittäjä ja normalisoija.

Luvun 5 keskeisin sisältö on rakennettu teoksen *A Course on Group Theory* [18, s. 68–87] pohjalta. Luvun keskeisimpinä tuloksina pidetään lauseita 5.11, 5.16 ja 5.23, joista jälkimmäistä kutsutaan ryhmätoimintojen luokkayhtälöksi.

5.1 Ryhmän toiminnan määritelmä ja ryhmän radat

Määritelmä 5.1. Olkoon $(G, *)$ ryhmä ja X epätyhjä joukko. Ryhmän G *(vasemmanpuoleinen) toiminta* joukossa X on kuvaus $\cdot\colon G \times X \to X$, jolle

(i) $e \cdot x = x$, missä e on ryhmän G neutraalialkio,

(ii) $(g_1 * g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$

aina, kun $x \in X$ ja $g_1, g_2 \in G$.

Ehtojen (i) ja (ii) pätiessä sanotaan, että *ryhmä G toimii (vasemmalta) joukossa X* ja joukko X on *G-joukko*. Lisäksi tällöin ryhmän G ja joukon X alkioiden sanotaan toimivan keskenään.

Huomautus. Selvissä tilanteissa merkitään lyhyemmin: $g \cdot x = gx$.

Esimerkki 5.1 (vrt. [11, s. 172] ja [18, s. 69])**.** Olkoon X epätyhjä joukko ja $G \leqslant S_X$. Määritellään permutaatioryhmän G toiminta joukossa X siten, että se on kuvaus $\cdot\colon G \times X \to X$, missä

$$(*) \qquad \sigma \cdot x = \sigma(x)$$

aina, kun $\sigma \in G$, $x \in X$. Osoitetaan nyt, että X on G-joukko.

Olkoon $x \in X$. Nyt $\mathrm{id}_X \cdot x = \mathrm{id}_X(x) = x$. Täten määritelmän 5.1 ehto (i) toteutuu.

Olkoot sitten $\sigma_1, \sigma_2 \in G$. Tällöin yhdistetyn kuvauksen määritelmän ja kuvauksen $(*)$ nojalla $(\sigma_1 \circ \sigma_2) \cdot x = (\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_1 \cdot (\sigma_2(x)) = \sigma_1 \cdot (\sigma_2 \cdot x)$. Määritelmän 5.1 ehto (ii) siis pätee.

Tästä seuraa, että X on G-joukko. Tällaista ryhmän toimintaa kutsutaan ryhmän *G luonnolliseksi toiminnaksi* joukossa X.

Tarkastellaan nyt joukossa X tapahtuvan ryhmän toiminnan ja symmetriaryhmän S_X välistä yhteyttä.

Lause 5.2. *Toimikoon ryhmä G epätyhjässä joukossa X. Tällöin jokaista $g \in G$ vastaa kuvaus $\rho_g \colon X \to X, \rho_g(x) = gx$, joka on joukon X permutaatio. Edelleen, kuvaus*

$$\rho \colon G \to S_X, \rho(g) = \rho_g$$

on homomorfismi.

Todistus (ks. [18, s. 69]). Olkoon $g \in G$. Nyt kuvaus $\rho_g \colon X \to X, \rho_g(x) = gx$ on selvästi hyvin määritelty. Osoitetaan, että se on bijektio. Olkoot $g_1, g_2 \in G$ ja $x \in X$. Tällöin ryhmän toiminnan määritelmän ehdon (ii) nojalla

$$\rho_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = g_1(\rho_{g_2}(x)) = \rho_{g_1}(\rho_{g_2}(x)) = (\rho_{g_1} \circ \rho_{g_2})(x),$$

joten

$$\rho_{g_1 g_2} = \rho_{g_1} \circ \rho_{g_2}. \tag{5.1}$$

Edelleen määritelmän ehdon (i) perusteella saadaan, että

$$\rho_e(x) = ex = x,$$

jolloin

$$\rho_e = \mathrm{id}_X \in S_X. \tag{5.2}$$

Yhtälöiden (5.1) ja (5.2) nojalla siis pätee, että

$$\rho_g \circ \rho_{g^{-1}} = \rho_{gg^{-1}} = \mathrm{id}_X = \rho_{g^{-1}g} = \rho_{g^{-1}} \circ \rho_g.$$

Tästä seuraa, että kuvaus ρ_g on kääntyvä, joten se on bijektio, ja erityisesti siis joukon X permutaatio. Yhtälöstä (5.1) seuraa myös suoraan, että kuvaus $\rho \colon G \to S_X, \rho(g) = \rho_g$ on homomorfismi. □

Määritelmä 5.3. Lauseen 5.2 homomorfismia ρ kutsutaan ryhmän G toimintaa vastaavaksi *permutaatioesitykseksi*.

Lause 5.4 määrittää konkreettisen ryhmän G toiminnan joukossa X sitä vastaavan permutaatioesityksen avulla. Tässä lauseessa näytetään, että mikä tahansa homomorfismi ryhmästä G symmetriaryhmään S_X on ryhmän G permutaatioesitys, kun itse toiminta määritellään sopivasti.

Lause 5.4. *Olkoon $\sigma \colon G \to S_X$ homomorfismi, missä X on epätyhjä joukko. Tällöin kuvaus*

$$\cdot \colon G \times X \to X, g \cdot x = (\sigma(g))(x)$$

määrittää ryhmän G toiminnan joukossa X eli X on G-joukko, ja ryhmän G permutaatioesitys tälle toiminnalle on σ.

Todistus (ks. [18, s. 69–70]). Olkoot $g_1, g_2 \in G$ ja $x \in X$. Tällöin yhdistetyn kuvauksen määritelmän sekä kuvauksen σ homomorfisuuden vuoksi

$$g_1 \cdot (g_2 \cdot x) = g_1 \cdot (\sigma(g_2)(x)) = \sigma(g_1)(\sigma(g_2)(x)) = ((\sigma(g_1) \circ \sigma(g_2))(x)$$
$$= (\sigma(g_1 g_2))(x) = (g_1 g_2) \cdot x$$

ja

$$e \cdot x = \sigma(e)(x) = \mathrm{id}_X(x) = x.$$

Asetettu kuvaus siis määrittää ryhmän G toiminnan joukossa X. Olkoon ryhmän G toimintaa vastaava permutaatioesitys ρ. Olkoon $g \in G$. Nyt $\rho(g)(x) = \rho_g(x) = gx = \sigma(g)(x)$, joten $\rho(g) = \sigma(g)$. Siis $\rho = \sigma$. □

Pyritään seuraavassa luomaan sellainen ekvivalenssirelaatio, jossa käytetään määritelmää 5.1. Tämän määritelmän avulla pystytään konstruoimaan kyseisen ekvivalenssirelaation ekvivalenssiluokat, joita kutsutaan radoiksi.

Määritelmä 5.5. Olkoon X G-joukko, missä G on ryhmä, X on epätyhjä joukko ja $x, y \in X$. Määritellään relaatio $\sim$ joukossa X siten, että

$$x \sim y, \text{ jos ja vain jos } gx = y \text{ jollain } g \in G.$$

Tällöin relaatiota $\sim$ kutsutaan *G-ekvivalenssiksi*.

Lause 5.6. *Olkoon X G-joukko, missä $(G, *)$ on ryhmä ja X on epätyhjä joukko. Tällöin G-ekvivalenssi on ekvivalenssirelaatio.*

Todistus (vrt. [9, s. 215]). Osoitetaan ensin, että määritelmän 5.5 relaatio $\sim$ on refleksiivinen. Olkoon $x \in X$. Tällöin $ex = x$, joten $x \sim x$.

Osoitetaan sitten, että $\sim$ on symmetrinen. Olkoot $x, y \in X$. Oletetaan, että $x \sim y$. Tällöin on olemassa $g \in G$ siten, että $gx = y$. Nyt määritelmän 5.1 nojalla $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1} * g) \cdot x = ex = x$, joten $y \sim x$.

Osoitetaan vielä lopuksi, että $\sim$ on transitiivinen. Olkoot $x, y, z \in X$. Oletetaan, että $x \sim y$ ja $y \sim z$. Täten on olemassa $g_1, g_2 \in G$ siten, että $g_1 x = y$ ja $g_2 y = z$. Edelleen $(g_2 * g_1) \cdot x = g_2 \cdot (g_1 \cdot x) = g_2 y = z$, joten $x \sim z$.

Täten relaatio $\sim$ on refleksiivinen, symmetrinen ja transitiivinen. Tällöin se on siis ekvivalenssirelaatio. □

Määritelmä 5.7. Olkoon X G-joukko, missä G on ryhmä ja X on epätyhjä joukko. G-ekvivalenssin määräämiä ekvivalenssiluokkia kutsutaan ryhmän G *radoiksi* joukossa X. Kun $x \in X$, niin alkion x määräämää rataa merkitään symbolilla O_x.

Alkion $x \in X$ määräämä rata on siis osajoukko

$$O_x = \{\, y \in X \mid x \sim y \,\} = \{\, y \in X \mid gx = y \text{ jollakin } g \in G \,\} = \{\, gx \mid g \in G \,\},$$

eli se koostuu niistä joukon X alkioista, jotka muodostuvat kaikkien ryhmän G alkioiden toimiessa alkion x kanssa.

Tarkastellaan edelleen epätyhjää joukkoa X, joka on G-joukko, missä G on ryhmä. Pyritään määrittelemään ryhmälle G aliryhmä, jonka avulla voidaan samaistaa kyseisen aliryhmän indeksi ryhmässä G joukon X kaikkien alkioiden ratojen koon kanssa.

Määritelmä 5.8. Olkoon G ryhmä, joka toimii epätyhjässä joukossa X, ja $x \in X$. Joukkoa

$$\mathrm{Stab}_G(x) := \{\, g \in G \mid gx = x \,\}$$

kutsutaan alkion x *stabilisaattoriksi*.

Lause 5.9. *Olkoon $(G, *)$ ryhmä, joka toimii epätyhjässä joukossa X. Tällöin alkion $x \in X$ stabilisaattori on ryhmän G aliryhmä.*

Todistus (ks. [11, s. 173]). Tarkastellaan alkion $x \in X$ stabilisaattoria $\mathrm{Stab}_G(x)$. Osoitetaan ensin neutraalialkion olemassaolo. Nyt $ex = x$, joten $e \in \mathrm{Stab}_G(x)$.

Osoitetaan sitten ryhmän G_x laskutoimituksen sulkeutuvuus. Olkoot $f, g \in G_x$. Tällöin $fx = x$ ja $gx = x$, joten $(f * g) \cdot x = f \cdot (g \cdot x) = fx = x$. Siis $fg \in \mathrm{Stab}_G(x)$.

Osoitetaan vielä käänteisalkion olemassaolo. Olkoon $h \in \mathrm{Stab}_G(x)$. Täten $hx = x$ ja $h^{-1}x = h^{-1} \cdot (h \cdot x) = (h^{-1} * h) \cdot x = ex = x$, joten $h^{-1} \in \mathrm{Stab}_G(x)$.

Saadaan siis, että $\mathrm{Stab}_G(x)$ on ryhmän G aliryhmä. □

Lause 5.10. *Toimikoon ryhmä G epätyhjässä joukossa X, ja olkoon ryhmän G toimintaa vastaava permutaatioesitys ρ. Tällöin*

$$\mathrm{Ker}(\rho) = \bigcap_{x \in X} \mathrm{Stab}_G(x).$$

Todistus. Tarkastellaan joukon X kaikkien alkioiden stabilisaattorien perhettä $\mathcal{A} = \{\mathrm{Stab}_G(x) \mid x \in X\}$. Olkoon $g \in \mathrm{Ker}(\rho)$. Koska $g \in \mathrm{Ker}(\rho)$, niin $\rho_g = \rho(g) = \mathrm{id}_X$. Täten kaikilla $x \in X$ pätee $gx = \rho_g(x) = \mathrm{id}_X(x) = x$, joten $g \in \mathrm{Stab}_G(x)$ kaikilla $x \in X$. Siis $g \in \bigcap \mathcal{A}$.

Oletetaan sitten, että $g \in \bigcap \mathcal{A}$. Silloin $g \in \mathrm{Stab}_G(x)$ kaikilla $x \in X$, jolloin $x = gx = \rho_g(x) = \rho(g)(x)$ kaikilla $x \in X$. Siis $\rho(g) = \mathrm{id}_X$, joten $g \in \mathrm{Ker}(\rho)$. □

Seuraavaksi esitettävä lause on yksi ryhmätoimintojen perustavaa laatua olevista tuloksista. Sen mukaan epätyhjän joukon X kaikkien alkioiden radat ovat yhtämahtavia näiden alkioiden stabilisaattorien indeksin kanssa.

Lause 5.11. *Olkoon $(G, *)$ ryhmä, joka toimii epätyhjässä joukossa X. Tällöin kaikilla $x \in X$ pätee, että*

$$(G : \mathrm{Stab}_G(x)) = |O_x|\,.$$

Todistus (vrt. [11, s. 173–174]). Olkoon $x \in X$. Merkitään $H = \mathrm{Stab}_G(x)$. Nyt $O_x = \{\, gx \mid g \in G \,\}$.

Osoitamme seuraavaksi, että on olemassa bijektio stabilisaattorin vasempien sivuluokkien joukosta G/H joukkoon O_x. Tarkastellaan kuvausta $f\colon G/H \to O_x$, $f(gH) = gx$.

Osoitetaan ensin, että kuvaus f on hyvinmääritelty. Olkoon $g_1H = g_2H$ joillain $g_1, g_2 \in G$. Lauseen 3.21 nojalla $g_1 = g_2h$ jollakin $h \in H$. Nyt $hx = x$, sillä $h \in H$. Täten $g_1x = (g_2 * h) \cdot x = g_2 \cdot (h \cdot x) = g_2x$. Siis $f(g_1H) = f(g_2H)$. Kuvaus f on täten hyvinmääritelty.

Osoitetaan nyt kuvauksen f injektiivisyys. Olkoon $f(g_1H) = f(g_2H)$, missä $g_1, g_2 \in G$. Silloin $g_1x = g_2x$. Edelleen $(g_2^{-1} * g_1) \cdot x = g_2^{-1} \cdot (g_1 \cdot x) = g_2^{-1} \cdot (g_2 \cdot x) =$

$(g_2^{-1} * g_2) \cdot x = ex = x$, joten $g_2^{-1} g_1 \in H$. Silloin lauseen 3.21 mukaan $g_1 H = g_2 H$. Kuvaus f on siis injektio.

Osoitetaan sitten, että kuvaus f on surjektio. Valitaan mielivaltainen $y \in O_x$. Tällöin on olemassa $g \in G$ siten, että $gx = y$. Nyt $f(gH) = gx = y$. Siis f on surjektio.

Koska kuvaus f on injektio ja surjektio, niin se on bijektio. Tästä seuraa, että halutut joukot ovat yhtämahtavia eli $(G : H) = |O_x|$. □

Esimerkki 5.2 (vrt. [18], tehtävä 189, s. 73)**.** Tarkastellaan symmetriaryhmää S_4 ja sen aliryhmän G luonnollista toimintaa joukossa $X = \{1, 2, 3, 4\}$. Nyt siis

$$O_x = \{\alpha(x) \mid \alpha \in G\} \text{ ja } \operatorname{Stab}_G(x) = \{\alpha \in G \mid \alpha(x) = x\}$$

kaikilla $x \in X$. Tutkitaan seuraavaksi edellisen lauseen kaavan toimivuutta kahdelle esimerkkitapaukselle.

Tarkastellaan ensin erityisesti aliryhmää $G = \langle (1\ 2\ 3) \rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. Havaitaan, että $O_1 = O_2 = O_3 = \{1, 2, 3\}$ ja $O_4 = \{4\}$. Edelleen $\operatorname{Stab}_G(x) = \{(1)\}$ kaikilla $x \in \{1, 2, 3\}$ ja $\operatorname{Stab}_G(4) = G$. Siis

$$(G : \operatorname{Stab}_G(x)) = \frac{|G|}{|\operatorname{Stab}_G(x)|} = \frac{3}{1} = 3 = |O_x|,$$

kun $x \in \{1, 2, 3\}$, ja $(G : \operatorname{Stab}_G(4)) = 1 = |O_4|$.

Tarkastellaan sitten aliryhmänä G alternoivaa ryhmää A_4. Luetellaan alternoivan ryhmän alkiot:

$$\begin{aligned} A_4 = \{&(1), (2\ 3\ 4), (2\ 4\ 3), (1\ 2) \circ (3\ 4), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), \\ &(1\ 3) \circ (2\ 4), (1\ 4\ 2), (1\ 4\ 3), (1\ 4) \circ (2\ 3)\}. \end{aligned}$$

Nyt $O_x = X$ kaikilla $x \in X$. Edelleen

$$\begin{aligned} \operatorname{Stab}_G(1) &= \{(1), (2\ 3\ 4), (2\ 4\ 3)\}, \\ \operatorname{Stab}_G(2) &= \{(1), (1\ 3\ 4), (1\ 4\ 3)\}, \\ \operatorname{Stab}_G(3) &= \{(1), (1\ 2\ 4), (1\ 4\ 2)\} \text{ ja} \\ \operatorname{Stab}_G(4) &= \{(1), (1\ 2\ 3), (1\ 3\ 2)\}. \end{aligned}$$

Siis kaikilla $x \in X$ pätee, että

$$(G : \operatorname{Stab}_G(x)) = \frac{|G|}{|\operatorname{Stab}_G(x)|} = \frac{12}{3} = 4 = |O_x|.$$

Määritelmä 5.12. Toimikoon ryhmä G epätyhjässä joukossa X. Ryhmän toiminnan sanotaan olevan *transitiivinen*, jos ryhmällä G on vain yksi rata.

Ryhmien toimintoja sovelletaan paljon tilanteissa, jossa ryhmä toimii jossain siihen liittyvässä ryhmässä tai siihen liittyvien ryhmien muodostamassa joukossa. Käsitellään seuraavaksi tärkeä esimerkki tällaisesta tilanteesta. Olkoon H ryhmän

G aliryhmä, ja olkoon joukko X nyt aliryhmän H kaikkien vasempien sivuluokkien joukko G/H. Havaitaan, että kuvaus

$$\cdot\colon G \times X \to X, g \cdot (xH) = (gx)H$$

määrittää ryhmän G toiminnan joukossa X (ks. [18, s. 73]). Huomataan myös, että ryhmän toiminta on transitiivinen: Jos relaatio $\sim$ on G-ekvivalenssi ja $xH, yH \in X$, niin $(yx^{-1}) \cdot (xH) = yH$, joten $xH \sim yH$ ($yx^{-1} \in G$). Tarkastellaan vasenta sivuluokkaa $xH \in X$. Nyt ryhmän toiminnan transitiivisuuden ja lauseen 1.13 perusteella $X = \bigcup\{O_{xH}\} = O_{xH}$, ja

$$\begin{aligned}\mathrm{Stab}_G(xH) &= \{g \in G \mid (gx)H = xH\} = \{g \mid x^{-1}gx \in H\} = \{g \mid x^{-1}gx = h, h \in H\} \\ &= \{g \mid g = xhx^{-1}, h \in H\} = xHx^{-1}.\end{aligned}$$

Täten sivuluokkien stabilisaattorit ovat niiden määräämiä aliryhmän H konjugaatteja. Edelleen lauseen 5.11 nojalla

$$(G : xHx^{-1}) = |O_{xH}| = |X| = (G : H).$$

Olkoon ρ^H tätä ryhmän G toimintaa vastaava permutaatioesitys, jolloin lauseesta 5.10 seuraa, että

$$\mathrm{Ker}(\rho^H) = \bigcap_{x \in G} xHx^{-1}.$$

Jos tässä valittaisiin $H = \{e\}$, niin $X = G/\{e\} = G$, ja ryhmän toiminta olisi kuvaus $\cdot\colon G \times G \to G, g \cdot x = gx$. Tätä vastaava permutaatioesitys olisi $\rho^1\colon G \to S_G, \rho(g) = \rho_g$, missä $\rho_g\colon G \to G, \rho_g(x) = gx$. Tästä seuraa itse asiassa Cayleyn lause 4.12, sillä sen lauseen merkinnöillä permutaatioesityksen kuva $\mathrm{Im}(\rho^1) = F(G)$ ja $\rho^1\colon G \cong \mathrm{Im}(\rho^1)$, missä $\mathrm{Im}(\rho^1) \leqslant S_G$. Edellä esitettyä ryhmän toimintaa joukossa G/H voidaan siis pitää Cayleyn lauseen laajennuksena.

Myöhemmin havaitaan, että tämä kyseinen ryhmän toiminta osoittautuu erittäin hyödylliseksi. Annetaan tämän vuoksi tälle ryhmän toiminnalle erillinen määritelmä, jossa kyseinen toiminta nimetään tehdyn havainnon perusteella Cayleyn toiminnaksi.

Määritelmä 5.13. Olkoon H ryhmän G aliryhmä, ja merkitään $X := G/H$. Tällöin seuraavaa ryhmän G toimintaa joukossa X, missä toiminta on kuvaus

$$\cdot\colon G \times X \to X, g \cdot (xH) = (gx)H,$$

kutsutaan *Cayleyn toiminnaksi*.

Tarkastellaan nyt erityisesti kaikkien ryhmän G alkioiden aliryhmän H konjugaattien leikkausta $\bigcap_{x \in G} xHx^{-1}$ ja sen ominaisuuksia.

Määritelmä 5.14. Olkoon $H \leqslant G$. Tällöin joukkoa

$$H_G := \bigcap_{x \in G} xHx^{-1}$$

kutsutaan aliryhmän H *keskiöksi* ryhmässä G.

Huomautus. Tutkielmassa käytetty terminologia ei ole välttämättä kovinkaan vakiintunutta. Useat englanninkielisten lähteiden nimitykset ovat yksinkertaisesti tekijän itsensä suomentamia. Yksi esimerkki tästä on määritelmän 5.14 englanninkielisen termin *core* suomennos keskiöksi.

Lause 5.15. *Oletetaan, että $H \leqslant G$. Tällöin $H_G \trianglelefteq G$ ja $H_G \leqslant H$. Edelleen, jos K on sellainen aliryhmän H aliryhmä, että $K \trianglelefteq G$, niin $K \leqslant H_G$.*

Todistus. Keskiön normaalius seuraa suoraan siitä, että se on aiemmin määritellyn ryhmän G toimintaa vastaavan permutaatioesityksen ρ^H, joka on homomorfismi, ydin. Vaihtoehtoisesti normaaliuuden voi todistaa muutoinkin: ks. esim. [11, s. 134]. Muiden kohtien todistaminen on suoraviivaista (vrt. [18], s. 38, tehtävä 90). □

Aliryhmän H keskiö ryhmässä G on siis maksimaalinen ryhmän G normaali aliryhmä, joka sisältyy aliryhmään H. Nyt voidaan todistaa yksinkertainen, mutta tärkeä tulos, jonka todistamisessa hyödynnetään Cayleyn toimintaa. Lauseen todistuksessa pätevät samat merkinnät kuin edellä.

Lause 5.16. *Olkoon H ryhmän G aliryhmä, jolla on äärellinen indeksi. Tällöin G/H_G voidaan upottaa symmetriaryhmään $S_{(G:H)}$.*

Todistus (vrt. [18, s. 74]). Merkitään $n = (G : H)$. Tällöin lauseen 4.2 nojalla $S_X \cong S_n (|I_n| = (G : H) = |X|)$. Olkoon $\sigma \colon S_X \to S_n$ näiden symmetriaryhmien välinen isomorfismi. Merkitään $\alpha = \sigma \circ \rho^H$, jolloin α on homomorfismi ryhmästä G symmetriaryhmään S_n. Nyt

$$\operatorname{Ker}(\alpha) = \operatorname{Ker}(\rho^H) = H_G,$$

sillä σ on bijektio, joten ensimmäisen isomorfialauseen nojalla $G/H_G \cong \operatorname{Im}(\alpha)$, missä $\operatorname{Im}(\alpha) \leqslant S_n$. Väite seuraa siis lauseesta 4.7. □

Lauseesta 5.16 voidaan johtaa mielenkiintoisia seurauksia, joista esitetään nyt neljä.

Seuraus 5.17. *Olkoon H ryhmän G aliryhmä, jolla on äärellinen indeksi. Tällöin on olemassa sellainen ryhmän G normaali aliryhmä K, joka on ryhmän H aliryhmä ja jonka indeksi ryhmässä G on äärellinen.*

Todistus. Valitaan $K = H_G$ ja tulos seuraa suoraan lauseesta 5.16. □

Seuraus 5.18. *Olkoon G äärellinen ryhmä ja H sen aito aliryhmä, jolla on äärellinen indeksi n. Oletetaan, että $|G|$ ei jaa lukua $n!$. Tällöin ryhmällä G on epätriviaali ja normaali aliryhmä.*

Todistus (vrt. [11, s. 175]). Koska $H < G$, niin $H_G \lhd G$. Lauseen 5.16 nojalla G/H_G on isomorfinen jonkin symmetriaryhmän S_n aliryhmän kanssa. Näin ollen Lagrangen lauseen perusteella $(G : H_G)$ jakaa luvun $n!$. Mutta koska $|G|$ ei jaa lukua $n!$, niin Lagrangen lauseesta seuraa, että $|H_G| \neq 1$, joten keskiö H_G on haluttu ryhmän G epätriviaali normaali aliryhmä. □

Seuraus 5.19. *Olkoon G äärellinen ryhmä, jonka kertaluku on pn, missä p on alkuluku ja $p \geq n$. Jos H on ryhmän G aliryhmä, jonka kertaluku on p, niin H on ryhmän G normaali aliryhmä.*

Todistus (vrt. [11, s. 177]). Olkoon $H \leqslant G$ ja $|H| = p$. Nyt $(G : H) = \frac{|G|}{|H|} = \frac{pn}{p} = n$. Tarkastellaan aliryhmän H keskiötä H_G. Nyt koska $H_G \leqslant H$, niin Lagrangen lauseesta seuraa, että joko $H_G = \{e\}$ tai $H_G = H$. Jos olisi $H_G = \{e\}$, niin lauseen 5.16 perusteella $G/\{e\} = G$ on isomorfinen jonkin symmetriaryhmän S_n aliryhmän kanssa. Siis ryhmän G kertaluku jakaa symmetriaryhmän S_n kertaluvun, jolloin $pn \mid n!$. Täten $p \mid (n-1)!$, joten $p \mid (n-i)$ jollakin $i \in \{1, \ldots, n-1\}$. Silloin $n > n - i = kp \geq p$, missä $k \in \mathbb{Z}_+$. Tämä on kuitenkin ristiriidassa oletuksen $p \geq n$ kanssa. Näin ollen $H = H_G$, joten $H \trianglelefteq G$. □

Seuraus 5.20. *Oletetaan, että G on äärellinen ryhmä ja p on ryhmän G kertaluvun pienin alkutekijä. Jos H on ryhmän G aliryhmä, jonka indeksi on p, niin $H \trianglelefteq G$.*

Todistus (vrt. [18, s. 75]). Oletetaan, että $H \leqslant G$ ja $(G : H) = p$. Tällöin Lagrangen lauseen perusteella $(G : H_G) = p(H : H_G)$. Oletetaan, että $(H : H_G) > 1$. Tällöin on olemassa alkuluku q, joka jakaa indeksin $(H : H_G)$. Tällöin q jakaa myös kertaluvun $|G|$, joten oletuksesta seuraa, että $q \geq p$. Nyt lauseen 5.16 mukaan G/H_G voidaan upottaa symmetriaryhmään S_p, joten on olemassa sellainen $K \leqslant S_p$, että $G/H_G \cong K$, jolloin $(G : H_G) = |K|$. Lisäksi Lagrangen lauseen nojalla $|K|$ jakaa symmetriaryhmän S_p kertaluvun, joka on $p!$. Siis indeksi $(G : H_G)$ jakaa luvun $p!$. Edelleen koska $q \mid (H : H_G)$, $(G : H) = p$ ja $(G : H_G) = (G : H)(H : H_G)$, niin $pq \mid (G : H_G)$. Siis $pq \mid p!$, joten $q \mid (p-1)!$. Näin ollen, koska q on alkuluku, niin q jakaa luvun $p - i$ jollakin $1 \leq i < p$. Siis $p > p - i = kq \geq q$, missä $k \in \mathbb{Z}_+$. Tämä on ristiriita, joten on oltava $(H : H_G) = 1$. Siis $H = H_G \trianglelefteq G$, sillä $H \leqslant H_G$. □

Lauseen 5.16 seurauksista erityisesti seuraus 5.18 osoittautuu hyödylliseksi myöhemmin, kun tarkastellaan äärellisten ryhmien yksinkertaisuutta luvussa 7.

5.2 Luokkayhtälöt ja konjugaattiluokat

Tarkastellaan yleisesti ryhmän G toimintaa epätyhjässä, ja erityisesti äärellisessä, joukossa X. Pyritään johtamaan joukon X kertaluvulle hyödyllinen lauseke, jota kutsutaan ryhmätoimintojen luokkayhtälöksi. Tästä yleisestä luokkayhtälöstä voidaan myöhemmin johtaa erikoistapauksena enemmän käytetty luokkayhtälö äärellisille ryhmille, kun tarkastellaan äärellisen ryhmän G toimintaa itseensä. Ensiksi esitettävä lause 5.21 on seurausta lauseesta 5.11.

Lause 5.21. *Olkoon G ryhmä, joka toimii epätyhjässä ja äärellisessä joukossa X. Tällöin*

$$|X| = \sum_{a \in A} (G : \mathrm{Stab}_G(a)),$$

missä A on joukon X osajoukko, joka sisältää täsmälleen yhden alkion jokaiselta ryhmän G radalta.

Todistus (vrt. [11, s. 174]). Oletetaan, että joukko X on äärellinen. Lauseen 5.6 perusteella G-ekvivalenssi on ekvivalenssirelaatio joukossa X, jolloin lauseen 1.13 nojalla joukko X voidaan osittaa ryhmän G erillisiin ratoihin. Näin ollen

$$X = \bigcup_{a \in A} \mathcal{O}_a.$$

Edelleen lauseen 5.11 nojalla $(G : \mathrm{Stab}_G(x)) = |\mathcal{O}_x|$ kaikilla $x \in X$, jolloin saadaan, että

$$|X| = \sum_{a \in A} |\mathcal{O}_a| = \sum_{a \in A} (G : \mathrm{Stab}_G(a)),$$

sillä X on äärellinen. □

Määritellään nyt, mitä tarkoitetaan joukon X alkion sekä itse joukon kiinnittämisellä.

Määritelmä 5.22. Olkoon G ryhmä ja X G-joukko. Olkoon $x \in X$ ja $g \in G$. Tällöin alkion g sanotaan *kiinnittävän* alkion x, jos $gx = x$. Jos $gx = x$ kaikilla $g \in G$, niin ryhmä G kiinnittää alkion x. Kaikkien niiden joukon X alkioiden joukkoa, jotka ryhmä G kiinnittää, merkitään symbolilla $\mathrm{Fix}_X(G)$. Toisin sanoen,

$$\mathrm{Fix}_X(G) := \{x \in X \mid gx = x \text{ kaikilla } g \in G\}.$$

Tätä joukon X osajoukkoa kutsutaan *ryhmän G kiinnittämäksi osajoukoksi*.

Havaitaan, että $\mathrm{Stab}_G(x) = G$ kaikilla $x \in \mathrm{Fix}_X(G)$. Ryhmän G kiinnittämän osajoukon $\mathrm{Fix}_X(G)$ alkiot muodostavat siis kukin oman ratansa, joka on yksiö: $x \in \mathrm{Fix}_X(G)$, jos ja vain jos $\mathcal{O}_x = \{x\}$. Tästä määritelmästä ja lauseesta 5.21 seuraakin ryhmätoimintojen luokkayhtälö:

Lause 5.23 (Ryhmätoimintojen luokkayhtälö)**.** *Olkoon X äärellinen G-joukko. Merkitään $X_0 = \mathrm{Fix}_X(G)$. Tällöin*

$$|X| = |X_0| + \sum_{a \in A \setminus X_0} (G : \mathrm{Stab}_G(a)),$$

missä A on joukon X osajoukko, joka koostuu joukon X G-ekvivalenssin kaikista eri edustajista.

Todistus (vrt. [15]). Nyt jos $x \neq y$, missä $x, y \in X_0$, niin $\{x\} \neq \{y\}$ eli $\mathcal{O}_x \neq \mathcal{O}_y$. Täten ryhmän G kiinnittämän osajoukon X_0 jokainen alkio määrittelee yksikäsitteisesti oman ratansa. Lisäksi $|\mathcal{O}_x| = 1$ kaikilla $x \in X_0$. Osajoukossa A on puolestaan täsmälleen yksi edustaja jokaisesta radasta, joten $X_0 \subseteq A$. Siis lauseesta 5.21 seuraa suoraan haluttu luokkayhtälö:

$$|X| = \sum_{a \in A} (G : \mathrm{Stab}_G(a)) = \sum_{a \in A \cap X_0} |\mathcal{O}_a| + \sum_{a \in A \setminus X_0} |\mathcal{O}_a| = |X_0| + \sum_{a \in A \setminus X_0} (G : \mathrm{Stab}_G(a)).$$

□

Huomautus. Oletetaan, että edeltävän lauseen oletukset ovat voimassa. Huomataan, että jos $X \neq \mathrm{Fix}_X(G)$, niin $A \setminus \mathrm{Fix}_X(G) \neq \emptyset$. Tämä voidaan perustella sillä, että on olemassa $x \in X \setminus \mathrm{Fix}_X(G)$, jolloin on tietysti olemassa sellainen $a \in A$, että $O_a = O_x$. Jos olisi $a \in \mathrm{Fix}_X(G)$, niin pätisi $a = x$, mikä on ristiriita. Siis $a \in A \setminus \mathrm{Fix}_X(G)$.

Tarkastellaan sitten kahta tärkeää ryhmän G aliryhmää: keskusta ja keskittäjää. Määritellään lisäksi tärkeät ekvivalenssiluokat, joita kutsutaan konjugaattiluokiksi.

Määritelmä 5.24. Ryhmän G kaikkien vaihdannaisten alkioiden joukkoa merkitään symbolilla $Z(G)$. Toisin sanoen,

$$Z(G) := \{\, g \in G \mid xg = gx \text{ kaikilla } x \in G \,\}.$$

Joukkoa $Z(G)$ kutsutaan ryhmän G *keskukseksi*.

Lause 5.25. *Ryhmän G keskus $Z(G)$ on ryhmän G vaihdannainen ja normaali aliryhmä.*

Todistus (vrt. [18], s. 47, tehtävä 117). Tarkastellaan alaluvun 4.1 lausekkeen (4.1) mukaista homomorfismia $\tau\colon G \to S_G$, missä jokainen ryhmän G alkio kuvautuu alkion määräämäksi sisäiseksi automorfismiksi. Nyt

$$\begin{aligned}\mathrm{Ker}(\tau) &= \{g \in G \mid \tau_g = (1)\} = \{g \in G \mid \tau_g(x) = x \text{ kaikilla } x \in G\} \\ &= \{g \in G \mid xg = gx \text{ kaikilla } x \in G\} = Z(G).\end{aligned}$$

Täten lauseen 4.5 nojalla $Z(G) \trianglelefteq G$. Keskuksen vaihdannaisuus seuraa suoraan sen määritelmästä. □

Määritelmä 5.26. Olkoon G ryhmä ja $x \in G$. Alkion x *keskittäjä* ryhmässä G, $C_G(x)$, on joukko

$$C_G(x) = \{g \in G \mid xg = gx\}.$$

Ryhmän G alkion x keskittäjä on siis kaikkien niiden ryhmän G alkioiden joukko, jotka ovat vaihdannaisia alkion x kanssa. Se on myös ryhmän G aliryhmä.

Lause 5.27. *Olkoon a ryhmän G alkio. Tällöin $C_G(a)$ on ryhmän G aliryhmä.*

Todistus. Ks. [11, s. 191] ja vertaa lauseen 5.9 todistukseen. □

Ryhmän G sisäisen automorfismin kautta määriteltiin (ks. määritelmä 4.8), mitä tarkoitettiin sillä, että ryhmän G alkiot ovat konjugaatteja keskenään. Tämän avulla voidaankin määritellä ekvivalenssirelaatio, ja edelleen ekvivalenssiluokat eli tässä tapauksessa konjugaattiluokat.

Määritelmä 5.28. Määritellään sellainen relaatio $\sim$ ryhmässä G, että kaikilla $x, y \in G$

$$x \sim y, \text{ jos ja vain jos } y \text{ on alkion } x \text{ konjugaatti.}$$

Relaatiota $\sim$ kutsutaan *konjugoinniksi* ryhmässä G.

Lause 5.29. *Konjugointi ryhmässä G on ekvivalenssirelaatio.*

Todistus. Ks. [11, s. 191] ja vertaa lauseen 5.6 todistukseen. □

Määritelmä 5.30. Ryhmän G konjugoinnin määräämiä ekvivalenssiluokkia kutsutaan *konjugaattiluokiksi*. Alkion $x \in G$ määräämää konjugaattiluokkaa merkitään symbolilla $C_l(x)$.

Havaitaan, että alkion ryhmän G alkion x määräämä konjugaattiluokka on joukko

$$\begin{aligned} C_l(x) &= \{y \in G \mid x \sim y\} = \{y \in G \mid y = gxg^{-1} \text{ jollakin } g \in G\} = \{gxg^{-1} \mid g \in G\} \\ &= \{t_g(x) \mid g \in G\} = \{\alpha(x) \mid \alpha \in \mathrm{Inn}(G)\}, \end{aligned}$$

eli kaikkien ryhmän G sisäisten automorfismien kuvat pisteessä x.

Aiemmin tutkittiin ryhmän G Cayleyn toimintaa joukossa G/H, missä $H \leqslant G$. Tarkastellaan nyt toista tärkeää ryhmän toimintaa, jossa ryhmä G toimii itsensä kanssa.

Määritelmä 5.31. Olkoon G ryhmä. Kuvaus

$$\cdot \colon G \times G \to G, g \cdot x = gxg^{-1}.$$

määrittää ryhmän G toiminnan itseensä (ks. [18, s. 78]). Tällaista ryhmän toimintaa kutsutaan ryhmän G *konjugaatioksi* itseensä, ja sanotaan, että ryhmä G toimii itsensä kanssa *konjugoimalla*.

Huomautus. Jos $H \trianglelefteq G$, niin ryhmän G konjugaatio sen aliryhmään H on myös ryhmän toiminta. Tällöin ryhmän toiminnan määrittävä kuvaus olisi $\cdot \colon G \times H \to H, g \cdot x = gxg^{-1}$. Oleellistä tässä on nimenomaan se, että aliryhmä H on normaali, jolloin $gxg^{-1} \in H$, kun $x \in H$ ja $g \in G$. Tämä varmistaa sen, että kuvaus on hyvin määritelty. Muutoin määritelmän 5.1 ehtojen toteaminen onnistuu täysin vastaavasti.

Havaitaan, että ryhmän G konjugaation itseensä määrittämät radat ja stabilisaattorit yhtyvät jo aiemmin määriteltyihin käsitteisiin. Olkoon nimittäin $x \in G$. Nyt alkion x määrämä rata on joukko

$$O_x = \{gx \mid g \in G\} = \{gxg^{-1} \mid g \in G\} = C_l(x),$$

eli alkion x konjugaattiluokka. Edelleen alkion x stabilisaattori on

$$\mathrm{Stab}_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid xg = gx\} = C_G(x),$$

eli alkion x keskittäjä. Tarkastellaan vielä ryhmän G kiinnittämää ryhmän G osajoukkoa $\mathrm{Fix}_G(G)$. Havaitaan, että se on itse asiassa ryhmän G keskus:

$$\begin{aligned} \mathrm{Fix}_G(G) &= \{x \in G \mid gx = x \text{ kaikilla } g \in G\} = \{x \in G \mid gxg^{-1} = x \text{ kaikilla } g \in G\} \\ &= \{x \in G \mid gx = xg \text{ kaikilla } g \in G\} = Z(G). \end{aligned}$$

Näin ollen lauseen 5.11 erikoistapauksena saadaan tulos, jossa kaikkien ryhmän G alkioiden konjugaattiluokat ovat yhtämahtavia näiden alkioiden keskittäjien indeksien kanssa.

Lause 5.32. *Olkoon x ryhmän G alkio. Tällöin*

$$|C_l(x)| = (G : C_G(x)).$$

Edelleen, kun tarkasteltavana ryhmän G toimintana on ryhmän G konjugaatio itseensä, niin ryhmätoimintojen luokkayhtälön eli lauseen 5.23 erikoistapauksena saadaan tärkeä ja vastaava tulos ryhmille, jota kutsutaan yksinkertaisesti luokkayhtälöksi.

Lause 5.33 (Luokkayhtälö)**.** *Olkoon G äärellinen ryhmä, ja A joukko, joka sisältää täsmälleen yhden alkion jokaiselta konjugaattiluokalta. Tällöin*

$$|G| = |Z(G)| + \sum_{a \in A \setminus Z(G)} (G : C_G(a)).$$

Huomautus. Suoraan määritelmästä 5.24 havaitaan, että G on Abelin ryhmä, jos ja vain jos $G = Z(G)$. Kiinnostavia ryhmiä luokkayhtälön kannalta ovat siis äärelliset ryhmät, jotka eivät ole vaihdannaisia.

Esimerkki 5.3 (vrt. [16], tehtävä 3, s. 152)**.** Tarkastellaan ryhmää $(\mathbb{Z}_2 \times S_3, *)$, missä ryhmän laskutoimitus on määritelty kuten lauseessa 1.35. Merkitään $G := \mathbb{Z}_2 \times S_3$. Pyritään määrittämään ryhmän G konjugaattiluokat, ja sen kertaluku luokkayhtälön mukaisesti. Olkoot $\overline{a}, \overline{b} \in \mathbb{Z}_2$ ja $\lambda, \mu \in S_3$. Tällöin

$$(\overline{a}, \lambda) * (\overline{b}, \mu) * (\overline{a}, \lambda)^{-1} = (\overline{a} + \overline{b}, \lambda \circ \mu) * (-\overline{a}, \lambda^{-1}) =$$
$$(\overline{a} + \overline{b} + (-\overline{a}), (\lambda \circ \mu) \circ \lambda^{-1}) = (\overline{b}, \lambda \circ \mu \circ \lambda^{-1}).$$

Riittää täten, että tarkastellaan symmetriaryhmän S_3 konjugaattiluokkia, sillä ryhmä $\mathbb{Z}_2$ on Abelin ryhmä (ja sille pätee siis, että $Z(\mathbb{Z}_2) = \mathbb{Z}_2$). Merkitään ryhmän S_3 alkiota seuraavasti:

$$S_3 = \{\, (1), (1\ \ 3\ \ 2), (1\ \ 2\ \ 3), (1\ \ 2), (1\ \ 3), (2\ \ 3) \,\} := \{\, (1), \alpha, \beta, \rho, \delta, \tau \,\}.$$

Määritetään ensin, mitkä ryhmän S_3 alkiot ovat alkion α konjugaatteja. Muodostetaan ryhmän S_3 kertotaulu tämän tarkastelun avuksi:

Taulukko 5.1: Ryhmän S_3 kertotaulu.

$\circ$	(1)	ρ	δ	τ	α	β
(1)	(1)	ρ	δ	τ	α	β
ρ	ρ	(1)	α	β	δ	τ
δ	δ	β	(1)	α	τ	ρ
τ	τ	α	β	(1)	ρ	δ
α	α	τ	ρ	δ	β	(1)
β	β	δ	τ	ρ	(1)	α

Nyt

$$\beta \circ \alpha \circ \beta^{-1} = \alpha,\ \rho \circ \alpha \circ \rho^{-1} = \beta,\ \delta \circ \alpha \circ \delta^{-1} = \beta \text{ ja } \tau \circ \alpha \circ \tau^{-1} = \beta.$$

Siis alkion α konjugaatti on β eli $\alpha \sim \beta$. Vastaavasti tutkimalla ryhmän S_3 loput alkiot taulukkoa 5.1 hyödyntämällä saadaan, että $\beta \sim \alpha$ ja $\rho \sim \delta \sim \tau$. Ryhmän G konjugaattiluokat ovat siis

$$\{(\overline{0}, (1))\},\ \{(\overline{0}, \alpha), (\overline{0}, \beta)\},\ \{(\overline{0}, \rho), (\overline{0}, \delta), (\overline{0}, \tau)\},\ \{(\overline{1}, (1))\}, \{(\overline{1}, \alpha), (\overline{1}, \beta)\},$$
$$\{(\overline{1}, \rho), (\overline{1}, \delta), (\overline{1}, \tau)\}.$$

Valitsemalla edustaja jokaisesta konjugaattiluokasta voidaan muodostaa ryhmän G kertaluku luokkayhtälön mukaan:

$$|G| = |Z(G)| + \Big(G : C((\overline{0}, \alpha))\Big) + \Big(G : C((\overline{0}, \rho))\Big) + \Big(G : C((\overline{1}, \alpha))\Big) +$$
$$\Big(G : C((\overline{1}, \rho))\Big) = \Big|\{(\overline{0}, (1)), (\overline{1}, (1))\}\Big| + \Big|C_l((\overline{0}, \alpha))\Big| + \Big|C_l((\overline{0}, \rho))\Big| + \Big|C_l((\overline{1}, \alpha))\Big| +$$
$$\Big|C_l((\overline{1}, \rho))\Big| = 2 + 2 + 3 + 2 + 3 = 12.$$

5.3 Ryhmän konjugaation yleistys

Tarkastellaan nyt ryhmän G toimintaa, jota voidaan pitää määritelmän 5.31 mukaisen ryhmän G konjugaation laajennuksena.

Määritelmä 5.34. Olkoon G ryhmä ja $\mathcal{L}(G)$ kaikkien ryhmän G epätyhjien osajoukkojen perhe. Olkoon U ryhmän G epätyhjä osajoukko, ja $g \in G$. Tällöin joukkoa

$$gUg^{-1} = \{gug^{-1} \mid u \in U\}$$

kutsutaan alkion g määräämäksi *joukon U konjugaatiksi*. Joukko $U \in \mathcal{L}(G)$ on joukon $T \in \mathcal{L}(G)$ *konjugaatti* eli joukot U ja T ovat konjugaatteja keskenään, jos on olemassa sellainen $g \in G$, että $U = gTg^{-1}$.

Merkintä 5.35. Olkoon U ryhmän G osajoukko ja x ryhmän G alkio. Olkoon $g \in G$. Jatkossa useissa tilanteissa käytetään alkion g määräämille joukon U ja alkion x konjugaateille gUg^{-1} ja gxg^{-1} lyhyempiä merkintöjä U^g ja x^g.

Kun ryhmän G osajoukko U on yksiö, määritelmä 5.34 palautuu määritelmään 4.8. Ryhmälle G voidaan nyt määritellä toiminta perheessä $\mathcal{L}(G)$.

Lause 5.36. *Olkoon G ryhmä. Kuvaus*

$$\cdot : G \times \mathcal{L}(G) \to \mathcal{L}(G), g \cdot U = U^g$$

määrittää ryhmän G toiminnan perheessä $\mathcal{L}(G)$.

Todistus. Kuvaus on selvästi hyvin määritelty. Olkoot $g_1, g_2 \in G$ ja $U \in \mathcal{L}(G)$. Tällöin

$$\begin{aligned} g_1 \cdot (g_2 \cdot U) &= g_1 \cdot (U^{g_2}) = (U^{g_2})^{g_1} = g_1(g_2 U g_2^{-1})g_1^{-1} \\ &= (g_1 g_2)U(g_1 g_2)^{-1} = U^{g_1 g_2} = (g_1 g_2) \cdot U \end{aligned}$$

ja

$$e \cdot U = U^e = U.$$

Ryhmä G siis toimii perheessä $\mathcal{L}(G)$. □

Määritelmä 5.37. Lauseen 5.36 kuvauksen määrittämää ryhmän G toimintaa perheessä $\mathcal{L}(G)$ kutsutaan ryhmän G *konjugaatioksi* perheessä $\mathcal{L}(G)$. Tällöin sanotaan, että ryhmä G toimii perheessä $\mathcal{L}(G)$ *konjugoimalla*.

Näin määritelty ryhmän toiminta palautuu määritelmän 5.31 ryhmän toiminnaksi, jos rajoitetaan tämä toiminta koskemaan perhettä sellaisista ryhmän G osajoukoista, jotka ovat yksiöitä. Tällainen rajoittuma voidaan itse asiassa yleistää.

Lause 5.38. *Toimikoon ryhmä G joukossa X, ja olkoon $\cdot\colon G \times X \to X$ tämän toiminnan määrittävä kuvaus. Olkoon $H \leqslant G$. Tällöin kuvauksen $\cdot$ rajoittuma*

$$\cdot \restriction (H \times X)$$

määrittää aliryhmän H toiminnan joukossa X. Tällöin sanotaan, että aliryhmä H toimii joukossa X ryhmän G toiminnan rajoittumana.

Todistus. Väite seuraa suoraan siitä, että X on G-joukko ja kuvauksen $f\colon A \to B$ rajoittuma johonkin joukon A osajoukkoon on myös kuvaus. □

Yleistetään nyt aiemmin määritelmässä 5.30 esitetty konjugaattiluokan käsite.

Määritelmä 5.39. Olkoon G ryhmä. Määritellään relaatio ϕ perheessä $\mathcal{L}(G)$ seuraavasti:

$$\phi = \{(H, K) \in \mathcal{L}(G) \times \mathcal{L}(G) \mid H \text{ on joukon } K \text{ konjugaatti}\}.$$

Relaatiota ϕ kutsutaan *konjugoinniksi* perheessä $\mathcal{L}(G)$.

Lause 5.40. *Konjugointi perheessä $\mathcal{L}(G)$ on ekvivalenssirelaatio.*

Todistus. Sivuutetaan. Todistus perustuu suoraan ekvivalenssirelaation määritelmään. □

Määritelmä 5.41. Perheen $\mathcal{L}(G)$ konjugoinnin määräämiä ekvivalenssiluokkia kutsutaan *konjugaattiluokiksi*. Joukon $U \in \mathcal{L}(G)$ ekvivalenssiluokkaa merkitään symbolilla $C_l(U)$.

Tarkastellaan ryhmän G konjugaatiota perheessä $\mathcal{L}(G)$. Olkoon $U \in \mathcal{L}(G)$. Havaitaan, että joukon U konjugaattiluokka on tällöin kyseisen joukon rata:

$$\begin{aligned} C_l(U) &= \{T \in \mathcal{L}(G) \mid (U,T) \in \phi\} = \{T \in \mathcal{L}(G) \mid (T,U) \in \phi\} \\ &= \{T \in \mathcal{L}(G) \mid T = U^g \text{ jollakin } g \in G\} = \{U^g \mid g \in G\} = \mathcal{O}_U. \end{aligned}$$

Edelleen sen stabilisaattori on $\mathrm{Stab}_G(U) = \{g \in G \mid U^g = U\}$. Kyseinen joukon U stabilisaattori on erityisen tärkeä, joten sille annetaan oma määritelmänsä.

Määritelmä 5.42. Olkoon U ryhmän G epätyhjä osajoukko. Joukkoa

$$N_G(U) := \{\, g \in G \mid U^g = U \,\}$$

kutsutaan joukon U *normalisoijaksi* ryhmässä G.

Suoraan lauseen 5.11 erikoistapauksena saadaankin nyt tulos, joka yleistää lauseen 5.32:

Lause 5.43. *Olkoon $U \in \mathcal{L}(G)$. Tällöin $|C_l(U)| = (G : N_G(U))$.*

Huomautus. Tässä käsitelty konjugaatio ja konjugaattiluokka ovat käytännössä täydellisessä analogiassa puhuttiinpa sitten niistä pelkästään ryhmän G tai sen muodostaman perheen $\mathcal{L}(G)$ yhteydessä. Puhuttaessa ryhmästä G tarkastellaan sen alkioita, ja niiden määräämiä konjugaattiluokkia tai ratoja. Käsiteltäessä perhettä $\mathcal{L}(G)$ tarkastellaan taas ryhmän G osajoukkoja sen alkioina, ja niiden määrittämiä vastaavia käsitteitä. Asiayhteyden perusteella on helppoa tunnistaa, kummasta kulloinkin puhutaan, pelkästä ryhmän konjugaatiosta vai sen yleistyksestä.

Lauseen 5.9 nojalla $N_G(U) \leqslant G$. Normalisoijan käsite on erityisen kiinnostava, kun tarkastellaan ryhmän G aliryhmiä. Oletetaan, että $H, K \leqslant G$. Nyt joukko $N_K(H) = \{k \in K \mid H^k = H\}$ on aliryhmän H normalisoija aliryhmässä K. Voidaan osoittaa, että se on aliryhmän K aliryhmä.

Lause 5.44. *Olkoot H ja K ryhmän G aliryhmiä. Tällöin $N_K(H) \leqslant K$.*

Todistus (vrt. [11, s. 193]). Havaitaan, että $N_K(H) = N_G(H) \cap K$, joten $N_K(H) \leqslant G$, sillä $N_G(H)$ ja K ovat ryhmän G aliryhmiä. Lisäksi $N_K(H) \subseteq K$, joten $N_K(H) \leqslant K$. □

Selvästi $N_G(H) = G$, kun H on ryhmän G normaali aliryhmä tai kun G on Abelin ryhmä. Todistetaan sitten hyödyllinen tulos, jonka avulla voidaan määritellä tekijäryhmä $N_G(H)/H$, kun $H \leqslant G$.

Lause 5.45. *Olkoon G ryhmä ja H sen aliryhmä. Tällöin H on ryhmän $N_G(H)$ normaali aliryhmä.*

Todistus. Olkoon $h \in H$. Selvästi $H = hHh^{-1}$, joten $H \subseteq N_G(H)$. Koska oletuksen ja lauseen 5.44 nojalla H ja $N_G(H)$ ovat ryhmän G aliryhmiä, ja $H \subseteq N_G(H)$, niin triviaalisti H on aliryhmän $N_G(H)$ aliryhmä (tällöinhän $H \subseteq N_G(H) \subseteq G$, joten väite seuraa suoraan aliryhmän määritelmästä). Määritelmän 5.42 mukaan $aHa^{-1} = H$ aina, kun $a \in N_G(H)$. Täten lauseen 3.33 nojalla H on ryhmän $N_G(H)$ normaali aliryhmä. □

Laajennettaan nyt ryhmän G alkion keskittäjän käsite koskemaan ryhmän G epätyhjän osajoukon keskittäjää.

Määritelmä 5.46. Olkoon U ryhmän G epätyhjä osajoukko. Tällöin joukkoa

$$C_G(U) := \{g \in G \mid ug = gu \text{ kaikilla } u \in U\}$$

kutsutaan joukon U *keskittäjäksi* ryhmässä G.

Ryhmän G epätyhjän joukon U keskittäjä koostuu siis niistä ryhmän G alkioista, jotka ovat vaihdannaisia joukon U alkioiden kanssa. Joukon U normalisoija sisältää taas ne ryhmän G alkiot, joilla niiden määräämät joukon U konjugaatit vastaavat tätä joukkoa.

Merkintä 5.47. Ryhmän G epätyhjän osajoukon U normalisoijan ja keskittäjän tyyppillisten merkintöjen $N_G(U)$ ja $C_G(U)$ sijaan käytetään jatkossa lyhyempiä merkintöjä $N(U)$ ja $C(U)$, kun sekaannuksen varaa ei ole ja näitä joukkoja tarkastellaan erityisesti ryhmän G osajoukkoina. Vastaavasti ryhmän G alkion x keskittäjälle käytetään merkintää $C(x)$.

Määritelmästä 5.46 nähdään, että $C(U) = \bigcap_{u\in U} C(u)$, joten $C(U) \leqslant G$ $(C(g) \leqslant G$ kaikilla $g \in G)$. Edelleen jos U on ryhmän G epätyhjä osajoukko, niin voidaan osoittaa, että $C(U) \trianglelefteq N(U)$ (ks. [18], s. 86, tehtävä 233). Lisäksi havaitaan, että $C_G(G) = Z(G)$. Kun $U = H$ on ryhmän G aliryhmä, voidaan todistaa hyödyllinen tulos, jonka mukaan aliryhmän H normalisoijan ja keskittäjän muodostama tekijäryhmä voidaan upottaa kaikkien aliryhmän H automorfismien ryhmään. Kyseistä tulosta kutsutaan joissakin lähteissä N/C-lauseeksi (ks. [19, s. 50]).

Lause 5.48. *Olkoon $H \leqslant G$. Tällöin $C(H) \trianglelefteq N(H)$ ja $N(H)/C(H)$ voidaan upottaa ryhmään* $\mathrm{Aut}(H)$.

Todistus (vrt. [18, s. 84]). Lauseen 5.45 nojalla $H \trianglelefteq N(H)$, joten on selvää, että $N(H)$ toimii aliryhmässä H konjugoimalla (ks. määritelmän 5.31 jälkeinen huomautus). Olkoon ρ tätä ryhmän $N(H)$ toimintaa vastaava permutaatioesitys. Tällöin kaikilla $g \in N(H)$

$$\rho(g)\colon H \to H, \rho(g)(h) = h^g.$$

Siis

$$\begin{aligned}\mathrm{Ker}(\rho) &= \{g \in N(H) \mid \rho(g) = \mathrm{id}_H\}\\ &= \{g \in N(H) \mid h^g = h \text{ kaikilla } h \in H\}\\ &= \{g \in N(H) \mid hg = gh \text{ kaikilla } h \in H\}\\ &= C(H). \quad (C(H) \subseteq N(H))\end{aligned}$$

Näin ollen lauseen 4.5 perusteella $C(H) \trianglelefteq N(H)$, ja ensimmäisen isomorfialauseen nojalla

$$\mathrm{Im}(\rho) \cong N(H)/C(H).$$

Olkoon $g \in N(H)$. Havaitaan, että tällöin permutaatio $\rho(g)$ on itse asiassa alkion g synnyttämä ryhmän G sisäisen automorfismin rajoittuma, joten se on automorfismi. Siis $\mathrm{Im}(\rho) \leqslant \mathrm{Aut}(H)$ ($\mathrm{Im}(\rho) \leqslant S_H$ ja $\mathrm{Im}(\rho) \subseteq \mathrm{Aut}(H)$). Täten lauseen 4.7 nojalla $N(H)/C(H)$ voidaan upottaa ryhmään $\mathrm{Aut}(H)$. □

Seuraus 5.49. *Olkoon G ryhmä. Tällöin*

$$G/Z(G) \cong \mathrm{Inn}(G).$$

Todistus (ks. [11, s. 161]). Asetetetaan $H = G$ lauseessa 5.48, ja edetään todistuksessa vastaavalla tavalla. □

6 Sylowin lauseet

Luvussa 6 todistetaan ensin Cauchyn[1] lause ja määritellään p-aliryhmät, jonka jälkeen Cauchyn lauseen ja ryhmätoimintojen avulla todistetaan Sylowin[2] lauseet. Keskiössä tässä luvussa on kolmen Sylowin lauseen todistus, ja niiden ympärillä oleva teoria. Tärkeitä käsitteitä tässä luvussa ovat p-ryhmä ja Sylowin p-aliryhmä. Ryhmätoimintojen merkitys tässä tutkielmassa korostuu sillä, että jokaisen Sylowin lauseen todistus pohjautuu tässä tutkielmassa ryhmätoimintoihin - täsmällisemmin siis lemmaan, joka nimetään Sylowin lemmaksi. Tämän luvun sisältö rakentuu kirjojen *Fundamentals of Abstract Algebra* [11, s. 190–206] ja *A Course on Group Theory* [18, s. 88–109] teorioiden varaan, joskin muitakin lähteitä on käytetty.

6.1 Cauchyn lause ja p-ryhmät

Tässä alaluvussa todistetaan tärkeä lause, joka antaa osittaisen käänteisen muodon Lagrangen lauseelle nimenomaan siinä tapauksessa, kun alkuluku p jakaa äärellisen ryhmän kertaluvun. Tätä lausetta kutsutaan Cauchyn lauseeksi. Todistetaan ensin seuraava lemma, jota voidaan kutsua Cauchyn lauseeksi Abelin ryhmille.

Lemma 6.1 (Cauchyn lause Abelin ryhmille)**.** *Oletetaan, että G on äärellinen Abelin ryhmä, jonka kertaluku on n. Oletetaan lisäksi, että alkuluku p jakaa luvun n. Tällöin ryhmä G sisältää alkion, jonka kertaluku on p.*

Todistus (vrt. [11, s. 196]). Todistetaan lemma induktiolla ryhmän G kertaluvun n suhteen. Jos $|G| = p$, missä p on alkuluku, niin seurauksen 3.26 nojalla G on syklinen ryhmä. Siis $G = \langle g \rangle$ jollakin $g \in G$. Edelleen lauseen 3.17 mukaan $\operatorname{ord}(g) = |\langle g \rangle| = |G| = p$ eli G sisältää alkion, jonka kertaluku on p. Erityisesti väite on siis tosi, kun $n = 2$.

Tehdään nyt induktio-oletus, että lemman väite on tosi kaikille ryhmille, jotka ovat kertalukua r, missä $2 \leq r < n$. Oletetaan, että $a \in G$, missä $a \neq e$, ja merkitään $m = \operatorname{ord}(a)$. Tarkastelemme erikseen tapaukset, joissa alkuluku p jakaa luvun m ja p ei jaa lukua m.

Oletetaan ensin, että $p \mid m$. Tällöin $m = pk$ jollakin $k \in \mathbb{Z}_+$. Tarkastellaan alkiota $a^k \in G$. Nyt $(a^k)^p = a^m = e$, joten $a^k \neq e$, sillä jos pätisi $a^k = e$, niin m ei olisikaan pienin positiivinen kokonaisluku, jolle $a^m = e$, vaan luku k olisi tätä pienempi (sillä $m = pk > k$). Tämä olisi ristiriita, sillä merkitsimme, että $m = \operatorname{ord}(a)$. Edelleen

[1] Augustin-Louis Cauchy (1789–1857) oli ranskalainen matematiikko, joka tuli tunnetuksi usealla matematiikan alalla, kuten kompleksianalyysissa, differentiaali- ja integraalilaskennassa, algebrassa ja geometriassa. Nykypäivän käsite funktion jatkuvuudesta on muun muassa Cauchyn käsialaa. [11, s. 98]

[2] Peter Ludvig Mejdell Sylow (1832–1918) oli norjalainen matemaatikko, joka on kehittänyt erityisesti äärellisten ryhmien teoriaa. Hän laajensi Cauchyn lauseena tunnetun tuloksen vuonna 1872 julkaisuksi, joka tunnetaan nykypäivänä Sylowin lauseina. [11, s. 222]

lauseen 1.38 kohdan (ii) nojalla

$$\operatorname{ord}(a^k) = \frac{m}{\operatorname{syt}(k,m)} = \frac{pk}{\operatorname{syt}(k,pk)} = \frac{pk}{k} = p.$$

Täten on olemassa ryhmän G alkio, tässä tapauksessa a^k, joka on kertalukua p. Lemman väite siis pätee.

Oletetaan sitten, että $p \nmid m$. Koska G on Abelin ryhmä, niin lauseen 3.34 nojalla ryhmän G syklinen aliryhmä $\langle a \rangle$ on normaali. Merkitään $H = \langle a \rangle$. Koska H on normaali, niin G/H on tekijäryhmä. Nyt tiedämme lauseen 3.17 perusteella, että $m = |\langle a \rangle| = |H|$. Täten Lagrangen lauseen nojalla $|G| = m\,(G : H)$. Nyt koska oletuksen nojalla $p \mid |G|$ ja $p \nmid m$, niin $p \mid (G : H)$. Edelleen $(G : H) = \frac{|G|}{|H|} = \frac{n}{m} < n$, jolloin induktio-oletuksen nojalla tekijäryhmällä G/H on olemassa sellainen alkio $bH \in G/H$, että $\operatorname{ord}(bH) = p$. Täten $b^p H = (bH)^p = eH$, joten lauseen 3.21 mukaan $e^{-1}b^p \in H$ eli $b^p \in H$. Nythän $H = \langle a \rangle$, jolloin $b^p = a^r$ jollakin $r \in \mathbb{Z}$. Tällöin $(b^m)^p = (b^p)^m = (a^r)^m = (a^m)^r = e^r = e$, sillä $m = \operatorname{ord}(a)$, joten seurauksen 1.39 perusteella pätee, että joko $b^m = e$ tai $\operatorname{ord}(b^m) = p$. Jos olisi $b^m = e$, niin $(bH)^m = b^m H = eH = H$. Nyt kuitenkin $\operatorname{ord}(bH) = p$, joten lauseen 1.38 kohdan (i) nojalla $p \mid m$, missä on ristiriita. Siis $b^m \neq e$ ja p on todellakin ryhmän G alkion b^m kertaluku, mikä siis todistaa väitteen. □

Seuraavaksi yleistetään lemma 6.1 koskemaan kaikkia äärellisiä ryhmiä höydyntämällä luokkayhtälöä. Todistetaan siis Cauchyn lause.

Lause 6.2 (Cauchyn lause)**.** *Oletetaan, että G on äärellinen ryhmä, jonka kertaluku on n, ja alkuluku p jakaa luvun n. Tällöin ryhmä G sisältää alkion, jonka kertaluku on p. Ryhmällä G on siis aliryhmä, jonka kertaluku on p.*

Todistus (vrt. [11, s. 196–197]). Todistetaan väite jälleen induktiolla ryhmän G kertaluvun n suhteen. Jos $n = 2$, niin G on Abelin ryhmä ja väite seuraa apulauseesta 6.1. Tehdään induktio-oletus, että väite on tosi kaikille kertalukua m oleville ryhmille, missä $2 \leq m < n$. Tarkastellaan ryhmän G luokkayhtälöä (ks. lause 5.33):

$$(*) \qquad |G| = |Z(G)| + \sum_{a \in A \setminus Z(G)} (G : C(a)),$$

missä A on joukko ryhmän G konjugaattiluokkien kaikista eri edustajista. Jos $G = Z(G)$, niin G on Abelin ryhmä, joten apulauseen 6.1 nojalla väite pätee.

Oletetaan nyt siis, että $G \neq Z(G)$. Silloin $A \setminus Z(G) \neq \emptyset$. Tarkastellaan alkiota $a \in A \setminus Z(G)$. Nyt $C(a) \neq G$, sillä $a \notin Z(G)$. Täten $C(a) < G$, jolloin $|G| > |C(a)|$ eli $|C(a)| < n$.

Jos nyt $p \mid |C(a)|$, niin induktio-oletuksen nojalla aliryhmällä $C(a)$, ja täten siis myös ryhmällä G, on olemassa alkio, jonka kertaluku on p.

Oletetaan sitten, että $p \nmid |C(a)|$ kaikilla $a \in A \setminus Z(G)$. Koska Lagrangen lauseen nojalla $|G| = (G : C(a))\,|C(a)|$ kaikilla $a \in A \setminus Z(G)$ ja $p \mid |G|$, niin $p \mid (G : C(a))$ kaikilla $a \in A \setminus Z(G)$. Näin ollen luokkayhtälössä $(*)$ p jakaa jokaisen summattavan termin ja $p \mid |G|$, jolloin $p \mid |Z(G)|$. Nythän $Z(G)$ on Abelin ryhmä, mistä lemman

6.1 nojalla saadaan, että on olemassa ryhmän G keskuksen alkio g, joka on tietysti myös ryhmän G alkio, jolle $\operatorname{ord}(g) = p$. Ryhmällä G on siis alkio, jonka kertaluku on p.

Osoitetaan vielä, että G sisältää nimenomaan aliryhmän, jonka kertaluku p. Nyt on siis olemassa $g \in G$, jolle $\operatorname{ord}(g) = p$. Edelleen lauseen 3.15 nojalla $H := \langle g \rangle$ on ryhmän G aliryhmä. Siis lauseen 3.17 perusteella $|H| = \operatorname{ord}(g) = p$. Tämä todistaa lauseen kokonaisuudessaan. □

Cauchyn lauseesta seuraa, että erityisesti äärellisten ja yksinkertaisten Abelin ryhmien kertaluku on alkuluku.

Seuraus 6.3. *Olkoon G epätriviaali ja äärellinen Abelin ryhmä. Tällöin pätee, että jos ryhmä G on yksinkertainen, niin ryhmän G kertaluku on alkuluku.*

Todistus. Oletetaan, että G on yksinkertainen. Nyt ryhmän G ainoat normaalit aliryhmät ovat $\{e\}$ ja G. Koska G on lisäksi Abelin ryhmä, niin lauseen 3.34 nojalla ryhmän G ainoat aliryhmät ovat $\{e\}$ ja G. Jos ryhmän G kertaluku olisi jokin positiivinen kokonaisluku m, joka ei ole alkuluku, niin Cauchyn lauseen perusteella ryhmällä G olisi aito epätriviaali aliryhmä, mikä on ristiriita. Näin ollen ryhmän G kertaluvun on oltava alkuluku. □

Seurauksen 6.3 perusteella voidaankin todeta, että äärellisille Abelin ryhmille pätee, että ryhmä on yksinkertainen, jos ja vain jos sen kertaluku on alkuluku.

Esimerkki 6.1 (vrt. [11], s. 178)**.** Olkoon G äärellinen ryhmä, jonka kertaluku on $2m$, missä luku m on pariton. Tällöin Cauchyn lauseen avulla voidaan osoittaa, että ryhmällä G on normaali aliryhmä, jonka kertaluku on m.

Tarkastellaan ryhmän G toimintaa $\cdot\colon G \times G \to G, g \cdot x = gx$ ja erityisesti tätä vastaavaa permutaatioesitystä $\rho\colon G \to S_G, \rho(g) = \rho_g$, missä $\rho_g\colon G \to G, \rho_g(x) = gx$. Merkitään $H = \operatorname{Im}(\rho)$. Nyt Cayleyn lauseen nojalla $\rho\colon G \cong H$ (Cayleyn lauseen merkinnöillä $F(G) = H$). Koska $|G|$ on parillinen, niin Cauchyn lauseen nojalla on olemassa sellainen $g \in G$, että $\operatorname{ord}(g) = 2$. Olkoon $a \in G$. Silloin

$$\rho_g(a) = ga \text{ ja } \rho_g(\rho_g(a)) = g^2 a = a,$$

joten ρ_g on erillisten vaihtojen tulo. Edelleen ryhmän G kertaluvun tekijänä on pariton luku, jolloin on oltava erityisesti pariton alkuluku p, joka jakaa ryhmän G kertaluvun. Tällöin Cauchyn lauseen perusteella on olemassa sellainen $h \in G$, että $\operatorname{ord}(h) = p$. Täten $\rho_h(a) = ha$ ja $\rho_h^p(a) = h^p a = a$, joten ρ_h on erillisten p-syklien tulo. Siis ρ_g on pariton ja ρ_h parillinen permutaatio. Määritellään sellainen kuvaus $f\colon H \to \{1, -1\}$, että

$$f(\alpha) = \epsilon(\alpha).$$

Näin määritelty kuvaus f on epimorfismi, sillä $\rho_g, \rho_h \in H$. Täten ensimmäisen isomorfialauseen nojalla $H/\operatorname{Ker}(f) \cong \{1, -1\}$. Siis

$$2 = |\{1, -1\}| = (H : \operatorname{Ker}(f)) = \frac{|H|}{\operatorname{Ker}(f)} = \frac{2m}{\operatorname{Ker}(f)},$$

joten $|\mathrm{Ker}(f)| = m$. Näin H sisältää normaalin aliryhmän, jonka kertaluku on m, joten koska $G \cong H$, niin myös G sisältää normaalin aliryhmän, jonka kertaluku on m (joka on tietysti $\rho^{-1}[\mathrm{Ker}(f)]$).

Osoitetaan nyt Cauchyn lausetta hyödyntämällä, että nimenomaan äärellisille Abelin ryhmille Lagrangen lause pätee kääntäen.

Lause 6.4. *Olkoon G äärellinen Abelin ryhmä, jonka kertaluku on n. Jos m on sellainen positiivinen kokonaisluku, että $m \mid n$, niin ryhmällä G on aliryhmä, jonka kertaluku on m.*

Todistus (vrt. [11, s. 197]). Oletetaan, että $m \in \mathbb{Z}_+$, jolle $m \mid n$. Jos $m = 1$, niin $\{e\}$ on ryhmän G aliryhmä, jonka kertaluku on m. Jos $n = 1$, niin $m = 1$ ja väite seuraa vastaavasti kuten edellä. Oletetaan nyt, että $m, n > 1$, ja osoitetaan väite induktiolla luvun n suhteen. Jos $n = 2$, niin $m = 1$ tai $m = 2$, jolloin molemmissa tapauksissa ryhmällä G on aliryhmä kertalukua m: jos $m = 1$, niin aliryhmä on $\{e\}$, ja jos $m = 2 = n$, niin aliryhmä on ryhmä G itse. Tehdään nyt induktio-oletus, että väite pätee kaikille Abelin ryhmille, jotka ovat kertalukua k, missä $2 \leq k < n$.

Olkoon p sellainen alkuluku, että $p \mid m$. Tällöin on olemassa sellainen $m_1 \in \mathbb{Z}_+$, että $m = pm_1$. Nyt koska $m \mid n$, niin myös $p \mid n$, jolloin Cauchyn lauseen 6.2 perusteella ryhmällä G on aliryhmä H, joka on kertalukua p. Koska G on Abelin ryhmä, niin lauseen 3.34 nojalla H on normaali aliryhmä ja täten G/H on tekijäryhmä.

Nyt Lagrangen lauseen nojalla

$$1 \leq |G/H| = \frac{|G|}{|H|} = \frac{n}{p} < n.$$

Koska $m \mid n$, niin $n = mm_2$ jollakin $m_2 \in \mathbb{Z}_+$. Täten

$$|G/H| = \frac{n}{p} = \frac{mm_2}{p} = \frac{pm_1m_2}{p} = m_1m_2,$$

joten $m_1 \mid |G/H|$. Tällöin induktio-oletuksesta seuraa, että tekijäryhmällä G/H on aliryhmä H', jolle $|H'| = m_1$. Erityisesti nyt toisen isomorfialauseen nojalla aliryhmä H' on muotoa K/H, missä K on ryhmän G aliryhmä. Täten Lagrangen lauseen nojalla pätee, että

$$|K| = (K : H)\,|H| = m_1p = m.$$

Siis K on ryhmän G aliryhmä, jonka kertaluku on m, mikä todistaa väitteen. □

Lukijan on tässä kohtaa hyvä huomata, että lause 6.4 ei kuitenkaan päde kaikille äärellisille ryhmille. Tästä voidaan mainita esimerkkinä ryhmän S_4 alternoiva aliryhmä A_4. Luku 6 nimittäin jakaa aliryhmän A_4 kertaluvun ($|A_4| = 4!/2 = 12$), mutta aliryhmällä A_4 ei ole aliryhmää, jonka kertaluku on 6 (ks. [11], tehtävä 19, s. 138).

Seuraavaksi määritellään p-ryhmän ja p-aliryhmän käsitteet.

Määritelmä 6.5. Olkoon p alkuluku. Ryhmän G sanotaan olevan *p-ryhmä*, jos ryhmän G jokaisen alkion kertaluku, neutraalialkiota lukuun ottamatta, on alkuluvun p potenssi eli muotoa p^n, missä $n \in \mathbb{Z}_+$. Ryhmän G aliryhmää H kutsutaan *p-aliryhmäksi*, jos H on p-ryhmä. Myös ryhmän G triviaali aliryhmä $\{e\}$ määritellään p-aliryhmäksi.

Määritelmässä 6.5 on mielekästä asettaa triviaali aliryhmä $\{e\}$ ryhmän G p-aliryhmäksi, koska $\operatorname{ord}(e) = 1 = p^0$. Seuraava lause antaa välttämättömän ja riittävän ehdon sille, että äärellinen ryhmä on p-ryhmä.

Lause 6.6. *Olkoon G epätriviaali ryhmä. Tällöin G on äärellinen p-ryhmä, jos ja vain jos $|G| = p^n$ jollakin $n \in \mathbb{Z}_+$.*

Todistus (vrt. [11, s. 198]). Olkoon $|G| = p^n$, missä $n \in \mathbb{Z}_+$. Olkoon $g \in G$. Nyt seuraus 3.25 sanoo, että äärellisen ryhmän jokaisen alkion kertaluku jakaa ryhmän kertaluvun, jolloin

$$p^n = |G| = k \cdot \operatorname{ord}(g), \text{ jollakin } k \in \mathbb{Z}_+.$$

Tällöin $\operatorname{ord}(g) = p^m$, missä $0 \leq m \leq n$ (sillä alkuluvun voi jakaa vain alkuluku itse tai luku 1), joten G on äärellinen p-ryhmä.

Oletetaan sitten toiseen suuntaan, että G on äärellinen p-ryhmä. Tehdään vastaoletus, että on olemassa jokin toinen alkuluku $q \neq p$ siten, että $q \mid |G|$. Tällöin Cauchyn lauseen nojalla ryhmällä G on olemassa alkio, jonka kertaluku on q, missä on ristiriita, sillä G on p-ryhmä. Täten $|G| = p^n$ jollakin $n \in \mathbb{Z}_+$. □

Ryhmän p-aliryhmän olemassaolo saadaan suoraan Cauchyn lauseesta yhdessä lauseen 6.6 kanssa. Tämä olemassaolo on toki kiinnostavaa vain, kun tarkastellaan epätriviaalien aliryhmien olemassaoloa. Lauseesta 6.6 seuraa suoraan, että kaikkien äärellisen ryhmän G p-aliryhmien konjugaatit ovat myös p-aliryhmiä.

Seuraus 6.7. *Olkoon G äärellinen ryhmä ja p alkuluku. Tällöin ryhmällä G on olemassa p-aliryhmä. Erityisesti, jos ryhmän G kertaluku on jaollinen alkuluvulla p, niin ryhmällä G on olemassa epätriviaali p-aliryhmä. Jos lisäksi P on ryhmän G p-aliryhmä, niin kaikki aliryhmän P konjugaatit ovat ryhmän G p-aliryhmiä.*

Todistus (vrt. [11, s. 203]). Voidaan olettaa, että G on epätriviaali. Jos p ei jaa ryhmän G kertalukua, niin triviaali aliryhmä $\{e\}$ on p-aliryhmä. Jos taas p jakaa ryhmän G kertaluvun, niin Cauchyn lauseen ja lauseen 6.6 nojalla ryhmällä G on olemassa epätriviaali p-aliryhmä.

Olkoon P ryhmän G p-aliryhmä. Jos p ei jaa ryhmän G kertalukua, niin P on triviaali aliryhmä. Oletetaan siis, että p jakaa ryhmän G kertaluvun. Olkoon $g \in G$. Lauseen 6.6 nojalla aliryhmän P kertaluku on alkuluvun p potenssi. Koska aliryhmät P^g ja P ovat yhtämahtavia eli niiden kertaluvut ovat samat lauseen 4.10 perusteella, niin myös P^g on p-ryhmä. □

Osoitetaan nyt luokkayhtälön perusteella, että epätriviaalin p-ryhmän keskus on epätriviaali.

Lause 6.8. *Olkoon G äärellinen ja epätriviaali p-ryhmä. Tällöin ryhmän G keskus $Z(G)$ on epätriviaali.*

Todistus (vrt. [11, s. 198]). Olkoon $A \subseteq G$ kaikkien eri konjugaattiluokkien edustajien joukko. Tarkastellaan ryhmän G luokkayhtälöä:

$$|G| = |Z(G)| + \sum_{a \in A \setminus Z(G)} (G : C(a)).$$

Jos $G = Z(G)$, niin väite seuraa suoraan oletuksesta. Oletetaan, että $Z(G) \subset G$. Olkoon $a \in G \setminus Z(G)$. Silloin $C(a) < G$. Koska G on lisäksi p-ryhmä, niin Lagrangen lauseen perusteella $p \mid (G : C(a))$. Näin ollen p jakaa myös summan $\sum_{a \in A \setminus Z(G)} (G : C(a))$. Koska p jakoi myös ryhmän G kertaluvun, niin p jakaa kirjoitetun luokkayhtälön perusteella myös keskuksen $Z(G)$ kertaluvun. Siis $|Z(G)| > 1$. □

Lauseen 6.8 avulla voidaan osoittaa, että mikään sellainen ryhmä, jonka kertaluku on alkuluvun p potenssi, ei ole yksinkertainen. Lisäksi keskuksen epätriviaalisuudesta seuraa, että ryhmät, joiden kertaluku on alkuluvun neliö, ovat vaihdannaisia.

Seuraus 6.9. *Olkoon p alkuluku ja $n > 1$ jokin kokonaisluku. Tällöin ryhmä, jonka kertaluku on p^n, ei ole yksinkertainen.*

Todistus (vrt. [11, s. 211]). Olkoon G ryhmä, jonka kertaluku on p^n, jolloin G on p-ryhmä. Tarkastellaan ryhmän G keskusta $Z(G)$. Lauseen 6.8 perusteella tiedetään nyt, että $Z(G)$ on epätriviaali.

Jos $G = Z(G)$, niin G on Abelin ryhmä. Jos G olisi myös yksinkertainen, niin seurauksen 6.3 nojalla ryhmän G kertaluku on alkuluku, mikä on ristiriidassa sen kanssa, että $|G| = p^n$. Täten G ei ole yksinkertainen.

Jos taas $G \neq Z(G)$, niin keskus $Z(G)$ on ryhmän G epätriviaali normaali aliryhmä. Siis G ei ole yksinkertainen. □

Seuraus 6.10. *Olkoon G ryhmä, jonka kertaluku on p^2, missä p on alkuluku. Tällöin G on Abelin ryhmä.*

Todistus (ks. [11, s. 198]). Koska G on p-ryhmä, sen keskus on epätriviaali. Lagrangen lauseen perusteella $|Z(G)|$ jakaa luvun p^2. Täten $|Z(G)| = p$ tai p^2. Oletetaan, että $|Z(G)| = p$. Tällöin $Z(G) \neq G$, joten on olemassa sellainen $a \in G$, että $a \notin Z(G)$. Nyt $C(a) \leqslant G$ ja $a \in C(a)$. Koska $Z(G) \subset C(a)$ ja $|Z(G)| = p$, niin $|C(a)| = p^2$, jolloin itse asiassa $G = C(a)$. Mutta tästähän seuraa, että koko ryhmä G koostuu sellaisista alkioista, jotka ovat vaihdannaisia alkion a kanssa, jolloin $a \in Z(G)$, mikä on ristiriita. Näin ollen $Z(G) = p^2$, joten $G = Z(G)$. Ryhmä G on siis vaihdannainen. □

Cauchyn lauseen ja lauseen 6.8 avulla voidaan todistaa myös p-ryhmiä koskeva hyödyllinen tulos, jonka avulla voidaan sanoa, että kertaluvun p^n, missä n on positiivinen kokonaisluku, omaavilla ryhmillä on normaali aliryhmä kertaluvulla p^{n-1}.

Lause 6.11. *Olkoon G ryhmä, jonka kertaluku on p^n, missä p on alkuluku ja $n \in \mathbb{Z}_+$. Tällöin mikä tahansa ryhmän G aliryhmä, jonka kertaluku on p^{n-1}, on normaali.*

Todistus (vrt. [11, s. 199–200]). Todistetaan tämä väite induktiolla luvun n suhteen. Jos $n = 1$, niin $|G| = p$ ja $\{e\}$ on tietysti ryhmän G normaali aliryhmä. Oletetaan, että väite on tosi kaikille ryhmille, joiden kertaluku on p^m, missä $1 \leq m < n$. Olkoon H ryhmän G aliryhmä, jonka kertaluku on p^{n-1}. Tarkastellaan aliryhmän H normalisoijaa $N(H)$. Jos $H \neq N(H)$, niin $H < N(H)$, joten $|N(H)| > p^{n-1}$. Täten on oltava $|N(H)| = p^n$, jolloin $G = N(H)$. Näin ollen lauseen 5.45 perusteella $H \trianglelefteq G$.

Oletetaan sitten, että $H = N(H)$. Tällöin $H^g = H$ kaikilla $g \in Z(G)$, sillä keskuksen $Z(G)$ alkiot ovat vaihdannaisia kaikkien ryhmän G alkioiden kanssa. Siis $Z(G) \leqslant H$ ja lauseen 6.8 perusteella $Z(G) \neq \{e\}$. Täten Cauchyn lauseen nojalla keskuksella $Z(G)$ on aliryhmä K, jonka kertaluku on p. Aliryhmä K on siis erityisesti syklinen, eli on olemassa $a \in Z(G)$, jolle $\langle a \rangle = K$. Nyt siitä, että a kuuluu ryhmän G keskukseen ja virittää aliryhmän K, seuraa suoraan, että $K \leqslant Z(G)$. Täten on selvää, että $K \trianglelefteq G$. Tietysti pätee myös, että $K \trianglelefteq H$. Nyt Lagrangen lauseen perusteella $(H : K) = p^{n-2}$ ja $(G : K) = p^{n-1}$. Näin ollen induktio-oletuksesta seuraa, että $H/K \trianglelefteq G/K$, joten toisen isomorfialauseen perusteella $H \trianglelefteq G$. □

Esimerkki 6.2. Tarkastellaan ryhmää $(\mathbb{Z}_6, +)$, $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Määritetään ryhmän $(\mathbb{Z}_6, +)$ kaikki p-aliryhmät. Nyt

$$6 \cdot \overline{1} = \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{6} = \overline{0},\ 3 \cdot \overline{2} = \overline{6} = \overline{0},\ 2 \cdot \overline{3} = \overline{0},$$
$$3 \cdot \overline{4} = \overline{0} \text{ ja } 6 \cdot \overline{5} = \overline{0}.$$

Havaitaan täten, että $\operatorname{ord}(\overline{1}) = \operatorname{ord}(\overline{5}) = 6 = 2 \cdot 3$, $\operatorname{ord}(\overline{2}) = \operatorname{ord}(\overline{4}) = 3$ ja $\operatorname{ord}(\overline{3}) = 2$. Siis ryhmällä $\mathbb{Z}_6$ on kaksi p-aliryhmää: 2-aliryhmä $\{\overline{0}, \overline{3}\}$ ja 3-aliryhmä $\{\overline{0}, \overline{2}, \overline{4}\}$. Itse asiassa muita aliryhmiä, kuin triviaalit aliryhmät näiden kahden lisäksi, ryhmällä $\mathbb{Z}_6$ ei ole.

Tarkastellaan seuraavaksi ryhmää $(\mathbb{Z}_{20}, +)$. Äskeisessä tapauksessa määritettiin ryhmän kaikki p-aliryhmät pitkälti suoraan määritelmään 6.5 pohjautuen. Määritetään nyt ryhmän $\mathbb{Z}_{20}$ kaikki p-aliryhmät lauseen 6.6 avulla. Nyt $|\mathbb{Z}_{20}| = 20 = 2^2 \cdot 5$, joten Lagrangen lauseen mukaan ainoat mahdolliset ryhmän $\mathbb{Z}_{20}$ aliryhmien kertaluvut ovat 1, 2, 4, 5, 10 ja 20. Kertalukuja 1 ja 20 vastaavat tietysti triviaalit aliryhmät $\{\overline{0}\}$ ja $\mathbb{Z}_{20}$. Kertaluvun 2 ainoa aliryhmä on $\{\overline{0}, \overline{10}\}$, joka on lauseen 6.6 nojalla 2-aliryhmä. Toinen 2-aliryhmä on puolestaan kertaluvun $4 (= 2^2)$ aliryhmä $\{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$. Kertalukua 5 vastaava aliryhmä on taas $\{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}\}$, joka on 5-aliryhmä. Ryhmän $\mathbb{Z}_{20}$ ainoa aliryhmä, joka ei ole p-aliryhmä, on puolestaan $\{2\overline{n} \mid \overline{n} \in \mathbb{Z}_{20}\}$ eli kertalukua 10 vastaava aliryhmä. Muita aliryhmiä ryhmällä $\mathbb{Z}_{20}$ ei ole, joten ryhmällä $\mathbb{Z}_{20}$ on aiemmin mainitut kaksi kappaletta epätriviaaleja 2-aliryhmiä ja yksi epätriviaali 5-aliryhmä.

6.2 Sylowin lauseet

Sylowin lauseiden avulla voidaan ymmärtää äärellisten ryhmien rakenteita. Ne laajentavat Cauchyn lausetta ja auttavat äärellisten ryhmien yksinkertaisuuksien tarkastelussa. Esitetään ensin kolmesta Sylowin lauseesta ensimmäinen, jossa äärellisen ryhmän kertaluku on jaollinen alkuluvun p potenssilla. Osoitetaan, että silloin kyseisellä ryhmällä on aliryhmä, joka on itse asiassa epätriviaali p-aliryhmä. Ennen Sylowin ensimmäistä lausetta todistetaan kuitenkin seuraava tärkeä lemma, joka johdetaan ryhmätoiminnoista, erityisesti ryhmätoimintojen luokkayhtälöstä ja Cayleyn toiminnasta. Tätä lemmaa tullaan hyödyntämään jokaisen Sylowin lauseen todistuksessa. Kyseinen lemma nimetään tässä sen tärkeyden vuoksi Sylowin lemmaksi.

Lemma 6.12 (Sylowin lemma)**.** *Olkoon G äärellinen ryhmä.*

(i) *Oletetaan, että G on p-ryhmä, joka toimii äärellisessä joukossa X. Tällöin*

$$|\mathrm{Fix}_X(G)| \equiv |X| \pmod{p}.$$

(ii) *Olkoon H ryhmän G p-aliryhmä. Oletetaan, että p jakaa indeksin $(G : H)$. Tällöin p jakaa indeksin $(N(H) : H)$.*

Todistus (vrt. [18, s. 88–89] ja [11, s. 176–177]). (i). Merkitään $X_0 = \mathrm{Fix}_X(G)$. Olkoon A joukon X osajoukko, joka sisältää täsmälleen yhden alkion jokaiselta ryhmän G radalta O_x, $x \in X$. Nyt ryhmätoimintojen luokkayhtälön perusteella.

$$|X| = |X_0| + \sum_{a \in A \setminus X_0} (G : \mathrm{Stab}_G(a)).$$

Tiedetään, että $(G : \mathrm{Stab}_G(a)) = |O_a| = 1$ kaikilla $a \in X_0$. On myös selvää, että $(G : \mathrm{Stab}_G(a))$ jakaa ryhmän G kertaluvun kaikilla $a \in A \setminus X_0$. Koska G on lisäksi p-ryhmä, niin sen kertaluku on alkuluvun p potenssi. Näin ollen indeksin $(G : \mathrm{Stab}_G(a))$ tekijänä on alkuluku p kaikilla $a \in A \setminus X_0$. Siis

$$\sum_{a \in A \setminus X_0} (G : \mathrm{Stab}_G(a)) = pk,$$

missä k on jokin positiivinen kokonaisluku. Täten

$$|X| = |X_0| + pk, \text{ joten}$$

$$|\mathrm{Fix}_X(G)| \equiv |X| \pmod{p}.$$

(ii). Tarkastellaan Cayleyn toimintaa

$$\cdot : G \times X \to X, g \cdot (xH) = (gx)H,$$

missä $X = G/H$. Lauseen 5.38 perusteella tämän kuvauksen $\cdot$ rajoittuma $\cdot \restriction (H \times X)$ määrittää aliryhmän H toiminnan joukossa X. Nyt kohdan (i) nojalla

$$|\mathrm{Fix}_X(H)| \equiv (G : H) \pmod{p},$$

sillä H on p-ryhmä. Edelleen $xH \in \mathrm{Fix}_X(H)$, joss $h(xH) = xH$ kaikilla $h \in H$, joss $x^{-1}hx \in H$ kaikilla $h \in H$, joss $x^{-1}Hx \subseteq H$. Koska H on äärellinen ja $|x^{-1}Hx| = |H|$, niin $x^{-1}Hx \subseteq H$, joss $x^{-1}Hx = H$, joss $x \in N(H)$. Siis $xH \in \mathrm{Fix}_X(H)$, joss $x \in N(H)$, joten $|\mathrm{Fix}_X(H)| = (N(H) : H)$. Siis $(N(H) : H) \equiv (G : H) \pmod{p}$, ja koska oletuksen mukaan $p \mid (G : H)$, niin $p \mid (N(H) : H)$. □

Nyt voidaan todistaa Sylowin ensimmäinen lause, jonka todistus perustuu tässä induktioon ja Sylowin lemmaan.

Lause 6.13 (Sylowin ensimmäinen lause)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, $r, m \in \mathbb{Z}_+$ ja p ja m ovat keskenään jaottomia. Tällöin ryhmällä G on aliryhmä, jonka kertaluku on p^k, aina, kun $0 \leq k \leq r$.*

Todistus (vrt. [11, s. 202]). Todistetaan lause käyttäen induktiota luvun k suhteen. Tarkastellaan ensin muutamia induktion perusaskeleita. Havaitaan aluksi, että ryhmällä G on aina triviaali aliryhmä $\{e\}$, joten lause on tosi, kun $k = 0$. Oletetaan sitten, että $k = 1$. Nyt $p \mid |G|$, joten Cauchyn lauseen nojalla ryhmällä G on aliryhmä, jonka kertaluku on $p = p^1 = p^k$. Lause on täten tosi, kun $k = 1$. Oletetaan, että $r \geq 1$. Tehdään induktio-oletus, että ryhmällä G on aliryhmä H, jonka kertaluku on p^k, missä $1 \leq k < r$. Tällöin H on ryhmän G aito p-aliryhmä (sillä $|G| > |H|$). Lauseen 5.44 nojalla $N(H)$ on ryhmän G aliryhmä, ja Lagrangen lauseen ja induktio-oletuksen perusteella $(G : H) = \frac{|G|}{|H|} = \frac{mp^r}{p^k}$, missä $1 \leq k < r$, joten $p \mid (G : H)$. Siis Sylowin lemman kohdan (ii) nojalla $p \mid (N(H) : H)$. Lauseen 5.45 nojalla H on aliryhmän $N(H)$ normaali aliryhmä, joten tekijäryhmä $N(H)/H$ voidaan määritellä. Nythän siis $p \mid |N(H)/H|$, joten tekijäryhmällä $N(H)/H$ on Cauchyn lauseen mukaan aliryhmä, jonka kertaluku on p. Tämä aliryhmä on toisen isomorfialauseen nojalla muotoa K/H, missä K on ryhmän $N(H)$ aliryhmä. Nyt Lagrangen lauseen perusteella

$$|K| = (K : H)\,|H| = pp^k = p^{k+1}.$$

Siis aliryhmällä $N(H)$, ja täten myös ryhmällä G, on aliryhmä, jonka kertaluku on p^{k+1}, aina, kun $1 \leq k < r$. Täten induktioperiaatteesta seuraa, että ryhmällä G on aliryhmä, jonka kertaluku on p^k, aina, kun $1 \leq k \leq r$, mikä riittää osoittamaan väitteen. □

Toinen tapa todistaa Sylowin ensimmäinen lause olisi käyttää induktiota ryhmän G kertaluvun suhteen, jolloin tarvitaan ryhmien luokkayhtälöä 5.33. Tässä todistuksessa ei tarvita Sylowin lemmaa, mutta itse lauseen todistus on jonkin verran pidempi ja hankalampi kuin aiemmin esitetty (vrt. [11, s. 201]). Molemmat todistukset pohjautuvat kuitenkin Cauchyn lauseeseen. Sylowin ensimmäinen voidaan tosin todistaa myös ilman Cauchyn lausetta (ks. esim. [18, s. 91–92]; tässä todistetaan ns. lievempi muoto: ryhmällä G on aliryhmä, jonka kertaluku on p^r).

Sylowin ensimmäisestä lauseesta seuraa välittömästi äärellisen ryhmän p-aliryhmän olemassaolo kaikilla mahdollisilla kertaluvuilla. Sylowin ensimmäisestä lauseesta seuraa myös lähes suoraan, että jos äärellisen ryhmän kertaluku on jaollinen alkuluvun potenssilla, niin sillä on saman alkuluvun potenssin kertaluvun omaava aliryhmä.

Seuraus 6.14. *Olkoon G äärellinen ryhmä, p alkuluku ja $n \in \mathbb{Z}_+$. Jos p^n jakaa ryhmän G kertaluvun, niin ryhmällä G on aliryhmä, jonka kertaluku on p^n.*

Todistus. Oletetaan, että $p^n \mid |G|$. Tällöin ryhmän G kertaluku voidaan kirjoittaa seuraavasti: $|G| = p^r m$, missä $m \in \mathbb{Z}_+$, $0 \leq n \leq r$ ja $\text{syt}(p, m) = 1$. Väite seuraa nyt Sylowin ensimmäisestä lauseesta. □

Otetaan nyt käyttöön tärkeä määritelmä Sylowin p-aliryhmistä.

Määritelmä 6.15. Olkoon G äärellinen ryhmä ja p alkuluku. Ryhmän G aliryhmää P kutsutaan *Sylowin p-aliryhmäksi*, jos P on ryhmän G p-aliryhmä ja se ei sisälly aidosti mihinkään muuhun ryhmän G p-aliryhmään, eli toisin sanoen: jos P on ryhmän G maksimaalinen p-aliryhmä. Puhuttaessa suoraan Sylowin p-aliryhmästä oletetaan aina, että p on alkuluku.

Merkintä 6.16. Symbolilla $\text{Syl}_p(G)$ merkitään perhettä, joka koostuu ryhmän G kaikista Sylowin p-aliryhmistä. $n_p(G)$ on taas kaikkien ryhmän G Sylowin p-aliryhmien lukumäärä eli $|\text{Syl}_p(G)|$. Kun asiayhteydestä on selvää, mitä ryhmää tarkoitetaan, merkitään tätä lukumäärää lyhemmin lukuna n_p.

Selvennettään vielä hieman Sylowin p-aliryhmän käsitettä määritelmän 1.3 avulla. Olkoon $\mathcal{P}$ perhe, joka koostuu kaikista ryhmän G p-aliryhmistä, missä p on alkuluku. Tällöin ryhmän G maksimaalisella p-aliryhmällä eli Sylowin p-aliryhmällä tarkoitetaan sellaista perheen $\mathcal{P}$ alkiota P, joka toteuttaa kaikille $H \in \mathcal{P}$ seuraavan ehdon: Jos $P \subseteq H$, niin $P = H$.

Käyttökelpoinen tapa todeta, milloin jokin ryhmä on Sylowin p-aliryhmä, perustuu siihen, milloin aliryhmän kertaluku vastaa ryhmän kertaluvun alkuluvun p suurinta mahdollista potenssia. Useissa lähteissä lausetta 6.17 käytetäänkin suoraan Sylowin p-aliryhmän määritelmänä (ks. esim. [2], [12] ja [18]).

Lause 6.17. *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, $r, m \in \mathbb{Z}_+$ ja $\text{syt}(p, m) = 1$, ja olkoon H ryhmän G aliryhmä. Tällöin H on ryhmän G Sylowin p-aliryhmä, jos ja vain jos $|H| = p^r$.*

Todistus (vrt. [11, s. 203]). Oletetaan ensin, että $H \in \text{Syl}_p(G)$. Tällöin H on ryhmän G p-aliryhmä, joten $|H| = p^k$ jollakin $k \in \mathbb{Z}_+$. Oletetaan, että $k \neq r$. Nyt $p \mid (G : H)$, joten Sylowin lemman kohdan (ii) nojalla $p \mid (N(H) : H)$. Täten tekijäryhmällä $N(H)/H$ on aliryhmä muotoa K/H, jonka kertaluku on p, missä $H \leqslant K \leqslant N(H)$, Cauchyn lauseen ja toisen isomorfialauseen nojalla. Siis $|K| = |H|\,(K : H) = p^{k+1}$. Koska $H \trianglelefteq N(H)$, $K \subseteq N(H)$ ja $|H| < |K|$, niin $H \triangleleft K$. Mutta tällöinhän H ei ole maksimaalinen p-aliryhmä, mikä on ristiriita. Täten $k = r$.

Oletetaan sitten, että $|H| = p^r$. Olkoon P ryhmän G p-aliryhmä, jolle $H \subseteq P$. Jos olisi $H \subset P$, niin $p^r = |H| < |P|$, mikä on ristiriita ryhmän G kertaluvun vuoksi. Siis $H = P$, joten $H \in \text{Syl}_p(G)$. □

Lauseesta 6.17 seuraa yhdessä Sylowin ensimmäisen lauseen kanssa, aivan kuten p-aliryhmien kohdalla seurauksessa 6.7, äärellisen ryhmän Sylowin p-aliryhmien olemassaolo sekä se, että mikä tahansa ryhmä, joka on Sylowin p-aliryhmän konjugaatti, on myös Sylowin p-aliryhmä.

Seuraus 6.18. *Olkoon G äärellinen ryhmä ja p alkuluku. Tällöin ryhmällä G on olemassa Sylowin p-aliryhmä. Jos lisäksi P on ryhmän G Sylowin p-aliryhmä, niin kaikki aliryhmän P konjugaatit ovat ryhmän G Sylowin p-aliryhmiä.*

Todistus (vrt. [11, s. 202–203]). Jos p ei jaa ryhmän G kertalukua, niin $\{e\}$ on haluttu Sylowin p-aliryhmä. Jos p jakaa kertaluvun $|G|$, niin olemassaolo seuraa suoraan Sylowin ensimmäisestä lauseesta ja lauseesta 6.17.

Olkoon $P \in \mathrm{Syl}_p(G)$, ja $g \in G$. Voidaan olettaa, että $|G| = p^r m$, missä $r, m \in \mathbb{Z}_+$ ja $\mathrm{syt}(p, m) = 1$. Tällöin $|P| = p^r$ lauseen 6.17 nojalla. Edelleen $|P^g| = |P| = p^r$ lauseen 4.10 perusteella. Siis $P^g \in \mathrm{Syl}_p(G)$. □

Tutkitaan seuraavassa esimerkissä alkuluvulla p jaollisen ryhmän G aliryhmää $P \cap K$ ja tekijäryhmän G/K aliryhmää PK/K, missä $P \in \mathrm{Syl}_p(G)$ ja $K \trianglelefteq G$. Osoitetaan näiden ryhmien olevan Sylowin p-aliryhmiä.

Esimerkki 6.3 (vrt. [13], s. 364)**.** Tarkastellaan äärellistä ryhmää G, jonka kertaluvun jakaa alkuluku p. Olkoon K ryhmän G normaali aliryhmä. Olkoon P lisäksi ryhmän G Sylowin p-aliryhmä. Osoitetaan, että tällöin $P \cap K$ on aliryhmän K Sylowin p-aliryhmä. Todistetaan myös, että tästä seuraa, että PK/K on tekijäryhmän G/K Sylowin p-aliryhmä.

Ryhmän G kertaluku on muotoa $|G| = p^r m$, missä $r, m \in \mathbb{Z}_+$ ja $\mathrm{syt}(p, m) = 1$. Ensinnäkin lauseiden 3.36 ja 3.37 perusteella $K \trianglelefteq PK \leqslant G$, jolloin PK/K on tekijäryhmä, ja erityisesti tekijäryhmän G/K aliryhmä. Koska $P \in \mathrm{Syl}_p(G)$, niin $|P| = p^r$. Nyt $P \cap K \leqslant K$, jolloin Lagrangen lauseen perusteella $|P \cap K| = p^i$, missä $i \leq r$. Aliryhmän K kertaluku on muotoa $|K| = p^s t$, missä $s, t \in \mathbb{Z}_+$, $s \leq r$ ja $\mathrm{syt}(p, t) = 1$. Oletetaan, että $s > i$. Nyt tulokaavan (lause 3.27) perusteella

$$|PK| = \frac{|P|\,|K|}{|P \cap K|} = \frac{p^r p^s t}{p^i} = p^{r+s-i} t,$$

missä $r+s-i > r$, jolloin $|PK| \nmid |G|$, mikä on ristiriita. Siis $s = i$, joten $|P \cap K| = p^s$. Näin ollen $P \cap K \in \mathrm{Syl}_p(K)$.

Edelleen Lagrangen lauseen ja tulokaavan nojalla

$$|G/K| = \frac{|G|}{|K|} = \frac{p^r m}{p^s t} = p^{r-s} \frac{m}{t}$$

ja

$$|PK/K| = \frac{|PK|}{|K|} = \frac{|P|\,|K|}{|K|\,|P \cap K|} = \frac{|P|}{|P \cap K|} = \frac{p^r}{p^s} = p^{r-s}.$$

Siis $PK/K \in \mathrm{Syl}_p(G/K)$.

Nyt voidaan todistaa Sylowin toinen lause, jonka mukaan ryhmän G Sylowin p-aliryhmät muodostavat täsmälleen yhden konjugaattiluokan.

Lause 6.19 (Sylowin toinen lause)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, $r, m \in \mathbb{Z}_+$ ja $\mathrm{syt}(p, m) = 1$. Tällöin ryhmän G Sylowin p-aliryhmät ovat konjugaatteja keskenään. Erityisesti $n_p = (G : N(P))$ kaikilla $P \in \mathrm{Syl}_p(G)$.*

Todistus (vrt. [11, s. 205] ja [18, s. 92]). Olkoot $H, K \in \mathrm{Syl}_p(G)$. Tarkastellaan jälleen seuraavaa Cayleyn toimintaa:

$$\cdot \colon G \times X \to X, g \cdot (xH) = (gx)H,$$

missä $X = G/H$. Edelleen K toimii tämän toiminnan rajoittumana joukossa X ja K on p-ryhmä, jolloin Sylowin lemman kohdan (i) nojalla

$$|\mathrm{Fix}_X(K)| \equiv (G : H) \pmod{p}.$$

Nyt $p \nmid (G : H)$, sillä $(G : H) = \frac{|G|}{|H|} = \frac{p^r m}{p^r} = m$ ja $\mathrm{syt}(p, m) = 1$, jolloin $|\mathrm{Fix}_X(K)| \neq 0$, joten voidaan valita $xH \in \mathrm{Fix}_X(K)$. Olkoon $k \in K$. Silloin $k(xH) = xH$, joten $x^{-1}kx \in H$, mistä seuraa $x^{-1}Kx \subseteq H$. Koska $|x^{-1}Kx| = |K| = |H|$, niin $H = x^{-1}Kx$. Näin ollen H ja K ovat konjugaatteja keskenään.

Koska on osoitettu, että ryhmän G Sylowin p-aliryhmät muodostavat yhden konjugaattiluokan, niin lauseen 1.13 perusteella $C_l(P) = \mathrm{Syl}_p(G)$ kaikilla $P \in \mathrm{Syl}_p(G)$. Edelleen siis lauseen 5.43 nojalla kaikilla $P \in \mathrm{Syl}_p(G)$ pätee $n_p = |\mathrm{Syl}_p(G)| = |C_l(P)| = (G : N(P))$. □

Sylowin toisesta lauseesta seuraa lähes suoraan ehto äärellisen ryhmän G Sylowin p-aliryhmän normaaliudelle. Kyseinen ehto on käytännöllinen yhdessä Sylowin kolmannen lauseen kanssa, kun halutaan selvittää, mitkä ryhmän G Sylowin p-aliryhmistä ovat normaaleja. Sen mukaan normaali Sylowin p-aliryhmä on ryhmän G ainoa Sylowin p-aliryhmä. Seurauksena on myös tulos, jonka mukaan kaikkien ryhmän G Sylowin p-aliryhmien lukumäärä ei ole jaollinen alkuluvulla p.

Seuraus 6.20. *Olkoon H äärellisen ryhmän G Sylowin p-aliryhmä. Tällöin H on ryhmän G normaali aliryhmä, jos ja vain jos $n_p = 1$.*

Todistus. Nyt Sylowin toisen lauseen perusteella $(G : N(H)) = n_p$. Siis $H \trianglelefteq G$, jos ja vain jos $N(H) = G$, jos ja vain jos $(G : N(H)) = 1$, jos ja vain jos $n_p = 1$. □

Seuraus 6.21. *Olkoon G äärellinen ryhmä ja p alkuluku. Tällöin alkuluku p ei jaa lukua n_p.*

Todistus (vrt. [12, s. 3–4]). Jos p ei jaa ryhmän G kertalukua, väite on selvä, sillä $n_p = 1$. Oletetaan, että $p \mid |G|$. Olkoon $|G| = p^r m$, missä r ja m ovat positiivisia kokonaislukuja ja p ja m ovat keskenään jaottomia. Olkoon $P \in \mathrm{Syl}_p(G)$. Merkitään $k = |N(P)|$. Sylowin toisen lauseen perusteella $n_p = (G : N(P))$, joten Lagrangen lauseen perusteella

$$n_p = (G : N(P)) = \frac{p^r m}{k}.$$

Nyt $P \leqslant N(P) \leqslant G$, jolloin $p^r \mid k$ ja $k \mid p^r m$, mistä seuraa, että luvulla n_p ei ole tekijänä alkuluvun p potenssia. Siis $p \nmid n_p$. □

Ennen viimeistä eli kolmatta Sylowin lausetta todistetaan kyseisessä lauseessa tarvittava lemma.

Lemma 6.22. *Olkoon H äärellisen ryhmän G Sylowin p-aliryhmä, ja $H \leqslant K \leqslant G$. Tällöin*

(i) *H on aliryhmän K Sylowin p-aliryhmä, ja*

(ii) *H on normalisoijan $N(H)$ yksikäsitteinen Sylowin p-aliryhmä.*

Todistus. (i). Vrt [18], s. 93, tehtävä 252. Olkoon $|G| = p^r m$, missä r ja m ovat positiivisia kokonaislukuja ja p ja m ovat keskenään jaottomia. Koska $H \in \mathrm{Syl}_p(G)$, niin $|H| = p^r$. Nyt Lagrangen lauseen nojalla aliryhmän K kertaluku jakaa ryhmän G kertaluvun, jolloin aliryhmän K kertaluku on muotoa $|K| = p^s t$, missä $t \in \mathbb{Z}_+$, $s \leq r$ ja $\mathrm{syt}(p, t) = 1$. Oletetaan, että $s < r$. Mutta silloinhan $|H| \nmid |K|$, mikä on ristiriita. Siis $r = s$, joten $H \in \mathrm{Syl}_p(K)$.

(ii). Ks. [18, s. 93]. Kohdasta (i) seuraa erityisesti, että H on normalisoijan $N(H)$ Sylowin p-aliryhmä. Olkoon $K \in \mathrm{Syl}_p(N(H))$. Tällöin Sylowin toisen lauseen perusteella on olemassa sellainen $g \in N(H)$, että $K = H^g$. Toisaalta, koska $g \in N(H)$, niin $H^g = H$. Siis $H = K$, mistä seuraa aliryhmän H yksikäsitteisyys. □

Nyt voidaan todistaa Sylowin kolmas lause, joka antaa käyttöön erittäin hyödyllisen kongruenssin, minkä avulla pystytään tehokkaasti rajaamaan mahdollisia Sylowin p-aliryhmien lukumääriä äärellisessä ryhmässä G.

Lause 6.23 (Sylowin kolmas lause)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, $r, m \in \mathbb{Z}_+$ ja $\mathrm{syt}(p, m) = 1$. Tällöin n_p jakaa luvun m, ja*

$$n_p \equiv 1 \pmod{p}.$$

Todistus (ks. [18, s. 93]). Olkoon $H \in \mathrm{Syl}_p(G)$. Nyt Sylowin toisesta lauseesta seuraa, että

$$m = (G : H) = (G : N(H))(N(H) : H) = n_p(N(H) : H),$$

joten $n_p \mid m$. Toimikoon ryhmä G perheessä $\mathrm{Syl}_p(G)$ konjugoimalla. Tällöin myös H toimii perheessä $\mathrm{Syl}_p(G)$ tämän ryhmän toiminnan rajoittumana, joten Sylowin lemman kohdan (i) perusteella

$$|\mathrm{Fix}_{\mathrm{Syl}_p(G)}(H)| \equiv n_p \pmod{p}.$$

Olkoon $K \in \mathrm{Syl}_p(G)$. Tällöin $K \in \mathrm{Fix}_{\mathrm{Syl}_p(G)}(H)$, joss $K^h = K$ kaikilla $h \in H$, joss $H \leqslant N(K)$. Nyt kuitenkin lemman 6.22 nojalla $H \leqslant N(K)$, joss $H = K$. Siis $\mathrm{Fix}_{\mathrm{Syl}_p(G)}(H) = \{H\}$, joten $|\mathrm{Fix}_{\mathrm{Syl}_p(G)}(H)| = 1$. Näin ollen $n_p \equiv 1 \pmod{p}$. □

Käsitellään nyt esimerkki, jossa osoitetaan Sylowin toisen lauseen avulla tulos, jota kutsutaan usein Frattinin argumentiksi. Frattinin argumentista voidaan mukavasti osoittaa myös tiettyjä seurauksia. Yksi mielenkiintoinen seuraus osoittaa erikoistapauksen tilanteelle, jossa toteutuu normaaliuden transitiivisuus: Ryhmän G normaalin aliryhmän Sylowin normaali p-aliryhmä on myös ryhmän G normaali aliryhmä. Yleisestihän siis siitä, että $K \trianglelefteq H$ ja $H \trianglelefteq G$ ei välttämättä seuraa, että $K \trianglelefteq G$. Tähän vastaesimerkiksi kelpaavat ryhmät $G = S_3 \times S_3$, $H = A_3 \times A_3$ ja $K = \{((1), (1)), ((1\ 2\ 3), (1\ 2\ 3)), ((1\ 3\ 2), (1\ 3\ 2))\}$ (ks. [18, s. 39–40]).

Esimerkki 6.4 (vrt. [2, s. 13] ja [18, s. 96])**.** Olkoon K ryhmän G äärellinen ja normaali aliryhmä. Olkoon P aliryhmän K Sylowin p-aliryhmä. Frattinin argumentti sanoo, että tällöin $G = KN(P)$. Todistetaan seuraavassa tämä tulos.

Olkoon $g \in G$. Nyt $K \trianglelefteq G$, joten $K^g = K$. Koska lisäksi $P \leqslant K$, niin $P^g \leqslant K^g$. Siis $P^g \leqslant K$. Lisäksi lauseen 4.10 nojalla $|P^g| = |P|$, joten $P^g \in \mathrm{Syl}_p(K)$. Nyt Sylowin toisen lauseen perusteella P^g ja P ovat konjugaatteja keskenään, jolloin siis on olemassa sellainen $k \in K$, että

$$P^g = P^k, \text{ eli}$$
$$k^{-1}gP(k^{-1}g)^{-1} = P.$$

Täten $k^{-1}g \in N(P)$, ja siis $g \in KN(P)$. Näin ollen Frattinin argumentti on todistettu.

Frattinin argumentista seuraa edelleen, että jos P on lisäksi aliryhmän K normaali aliryhmä, niin se on myös ryhmän G normaali aliryhmä. Jos nimittäin $P \trianglelefteq K$, niin $K \subseteq N(P)$. Näin ollen $KN(P) = N(P)$, joten Frattinin argumentin perusteella $G = N(P)$. Täten $P \trianglelefteq G$.

Olkoon $P' \in \mathrm{Syl}_p(G)$ ja H sellainen ryhmän G aliryhmä, joka sisältää normalisoijan $N(P')$. Frattinin argumentista voidaan osoittaa tällöin, että $N(H) = H$. Nyt $P' \trianglelefteq N(P')$, joten $P' \leqslant H \leqslant N(H)$. Täten lemman 6.22 kohdan (i) perusteella $P' \in \mathrm{Syl}_p(N(H))$. Tällöin Frattinin argumentin nojalla

$$N(H) = HN_{N(H)}(P').$$

Edelleen $N_{N(H)}(P') \leqslant N(P') \leqslant H$, joten $N(H) = H$.

Conrad ja Mann (ks. [2] ja [12]) pitävät yhtenä osana Sylowin lauseita tulosta, jonka mukaan mikä tahansa ryhmän G p-aliryhmä sisältyy johonkin ryhmän G Sylowin p-aliryhmistä. Kyseinen väite ei seuraa kuitenkaan suoraan aiemmin todistetuista Sylowin kolmesta lauseesta. Pyritään seuraavassa osoittamaan tämä tulos. Aloitetaan lemmalla.

Lemma 6.24. *Olkoon P äärellisen ryhmän G Sylowin p-aliryhmä, ja olkoon Q ryhmän G p-aliryhmä. Tällöin $Q \cap P = Q \cap N(P)$.*

Todistus (vrt. [12, s. 5]). Koska $P \subseteq N(P)$, niin $Q \cap P \subseteq Q \cap N(P)$. Riittää osoittaa, että $Q \cap N(P) \subseteq Q \cap P$. Merkitään $H = Q \cap N(P)$. Nyt siis $H \leqslant Q$ ja Q on p-aliryhmä, joten Lagrangen lauseen perusteella H on p-aliryhmä.

Nyt $P \trianglelefteq N(P)$ ja $P \in \mathrm{Syl}_p(G)$, joten p ei voi jakaa tekijäryhmän $N(P)/P$ kertalukua. Tällöin seurauksen 3.25 perusteella tekijäryhmällä $N(P)/P$ ei ole yhtään sellaisia alkioita, joiden kertaluku olisi alkuluvun p potenssi.

Olkoon $x \in H \setminus \{e\}$, jolloin $\mathrm{ord}(x) = p^k$ jollakin $k \in \mathbb{Z}_+$. Merkitään $q = p^k$. Nyt $(xP)^q = x^qP = eP$, joten seurauksen 1.39 mukaan $xP = eP$ tai tekijäryhmän $N(P)/P$ alkion xP kertaluku on alkuluvun p potenssi. Näistä väitteistä jälkimmäinen johtaa ristiriitaan. Siis $xP = eP$, joten $x \in P$. Siis $H \subseteq P$. Koska lisäksi $H \subseteq Q$, niin $H \subseteq Q \cap P$. □

Lause 6.25. *Olkoon H äärellisen ryhmän G p-aliryhmä. Tällöin H sisältyy johonkin ryhmän G Sylowin p-aliryhmään.*

Todistus (vrt. [12, s. 6]). Toimikoon aliryhmä H perheessä $\mathrm{Syl}_p(G)$ konjugoimalla ryhmän G vastaavan toiminnan rajoittumana. Merkitään $X_0 = \mathrm{Fix}_{\mathrm{Syl}_p(G)}(H)$. Nyt Sylowin lemman kohdan (i) nojalla

$$|X_0| \equiv n_p \pmod{p}.$$

Koska lisäksi seurauksen 6.21 mukaan $p \nmid n_p$, niin $|X_0| \neq 0$. Olkoon $P_0 \in X_0$. Nyt lauseen 5.11 nojalla

$$1 = |\mathcal{O}_{P_0}| = (H : \mathrm{Stab}_H(P_0)) = (H : N_H(P_0)) = (H : H \cap N(P_0)).$$

Näin ollen Lagrangen lauseesta seuraa, että $H = H \cap N(P_0)$. Koska H on p-ryhmä ja $P_0 \in \mathrm{Syl}_p(G)$, niin lemman 6.24 perusteella $H \cap N(P_0) = H \cap P_0$. Siis $H = H \cap P_0$, joten $H \leqslant P_0$. □

Conradin (ks. [2]) mukaan Sylowin ensimmäisen lause kertookin, että ryhmän G Sylowin p-aliryhmä on olemassa ja sisältyy johonkin tämän ryhmän p-aliryhmään (lause 6.25 ja seuraus 6.18 siis yhdistettynä). Mann (ks. [12]) puolestaan pitää seurausta 6.18 Sylowin ensimmäisenä ja lausetta 6.25 Sylowin kolmantena lauseena. Tämän tutkielman Sylowin kolmannen lauseen Mann laskee vielä erikseen Sylowin neljänneksi lauseeksi. Myös Rose (ks. [18]) käsittää Sylowin ensimmäisen lauseen Sylowin p-aliryhmän olemassaolona, mutta muut kaksi lausetta tutkielman kanssa vastaavasti. Malik ym. (ks. [11]) tulkitsevat Sylowin lauseet samalla tavalla kuten tutkielmassa.

7 Sylowin lauseiden sovelluksia

Tiivistetään tämän luvun alkuun Sylowin kaikki kolme lausetta vielä yhdeksi lauseeksi. [1]

Lause 7.1 (Sylowin lauseet)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, $r, m \in \mathbb{Z}_+$ ja* $\mathrm{syt}(p, m) = 1$. *Tällöin seuraavat ehdot pätevät.*

(1) *Ryhmällä G on jokaisella $k \in \{0, \ldots, r\}$ aliryhmä, jonka kertaluku on p^k.*

(2) *Ryhmän G Sylowin p-aliryhmät ovat konjugaatteja keskenään. Erityisesti $n_p = (G : N(P))$ kaikilla $P \in \mathrm{Syl}_p(G)$.*

(3) *n_p jakaa luvun m, ja $n_p \equiv 1 \pmod{p}$.*

Mihin Sylowin lauseita voidaan sitten äärellisessä ryhmäteoriassa hyödyntää? Sylowin lauseiden avulla pystytään tutkimaan, millaisia tietyn kertaluvun omaavat ryhmät ylipäänsä ovat. Ovatko tutkittavat ryhmät esimerkiksi yksinkertaisia tai syklisiä? Voiko jokin ryhmä vaihtoehtoisesti olla syklinen tai diedriryhmä? Miten ryhmän vaihdannaisuus vaikuttaa siihen, millaisia ryhmät voivat olla? Ja saadaanko tällöin näille tapauksille esitettyä joitakin konkreettisia esimerkkiryhmiä? Luvussa 7 pyritään antamaan joitakin vastauksia näihin kysymyksiin.

Tutkielmassa on tähän mennessä määritetty jo muutamia tuloksia, jotka kertovat jotakin siitä, millainen tietyn kertaluvun omaava ryhmä on. Seuraukset 5.18, 6.9 ja esimerkki 6.1 kertovat nimittäin jo jonkin verran äärellisen ryhmän yksinkertaisuudesta. Alaluvussa 7.1 keskitytään tarkastelemaan pelkästään äärellisten ryhmien yksinkertaisuutta, ja alaluku 7.2 tarkastelee yksinkertaisella tasolla sitä, millä tavalla ryhmiä voidaan luokitella isomorfisuuden perusteella. Luvun 7 sisältö on kasattu useasta eri lähteestä.

---

[1] Sylow itse todisti Sylowin lauseet seuraavassa muodossa (eri merkinnöillä ja käsitteillä toki):

(1) Sylowin p-aliryhmä on aina olemassa ja $(G : N(P)) \equiv 1 \pmod{p}$ kaikilla $P \in \mathrm{Syl}_p(G)$.

(2) Olkoon $P \in \mathrm{Syl}_p(G)$. Tällöin $n_p = (G : N(P))$ ja kaikki Sylowin p-aliryhmät ovat konjugaatteja keskenään.

(3) Jokainen äärellinen p-ryhmä sisältää seuraavan kasvavan sarjan aliryhmiä

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_d \subset G,$$

missä $|G_i| = p^i$ kaikilla i.

Kun tätä Sylowin omaa kolmatta lausetta sovelletaan äärellisen ryhmän Sylowin p-aliryhmään, saadaan itse asiassa Sylowin ensimmäinen lause. [3, s. 4]

7.1 Äärellisten ryhmien yksinkertaisuudesta

Tässä alaluvussa on tarkoituksena pohtia, miten Sylowin lauseiden avulla voidaan tarkastella äärellisten ryhmien yksinkertaisuutta. Eli yksinkertaisesti sitä, että onko tietyn kertaluvun omaava ryhmä yksinkertainen vai ei. Lähdetään tutkimaan nyt yleisiä tuloksia ryhmistä, joilla on kohtuullisen yksinkertainen kertaluku alkulukujen tuloista.

Perusstrategiana on edetä ryhmän kertaluvun alkutekijöiden lukumäärän mukaan: Ensinnäkin alkulukukokoiset ryhmät ovat syklisiä ja yksinkertaisia, jonka jälkeen havaitaan, että kahden alkuluvun tulon kokoinen ryhmä ei tuota yksinkertaisia ryhmiä. Edelleen siirrytään kertalukuun, jonka alkulukujen tulossa esiintyy alkuvun neliö kerrottuna toisella alkuluvulla, ja lopuksi osoitetaan kolmen eri alkuluvun tulon muodostaman kertaluvun omaavan ryhmän epäyksinkertaisuus.

Lause 7.2. *Olkoot p ja q eri alkulukuja. Tällöin ryhmä, jonka kertaluku on pq, ei ole yksinkertainen.*

Todistus (ks. [11, s. 211]). Olkoon G ryhmä, jolle $|G| = pq$. Voidaan olettaa, että $p > q$. Nyt Sylowin kolmannen lauseen nojalla $n_p \equiv 1 \pmod{p}$ ja $n_p \mid q$. Siis $n_p = 1 + kp$ jollakin $k \in \mathbb{N}$. Edelleen $1 + kp = n_p \leq q < p$, joten on oltava $k = 0$. Näin ollen $n_p = 1$, joten ryhmällä G on vain yksi Sylowin p-aliryhmä, olkoon se H. Nyt kuitenkin seurauksen 6.20 perusteella H on normaali, ja lisäksi $|H| = p$, joten $H \lhd G$. Tästä seuraa, että G ei ole yksinkertainen. □

Jatketaan vielä kahden vastaavan yleisen tapauksen tarkastelua. Todistetaan näitä tuloksia varten kuitenkin ensin hyödyllinen lemma.

Lemma 7.3. *Olkoon p alkuluku ja m sellainen positiivinen kokonaisluku, että* $\operatorname{syt}(p, m) = 1$. *Olkoon G ryhmä, jonka kertaluku on pm ja oletetaan, että $n_p > 1$. Tällöin ryhmällä G on $n_p(p-1)$ eri alkiota, joiden kertaluku on p.*

Todistus. Nyt $n_p > 1$, joten voidaan valita kaksi ryhmän G eri Sylowin p-aliryhmää P ja P'. Nyt $P \cap P' < P$, joten Lagrangen lauseesta seuraa, että $P \cap P' = \{e\}$. Lisäksi kaikkien ryhmän G Sylowin p-aliryhmien alkioiden kertaluvut vastaavat, neutraalialkioita lukuunottamatta, alkulukua p. Näin ollen ryhmällä G on $n_p(p-1)$ eri alkioita, joiden kertaluku on p. □

Lause 7.4. *Olkoon G ryhmä, jonka kertaluku on p^2q, missä p ja q ovat eri alkulukuja. Tällöin ryhmä G ei ole yksinkertainen.*

Todistus (vrt. [18, s. 97–98]). Olkoot n_p ja n_q ryhmän G Sylowin p- ja q-aliryhmien lukumäärät. Oletetaan vastoin väitettä, että G on yksinkertainen. Tällöin seurauksen 6.20 perusteella $n_p > 1$ ja $n_q > 1$. Nyt Sylowin kolmannen lauseen nojalla $n_p \mid q$, ja koska q on alkuluku ja $n_p > 1$, niin $n_p = q$. Lisäksi $n_p \equiv 1 \pmod{p}$, joten $n_p = 1 + kp$ jollakin $k \in \mathbb{Z}_+$ ($k \neq 0$, sillä $n_p > 1$). Siis $q = 1 + kp$, joten $q > p$. Toisaalta Sylowin kolmannen lauseen mukaan $n_q \mid p^2$, joten $n_q = p$ tai $n_q = p^2$. Nyt lemman 7.3 nojalla ryhmällä G on $n_q(q-1)$ eri alkioita, joiden kertaluku on q. Täten,

jos $n_q = p^2$, niin ryhmällä G on $p^2q - p^2(q-1) = p^2$ alkioita, joiden kertaluku ei ole q. Toisaalta, jos $P \in \mathrm{Syl}_p(G)$, niin $|P| = p^2$ ja aliryhmällä P ei tietenkään ole alkioita, joiden kertaluku on q. Täten Sylowin p-aliryhmä P on itse asiassa yksikäsitteinen, joten $n_p = 1$, mikä on ristiriidassa vastaoletuksen kanssa. Näin ollen $n_q = p$. Mutta koska $n_q \equiv 1 \pmod{q}$, niin $p = n_q = 1 + k'q$, missä $k' \in \mathbb{Z}_+$, jolloin $p > q$, mikä on taas ristiriita, sillä aiemmin pääteltiin, että $p < q$. □

Lause 7.5. *Olkoot p, q ja r eri alkulukuja. Olkoon G ryhmä, jonka kertaluku on pqr. Tällöin ryhmä G ei ole yksinkertainen.*

Todistus (ks. [18, s. 98]). Voidaan olettaa, että $p > q > r$. Oletetaan vastoin väitettä, että G on yksinkertainen. Koska G on yksinkertainen, niin sillä ei ole aitoja normaaleja Sylowin p-, q- ja r-aliryhmiä. Täten seurauksen 6.20 perusteella $n_p > 1$, $n_q > 1$ ja $n_r > 1$. Nyt lemman 7.3 nojalla ryhmällä G on $n_p(p-1)$ alkioita, joiden kertaluku on p, $n_q(q-1)$ alkioita, joiden kertaluku on q ja $n_r(r-1)$ alkioita, joiden kertaluku on r. Siis

$$|G| = pqr \geq 1 + n_p(p-1) + n_q(q-1) + n_r(r-1).$$

Sylowin kolmannen lauseen nojalla $n_p \mid qr$ ja $n_p \equiv 1 \pmod{p}$. Koska $n_p > 1$, niin $n_p > p > q > r$, joten $n_p = qr$. Toisaalta $n_q \mid pr$ ja $n_q \equiv 1 \pmod{q}$, jolloin $n_q = p$ tai $n_q = pr$, sillä $n_q > q > r$. Siis $n_q \geq p$. Edelleen $n_r > 1$ ja $n_r \mid pq$, joten $n_r \geq q$. Täten saadaan:

$$pqr \geq 1 + qr(p-1) + p(q-1) + q(r-1),$$

mistä seuraa, että

$$0 \geq (p-1)(q-1),$$

mikä on tietysti mahdotonta. □

Käsitellään nyt perustavaa laatua oleva esimerkki, joka käsittelee alhaisten kertalukujen omaavien ryhmien yksinkertaisuutta. Tässä esimerkissä tulee hyvin ilmi, että kaikkien yksinkertaisten ryhmien löytäminen on varsin työläs tehtävä. Esimerkissä käytetään useita aiemmissa luvuissa olleita tuloksia.

Esimerkki 7.1 (vrt. [11, s. 211–212; 217], [18, s. 99–100] ja [2, s. 6–7])**.** Osoitetaan tässä esimerkissä aiempien tulosten pohjalta, että kaikki ryhmät, joiden alkuluvuton kertaluku on lukujen 1 ja 100 välillä eivät ole yksinkertaisia lukua 60 lukuun ottamatta.

Olkoon G tarkasteltava äärellinen ryhmä. Tapaus $|G| = 1$ on triviaali. Jos ryhmän kertaluku on alkuluku, niin ryhmä on yksinkertainen. Näin ollen kertaluvun 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 tai 97 omaavat ryhmät ovat yksinkertaisia. Kun $|G|$ on $6 (= 2 \cdot 3)$, $10 (= 2 \cdot 5)$, $12 (= 3 \cdot 2^2)$, $14 (= 2 \cdot 7)$, $15 (= 3 \cdot 5)$, $18 (= 2 \cdot 3^2)$, $20 (= 2^2 \cdot 5)$, $21 (= 3 \cdot 7)$, $22 (= 2 \cdot 11)$, $26 (= 2 \cdot 13)$, $28 (= 2^2 \cdot 7)$, $30 (= 2 \cdot 3 \cdot 5)$, $33 (= 3 \cdot 11)$, $34 (= 2 \cdot 17)$, $35 (= 5 \cdot 7)$, $38 (= 2 \cdot 19)$, $(= 3 \cdot 13)$, $42 (= 2 \cdot 3 \cdot 7)$, $44 (= 2^2 \cdot 11)$, $45 (= 3^2 \cdot 5)$, $46 (= 2 \cdot 23)$, $50 (= 2 \cdot 5^2)$, $51 (= 3 \cdot 17)$, $52 (= 2^2 \cdot 13)$, $55 (= 5 \cdot 11)$, $57 (= 3 \cdot 19)$, $58 (= 2 \cdot 29)$, $62 (= 2 \cdot 31)$, $63 (= 3^2 \cdot 7)$, $65 (= 5 \cdot 13)$, $66 (= 2 \cdot 3 \cdot 11)$, $68 (= 2^2 \cdot 17)$, $69 (= 3 \cdot 23)$, $70 (= 2 \cdot 5 \cdot 7)$, $74 (= 2 \cdot 37)$, $75 (= 3 \cdot 5^2)$, $76 (= 2^2 \cdot 19)$, $77 (= 7 \cdot 11)$, $78 (=$

$2 \cdot 3 \cdot 13), 82\ (= 2 \cdot 41), 85\ (= 5 \cdot 17), 86\ (= 2 \cdot 43), 87\ (= 3 \cdot 29), 91\ (= 7 \cdot 13), 92\ (= 2^2 \cdot 23), 93\ (= 3 \cdot 31), 94\ (= 2 \cdot 47), 95\ (= 5 \cdot 19), 97\ (= 3 \cdot 29), 98\ (= 2 \cdot 7^2)$ tai $99\ (= 3^2 \cdot 11)$, niin lauseiden 7.2, 7.4 ja 7.5 nojalla G ei ole yksinkertainen. Jos taas $|G|$ on $4\ (= 2^2), 8\ (= 2^3), 9\ (= 3^2), 16\ (= 2^4), 25\ (= 5^2), 27\ (= 3^3), 32\ (= 2^5), 49\ (= 7^2), 64\ (= 2^6)$ tai $81\ (= 3^4)$, niin seurauksen 6.9 perusteella G ei ole yksinkertainen.

Tarkastellaan ryhmää G kertaluvulla $24 = 2^3 \cdot 3$. Nyt ryhmällä G on Sylowin 2-aliryhmä H, jonka kertaluku on 2^3. Tällöin $(G : H) = 3$, mutta $|G| \nmid 3!$. Näin ollen seurauksen 5.18 nojalla G ei ole yksinkertainen. Täysin vastaavasti saadaan, että ryhmät, joiden kertaluku on 36, 48, 80, 96 tai 100, eivät ole yksinkertaisia. Esimerkistä 6.1 seuraa puolestaan, että kertaluvun $54\ (= 2 \cdot 27)$ tai $90\ (= 2 \cdot 45)$ omaavat ryhmät eivät ole yksinkertaisia. Kootaan tähän asti saadut tulokset taulukkoon, josta voidaan lukea nopeasti, mikä tulos johtaa siihen, että tietyn kertaluvun omaava ryhmä ei ole yksinkertainen. Taulukkoon 7.1 on lueteltu kaikki ryhmän G kertaluvut numerosta 1 numeroon 100 saakka. Alkuluvuttomia kertalukuja vastaavat tässä taulukossa ne tulokset, jotka osoittavat, että näillä kertaluvuilla varustetut ryhmät eivät ole yksinkertaisia.

Taulukko 7.1: Äärellisen ryhmän kertaluvut numerosta 1 numeroon 100 asti. Kertalukuja vastaavat tulokset osoittavat, että ryhmä ei ole yksinkertainen tai on Abelin ryhmä. Alkuluvullisen kertaluvun omaavat ryhmät ovat tietysti Abelin ryhmiä.

1	triviaali	26	lause 7.2	51	lause 7.2	76	lause 7.4
2	alkuluku	27	seuraus 6.9	52	lause 7.4	77	lause 7.2
3	alkuluku	28	lause 7.4	53	alkuluku	78	lause 7.5
4	seuraus 6.9	29	alkuluku	54	esim. 6.1	79	alkuluku
5	alkuluku	30	lause 7.5	55	lause 7.2	80	seuraus 5.18
6	lause 7.2	31	alkuluku	56	–	81	seuraus 6.9
7	alkuluku	32	seuraus 6.9	57	lause 7.2	82	lause 7.2
8	seuraus 6.9	33	lause 7.2	58	lause 7.2	83	alkuluku
9	seuraus 6.9	34	lause 7.2	59	alkuluku	84	–
10	lause 7.2	35	lause 7.2	60	–	85	lause 7.2
11	alkuluku	36	seuraus 5.18	61	alkuluku	86	lause 7.2
12	lause 7.4	37	alkuluku	62	lause 7.2	87	lause 7.2
13	alkuluku	38	lause 7.2	63	lause 7.4	88	–
14	lause 7.2	39	lause 7.2	64	seuraus 6.9	89	alkuluku
15	lause 7.2	40	–	65	lause 7.2	90	esim. 6.1
16	seuraus 6.9	41	alkuluku	66	lause 7.5	91	lause 7.2
17	alkuluku	42	lause 7.5	67	alkuluku	92	lause 7.4
18	lause 7.4	43	alkuluku	68	lause 7.4	93	lause 7.2
19	alkuluku	44	lause 7.4	69	lause 7.2	94	lause 7.2
20	lause 7.4	45	lause 7.4	70	lause 7.5	95	lause 7.2
21	lause 7.2	46	lause 7.2	71	alkuluku	96	seuraus 5.18
22	lause 7.2	47	alkuluku	72	–	97	alkuluku
23	alkuluku	48	seuraus 5.18	73	alkuluku	98	lause 7.4
24	seuraus 5.18	49	seuraus 6.9	74	lause 7.2	99	lause 7.4
25	seuraus 6.9	50	lause 7.4	75	lause 7.4	100	seuraus 5.18

Kuten taulukosta 7.1 havaitaan, selvittämättä on vielä kertaluvun 40, 56, 60, 72, 84 ja 88 omaavien ryhmien yksinkertaisuus. Lauseen 3.45 perusteella on olemassa sellainen ryhmä, joka on yksinkertainen ja jonka kertaluku on 60, nimittäin alternoiva ryhmä A_5. Tarkastellaan sitten ryhmää G, jonka kertaluku on $40 = 2^3 \cdot 5$. Sylowin kolmannen lauseen perusteella $n_5 \equiv 1 \pmod 5$ ja $n_5 \mid 8$. Tästä seuraa, että $n_5 = 1$, joten ryhmällä G on vain yksi Sylowin 5-aliryhmä, joka seurauksen 6.20 nojalla on normaali. Täten G ei ole yksinkertainen. Vastaavalla tavalla voidaan osoittaa, että kertaluvuilla 84 tai 88 varustetut ryhmät eivät ole yksinkertaisia.

Olkoon $|G| = 56 = 2^3 \cdot 7$. Jälleen hyödyntämällä Sylowin kolmatta lausetta saadaan, että $n_7 \equiv 1 \pmod 7$ ja $n_7 \mid 8$ sekä $n_2 \equiv 1 \pmod 2$ ja $n_2 \mid 7$. Tästä vaihtoehdoiksi jää, että $n_7 = 1$ tai $n_7 = 8$ ja $n_2 = 1$ tai $n_2 = 7$. Oletetaan, että G on yksinkertainen. Ryhmän G yksinkertaisuudesta voidaan päätellä seurauksen 6.20 nojalla, että $n_7 = 8$ ja $n_2 = 7$. Nyt lemman 7.3 perusteella ryhmällä G on $48\ (= 8 \cdot (7-1))$ alkioita, joiden kertaluku on 7. Tiedetään lisäksi, että ryhmällä G on 7 Sylowin 2-aliryhmää, olkoot ne $B_1, \ldots, B_7$. Koska $|B_i| = 2^3 = 8$ kaikilla $i \in \{1, \ldots, 7\}$ ja $B_1 \neq B_2$, niin ryhmällä G on vähintään 9 eri alkioita, joiden kertaluku ei ole 7. Siis $|G| \geq 48 + 9 = 57$, mikä on ristiriita. Näin ollen ryhmä G ei ole yksinkertainen.

Enää jäljellä tarkasteltavana on tapaus $|G| = 72 = 2^3 \cdot 3^2$. Nyt Sylowin kolmannen lauseen nojalla $n_3 \equiv 1 \pmod 3$ ja $n_3 \mid 8$, joten $n_3 = 1$ tai $n_3 = 2^2$. Jos $n_3 = 1$, niin G ei ole yksinkertainen. Oletetaan siis, että $n_3 = 2^2$. Olkoot H_1, H_2, H_3 ja H_4 tarkastelevat Sylowin 3-aliryhmät. Nyt $H_1 \cap H_2 \leqslant H_1, H_2$. Koska $|H_1| = 9$, niin $|H_1 \cap H_2| = 1, 3$ tai 9. Jos $|H_1 \cap H_2| = 9$, niin $H_1 = H_2$, mikä on ristiriita. Jos taas $|H_1 \cap H_2| = 1$, niin tulokaavan perusteella

$$|H_1 H_2| = \frac{|H_1|\,|H_2|}{|H_1 \cap H_2|} = \frac{9 \cdot 9}{1} = 81,$$

mikä on ristiriita, sillä ryhmässä G on 72 alkioita. Siis $|H_1 \cap H_2| = 3$. Merkitään $B = N(H_1 \cap H_2)$. Nyt lauseen 6.11 nojalla $H_1 \cap H_2 \trianglelefteq H_1, H_2$, jolloin $H_1, H_2 \leqslant B$. Edelleen vastaavasti tulokaavan nojalla $|H_1 H_2| = 27$, joten $|B| \geq 27$. Täten Lagrangen lauseen perusteella $|B| = 36$ tai $|B| = 72$. Jos $|B| = 36$, niin $(G : B) = 2$ ja $|G| \nmid 2!$, joten seurauksen 5.18 perusteella G ei ole yksinkertainen. Jos taas $|B| = 72$, niin $B = G$. Tällöin lauseen 5.45 perusteella $H_1 \cap H_2$ on ryhmän G normaali aliryhmä, joten G ei ole tällöinkään yksinkertainen.

Käsitellään vielä seuraavassa esimerkissä eräs vaihtoehtoinen menetelmä äärellisen ryhmän yksinkertaisuuden tarkasteluun. Otetaan tarkasteluun ryhmä kertaluvulla 1568.

Esimerkki 7.2 (vrt. [10, s. 13–14] [2])**.** Olkoon G ryhmä, jonka kertaluku on $1568 = 2^5 \cdot 7^2$. Osoitetaan, että ryhmä G ei ole tällöin yksinkertainen. Nyt Sylowin kolmannen lauseen avulla saadaan, että n_2 on 1, 7 tai 7^2 ja n_7 on 1 tai 8. Oletetaan vastoin väitettä, että G on yksinkertainen, jolloin n_2 on 7 tai 7^2 ja $n_7 = 8$. Toimikoon G perheessä $X = \mathrm{Syl}_7(G)$ konjugoimalla, jolloin toiminta on

$$\cdot \colon G \times X \to X, g \cdot S = S^g.$$

Tarkastellaan tätä toimintaa vastaavaa permutaatioesitystä

$$\rho \colon G \to S_X, \rho(g) = \rho_g,$$

[2]Lähteessä [10] Ling ja Miller vain toteavat kertaluvun 1568 omaavan ryhmän yksinkertaisuuden vetoamalla yleisempään tunnettuun tulokseen, joka perustuu ryhmien ratkeavuuteen (engl. soluble tai solvable) tapauksessa, jossa ryhmän kertaluku esitetään kahden eri alkuluvun potenssien tulona.

missä

$$\rho_g \colon X \to X, \rho_g(S) = S^g.$$

Nyt $|X| = n_7 = 8$, joten $S_X \cong S_8$. Näin ollen on olemassa isomorfismi $f \colon S_X \to S_8$, ja siis

$$\phi = f \circ \rho \colon G \to S_8$$

on homomorfismi. Oletetaan nyt, että ϕ ei ole injektio. Tällöin $\mathrm{Ker}(\phi) \neq \{\mathrm{id}_X\}$, ja lisäksi $\mathrm{Ker}(\phi) \trianglelefteq G$. Edelleen, jos olisi $\mathrm{Ker}(\phi) = G$, niin pätisi toki myös, että $\mathrm{Ker}(\rho) = G$, sillä f on bijektio. Tällöin kaikilla $g \in G$ pätisi $\rho_g = \mathrm{id}_X$. Olkoon $S \in X$ ja $g \in G$. Nyt siis

$$S^g = \rho_g(S) = \mathrm{id}_X(S) = S.$$

Tästä tosin seuraa, että S on normaali, jolloin seurauksen 6.20 nojalla $n_7 = 1$, mikä on ristiriita. Siis $\mathrm{Ker}(\phi) \trianglelefteq G$, joten ryhmällä G on epätriviaali ja normaali aliryhmä, mikä on ristiriidassa sen kanssa, että G on yksinkertainen. Siis ϕ on injektio. Silloin G voidaan upottaa symmetriaryhmään S_8, joten $G \cong T$, missä $T \leqslant S_8$. Näin ollen Lagrangen lauseesta seuraa, että $|G|$ jakaa symmetriaryhmän S_8 kertaluvun 8!. Tämä on kuitenkin ristiriita, sillä selvästi $1568 \nmid 8!$. Täten ryhmä G ei voi olla yksinkertainen.

Äärellisten yksinkertaisten ryhmien täydellinen luokittelu saatiin valmiiksi vuonna 1981. Sadat matemaatikot osallistuivat tämän tuloksen saavuttamiseen; muiden muassa M. Aschbacher, R. L. Griess, Emil Mathieu, F. N. Cole, G. A. Miller, L. E. Dickson, Jean Dieudonné, Claud Chevalley, Richard Brauer, F. A. Fowler, Daniel Gorenstein ja J. H. Conway. Tässä tutkielmassa ei ilmeisistä syistä mennä aivan niin pitkälle, joskin seuraavassa alaluvussa tullaan antamaan esimakua äärellisten ryhmien luokittelusta, ja erityisesti siitä, miten Sylowin lauseita voidaan tässä luokittelussa hyödyntää. [11, s. 214]

7.2 Äärellisten ryhmien luokittelua

Aiemmin osoitettiin siis, että melkein kaikki ryhmät, joiden kertaluku on väliltä 1 ja 100, eivät ole yksinkertaisia tai ovat vaihdannaisia. Kertaluku 60 näyttää kuitenkin poikkeuksen, sillä alternoiva ryhmä A_5 on yksinkertainen. Toisaalta koska 60 ei ole alkuluku, niin yksikään Abelin ryhmä kertaluvulla 60 ei ole yksinkertainen. Onko A_5 sitten ainoa isomorfiaa vaille oleva yksinkertainen ryhmä, jonka kertaluku on 60? Aloitetaan tämän kysymyksen tutkiminen todistamalla seuraava lemma.

Lemma 7.6. *Olkoon G yksinkertainen ryhmä, jonka kertaluku on 60. Tällöin G sisältää aliryhmän, jonka kertaluku on 12.*

Todistus (ks. [11, s. 213]. Nyt $|G| = 5 \cdot 3 \cdot 2^2$. Oletetaan vastoin väitettä, että ryhmällä G ei ole aliryhmää, jonka kertaluku on 12. Sylowin kolmannesta lauseesta seuraa, että $n_5 = 1$ tai $n_5 = 6$. Koska G on yksinkertainen, niin $n_5 \neq 1$, joten $n_5 = 6$. Lemman 7.3 nojalla ryhmällä G on $6 \cdot (5 - 1) = 24$ alkioita, joiden kertaluku

on 5. Edelleen Sylowin kolmannesta lauseesta saadaan, että n_2 on 1, 3, 5 tai 15. Ryhmän G yksinkertaisuudesta johtuen $n_2 \neq 1$. Oletetetaan, että $n_2 = 15$. Olkoot B_i, $i \in \{1, \ldots, 15\}$, 15 Sylowin 2-aliryhmää. Jos olisi $B_i \cap B_j = \{e\}$ kaikilla $i, j \in \{1, \ldots, 15\}(i \neq j)$, niin näiden kaikkien Sylowin 2-aliryhmien yhdiste sisältäisi $15 \cdot (4-1) + 1 = 46$ alkioita, joiden kertaluku ei ole 5. Silloin $|G| \geq 24 + 46 = 70$, mikä on ristiriita. On siis olemassa sellaiset $i, j \in \{1, \ldots, 15\}, i \neq j$, että $B_i \cap B_j \neq \{e\}$. Merkitään $A = N(B_i \cap B_j)$. Lagrangen lauseesta, ja siitä, että leikkaavat neljän alkion ryhmät B_i ja B_j ovat eri ryhmiä, seuraa suoraan, että leikkauksessa on 1 tai 2 alkiota. Siis $|B_i \cap B_j| = 2$. Näin ollen lauseen 6.11 nojalla $B_i \cap B_j$ on B_i:n ja B_j:n normaali aliryhmä. Täten $B_i, B_j \subseteq A$, jolloin tulokaavan perusteella

$$|A| \geq |B_i B_j| = \frac{|B_i||B_j|}{|B_i \cap B_j|} = \frac{4 \cdot 4}{2} = 8.$$

Silloin Lagrangen lauseen nojalla $|A|$ on 12, 20, 30 tai 60. Oletuksesta seuraa, että $|A| \neq 12$. Jos $|A| = 20$ tai $|A| = 30$, niin seurauksen 5.18 perusteella G ei ole yksinkertainen, mikä on ristiriita. Jos taas $|A| = 60$, niin $G = A$, jolloin $B_i \cap B_j$ on ryhmän G normaali aliryhmä, joten G ei ole yksinkertainen. Jälleen ristiriita.

Oletetaan vielä, että n_2 on 3 tai 5. Olkoon P Sylowin 2-aliryhmä. Sylowin toisen lauseen perusteella $n_2 = (G : N(P))$, joten

$$|N(P)| = \frac{|G|}{n_2}.$$

Siis $|N(P)|$ on 12 tai 20. Koska oletuksen perusteella $|N(P)| \neq 12$, niin $|N(P)| = 20$, mikä johtaa ristiriitaan kuten aiemmin. Näin ollen ryhmällä G on oltava aliryhmä, jonka kertaluku on 12. □

Havaitaan, että lemman 7.6 avulla voidaan todistaa, että kaikki kertaluvun 60 omaavat yksinkertaiset ryhmät ovat isomorfisia alternoivan ryhmän A_5 kanssa.

Lause 7.7. *Jokainen yksinkertainen ryhmä, jonka kertaluku on 60, on isomorfinen alternoivan ryhmän A_5 kanssa.*

Todistus (vrt. [11, s. 213] ja [2, s. 15]). Olkoon G yksinkertainen ryhmä, jonka kertaluku on 60. Lemman 7.6 nojalla ryhmällä G on olemassa aliryhmä H, jonka kertaluku on 12. Nyt $(G : H) = 5$. Koska G on yksinkertainen, niin $H_G = \{e\}$. Täten lauseen 5.16 nojalla $G/\{e\} = G$ on isomorfinen ryhmän S_5 aliryhmän, sanotaan K, kanssa. Pyritään nyt osoittamaan, että $K \subseteq A_5$.

Oletetaan vastoin tätä, että K sisältää parittoman permutaation. Tällöin kuvaus

$$f \colon K \to \{-1, 1\}, f(\alpha) = \epsilon(\alpha)$$

on epimorfismi, joten $\mathrm{Im}(f) = \{-1, 1\}$. Edelleen ensimmäisen isomorfialauseen perusteella $K/\operatorname{Ker}(f) \cong \{-1, 1\}$, joten

$$2 = |\{-1, 1\}| = (K : \operatorname{Ker}(f)).$$

Näin ollen aliryhmällä K on epätriviaali ja normaali aliryhmä, nimittäin $\mathrm{Ker}(f)$. Koska lisäksi $G \cong K$, niin myös ryhmällä G on epätriviaali ja normaali aliryhmä. Tämä on kuitenkin ristiriita, sillä G on yksinkertainen. Täten $K \subseteq A_5$. Mutta nythän $|A_5| = 60 = |G| = |K|$, joten $K = A_5$. Siis $G \cong A_5$. □

Tarkastellaan muutamaa yksinkertaista yleistä tapausta, jossa Sylowin lauseita voidaan hyödyntää luokittelemaan ryhmiä. Ensimmäisenä käsitellään tapausta, jossa ryhmän kertaluku on kahden eri alkuluvun tulo. Osoitetaan, että tällöin (pienen lisäoletuksen kanssa) tarkasteltava ryhmä on syklinen.

Lause 7.8. *Olkoon G ryhmä ja p ja q eri alkulukuja niin, että $p > q$. Oletetaan, että $|G| = pq$ ja $q \nmid (p-1)$. Tällöin G on syklinen ryhmä.*

Todistus (vrt. [11, s. 214]). Cauchyn lauseen perusteella ryhmällä G on sellainen alkio g, jonka kertaluku on p. Olkoon $P = \langle g \rangle$. Nyt lauseen 3.17 nojalla

$$|P| = |\langle g \rangle| = \mathrm{ord}(g) = p,$$

jolloin $P \in \mathrm{Syl}_p(G)$. Täysin vastaavasti kuten lauseen 7.2 todistuksessa, voidaan todeta, että $n_p = 1$, joten $P \lhd G$.

Toisaalta Cauchyn lauseesta seuraa, että ryhmällä G on olemassa sellainen alkio g', että $\mathrm{ord}(g') = q$. Olkoon $Q = \langle g' \rangle$. Vastaavasti toki Q on myös Sylowin q-aliryhmä. Nyt Sylowin kolmannen lauseen perusteella $n_q \mid p$ ja $n_q \equiv 1 \pmod{q}$. On olemassa siis sellainen luonnollinen luku k, että $n_q = 1 + kq$. Siis $1 + kq$ jakaa alkuluvun p. Koska p on alkuluku, niin tästä seuraa, että joko $1+kq = 1$ tai $1+kq = p$. Siis $k = 0$ tai $q \mid (p-1)$. Oletuksen perusteella pätee, että $k = 0$, jolloin $n_q = 1$, ja siis $Q \lhd G$. Edelleen $P \cap Q = \{e\}$, joten tulokaavan nojalla

$$|PQ| = \frac{|P|\,|Q|}{|P \cap Q|} = |P|\,|Q| = pq = |G|\,.$$

Siis $PQ = G$. Toisaalta lauseen 4.19 perusteella $PQ \cong P \times Q$, joten $G \cong P \times Q$. Lisäksi lauseen 3.30 nojalla $P \times Q$ on syklinen ryhmä, ja näin ollen myös ryhmä G syklinen. □

Toisessa yleisessä tapauksessa osoitetaan puolestaan, että ryhmä kertaluvulla $2p$, missä p on lukua 2 suurempi alkuluku, on joko syklinen ryhmä tai diedriryhmä.

Lause 7.9. *Olkoon G ryhmä, jonka kertaluku on $2p$, missä $p > 2$ on alkuluku. Tällöin ryhmä G on syklinen tai diedriryhmä.*

Todistus (vrt. [11, s. 215]). Cauchyn lauseen nojalla ryhmällä G on alkio a, jonka kertaluku on p ja alkio b, jonka kertaluku on 2. Olkoon $H = \langle a \rangle$. Nyt $H \trianglelefteq G$, sillä $(G : H) = 2$. Täten $bab = bab^{-1} \in H$. Tarkastellaan alkion b synnyttämän sisäisen automorfismin

$$\tau_b \colon G \to G, \tau_b(x) = x^b$$

rajoittumaa $f_b := \tau_b \restriction H$, joka on automorfismi ja jolle tietysti pätee, että $f_b(a^k) = (f_b(a))^k$ (induktiolla voidaan yleisesti osoittaa, että isomorfismille $f \colon G \to G'$ pätee,

että $f(a^n) = (f(a))^n$, missä $n \in \mathbb{Z}_+$). Edelleen koska $bab \in H$, niin on olemassa sellainen $a^i \in H$, että $bab = a^i$, missä $i \in \{0, \ldots, p-1\}$. Nyt

$$a^{i^2} = (a^i)^i = (bab)^i = (f_b(a))^i = f_b(a^i) = ba^ib.$$

Toisaalta koska $bab = a^i$, niin $a = ba^ib$. Siis $a = a^{i^2}$, joten $a^{i^2-1} = e$. Koska lisäksi $\operatorname{ord}(a) = p$, niin lauseen 1.38 perusteella $p \mid (i^2 - 1)$. Näin ollen $p \mid (i-1)$ tai $p \mid (i+1)$.

Oletetaan, että $p \mid (i-1)$, jolloin $i - 1 = 0$, sillä $i < p$. Siis $i = 1$ ja $bab = a$, eli $ab = ba$. Edelleen lauseiden 3.17 ja 3.29 nojalla

$$|\langle ab \rangle| = \operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b) = 2p = |G|,$$

joten $\langle ab \rangle = G$. Siis G on syklinen ryhmä.

Oletetaan sitten, että $p \mid (i+1)$. Tällöin $i + 1 = mp$ jollakin $m \in \mathbb{N}$. Nyt $mp = i + 1 < p + 1$, joten $m = 0$ tai $m = 1$. Jos $m = 0$, niin $i = -1$ ja jos $m = 1$, niin $i = p - 1$. Koska $a^{p-1} = a^{-1}$, niin tästä seuraa jokatapauksessa, että $bab = a^{-1}$. Täten $ba = a^{-1}b$. Lisäksi $\operatorname{ord}(a) = p$, $\operatorname{ord}(b) = 2$ ja selvästi $\langle a, b \rangle = G$. Ryhmä G on siis diedriryhmä. □

Osoitetaan vielä tulos, joka luokittelee täsmällisesti sellaiset ryhmät joiden kertaluku on alkuluvun neliö.[3]

Lause 7.10. *Olkoon G ryhmä, jonka kertaluku on p^2, missä p on alkuluku. Tällöin $G \cong \mathbb{Z}_{p^2}$ tai $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

Todistus. Seurauksen 6.10 perusteella tiedetään jo, että G on Abelin ryhmä. Oletetaan ensin, että ryhmällä G on alkio g, jonka kertaluku on p^2. Tällöin $|\langle g \rangle| = \operatorname{ord}(g) = p^2 = |G|$, joten $G = \langle g \rangle$, jolloin G on syklinen, ja siis lauseen 4.3 perusteella $G \cong \mathbb{Z}_{p^2}$.

Oletetaan sitten, että ryhmällä G ei ole alkiota, jonka kertaluku on p^2. Tällöin seurauksen 3.25 nojalla $\operatorname{ord}(g) = p$ kaikilla $g \in G \setminus \{e\}$. Olkoon $e \neq h \in G$. Merkitään $H = \langle h \rangle$. Valitaan lisäksi $k \in G \setminus H$, ja merkitään $K = \langle k \rangle$. Nyt lauseen 6.11 nojalla $H, K \trianglelefteq G$. Nyt $H \cap K < K$, joten Lagrangen lauseen perusteella $H \cap K = \{e\}$. Edelleen tulokaavan nojalla

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2 = |G|,$$

joten $G = HK$. Nyt lauseiden 4.3 ja 4.19 perusteella

$$G = HK \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Lisäksi $\mathbb{Z}_{p^2} \ncong \mathbb{Z}_p \times \mathbb{Z}_p$, sillä ryhmällä $\mathbb{Z}_{p^2}$ on alkio, jonka kertaluku on p^2, mutta ryhmällä $\mathbb{Z}_p \times \mathbb{Z}_p$ ei ole. □

[3]Lausetta 7.10 yleisempää tulosta kutsutaan *äärellisten Abelin ryhmien peruslauseeksi* (the fundamental theorem of finite Abelian groups), jonka mukaan jokainen äärellinen Abelin ryhmä voidaan esittää syklisten p-ryhmien karteesisena tulona. [11, s. 251]

Pyritään seuraavaksi luokittelemaan kaikki ryhmät kertaluvuilla yhdestä kymmeneen. Tutkitaan siis, kuinka monta isomorfiaa vaille erilaista ryhmää kunkin kertaluvun omaavalla ryhmällä on.

Esimerkki 7.3 (vrt. [6, s. 1–2] ja [11, s. 215–216])**.** Olkoon G äärellinen ryhmä kertaluvulla n. Jos $n = 1$, niin $G = \{e\}$, jolloin G on triviaalisti syklinen. Jos $n = 2, 3, 5$ tai 7, niin ryhmän G kertaluku on alkuluku, jolloin G on syklinen ryhmä. Edelleen, jos $n = 4$, niin lauseen 7.10 perusteella $G \cong \mathbb{Z}_4$ tai $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Vastaavasti, jos $n = 9$, niin $G \cong \mathbb{Z}_9$ tai $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Jos taas $n = 6$, niin lauseen 7.9 nojalla G on isomorfinen joko ryhmän $\mathbb{Z}_6$ tai ryhmän $D_3 \cong S_3$ kanssa. Ja tapaus $n = 10$ menee vastaavasti: $G \cong Z_{10}$ tai $G \cong D_5$. Jäljelle jää siis tarkasteltavaksi tapaus $n = 8$.

Olkoon siis $n = 8 = 2^3$. Ensin havaitaan, että jos ryhmällä G on olemassa alkio a, jonka kertaluku on 8, niin $|\langle a\rangle| = \text{ord}(a) = 8$, jolloin G on syklinen ryhmä, ja siis myös vaihdannainen. Tällöin $G \cong \mathbb{Z}_8$. Tästä edespäin voidaan siis olettaa, että ryhmällä G ei ole alkiota, jonka kertaluku on 8. Tarkastelu jakaantuu kahtia nyt sen perusteella, tarkastellaanko ryhmää G Abelin ryhmänä.

Oletetaan ensin, että G ei ole vaihdannainen, jolloin G ei myöskään ole syklinen. Oletetaan nyt, että ryhmällä G ei ole alkiota, jonka kertaluku on 4. Tällöin itse asiassa seurauksen 3.25 perusteella ryhmän G kaikki alkiot, neutraalialkiota lukuun ottamatta, ovat kertalukua 2. Tällöin $g^2 = e$ kaikilla $g \in G$. Olkoot $x, y \in G$. Nyt $(xy)^2 = e$, joten $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Ryhmä G on näin ollen vaihdannainen, mikä on ristiriita. Ryhmällä G on siis olemassa sellainen alkio a, jonka kertaluku on 4. Olkoon $H = \langle a\rangle$, jolloin $|H| = |\langle a\rangle| = \text{ord}(a) = 4$. Täten lauseen 6.11 nojalla $H \trianglelefteq G$. Olkoon $b \in G \setminus H$. Nyt siis $(G : H) = 2$, $G/H = \{H, Hb\}$, $G = H \cup Hb$ ja $H \cap Hb = \emptyset$. Koska lisäksi $|G| = 8$, niin

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\} = \langle a, b\rangle.$$

Tarkastellaan nyt aliryhmän H alkiota bab^{-1} ($bab^{-1} \in H$, sillä $H \trianglelefteq G$). Nyt siis $bab^{-1} = a^i$ missä $i \in \{1, 2, 3, 4\}$. Alkiota b vastaa sisäinen automorfismi f_b, joka säilyttää kertaluvut, jolloin $\text{ord}(bab^{-1}) = \text{ord}(f_b(a)) = \text{ord}(a)$. Siis bab^{-1} on a tai a^3. Jos se olisi a, niin pätisi $ab = ba$, mistä seuraisi ryhmän G vaihdannaisuus, mikä on ristiriita. Täten on oltava $bab^{-1} = a^3$. Jos pätisi $b^2 \notin H$, niin $b^2 \in Hb$, joten $b^2 = hb$ jollakin $h \in H$. Silloin $b = h \in H$, mikä on ristiriita. Siis $b^2 \in H$. Tiedetään, että alkion b kertaluku on joko 2 tai 4. Tarkastellaan nämä kaksi tapausta erikseen.

1) Oletetaan, että $\text{ord}(b) = 2$. Lisäksi pätee, että $\text{ord}(a) = 4$, $ba = a^{-1}b$ ja G on alkioiden a ja b virittämä. Täten $G \cong D_4$.

2) Oletetaan, että $\text{ord}(b) = 4$. Nyt $b^2 \in H$, joten $b^2 = a^i$ jollakin $i \in \{1, 2, 3, 4\}$. Tapaus $b^2 = e$ on ristiriidassa alkion b kertaluvun kanssa. On lisäksi helppoa osoittaa, että jos $b^2 = a$ tai $b^2 = a^3$, niin $\text{ord}(b) = 8$, mikä on ristiriita. Siis $b^2 = a^2$. Näin ollen G on alkioiden a ja b virittämä ryhmä niin, että $\text{ord}(a) = 4$, $a^2 = b^2$ ja $ba = a^{-1}b$. Tästä seuraakin, että G on itseasiassa isomorfinen kvaternaariryhmän[4] Q_8 kanssa.

[4]Kvaternaariryhmä Q_8 voidaan määritellä vastaavalla tavalla kuin diedriryhmä. Tarkempaa tietoa kvaternaariryhmästä voi katsoa kirjallisuudesta, esim. [11, s. 169].

Olkoon ryhmä G sitten Abelin ryhmä. Tarkastellaan jälleen kahta eri tapausta: joko ryhmällä on alkio, jonka kertaluku on 4 tai sillä ei ole tällaista alkiota.

1) Olkoon a ryhmän G alkio, jolla on kertaluku 4. Merkitään $H = \langle a \rangle$. Osoitetaan nyt, että ryhmällä G on olemassa sellainen alkio, joka ei kuulu aliryhmään H ja jonka kertaluku on 2. Olkoon $b \in G \setminus H$. Täysin vastaavasti kuin aiemmin, voidaan todeta, että

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\} = \langle a, b \rangle,$$

ja $b^2 \in H$. Nyt siis $b^2 = a^i$, missä $i \in \{1, 2, 3, 4\}$. Tapaukset $b^2 = a$ ja $b^2 = a^3$ johtavat ristiriitaan, kuten edellä. Jos taas $b^2 = e$, niin $\operatorname{ord}(b) = 2$, joten itse b on haluttu alkio. Oletetaan vielä, että $b^2 = a^2$. Tällöin ryhmän G vaihdannaisuudesta seuraa, että

$$(ab)^2 = (ab)(ab) = a^2b^2 = a^4 = e,$$

joten $ab \in G \setminus H$ ja $\operatorname{ord}(ab) = 2$. Ryhmällä G on siis joka tapauksessa olemassa tällainen alkio, olkoon se nyt g. Olkoon $K = \langle g \rangle$. Nyt selvästi $H \cap K = \{e\}$ (jos näin ei olisi, pätisi $b \in H$) ja $K, H \trianglelefteq G$, sillä G on Abelin ryhmä. Lisäksi tulokaavan perusteella

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{4 \cdot 2}{1} = 8 = |G|,$$

joten $G = HK$. Näin ollen lauseiden 4.3 ja 4.19 perusteella

$$G \cong H \times K \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

2) Oletetaan sitten, että ryhmällä G ei ole olemassa alkiota kertaluvulla 4. Tällöin siis $\operatorname{ord}(g) = 2$ kaikilla $g \in G \setminus \{e\}$. Tarkastellaan ryhmän G eri alkioita a ja b ($a, b \neq e$). Merkitään $H = \langle a \rangle$ ja $K = \langle b \rangle$. Nyt selvästi $H \cap K = \{e\}$, $H, K \trianglelefteq G$ ja

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{2 \cdot 2}{1} = 4.$$

On toki myös olemassa alkio $c \in G \setminus \{e, a, b, ab\}$, sillä $|G| = 8$. Merkitään $L = \langle c \rangle$. Edelleen pätee, että $(HK) \cap L = \{e\}$ ja $HK \trianglelefteq G$, sillä G on vaihdannainen. Jälleen tulokaavasta saadaan, että

$$|HKL| = \frac{|HK|\,|L|}{|(HK) \cap L|} = \frac{4 \cdot 2}{1} = 8 = |G|,$$

joten $HKL = G$. Siis lauseiden 4.3 ja 4.19 nojalla

$$G = (HK)L \cong (HK) \times L \cong H \times K \times L \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Vielä on hyvä todeta, että ryhmällä $\mathbb{Z}_8$ on alkio, jonka kertaluku 8, mutta ryhmillä $\mathbb{Z}_4 \times \mathbb{Z}_2$ ja $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ei ole. Lisäksi ryhmällä $\mathbb{Z}_4 \times \mathbb{Z}_2$ on alkio kertaluvulla 4, jota taas ei ole ryhmällä $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Täten lauseen 4.5 kohdan g) perusteella nämä kolme Abelin ryhmää eivät ole keskenään isomorfisia. Näin ollen on olemassa isomorfiaa vaille täsmälleen 5 ryhmää, joiden kertaluku on 8.

Esitetään vielä tästä esimerkistä tiivistettynä taulukko, jossa näkyvät kaikki isomorfiaa vaille erilaiset ryhmät tarkastelluilla kertaluvuilla.

Taulukko 7.2: Ryhmät luokiteltuina kertaluvuilla 1–10.

Ryhmän kertaluku	Ryhmien lukumäärä	Ryhmät
1	1	$\{e\} = \mathbb{Z}_1$
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6, S_3$
7	1	$\mathbb{Z}_7$
8	5	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, (\mathbb{Z}_2)^3, D_4, Q_8$
9	2	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$
10	2	$\mathbb{Z}_{10}, D_5$

Esimerkissä 7.3 ryhmien luokitteluun ei tarvittu lainkaan Sylowin lauseita. Tarkastellaan vielä ryhmää G, jonka kertaluku on pqr, missä p, q ja r ovat eri alkulukuja. Onko mahdollista osoittaa, että G olisi syklinen joillakin ehdoilla? Havaitaan, että ryhmän G syklisyys voidaan todellakin osoittaa tietyin ehdoin ja todistuksessa tullaan tarvitsemaan myös Sylowin lauseita. Yleisesti tämä ryhmä ei toki ole syklinen, sillä voidaan osoittaa, että ryhmä kertaluvulla $70 = 2 \cdot 5 \cdot 7$ voi olla isomorfinen diedriryhmän D_{35} kanssa (ks. [11, s. 613]). Todistetaan ensin kaksi lemmaa, joita tarvitaan ryhmän G syklisyyden osoittamisessa.

Lemma 7.11. $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$, *missä* $n \geq 2$ *on kokonaisluku.*

Todistus (vrt. [8, s. 3]). Olkoon x ryhmän $\mathbb{Z}_n$ virittäjä. Olkoon $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ homomorfismi. Nyt on olemassa yksikäsitteinen $a \in \{1, \ldots, n\}$ niin, että $f(x) = x^a$. Jos näin ei nimittäin olisi, niin pätisi myös $f(x) = x^b$ jollakin $b \neq a$, jolloin $x^a = x^b$, ja edelleen $x^{a-b} = e$, mikä on ristiriidassa sen kanssa, että $\mathrm{ord}(x) = n$. Voidaan siis merkitä, että $f = f_a$ yksikäsitteisellä kokonaisluvulla $a \in \{1, \ldots, n\}$. Tietysti pätee edelleen, että $f_a = f_{a+mn}$ kaikilla $m \in \mathbb{Z}$.

Nyt $\mathrm{syt}(a, n) = 1$, joss $\mathrm{ord}(x^a) = n = \mathrm{ord}(x)$, joss $\langle x^a \rangle = \mathbb{Z}_n = \langle x \rangle$. Edelleen, voidaan osoittaa, että $\mathrm{syt}(a, n) = 1$, jos ja vain jos f_a on isomorfismi. Oletetaan siis, että $\mathrm{syt}(a, n) = 1$. Merkitään $y = x^a$. Nyt siis sekä x että y virittävät ryhmän $\mathbb{Z}_n$. Määritellään kuvaus $f_a\colon \mathbb{Z}_n \to \mathbb{Z}_n$ seuraavasti:

$$f_a(x^i) = y^i \text{ kaikilla } i \in \mathbb{Z}.$$

Näin määriteltynä voidaan helposti osoittaa, että $f_a \in \mathrm{Aut}(\mathbb{Z}_n)$. Lisäksi f_a on yksikäsitteinen. Jos taas f_a on isomorfismi, niin $\mathrm{ord}(x) = \mathrm{ord}(f_a(x)) = \mathrm{ord}(x^a)$, joten $\mathrm{syt}(a, n) = 1$. Tästä seuraa, että voidaan määritellä seuraava bijektiivinen kuvaus ϕ:

$$\phi\colon \mathrm{Aut}(Z_n) \to Z_n^*, \phi(f_a) = \overline{a}, \text{ kun } a \in \mathbb{Z} \text{ ja } \mathrm{syt}(a, n) = 1.$$

Osoitetaan vielä, että ϕ on homomorfismi. Olkoot $f_a, f_b \in \mathrm{Aut}(Z_n)$. Tällöin

$$(f_a \circ f_b)(x) = f_a(x^b) = (x^b)^a = x^{ab} = f_{ab}(x),$$

joten

$$\phi(f_a \circ f_b) = \phi(f_{ab}) = \overline{ab} = \overline{a}\overline{b} = \phi(f_a)\phi(f_b).$$

Siis $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$. □

Lemma 7.12. *Olkoon G ryhmä niin, että $G/Z(G)$ on syklinen. Tällöin G on Abelin ryhmä.*

Todistus. Olkoon $xZ(G)$ tekijäryhmän $G/Z(G)$ virittäjä. Olkoon $g \in G$. Nyt siis

$$x^m Z(G) = (xZ(G))^m = gZ(G) \text{ jollakin } m \in \mathbb{Z}.$$

Täten $x^{-m}g \in Z(G)$, jolloin $x^{-m}g = z$, missä $z \in Z(G)$. Siis $g = x^m z$.

Jokainen $g \in G$ voidaan esittää täten muodossa $g = x^m z$, missä $m \in \mathbb{Z}$ ja $z \in Z(G)$. Olkoot $g_1, g_2 \in G$. Tällöin on olemassa sellaiset $m_1, m_2 \in \mathbb{Z}$ ja $z_1, z_2 \in Z(G)$, että $g_1 = x^{m_1} z_1$ ja $g_2 = x^{m_2} z_2$. On rutiininomaista osoittaa, että $g_1 g_2 = g_2 g_1$. Siis G on Abelin ryhmä. □

Nyt voidaan osoittaa, että ryhmä kertaluvulla pqr on syklinen, kun alkuluvuille p, q ja r pätee tietyt ehdot.

Lause 7.13. *Olkoon G ryhmä, jonka kertaluku on pqr, missä p, q ja r ovat eri alkulukuja niin, että $p > q > r$. Oletetaan, että $q \nmid p-1$, $r \nmid p-1$ ja $r \nmid q-1$. Tällöin G on syklinen ryhmä.*[5]

Todistus (vrt. [1, s. 73–75] ja [11, s. 219]). Osoitetaan ensin, että ryhmällä G on joko normaali Sylowin p- tai q-aliryhmä. Oletetaan vastoin tätä, että ryhmällä G ei ole normaaleita Sylowin p- ja q-aliryhmiä. Tällöin seurauksen 6.20 perusteella $n_p > 1$ ja $n_q > 1$. Täysin vastaavalla tavalla kuten lauseen 7.5 todistuksessa, voidaan päätellä nyt, että

$$\begin{aligned} pqr = |G| &\geq 1(r-1) + p(q-1) + qr(p-1) = pq - p - qr + r - 1 + pqr \\ &= (p-r)(q-1) - 1 + pqr > pqr, \end{aligned}$$

sillä $(p-r)(q-1) \geq 2$. Tämä on ristiriita. Siis ryhmällä G on joko normaali Sylowin p- tai q-aliryhmä.

Oletetaan, että ryhmällä G on normaali Sylowin p-aliryhmä, joka on tietysti myös yksikäsitteinen ja syklinen. Olkoon P tämä Sylowin p-aliryhmä. Siis $N(P) = G$ ja lemman 7.11 nojalla

$$|\mathrm{Aut}(P)| = |\mathrm{Aut}(\mathbb{Z}_p)| = |\mathbb{Z}_p^*| = p - 1.$$

[5] Burnley (ks. [1]) on todistanut saman tuloksen, mutta yleisimmillä menetelmillä. Malik ym. (ks. [11]) ovat puolestaan käsitelleet ryhmää kertaluvulla 455 yksittäistapauksena syklisestä ryhmästä.

Edelleen lauseen 5.48 perusteella $C(P) \trianglelefteq G$ ja $G/C(P)$ on isomorfinen ryhmän $\mathrm{Aut}(P)$ aliryhmän kanssa. Merkitään $n = (G : C(P))$. Täten Lagrangen lauseen perusteella $n \mid p-1$. Lisäksi toki pätee myös, että $n \mid pqr$. Näistä kahdesta, yhdessä oletusten $q \nmid p-1$ ja $r \nmid p-1$ kanssa, seuraa, että $n = 1$. Siis $G = C(P)$, joten selvästi $P \leqslant Z(G)$. Täten Lagrangen lauseen perusteella $|Z(G)| = p, pq, pr$ tai pqr, jolloin

$$|G/Z(G)| = qr, q, r \text{ tai } 1.$$

Nyt lisäksi $r \nmid q-1$, joten lauseen 7.8 nojalla $G/Z(G)$ on syklinen, jolloin lemman 7.12 perusteella G on Abelin ryhmä.

Lauseen 3.34 perusteella ryhmän G kaikki aliryhmät ovat siis normaaleja, joten seurauksen 6.20 nojalla ryhmällä G on myös yksikäsitteiset Sylowin q- ja r-aliryhmät Q ja R, jotka ovat myös syklisiä. Selvästi $PQ \trianglelefteq G$ ja $P \cap Q = \{e\}$. Siis tulokaavan perusteella

$$|PQ| = \frac{|P|\,|Q|}{|P \cap Q|} = pq.$$

Edelleen $(PQ) \cap R = \{e\}$, sillä ryhmällä R on neutraalialkion lisäksi vain kertaluvulla r olevia alkioita ja ryhmällä PQ ei ole. Siis

$$|PQR| = \frac{|PQ|\,|R|}{|(PQ) \cap R|} = pqr = |G|,$$

joten $G = PQR$. Edelleen lauseen 4.19 perusteella

$$G = (PQ)R \cong PQ \times R \cong P \times Q \times R,$$

ja lauseen 3.31 nojalla $P \times Q \times R$ on syklinen, jolloin myös G on syklinen. Täysin vastaavasti osoitetaan, että G on syklinen, jos ryhmällä G on normaali Sylowin q-aliryhmä. □

Lähteet

[1] Burnley A., *Classification of some groups of order pqr* [verkkodokumentti], 2008 [viitattu 11.10.2017]. URL: http://users.hawknetwork.org/~adam/ClassifyPQR-FINAL.pdf

[2] Conrad K., *Consequences of the Sylow theorems* [verkkodokumentti], Expository papers, University of Connecticut, 2015 [viitattu 9.1.2017]. URL: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/sylowapp.pdf

[3] Conrad K., *More on the Sylow theorems* [verkkodokumentti], Expository papers, University of Connecticut, 2015 [viitattu 10.10.2017]. URL: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/sylowmore.pdf

[4] Conrad K., *The sign of a permutation* [verkkodokumentti], Expository papers, University of Connecticut, 2015 [viitattu 18.4.2016]. URL: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/sign.pdf

[5] Conrad K., *Dihedral groups II* [verkkodokumentti], Expository papers, University of Connecticut, 2015 [viitattu 6.11.2017]. URL: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral2.pdf

[6] Conrad K., *Groups of order p^3* [verkkodokumentti], Expository papers, University of Connecticut, 2015 [viitattu 10.10.2017]. URL: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/groupsp3.pdf

[7] Hella L., *Joukko-oppi*, luentomoniste [verkkodokumentti], 2011 [viitattu 7.4.2016]. URL: http://www.sis.uta.fi/~klkelu/kurssit/joukko-oppi/JO2011.pdf

[8] Ikenaga B., *Automorphism groups* [verkkodokumentti], Millersville University, 2012 [viitattu 10.10.2017]. URL: http://sites.millersville.edu/bikenaga/abstract-algebra-2/automorphism-groups/automorphism-groups.pdf

[9] Judson T. W., *Abstract Algebra: Theory and Applications* [verkkodokumentti], Stephen F. Austin State University, Texas, 2014 [viitattu 18.10.2016]. URL: http://abstract.ups.edu/download/aata-20140815.pdf

[10] Ling G. H. ja Miller G. A., *Proof that there is no Simple Groups whose Order Lies Between 1092 and 2001*. American Journal of Mathematics, Vol. 22, No. 1 (1900), s. 13 – 26.

[11] Malik D. S., Mordeson J. N. ja Sen M. K., *Fundamentals of Abstract Algebra*. United States of America: The McGraw-Hill Companies, Inc., 1997.

[12] Mann K., *Notes on Sylow's theorems* [verkkodokumentti], University of California, 2014 [viitattu 9.1.2017]. URL: https://math.berkeley.edu/~kpmann/SylowNotes.pdf

[13] Marshall H. Jr., *On the Number of Sylow Subgroups in a Finite Group*. Journal of Algebra 7 (1967), s. 363 – 371.

[14] Merikoski J., Virtanen A. ja Koivisto P., *Johdatus diskreettiin matematiikkaan*. Helsinki: WSOY, 2004.

[15] Naik V., *Class equation of a group action* [verkkodokumentti], The Group Properties Wiki, 2009 [viitattu 19.10.2016]. URL: http://groupprops.subwiki.org/wiki/Class_equation_of_a_group_action

[16] Papantonopoulou A., *Algebra Pure & Applied*. United States of America: Prentice-Hall, Inc., 2002.

[17] Proofwiki, *Group Direct Product of Cyclic Groups*, 2017 [viitattu 16.2.2017]. URL: https://proofwiki.org/wiki/Group_Direct_Product_of_Cyclic_Groups

[18] Rose J. S., *A Course on Group Theory*. Cambridge University Press, England: Dover Publication, Inc., 1978.

[19] Scott W. R., *Group Theory*. United States of America: Dover Publications, Inc., 1987.

[20] Sylow P. L. M., *Théorèms sur les groupes de substitution*, Mathematische Annalen 5 (1872), s. 584–594.

[21] Tampereen yliopisto, *Algebra 1*, opintomoniste [verkkodokumentti], 2012 [viitattu 15.2.2017]. URL: http://www.uta.fi/sis/mtt/mttma3/algebra2012.pdf

[22] University of St Andrews, *Joseph-Louis Lagrange*, School of Mathematics and Statistics, Scotland [verkkodokumentti], 1999 [viitattu 6.11.2017]. URL: http://www-history.mcs.st-and.ac.uk/Biographies/Lagrange.html