
TAMPEREEN YLIOPISTO
Matematiikan pro gradu -työ

Seppo Janhonen

Ryhmäteoriaa

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Kesäkuu 2001

Hänessä kaikki viisauden ja tiedon aarteet ovat kätkeytyinä.

Vrt. Paavalin kirje kolossalaisille 2:2-3.

Sisältö

Käytetyt merkinnät

Johdanto

1 Ryhmän määrittely	2
2 Aliryhmät ja normaalit aliryhmät	5
2.1 Aliryhmien määrittely	5
2.2 Sykliset ryhmät	6
2.3 Lagrangen lause	10
2.4 Normaalit aliryhmät ja tekijäryhmät	12
2.5 Aliryhmän määräämä kongruenssirelaatio	15
3 Ryhmähomomorfismit ja -isomorfismit	16
3.1 Ryhmähomomorfismit	16
3.2 Isomorfia- ja vastaavuuslauseet	20
4 Ryhmän vaikutukset	28
5 Ryhmien ulkoiset ja sisäiset suorat tulot	33
6 Sylowin lauseet	35
6.1 Konjugaattiluokat	35
6.2 Cauchyn lause ja p -ryhmät	38
6.3 Sylowin lauseet	40
7 Ratkeavat ja nilpotentit ryhmät	44
7.1 Ratkeavat ryhmät	44
7.2 Nilpotentit ryhmät	49
8 Loppukommentit	52
Kirjallisuus	53

Käytetyt merkinnät

\in	kuuluu joukkoon
\notin	ei kuulu joukkoon
\subseteq	osajoukko
\subset	aito osajoukko
\supseteq	sisältää
\supset	sisältää aidosti
(a, b)	järjestetty pari
\mathbf{N}	luonnollisten lukujen joukko
\mathbf{Z}	kokonaislukujen joukko
\mathbf{Z}^+	positiivisten kokonaislukujen joukko
\mathbf{Q}	rationaalilukujen joukko
\mathbf{R}	reaalilukujen joukko
\mathbf{C}	kompleksilukujen joukko
\cup	unioni
\cap	leikkaus
$n!$	luvun n kertoma
$p \mid m$	p jakaa luvun m
$p \nmid m$	p ei jaa lukua m
$\text{sy}(a, b)$	lukujen a ja b suurin yhteinen tekijä
\equiv_n	kongruenssi modulo n
$a \equiv b \pmod{n}$	a on kongruentti luvun b kanssa modulo n
$f : A \rightarrow B$	kuvaus f joukolta A joukkoon B
$f(x)$	alkion x kuva kuvauksessa f
$g \circ f$	yhdistetty kuvaus
f^{-1}	kuvauksen f käänteiskuvaus
$f^{-1}(x)$	alkion x alkukuva kuvauksessa f
I_n	$I_n = \{1, 2, \dots, n\}$
$ G $	ryhmän G kertaluku eli alkioiden lukumäärä
$o(a)$	alkion a kertaluku
\mathbf{Z}_n	jäännösluokkien joukko modulo n
$Z(G)$	ryhmän G keskus
G/H	normaalin aliryhmän H määräämä ryhmän G tekijäryhmä
aH, Ha	alkion a määräämä aliryhmän H vasen ja oikea sivuluokka
$[G : H]$	aliryhmän H indeksi ryhmässä G
S_n	n alkiota sisältävä symmetrinen ryhmä
A_n	n alkiota sisältävä alternoiva ryhmä
$\langle S \rangle$	joukon S generoima aliryhmä
$\langle a \rangle$	alkion a generoima aliryhmä
$N(H)$	aliryhmän H normalisoija
$C(a)$	alkion a normalisoija
$\text{Ker } f$	kuvauksen f ydin
\simeq	isomorfia
G_a	alkion a stabiloija eli isotropiaryhmä
$C_l(a)$	alkion a konjugaattiluokka
\square	todistuksen päätös

Johdanto

Algebrassa tutkitaan *algebrallisia struktuureja*: joukkoja, joissa on määritelty yksi tai useampia *laskutoimituksia*. Laskutoimituksia säätelevät *laskulait*, aksioomat. Sen mukaan millaisia laskutoimitukset ovat, saadaan erilaisia algebrallisia struktuureja, kuten esimerkiksi *monoidit*, *ryhmät*, *renkaat*, *kokonaisalueet*, *kunnat* ja *lineaariavaruudet* (ks. [8], s. 46).

Tämän tutkielman aihe ovat ryhmät. Esityksessä kuvataan ryhmien rakenteita ja ominaisuuksia. *Ryhmäteoria* on syntynyt lähinnä neljän tutkimusalan piirissä: klassinen algebra, lukuteoria, geometria ja analyysi (ks. [7], s. 57).

Kappaleessa 1 esitetään käsitteitä, jotka tarvitaan aiheen varsinaisen käsittelyn pohjaksi. Näihin kuuluvat esimerkiksi *algebrallinen struktuuri* ja *ryhmä* perusominaisuuksineen. Kappaleessa 2 tarkastellaan *aliryhmiä* ja niihin liittyviä käsitteitä. *Lagrange'n lausetta* voidaan pitää työn keskeisimpänä lauseena. Hyvin tärkeä on myös *normaali* aliryhmä, jonka avulla esimerkiksi määritellään *tekijäryhmä*. Tekijäryhmällä on puolestaan monia hyödyllisiä ominaisuuksia. Kappaleessa 3 käsitellään *ryhmähomomorfismeja* ja *-isomorfismeja*, jotka ovat eräänlaisia ryhmien välisiä kuvauksia. Niiden avulla voidaan selvittää monia ryhmien rakenteisiin liittyviä asioita.

Työn painopiste on *äärellisten* ryhmien tarkastelussa. Näiden ryhmien analysoinnissa tarvitaan usein keinoja, joilla voidaan määrittää esimerkiksi alkioiden lukumääriä. Kappaleessa 4 käsiteltävät *ryhmän vaikutukset* tarjoavat tähän käyttökelpoisen menetelmän. *Ryhmien suoran tulon* avulla pienemmistä ryhmistä voidaan muodostaa suurempia tai suurempi voidaan ilmaista aitojen aliryhmiensä eräänlaisena yhdistelmänä. Tätä tarkastellaan kappaleessa 5. Kappaleen 6 pääaiheena ovat *Sylowin lauseet*, joiden avulla saadaan hyödyllistä tietoa äärellisten ryhmien aliryhmien olemassaolosta ja lukumääristä. *Ratkeavien ja nilpotenttien ryhmien* yhteydessä tarkastellaan eräänlaisia aliryhmien ketjuja kappaleessa 7.

Kappaleessa 8 esitetään vielä yhteenveto työssä formuloiduista ja todistetuista lauseista, havainnollistavista esimerkeistä sekä kootaan yhteen päälähteestä [7] (Malik, D. S. & Mordeson, J. N. & Sen, M. K., Fundamentals of Abstract Algebra) löydetty virheet ja epäjohdonmukaisuudet.

Aiheiden käsittelyjärjestys ja käytettävät merkinnät noudattavat pääosin lähteen [7] esitystapaa. Esitystä täydentävät ja havainnollistavat lisäykset ovat pääosin tässä lähteessä esitettyjä ratkaisemattomia tehtäviä. Nämä tehtävät on työssä useimmiten määritelty esimerkeiksi riippumatta siitä, onko kyseessä yleistä mielenkiintoa omaavan algebrallisen väitteen (lauseen) todistus vai yksittäinen erikoistapaus.

1 Ryhmän määrittely

Tässä kappaleessa esitettävät asiat luovat pohjaa varsinaiselle aihepiirin käsittelylle.

Määritelmä 1.1 *Olkoot A ja B epätyhjiä joukkoja. Relaatiota f joukosta A joukkoon B kutsutaan **funktioksi (kuvaukseksi)** joukolta A joukkoon B , jos*

- (i) $\mathcal{D}(f) = A$ eli kuvauksen määrittelyjoukko on sama kuin lähtöjoukko A ja
- (ii) aina, kun $(x, y), (x', y') \in f$, niin ehdosta $x = x'$ seuraa, että $y = y'$.

*Kun relaatio f täyttää ehdon (ii), niin f on **hyvin määritelty eli yksiarvoinen (single-valued)**. (Vrt. [7], s. 40.)*

Määritelmä 1.2 *Olkoon S epätyhjä joukko. Silloin **laskutoimitus (binäärioperaatio)** joukossa S on kuvaus $S \times S \rightarrow S$.*

Merkitään laskutoimitusta symbolilla $*$. Laskutoimitus liittyy jokaiseen järjestettyyn pariin $(x, y) \in S \times S$ joukon S erään alkion $x * y$. Nyt siis $x * y \in S$ aina, kun $x, y \in S$. Tavanomaisia laskutoimituksen merkintätapoja ovat myös $x + y, x \cdot y, xy, x \circ y$. Koska laskutoimituksen arvojoukko on joukon S osajoukko, niin sanotaan, että S on **suljettu laskutoimituksen suhteen**.

Määritelmä 1.3 *Joukon S laskutoimitus $*$ on **assosiatiivinen (liitännäinen)**, jos $x*(y*z) = (x*y)*z$ aina, kun $x, y, z \in S$. Laskutoimitus $*$ on **kommutatiivinen (vaihdannainen)**, jos $x*y = y*x$ aina, kun $x, y \in S$.*

Määritelmä 1.4 *Pari $(S, *)$, missä S on epätyhjä joukko ja $*$ siihen liittyvä laskutoimitus, on (yhden laskutoimituksen) **algebraallinen struktuuri**.*

Määritelmä 1.5 Ryhmä *on pari $(G, *)$, missä G on epätyhjä joukko ja $*$ on sellainen joukossa G määritelty laskutoimitus, että seuraavat ominaisuudet ovat voimassa:*

(G1) $a * (b * c) = (a * b) * c$ aina, kun $a, b, c \in G$ (liitäntälaki).

(G2) On olemassa sellainen alkio $e \in G$, että $a * e = a = e * a$ aina, kun $a \in G$ (neutraalialkion olemassaolo).

(G3) Jokaista alkioa $a \in G$ kohti on olemassa sellainen $b \in G$, että $a * b = b * a = e$ (käänteisalkion olemassaolo).

(Ks. [7], s. 58.)

Ryhmä on siis algebraallinen struktuuri, joka täyttää aksioomat G1, G2 ja G3.

Lause 1.1 *Olkoon $(G, *)$ ryhmä.*

(i) *On olemassa sellainen yksikäsitteinen alkio (neutraalialkio) $e \in G$, että $e * a = a = a * e$ aina, kun $a \in G$.*

(ii) *Aina kun $a \in G$, on olemassa sellainen yksikäsitteinen alkio (käänteisalkio) $b \in G$, että $a * b = e = b * a$.*

Todistus. Ks. [7], s. 58-59.

Ryhmän alkion a käänteisalkiota merkitään symbolilla a^{-1} .

Kun laskutoimitus on yhteenlaskunkaltainen, neutraalialkioita sanotaan **nollaalkioksi** ja käänteisalkiota **vasta-alkioksi**; kertolaskunkaltaisen laskutoimituksen yhteydessä neutraalialkioita kutsutaan **ykkösalkioksi**. Tässä työssä tarkastellaan ryhmää useimmiten abstraktilla tasolla siten, ettei laskutoimituksen luonnetta

ole tässä tarkoitettussa mielessä määrätty; näin ollen yleensä käytetään nimityksiä neutraalialkio ja käänteisalkio.

Jos ryhmälle $(G, *)$ pätee ehto $a * b = b * a$ aina, kun $a, b \in G$, niin $(G, *)$ on **kommutatiivinen** ryhmä eli **Abelin ryhmä**. Tällaista ryhmää kutsutaan myös vaihdannaiseksi. Jos $a * b = b * a$, niin sanotaan, että a ja b **kommutoivat**. Ryhmä G on ei-kommutatiivinen, jos se ei ole kommutatiivinen.

Lause 1.2 *Olkoon $(G, *)$ ryhmä.*

(i) $(a^{-1})^{-1} = a$ aina, kun $a \in G$.

(ii) $(a * b)^{-1} = b^{-1} * a^{-1}$ aina, kun $a, b \in G$.

(iii) **(Supistamislaki)** *Olkoot $a, b, c \in G$. Silloin*

$$a * c = b * c \Rightarrow a = b,$$

$$c * a = c * b \Rightarrow a = b.$$

(iv) *Yhtälöillä $a * x = b$ ja $y * a = b$ on yksikäsitteiset ratkaisut x ja y ryhmässä G aina, kun $a, b \in G$.*

Todistus. Ks. [7], s. 62-63.

Määritelmä 1.6 *Olkoon $(G, *)$ ryhmä, $a \in G$ ja $n \in \mathbf{Z}$. Alkion a **potenssi** a^n määritellään kaavoilla*

$$a^0 = e,$$

$$a^n = a * a^{n-1}, \text{ jos } n > 0,$$

$$a^n = (a^{-1})^{-n} = (a^{-n})^{-1}, \text{ jos } n < 0.$$

(Ks. [7], s. 67.)

Jos ryhmän laskutoimitus on yhteenlaskunkaltainen, on mielekkäämpää puhua *monikerrasta* kuin potenssista. Määritelmää 1.6 vastaavat merkinnät ovat tällöin

$$0a = 0,$$

$$na = a + (n - 1)a, \text{ jos } n > 0,$$

$$na = (-n)(-a), \text{ jos } n < 0.$$

Lause 1.3 *Olkoon $(G, *)$ ryhmä ja olkoon $a \in G$. Silloin*

(i) $a^m * a^n = a^{m+n} = a^n * a^m$,

(ii) $(a^m)^n = a^{mn}$

aina, kun $m, n \in \mathbf{Z}$.

Todistus. Todistus potenssin määritelmän ja laskutoimituksen assosiatiivisuuden perusteella (sivuutetaan).

Lause 1.4 *Olkoon $(G, *)$ Abelin ryhmä ja olkoot $a, b \in G$. Silloin*

$(a * b)^n = a^n * b^n$ aina, kun $n \in \mathbf{Z}$.

Todistus. Helppo induktiotodistus sivuutetaan.

Määritelmä 1.7 *Ryhmää $(G, *)$ kutsutaan **äärelliseksi**, jos siinä on äärellinen määrä alkioita. Ryhmän $(G, *)$ **kertaluku** $|G|$ on ryhmän G alkioden lukumäärä. Ryhmä on **ääretön**, jos sen alkioden määrä on ääretön. (Ks. [7], s. 68.)*

Määritelmä 1.8 Olkoon $(G, *)$ ryhmä ja olkoon $a \in G$. Jos on olemassa sellainen positiivinen kokonaisluku n , että $a^n = e$, niin pienintä tämän ehdon täyttävää positiivista kokonaislukua kutsutaan alkion a **kertaluvuksi**. Alkion a kertaluku merkitään symbolilla $o(a)$. Jos sellaista positiivista kokonaislukua ei ole olemassa, niin alkion a kertaluku on ääretön. (Ks. [7], s. 68.)

Esitetään nyt muutamia esimerkkejä.

Esimerkki 1.1 Pari $(\mathbf{Z}, +)$ on Abelin ryhmä. Todistus. Ks. [7], s. 59.

Esimerkki 1.2 Olkoon $n \in \mathbf{Z}^+$ kiinteä. Olkoon \mathbf{Z}_n kaikkien jäännösluokkien joukko $(\text{mod } n)$. Silloin pari $(\mathbf{Z}_n, +_n)$ on Abelin ryhmä, josta käytetään nimeä jäännösluokkaryhmä $(\text{mod } n)$. Todistus. Ks. [7], s. 59-60.

Ryhmä $(\mathbf{Z}, +)$ on ääretön. Ryhmän $(\mathbf{Z}_n, +_n)$ kertaluku on n , joten tämä ryhmä on äärellinen. Esimerkkien 1.1 ja 1.2 ryhmiin tullaan viittaamaan tämän työn useassa kohdassa.

Esimerkki 1.3 Parit $(\mathbf{Q}, +), (\mathbf{R}, +), (\mathbf{C}, +), (\mathbf{Q} \setminus \{0\}, \cdot), (\mathbf{R} \setminus \{0\}, \cdot)$ ja $(\mathbf{C} \setminus \{0\}, \cdot)$ ovat äärettömiä Abelin ryhmiä. (Todistukset sivuutetaan.)

Esimerkki 1.4 Pari (\mathbf{Z}, \cdot) ei ole ryhmä, sillä esimerkiksi alkiolla 6 ei ole käänteisalkiota, joka kuuluu joukkoon \mathbf{Z} .

Määritellään seuraavaksi symmetrinen ryhmä, jolle löytyy myös geometrinen havainnollistus.

Määritelmä 1.9 Olkoon X epätyhjä joukko. Joukon X permutaatio π on joukon X bijektio itselleen. (Ks. [7], s. 83.)

Voidaan osoittaa, että äärellisen joukon X permutaatioita on yhteensä $n!$ kappaletta, missä n on joukon X alkioiden lukumäärä.

Määritelmä 1.10 Ryhmää $(G, *)$ kutsutaan epätyhjään joukkoon X liittyväksi **permutaatioryhmäksi**, jos ryhmän G alkiot ovat joukon X permutaatioita ja laskutoimitus $*$ on kuvausten yhdistäminen. (Ks. [7], s. 83.)

Olkoon $I_n = \{1, 2, \dots, n\}$, $n \geq 1$. Olkoon π jokin joukon I_n permutaatio. Silloin $\pi = \{(1, \pi(1)), (2, \pi(2)), \dots, (n, \pi(n))\}$. Tämä voidaan kirjoittaa myös kaksirivisellä merkintätavalla muodossa

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}.$$

Lause 1.5 Olkoon S_n joukon I_n , $n \geq 1$, kaikkien permutaatioiden joukko ja \circ kuvausten yhdistäminen. Silloin (S_n, \circ) on ryhmä aina, kun $n \geq 1$.

Todistus. Ks. [7], s. 86-87.

Ryhmää (S_n, \circ) kutsutaan **symmetriseksi ryhmäksi**. Nyt S_n on selvästi permutaatioryhmä.

Ryhmällä S_n on mielenkiintoinen geometrinen analogia. Sen alkiot vastaavat niitä tapoja, joilla kaksi säännöllistä n -kulmiota voidaan asettaa päällekkäin siten, että kulmiot peittävät toisensa. Siksi ryhmää S_n sanotaan myös **säännöllisen n -kulmion symmetrioiden ryhmäksi** (group of symmetries of the regular n -gon). Tästä ryhmästä käytetään usein merkintää D_n . (Ks. [3], s. 44-45.)

Olkoon nyt A_n joukon S_n kaikkien *parillisten* permutaatioiden joukko, $n \geq 2$.

Lause 1.6 *Pari* (A_n, \circ) on ryhmä, jota kutsutaan **alternoivaksi ryhmäksi**, kun $n \geq 2$.

Todistus. Ks. [7], s. 94.

2 Aliryhmät ja normaalit aliryhmät

2.1 Aliryhmien määrittely

Määritelmä 2.1 *Olkoon* $(G, *)$ *ryhmä ja* H *joukon* G *epätyhjä osajoukko. Silloin* *algebraallinen struktuuri* $(H, *)$ *on ryhmän* $(G, *)$ **aliryhmä**, jos $(H, *)$ on ryhmä.

Jos $(G, *)$ on ryhmä, niin ryhmiä $(\{e\}, *)$ ja $(G, *)$ sanotaan sen *triviaaleiksi* aliryhmiksi.

Tästä lähtien ryhmä $(G, *)$ merkitään lyhyesti symbolilla G , jos väärinkäsityksen vaaraa ei ole. Laskutoimitus $a * b$ merkitään vastaavasti muodossa ab .

Lause 2.1 *Olkoon* G *ryhmä ja* H *joukon* G *epätyhjä osajoukko. Silloin* H *on ryhmän* G *aliryhmä, jos ja vain jos* $ab^{-1} \in H$ *aina, kun* $a, b \in H$.

Todistus. (Vrt. [7], s. 100.) Oletetaan, että H on ryhmän G aliryhmä. Osoitetaan, että $ab^{-1} \in H$ aina, kun $a, b \in H$. Olkoot $a, b \in H$. Oletuksesta seuraa, että $b^{-1} \in H$. Koska H on suljettu ryhmän laskutoimituksen suhteen, niin nyt $ab^{-1} \in H$.

Oletetaan kääntäen, että H on joukon G sellainen epätyhjä osajoukko, että ehdosta $a, b \in H$ seuraa, että $ab^{-1} \in H$. Osoitetaan, että H on ryhmän G aliryhmä. Olkoot $a, b \in H$. Oletuksesta seuraa, että $aa^{-1} = e \in H$, toisin sanoen H sisältää neutraalialkion. Oletuksesta seuraa myös, että $b^{-1} = eb^{-1} \in H$ aina, kun $b \in H$. Jokaisella joukon H alkion a on siis käänteisalkio joukossa H . Näin ollen $ab = a(b^{-1})^{-1} \in H$, joten H on suljettu ryhmän G laskutoimituksen suhteen. Selvästi liitântälaki on voimassa joukossa H . Näin on todettu, että H toteuttaa ryhmän aksioomat, joten H on ryhmä. Siten H on ryhmän G aliryhmä. \square

Lause 2.2 *Olkoon* G *ryhmä ja* $Z(G) = \{b \in G \mid ab = ba \text{ aina, kun } a \in G\}$. *Silloin* $Z(G)$ *on ryhmän* G *kommutatiivinen aliryhmä, ja sitä kutsutaan ryhmän* G **keskukseksi**.

Todistus. Ks. [7], s. 101.

Lause 2.3 *Olkoon* G *ryhmä ja* $\{H_\alpha \mid \alpha \in I\}$ *mielivaltainen epätyhjä ryhmän* G *aliryhmien kokoelma. Silloin* $\bigcap_{\alpha \in I} H_\alpha$ *on ryhmän* G *aliryhmä*.

Todistus. Ks. [7], s. 101.

Lause 2.4 *Olkoon* S *ryhmän* G *epätyhjä osajoukko. Silloin* S *generoi ryhmän* G *aliryhmän* $\langle S \rangle$, *joka on muotoa*

$$\langle S \rangle = \{s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n} \mid s_i \in S, e_i = \pm 1, i = 1, 2, \dots, n; n = 1, 2, \dots\}.$$

Todistus. Ks. [7], s. 102.

Joukko S generoi ryhmän G aliryhmän siinä mielessä, että $\langle S \rangle$ sisältää joukon S alkioiden ja niiden käänteisalkioiden tulot. Aliryhmä $\langle S \rangle$ on pienin joukon S alkioita sisältävä aliryhmä.

Määritelmä 2.2 Olkoot H ja K ryhmän G epätyhjiä osajoukkoja. Joukkojen H ja K tulolla tarkoitetaan joukkoa $HK = \{hk \mid h \in H, k \in K\}$.

Lause 2.5 Olkoot H ja K ryhmän G aliryhmiä. Silloin HK on ryhmän G aliryhmä, jos ja vain jos $HK = KH$.

Todistus. Ks. [7], s. 103-104.

Esimerkki 2.1 Osoitetaan, että ryhmä ei voi olla kahden aidon aliryhmänsä yhdiste.

Ratkaisu. Olkoon G ryhmä, ja olkoot H ja K ryhmän G aitoja aliryhmiä, $H \neq G \neq K$. Jos $H = K$, niin ryhmällä G on vain yksi aito aliryhmä. Oletetaan siksi, että $H \neq K$. Tehdään nyt vasta oletus, että $G = H \cup K$. Valitaan sellaiset mielivaltaiset alkio $h \in H$, $k \in K$, että $h \notin K$ ja $k \notin H$. Selvästi tällaiset h ja k ovat olemassa. Koska nyt $hk \in G$, niin vasta oletuksen nojalla $hk \in H$ tai $hk \in K$. Oletetaan yleisyyden kärsimättä, että $hk \in H$. Tällöin on olemassa sellainen $h' \in H$, että $h' = hk$. Tästä seuraa, että $k = h^{-1}h'$. Nyt $h^{-1} \in H$ ja $h' \in H$, joten myös $h^{-1}h' \in H$, sillä H on suljettu laskutoimituksen suhteen. Näin todetaan, että $k \in H$. Tämä on ristiriidassa oletuksen $k \notin H$ kanssa, joten vasta oletus on väärä. Näin ollen $G \neq H \cup K$. ([7], tehtävä 16, s. 109)

2.2 Sykliset ryhmät

Lause 2.4 esitti osajoukon generoiman aliryhmän. Yksittäisen alkion synnyttämät aliryhmät ovat erityisen tärkeitä.

Määritelmä 2.3 Ryhmää G sanotaan **sykliseksi ryhmäksi**, jos on olemassa sellainen $a \in G$, että $G = \{a^n \mid n \in \mathbf{Z}\}$. Tällöin käytetään merkintää $G = \langle a \rangle$ ja alkioita a kutsutaan ryhmän G **generaattoriksi** (virittäjäksi) ja ryhmää G sanotaan alkion a **generoimaksi** (virittämäksi). (Ks. [7], s. 110.)

Olkoon $G = \langle a \rangle$ syklinen ryhmä. Olkoot $b, c \in G$. Tällöin ovat olemassa sellaiset $m, n \in \mathbf{Z}$, että $b = a^m, c = a^n$. Valitaan tällaiset luvut m, n . Nyt $bc = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = cb$, joten **syklinen ryhmä on Abelin ryhmä**.

Kaikki Abelin ryhmät eivät ole syklisiä. Esimerkiksi **Kleinin neliryhmä** on kommutatiivinen mutta ei syklinen (ks. [7], s. 111).

Lause 2.6 Olkoon G ryhmä. Silloin ryhmän G jokainen alkio generoi ryhmän G syklisen aliryhmän.

Todistus. Olkoon $a \in G$ ja olkoon $H = \{a^k \mid k \in \mathbf{Z}\}$. Selvästi H on epätyhjä. Nyt selvästi $H \subseteq G$. Olkoot nyt $m, n \in \mathbf{Z}$. Tällöin $a^m, a^n \in H$. Myös $(a^n)^{-1} = a^{-n} \in H$, sillä $-n \in \mathbf{Z}$. Nyt $a^m a^{-n} = a^{m-n}$, missä $m-n \in \mathbf{Z}$. Koska $m-n \in \mathbf{Z}$, niin $a^{m-n} \in H$. Siis lauseen 2.1 nojalla $H = \langle a \rangle$ on ryhmän G aliryhmä. \square

Lausetta 2.6 apuna käyttäen voidaan todistaa seuraava lause.

Lause 2.7 *Jokaisella ryhmällä G on ainakin yksi syklinen aliryhmä. Erityisesti jos $|G| > 1$, niin on olemassa sellainen syklinen aliryhmä H , että $|H| > 1$.*

Todistus. Olkoon G ryhmä. Lauseen 2.6 nojalla ryhmän G jokainen alkio generoi syklisen ryhmän, joka on ryhmän G aliryhmä. Jos $|G| = 1$, niin $H = \langle e \rangle = \{e\}$ on etsitty syklinen aliryhmä. Oletetaan nyt, että $|G| > 1$. Tehdään vastaoletus, että ryhmän G jokaisen syklisen aliryhmän H kertaluku on 1. Nyt siis $H = \langle a \rangle = \{e\}$ aina, kun $a \in G$. Näin ollen ryhmän G jokainen alkio generoi aliryhmän $\{e\}$, joten $G = \{e\}$. Tällöin $|G| = 1$, mikä on ristiriidassa oletuksen kanssa. Vastaoletus on siis väärä, ja väite on oikea. \square

Seuraava lause on lauseen 2.6 välitön seuraus.

Lause 2.8 *Olkoon G ryhmä. Silloin ryhmän G jokainen alkio kuuluu johonkin syklisteen aliryhmään.*

Matematiikassa jokin ominaisuus on sitä mielenkiintoisempi, mitä yleisempi se on. Lauseet 2.7 ja 2.8 ilmentävät syklisten ryhmien tärkeitä asemaa ryhmäteoriassa. Lisäksi näiden lauseiden avulla voidaan perustella se, että syklistyys määritellään nimenomaan aliryhmien yhteydessä; alkio generoi aina syklisen aliryhmän, mutta syklistyys ei välttämättä ole koko ryhmän ominaisuus. Tähän havaintoon liittyykin eräänlainen paradoksi: jokaisen ryhmän jokainen alkio kuuluu johonkin syklisteen aliryhmään, mutta huomattava osa äärellisten ryhmien teorian kehittämisestä tähtää sellaisten ryhmien rakenteiden selvittämiseen, jotka eivät ole syklisiä.

Lause 2.9 *Jokaisella ryhmällä on Abelin aliryhmä.*

Todistus. Lauseen 2.7 nojalla jokaisella ryhmällä on syklinen aliryhmä. Syklinen ryhmä on Abelin ryhmä. \square

Esimerkki 2.2 *Olkoon $G \neq \{e\}$ ryhmä, jolla on korkeintaan kaksi ei-triviaalia aliryhmää. Osoitetaan, että G on syklinen.*

Ratkaisu. Oletetaan ensiksi, että ryhmällä G ei ole ei-triviaaleja aliryhmiä; toisin sanoen ainoat aliryhmät ovat G ja $\{e\}$. Lauseen 2.6 perusteella jokainen alkio $a \in G$ generoi aliryhmän, joten nyt jokainen $a \neq e$ generoi koko ryhmän G . Täten G on syklinen.

Oletetaan toiseksi, että ryhmällä G on yksi ei-triviaali aliryhmä H . Tällöin on olemassa sellainen $a \in G$, että $a \notin H$. Valitaan tällainen a . Koska alkio a generoi aliryhmän, joka oletuksen takia ei voi olla ei-triviaali, alkio a generoi nyt koko ryhmän G . Ryhmä G on näin ollen tässäkin tapauksessa syklinen.

Oletetaan lopuksi, että ryhmällä G on kaksi ei-triviaalia aliryhmää H ja K . Esimerkissä 2.1 osoitettiin, että ryhmää G ei voida esittää kahden aidon aliryhmänsä yhdisteenä. Näin ollen tässäkin tapauksessa on olemassa sellainen $a \in G$, että $a \notin H, a \notin K$. Valitaan tällainen a . Koska alkio a generoi aliryhmän, joka oletuksen vuoksi ei voi olla ei-triviaali, alkio a generoi nyt koko ryhmän G . Ryhmä G on siis tässäkin tapauksessa syklinen. Näin koko väite on osoitettu oikeaksi. ([7], tehtävä 8, s. 115)

Esimerkki 2.3 *Oletetaan, että G on ei-kommutatiivinen ryhmä. Osoitetaan, että ryhmällä G on ei-triviaali aliryhmä.*

Ratkaisu. Olkoon $a \in G, a \neq e$. Lauseen 2.6 nojalla a generoi ryhmän G erään syklisen aliryhmän. Tehdään vastaoletus, että ryhmällä G on vain triviaalit aliryhmät. Vastaoletuksen nojalla a generoi koko ryhmän G , joten G on syklinen. Syklisenä G on kommutatiivinen, mikä on ristiriidassa oletuksen kanssa. Vastaoletus on siis väärä, joten ryhmällä G on ei-triviaali aliryhmä. ([7], tehtävä 10, s. 115)

Esimerkki 2.4 *Esitetään muutamia esimerkkejä syklisistä ryhmistä.*

- (i) $(\mathbf{Z}, +)$ on syklinen ryhmä, sillä $\mathbf{Z} = \langle 1 \rangle$.
- (ii) $(\mathbf{Z}_n, +_n)$ on syklinen ryhmä, sillä $\mathbf{Z}_n = \langle [1] \rangle$.
- (iii) Kompleksilukujen joukko $I = \{1, -1, i, -i\}$ muodostaa ryhmän kertolaskun suhteen. Ryhmän kertaluku on 4. Muodostetaan kertolaskutaulu, joka havainnollistaa ryhmän rakennetta. Taulukosta 1 havaitaan nyt helposti, että luku i generoi ryhmän I , joten ryhmä on syklinen.

Taulukko 1. Ryhmän I kertolaskutaulu

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Seuraavaksi luetellaan ilman todistuksia eräitä keskeisiä syklisten ryhmien ominaisuuksia. Jokainen äärellisen kertaluvun n omaava syklinen ryhmä G voidaan kirjoittaa muodossa $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$, missä a on ryhmän generaatordi. Äärellisen syklisen ryhmän suhteen on voimassa ehto $o(a) = |\langle a \rangle|$. Äärellinen ryhmä G on syklinen, jos ja vain jos on olemassa sellainen $a \in G$, että $o(a) = |G|$. *Todistukset.* Ks. [7], s. 111-112.

Lause 2.10 *Syklisen ryhmän jokainen aliryhmä on syklinen.*

Todistus. Ks. [7], s. 112.

Lause 2.11 *Olkoon G syklinen ryhmä, jonka kertaluku m on > 1 , ja olkoon H ryhmän G aito aliryhmä. Silloin $H = \langle a^k \rangle$ jollakin sellaisella kokonaisluvulla $k > 1$, joka jakaa luvun m . Lisäksi $|H|$ jakaa luvun m .*

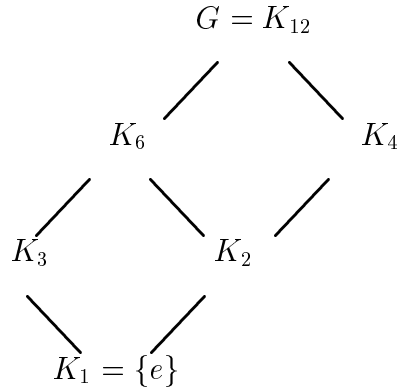
Todistus. Ks. [7], s. 112-113.

Lause 2.12 *Olkoon G äärellinen syklinen ryhmä, jonka kertaluku on m . Silloin jokaista luvun m positiivista jakajaa d kohti on olemassa yksikäsitteinen ryhmän G aliryhmä, jonka kertaluku on d .*

Todistus. Ks. [7], s. 113.

Esimerkki 2.5 *Oma esimerkki.* Olkoon $y \in \mathbf{R}$. Eulerin kaava $e^{iy} = \cos y + i \sin y$ kuvaa yksikköympyrää kompleksitasossa. Tässä e on Neperin luku ja i on imaginääriyksikkö. Olkoon nyt $y = \frac{\pi}{6}$. Osoitetaan, että luku $e^{i\frac{\pi}{6}}$ generoi äärellisen, syklisen ryhmän kompleksilukujen kertolaskun suhteen.

Ratkaisu. Havaitaan ensinnäkin, että $(e^{i\frac{\pi}{6}})^{12} = e^{i2\pi} = e^{i0} = 1$. Toisaalta $(e^{i\frac{\pi}{6}})^n \neq 1$ aina, kun $1 \leq n < 12$. Merkitään $G = \{e^{i\frac{n\pi}{6}} \mid n \in \mathbf{Z}\}$. Neutraalialkio $e^{i0} = \cos 0 + i \sin 0 = 1 \in G$. Alkion $e^{i\frac{n\pi}{6}}$, $n \in \mathbf{Z}$, käänteisalkio on $e^{-i\frac{n\pi}{6}} \in G$, sillä $e^{i\frac{n\pi}{6}} e^{-i\frac{n\pi}{6}} = e^{-i\frac{n\pi}{6}} e^{i\frac{n\pi}{6}} = e^{i0} = 1$. Joukko G on suljettu kertolaskun suhteen, sillä $(e^{i\frac{\pi}{6}})^m (e^{i\frac{\pi}{6}})^n = (e^{i\frac{\pi}{6}})^{m+n} \in G$ aina, kun $m, n \in \mathbf{Z}$. Selvästi vaihdantalaki on voimassa. Näin on osoitettu, että G on syklinen ryhmä, jonka kertaluku on 12. Lauseen 2.12 nojalla G sisältää kertalukua r edustavan aliryhmän K_r aina, kun $r \in \{1, 2, 3, 4, 6, 12\}$. Lauseen 2.10 perusteella kaikki nämä aliryhmät ovat syklisiä. Seuraava *hilakaavio* (lattice diagram) havainnollistaa ryhmän G ja sen aliryhmien suhteita. (Tähän esimerkkiin viitataan myös sivulla 22.)



Kuvio 1. Ryhmän G aliryhmärakenteet.

Esimerkki 2.6 *Osoitetaan, että ryhmä $(\mathbf{R}, +)$ ei ole syklinen.*

Ratkaisu. Ryhmä $(\mathbf{Q}, +)$ on selvästi ryhmän $(\mathbf{R}, +)$ aliryhmä. Lauseen 2.10 nojalla syklisen ryhmän jokainen aliryhmä on syklinen. Voidaan osoittaa, että $(\mathbf{Q}, +)$ ei ole syklinen (ks. [7], s. 113). Koska $(\mathbf{Q}, +)$ ei ole syklinen, ei myöskään $(\mathbf{R}, +)$ ole syklinen. ([7], tehtävä 4, s. 115)

Syklisillä ryhmillä on erityisen tärkeä merkitys ryhmien analysoinnissa. Syklinen ryhmä on rakenteeltaan yksinkertainen ja sen ominaisuudet ovat helpompia käsitellä kuin muiden ryhmien. Voidaan osoittaa, että sykliset ryhmät ovat kaikkien äärellisten Abelin ryhmien rakenneosia; syklisiä ryhmiä voidaan pitää eräänlaisina Abelin ryhmien alkeismuotoina (ks. [3], s. 58). Lauseessa 2.7 on jo osoitettu, että jokaisella ryhmällä G on syklinen aliryhmä; tämä ei riipu siitä, onko ryhmä G kommutatiivinen.

Olkoon G sellainen syklinen ryhmä, että $|G| = n > 0$. Tällöin $G = \langle a \rangle$, missä a on ryhmän G generaattori, jonka kertaluku $o(a)$ on n . Osoitetaan, että ryhmän G jokaisen alkion n . potenssi on neutraalialkio e . Valitaan mielivaltainen $a' \in G$. Tällöin $a' = a^k$, $0 \leq k \leq n - 1$. Nyt $(a')^n = (a^k)^n = a^{kn} = (a^n)^k = e^k = e$. Tämä ei kuitenkaan tarkoita sitä, että ryhmän G jokaisen alkion kertaluku on n , sillä ryhmällä G voi olla aito aliryhmä, jonka alkioden kertaluvut ovat luonnollisesti pienempiä kuin n .

Ryhmät \mathbf{Z}_n ja \mathbf{Z} ovat tavallaan syklisten ryhmien perusmuotoja, jotka edustavat algebrallisessa mielessä kaikkia syklisiä ryhmiä. Tämä voidaan ilmaista niinkin, että on oikeastaan olemassa vain yksi kutakin kertalukua edustava syklinen ryhmä. Vaikka on olemassa useita erilaisia muotoa $\{a^n \mid n \in \mathbf{Z}\}$ olevia joukkoja, on vain yksi tapa käsitellä näitä joukkoja. Tämä tapa riippuu ryhmän generaattorin a kertaluvusta. (Vrt. [4], s. 71.)

2.3 Lagrangen lause

Lagrangen lause on hyvin tärkeä äärellisten ryhmien teoriassa. Esitetään aluksi seuraava määritelmä.

Määritelmä 2.4 *Olkoon H ryhmän G aliryhmä ja olkoon $a \in G$. Alkion a määrittämä aliryhmän H vasen sivuluokka ryhmässä G on joukko $aH = \{ah \mid h \in H\}$. Vastaavasti oikea sivuluokka on joukko $Ha = \{ha \mid h \in H\}$. (Ks. [7], s. 116).*

Jos G on kommutatiivinen, niin vasen ja oikea sivuluokka ovat samat; toisin sanoen $aH = Ha$ aina, kun $a \in G$.

Määritelmä 2.5 *Olkoon H ryhmän G aliryhmä. Aliryhmän H erillisten vasempien (oikeiden) sivuluokkien lukumäärä on aliryhmän H indeksi ryhmässä G . Indeksistä käytetään merkintää $[G : H]$. (Ks. [7], s. 119).*

Lause 2.13 *Olkoon H ryhmän G aliryhmä, $a, b \in G$. Silloin*

- (i) $a \in aH$,
- (ii) $aH = bH$, jos ja vain jos $b^{-1}a \in H$,
- (iii) $aH = bH$ tai $aH \cap bH = \emptyset$.

Todistus. (Vrt. [7], s. 118.) (i) Olkoon $a \in G$. Koska $a = ae$ ja $e \in H$, niin $a = ae \in aH$.

(ii) Olkoot $a, b \in G$. Oletetaan aluksi, että $aH = bH$. Koska $a \in aH$ ja $aH = bH$, niin on olemassa sellainen $h' \in H$, että $a = bh'$. Tästä seuraa, että $b^{-1}a = h' \in H$.

Oletetaan kääntäen, että $b^{-1}a = h' \in H$. Olkoon $h \in H$. Osoitetaan aluksi, että $aH \subseteq bH$. Nyt $ah \in aH$. Oletuksesta seuraa, että $a = bh'$. Silloin $ah = bh'h \in bH$. Tästä seuraa, että $aH \subseteq bH$. Seuraavaksi osoitetaan, että $bH \subseteq aH$. Nyt $bh \in bH$. Oletuksesta $b^{-1}a = h'$ seuraa, että $a(h')^{-1} = b$. Silloin $bh = a(h')^{-1}h \in aH$. Näin ollen $bH \subseteq aH$. Koska nyt on osoitettu, että $aH \subseteq bH$ ja $bH \subseteq aH$, niin $aH = bH$.

(iii) Jos $aH \cap bH = \emptyset$, niin sivuluokat ovat erilliset. Oletetaan nyt, että $aH \cap bH \neq \emptyset$. Osoitetaan, että $aH = bH$. Koska $aH \cap bH \neq \emptyset$, niin on olemassa $c \in aH \cap bH$. Valitaan tällainen c . Silloin $c \in aH$ ja $c \in bH$, joten on olemassa sellaiset $h_1, h_2 \in H$, että $c = ah_1$ ja $c = bh_2$. Näin ollen $ah_1 = bh_2$, mistä seuraa, että $b^{-1}a = h_2h_1^{-1}$. Siten $b^{-1}a \in H$. Kohdan (ii) perusteella nyt $aH = bH$. Näin on todistettu, että sivuluokat ovat joko erilliset tai samat. \square

Lause 2.14 *Olkoon H ryhmän G aliryhmä. Silloin aliryhmän H kertaluku on sama kuin minkä tahansa sivuluokan aH tai Ha alkioden lukumäärä.*

Todistus. Ks. [7], s. 119.

Lause 2.15 (Lagrange) *Olkoon H äärellisen ryhmän G aliryhmä. Silloin aliryhmän H kertaluku jakaa ryhmän G kertaluvun. Lisäksi on voimassa yhtälö*

$$[G : H] = |G|/|H|.$$

Todistus. (Vrt. [7], s. 120.) Koska G on äärellinen, niin aliryhmän H erillisten vasempien sivuluokkien lukumäärä on äärellinen. Olkoon $\{a_1H, a_2H, \dots, a_rH\}$ aliryhmän H kaikkien erillisten vasempien sivuluokkien joukko ryhmässä G . Silloin jokaista alkioita $a \in G$ kohti on olemassa sellainen a_i , $1 \leq i \leq r$, että $aH = a_iH$. Lisäksi lauseen 2.13 kohdan (i) nojalla $a \in aH$. Näin ollen jokainen ryhmän G alkio kuuluu yhteen sivuluokista a_iH , joten $G = a_1H \cup a_2H \cup \dots \cup a_rH$. Lauseen

2.13 kohdan (iii) perusteella tämä yhdiste koostuu erillisistä joukoista, niin että $|G| = |a_1H| + |a_2H| + \dots + |a_rH|$. Näin ollen $[G : H] = r$. Lauseen 2.14 nojalla $|a_iH| = |H|$ aina, kun $1 \leq i \leq r$, joten $|G| = r|H|$. Näin ollen $|G| = [G : H]|H|$. \square

Lause 2.16 *Olkoon G äärellinen ryhmä, jonka kertaluku on n . Silloin ryhmän G minkä tahansa alkion a kertaluku jakaa luvun n ja $a^n = e$.*

Todistus. Ks. [7], s. 120-121.

Seuraava lause on usein käyttökelpoinen äärellisten ryhmien teoriassa.

Lause 2.17 *Olkoon G sellainen äärellinen ryhmä, että $|G| = p$, missä p on alkuluku. Silloin G on syklinen.*

Todistus. (Vrt. [7], s. 121.) Lauseen 2.7 nojalla ryhmällä G on syklinen aliryhmä H , jonka kertaluku on > 1 . Koska Lagrangen lauseen mukaan $|H|$ jakaa luvun p , niin $|H| = p$. Koska $H \subseteq G$, G on äärellinen ja $|H| = |G|$, niin $H = G$. Koska H on syklinen, niin G on syklinen. \square

Lause 2.18 *Olkoon G sellainen äärellinen ryhmä, että $|G| = p > 1$, p alkuluku. Tällöin jokainen ryhmän G alkio $\neq e$ on ryhmän G generaattori. Lisäksi jokaisen alkion $\neq e$ kertaluku on p .*

Todistus. Olkoon $a \in G, a \neq e$. Nyt $H = \langle a \rangle$ on ryhmän G syklinen aliryhmä lauseen 2.6 perusteella. Lagrangen lauseen nojalla $|H|$ jakaa luvun p . Jos $|H| = 1$, niin $a = e$, mikä on ristiriidassa oletuksen kanssa. Siis $|H| > 1$. Lagrangen lauseesta seuraa nyt, että $|H| = p$. Koska G on äärellinen, $H \subseteq G$ ja $|H| = |G|$, niin $H = \langle a \rangle = G$. Siis a on ryhmän G generaattori. Nyt selvästi $o(a) = |\langle a \rangle| = p$. \square

Lause 2.19 *Olkoot H ja K ryhmän G äärellisiä aliryhmiä. Silloin*

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

Todistus. Ks. [7], s. 121-122.

Lause 2.20 *Olkoon G sellainen ryhmä, että $|G| > 1$. Tällöin ryhmällä G on ainoastaan triviaalit aliryhmät, jos ja vain jos $|G|$ on alkuluku.*

Todistus. Ks. [7], esimerkki 5, s. 123-124.

Todistetaan vielä seuraava lause Lagrangen lauseen avulla.

Lause 2.21 *Olkoon G äärellinen ryhmä ja olkoot H ja K sen sellaisia aliryhmiä, että $\text{syt}(|H|, |K|) = 1$. Silloin $H \cap K = \{e\}$.*

Todistus. Lauseen 2.3 perusteella $H \cap K$ on ryhmän G aliryhmä. Koska $H \cap K \subseteq H$, niin $H \cap K$ on ryhmän H aliryhmä. Lagrangen lauseen mukaan nyt $|H \cap K|$ jakaa luvun $|H|$. Vastaavasti päätellään, että $|H \cap K|$ jakaa luvun $|K|$. Koska $\text{syt}(|H|, |K|) = 1$, niin $|H \cap K| = 1$. Tästä seuraa, että $H \cap K = \{e\}$. \square

On huomattava, että Lagrangen lause kertoo mahdollisten aliryhmien kertaluvut, mutta ei todista niiden olemassaoloa. Tämä huomataan esimerkiksi vaihtelevan ryhmän A_4 yhteydessä. Ryhmän A_4 kertaluku on 12, mutta sillä ei ole aliryhmiä, jonka kertaluku on 6 (todistus, ks. [4], s. 139). Tämä esimerkki osoittaa, että Lagrangen lauseelle käänteinen väite on yleisessä tapauksessa epätosi.

2.4 Normaalit aliryhmät ja tekijäryhmät

Normaali aliryhmä on yksi ryhmäteorian tärkeimmistä käsitteistä.

Määritelmä 2.6 *Olkoon G ryhmä. Ryhmän G aliryhmää H kutsutaan ryhmän G normaaliksi aliryhmäksi, jos $aH = Ha$ aina, kun $a \in G$. Normaalialiryhmää kutsutaan myös invariantiksi. (Ks. [7], s. 128.)*

Jos H on ryhmän G normaali aliryhmä, niin voidaan myös sanoa, että H on normaali ryhmässä G . Määritelmästä seuraa välittömästi, että G ja $\{e\}$ ovat ryhmän G normaaleja aliryhmiä.

On huomattava, että ryhmän G normaalissa aliryhmässä H ei aina ole voimassa ehto $ah = ha$, kun $h \in H$ ja $a \in G$. Normaalius on tässä yhteydessä ryhmätason, mutta ei alkiotason, ilmiö. Voidaan sanoa niinkin, että normaalius on ryhmätason käsite ja sellaisena analoginen alkiotasolla ilmenevälle kommutatiivisuudelle.

Lause 2.22 *Olkoon H ryhmän G aliryhmä. Silloin H on ryhmän G normaali aliryhmä, jos ja vain jos $aHa^{-1} \subseteq H$ aina, kun $a \in G$.*

Todistus. Ks. [7], s. 128-129.

Lause 2.23 *Olkoon H ryhmän G normaali aliryhmä. Silloin $aHa^{-1} = H$ aina, kun $a \in G$.*

Todistus. (Vrt. [5], s. 85.) Olkoon $a \in G$. Lauseen 2.22 mukaan $aHa^{-1} \subseteq H$. Nyt $H = a^{-1}(aHa^{-1})a \subseteq a^{-1}Ha = a^{-1}H(a^{-1})^{-1} \subseteq H$, joten $a^{-1}Ha = H$ aina, kun $a \in G$. \square

Lauseen 2.23 nojalla ryhmän G aliryhmän H normaaliuden ehto on $aHa^{-1} = H$ aina, kun $a \in G$. Monissa tapauksissa tämä normaaliuden ehto on käyttökelpoisempi kuin edellä olevan määritelmän ehto.

Esimerkki 2.7 *Olkoon H ryhmän G aliryhmä. Osoitetaan, että H on ryhmän G normaali aliryhmä, jos ja vain jos $aha^{-1} \in H$ aina, kun $a \in G, h \in H$.*

Ratkaisu. Oletetaan ensin, että H on normaali ryhmässä G . Osoitetaan, että $aha^{-1} \in H$ aina, kun $a \in G, h \in H$. Olkoon $a \in G$ ja $h \in H$. Oletuksen perusteella nyt $aHa^{-1} = H$. Nyt on olemassa sellainen $h_1 \in H$, että $aha^{-1} = h_1$, joten $aha^{-1} \in H$ aina, kun $a \in G, h \in H$.

Oletetaan kääntäen, että $aha^{-1} \in H$ aina, kun $a \in G, h \in H$. Osoitetaan, että H on normaali ryhmässä G . Olkoon $a \in G$ ja $h \in H$. Oletuksesta seuraa, että $aHa^{-1} \subseteq H$ aina, kun $a \in G$. Väite on nyt tosi lauseen 2.22 nojalla. ([7], tehtävä 3, s. 136)

Esimerkki 2.8 *Osoitetaan, että ryhmän G keskus $Z(G)$ on ryhmän G normaali aliryhmä.*

Ratkaisu. Nyt $Z(G) = \{b \in G \mid ab = ba \text{ aina, kun } a \in G\}$. Olkoon $a \in G$ ja $b \in Z(G)$. Tällöin $ab = ba$, joten $b = aba^{-1}$. Tästä seuraa, että $b = aba^{-1} \in Z(G)$ aina, kun $a \in G$ ja $b \in Z(G)$. Väite seuraa nyt esimerkistä 2.7. ([7], tehtävä 6, s. 137)

Esimerkki 2.9 *Olkoon G ryhmä ja H sen normaali aliryhmä. Olkoon K ryhmän G aliryhmä. Osoitetaan, että $H \cap K$ on aliryhmän K normaali aliryhmä.*

Ratkaisu. Koska H ja K ovat aliryhmän K aliryhmiä, niin $H \cap K$ on ryhmän K aliryhmä lauseen 2.3 nojalla. Selvästi $H \cap K \neq \emptyset$. Olkoon $a \in H \cap K$ ja $k \in K$. Tarkastellaan joukkoa $k(H \cap K)k^{-1}$. Nyt $kak^{-1} \in k(H \cap K)k^{-1}$. Koska $a \in H \cap K$, niin $a \in H$ ja $a \in K$. Nyt H on ryhmän G normaali aliryhmä, joten $kak^{-1} \in kHk^{-1} \subseteq H$ lauseen 2.22 perusteella. Toisaalta selvästi $kak^{-1} \in K$, joten $kak^{-1} \in H \cap K$. Tästä seuraa, että $k(H \cap K)k^{-1} \subseteq H \cap K$ aina, kun $k \in K$. Lauseen 2.22 mukaan väite on nyt tosi. ([7], tehtävä 8, s. 137)

Esimerkki 2.10 *Olkoon G ryhmä ja olkoot H ja K sen normaaleja aliryhmiä. Olkoon $H \cap K = \{e\}$. Osoitetaan, että $hk = kh$ aina, kun $h \in H, k \in K$.*

Ratkaisu. Olkoon $h \in H$ ja $k \in K$. Oletuksen mukaan $aHa^{-1} = H$ aina, kun $a \in G$. Tästä seuraa, että $kHk^{-1} = H$, joten $khk^{-1} \in H$. Nyt $(khk^{-1})h^{-1} = khk^{-1}h^{-1} \in H$.

Oletuksen mukaan vastaavasti $hKh^{-1} = K$, joten $hk^{-1}h^{-1} \in K$, missä $k^{-1} \in K$. Siksi $k(hk^{-1}h^{-1}) = khk^{-1}h^{-1} \in K$.

On todettu, että $khk^{-1}h^{-1} \in H$ ja $khk^{-1}h^{-1} \in K$, joten $khk^{-1}h^{-1} \in H \cap K = \{e\}$. Siksi $khk^{-1}h^{-1} = e$ eli $kh(hk)^{-1} = e$. Näin ollen $kh = hk$. Tästä seuraa, että $kh = hk$ aina, kun $h \in H, k \in K$. ([7], tehtävä 12, s. 137)

On huomattava, että esimerkissä 2.10 ei oleteta ryhmän G kommutatiivisuutta.

Lause 2.24 *Olkoot H ja K ryhmän G normaaleja aliryhmiä. Silloin*

- (i) $H \cap K$ on ryhmän G normaali aliryhmä,
- (ii) $HK = KH$ on ryhmän G normaali aliryhmä,
- (iii) $\langle H \cup K \rangle = HK$.

Todistus. Ks. [7], s. 129.

Todistetaan seuraavaksi tärkeä yksityiskohta, joka lähteessä [7] jää rivien väliin.

Esimerkki 2.11 *Olkoon G Abelin ryhmä. Osoitetaan, että ryhmän G jokainen aliryhmä on normaali aliryhmä.*

Ratkaisu. Olkoon H ryhmän G aliryhmä. Olkoon $a \in G$ ja $h \in H$. Koska G on kommutatiivinen, niin $aha^{-1} = aa^{-1}h = h \in H$. Väite on nyt tosi esimerkin 2.7 nojalla. ([7], tehtävä 15, s. 137)

Lause 2.25 *Olkoon G syklinen ryhmä. Silloin ryhmän G jokainen aliryhmä on normaali aliryhmä.*

Todistus. Syklisten ryhmien yhteydessä osoitettiin, että syklinen ryhmä on Abelin ryhmä. Väite seuraa nyt suoraan esimerkistä 2.11. \square

Esimerkki 2.12 *Olkoot H ja K ryhmän G aliryhmiä. Olkoon lisäksi H normaali ryhmässä G . Osoitetaan, että HK on ryhmän G aliryhmä.*

Ratkaisu. Tarkastellaan joukkoa $HK = \{hk \mid h \in H, k \in K\}$. Koska H on ryhmän G normaali aliryhmä, niin $aH = Ha$ aina, kun $a \in G$. Näin ollen $kH = Hk$ aina, kun $k \in K \subseteq G$. Tästä seuraa, että $KH = HK$. Lauseen 2.5 nojalla väite on tosi. ([7], tehtävä 13, s. 137)

Lause 2.26 *Olkoon H ryhmän G normaali aliryhmä. Olkoon G/H kaikkien vasempien sivuluokkien joukko $\{aH \mid a \in G\}$. Määritellään laskutoimitus $*$ joukossa G/H lailla $(aH) * (bH) = abH$. Silloin $(G/H, *)$ on ryhmä ja sitä kutsutaan **aliryhmän H määräämäksi ryhmän G tekijäryhmäksi**.*

Todistus. Ks. [7], s. 131.

Jatkossa tekijäryhmän laskutoimitus $*$ jätetään yleensä merkitsemättä.

Osoitetaan, että tekijäryhmän G/H neutraalialkio on eH . Olkoon $aH \in G/H$. Nyt $eHaH = eaH = aH = aeH = aHeH$. Lisäksi alkion aH käänteisalkio on $a^{-1}H$, sillä $aHa^{-1}H = aa^{-1}H = eH = a^{-1}aH = a^{-1}HaH$. Merkinnällä aH on tässä toinen merkitys kuin edellä, kun tarkasteltiin vain sivuluokkia. Ryhmän G sivuluokka aH on eräs joukko, kun taas tekijäryhmän G/H yhteydessä sama symboli on sekä sivuluokka että tekijäryhmän alkio. Symbolin tulkinta riippuu asiayhteydestä.

Tekijäryhmän määrittelyssä edellytetään, että aliryhmä H on normaali. Tämä on välttämätöntä, jotta laskutoimitus olisi hyvin määritelty (ks. [7], s. 131).

Esimerkki 2.13 *Olkoon G Abelin ryhmä ja H sen normaali aliryhmä. Osoitetaan, että tekijäryhmä G/H on kommutatiivinen.*

Ratkaisu. Olkoot $a, b \in G$. Koska H on ryhmän G normaali aliryhmä (esimerkin 2.11 nojalla Abelin ryhmän jokainen aliryhmä on normaali), niin tekijäryhmä G/H voidaan määritellä. Nyt $aH, bH \in G/H$, joten $aHbH = abH$. Koska G on Abelin ryhmä, niin $abH = baH = bHaH$. Nyt siis $aHbH = bHaH$. ([7], tehtävä 10, s. 137)

Esimerkki 2.14 *Olkoon G syklinen ryhmä ja olkoon H sen aliryhmä. Osoitetaan, että tekijäryhmä G/H on syklinen.*

Ratkaisu. Nyt H on ryhmän G normaali aliryhmä lauseen 2.25 nojalla. Siten tekijäryhmä G/H voidaan muodostaa. Määritellään kuvaus f seuraavasti. Olkoon $f : G \rightarrow G/H, f(a) = aH$ aina, kun $a \in G$. Kuvauksen f määritelmästä seuraa, että ryhmän G/H jokaisella alkiolla aH on alkukuva $f^{-1}(aH) = aH \ni a$, missä $a \in G$. Olkoon a nyt ryhmän G generaattori, toisin sanoen $G = \langle a \rangle$. Koko ryhmä G tulee siis määritellyksi alkion a potenssien $a^k, k \in \mathbf{Z}$, avulla. Koska $G = \langle a \rangle$ ja ryhmästä G löytyy alkukuva jokaiselle tekijäryhmän G/H alkioille aH , niin jokaisesta sivuluokkaa bH kohti on olemassa sellainen $k \in \mathbf{Z}$, että $a^kH = bH$. Näin ollen aH generoi tekijäryhmän G/H , toisin sanoen $G/H = \langle aH \rangle$.

Määritelmä 2.7 *Olkoon G ryhmä. Silloin ryhmää G kutsutaan **yksinkertaiseksi**, jos $G \neq \{e\}$ ja ryhmän G ainoat normaalit aliryhmät ovat $\{e\}$ ja G .*

Olkoon G syklinen ryhmä, jonka kertaluku on p , missä p on alkuluku. Lagrangen lauseesta ja lauseesta 2.12 seuraa, että ryhmällä G on ainoastaan aliryhmät G ja $\{e\}$. Näin ollen G on yksinkertainen. Syklisenä G on myös kommutatiivinen.

2.5 Aliryhmän määräämä kongruenssirelaatio

Ryhmän alkioiden suhteiden tarkastelua voidaan tehostaa ekvivalenssirelaatioiden avulla. Eräs tällainen käsite on *aliryhmän määräämä kongruenssirelaatio*.

Määritelmä 2.8 *Olkkoon G ryhmä ja olkkoon H ryhmän G aliryhmä. Olkkoot $a, b \in G$. Silloin sanotaan, että a on **vasemmanpuoleisesti kongruentti alkion b kanssa modulo H** , jos ja vain jos $a^{-1}b \in H$. Tästä käytetään merkintää*

$$a \equiv_L b \pmod{H} \Leftrightarrow a^{-1}b \in H.$$

*Vastaavasti sanotaan, että a on **oikeanpuoleisesti kongruentti alkion b kanssa modulo H** , jos ja vain jos $ab^{-1} \in H$. Tästä käytetään merkintää*

$$a \equiv_R b \pmod{H} \Leftrightarrow ab^{-1} \in H.$$

Lause 2.27 *Olkkoon G ryhmä ja olkkoon H ryhmän G aliryhmä. Silloin vasemmanpuoleinen ja oikeanpuoleinen kongruenssi modulo H ovat ekvivalenssirelaatioita ryhmässä G .*

Todistus. (Ks. [9], s. 92.) Olkkoon $a \in G$. Nyt $a \equiv_L a \pmod{H}$, sillä $a^{-1}a = e$ ja $e \in H$. Näin ollen vasemmanpuoleinen kongruenssi modulo H on refleksiivinen.

Olkkoot $a, b \in G$. Olkkoon $a \equiv_L b \pmod{H}$. Tällöin $a^{-1}b \in H$. Koska H on ryhmän G aliryhmä, niin $(a^{-1}b)^{-1} = b^{-1}a \in H$ lauseen 1.2 nojalla. Tämä merkitsee sitä, että $b \equiv_L a \pmod{H}$, joten vasemmanpuoleinen kongruenssi modulo H on symmetrinen.

Olkkoot $a, b, c \in G$. Olkkoon $a \equiv_L b \pmod{H}$ ja $b \equiv_L c \pmod{H}$. Tällöin $a^{-1}b \in H$ ja $b^{-1}c \in H$. Tästä seuraa, että $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. Tämä merkitsee sitä, että $a \equiv_L c \pmod{H}$, joten vasemmanpuoleinen kongruenssi modulo H on transitiiivinen.

Näin on osoitettu, että vasemmanpuoleinen kongruenssi modulo H on ekvivalenssirelaatio. Oikeanpuoleisen kongruenssin modulo H todistus on vastaavanlainen. \square

Olkkoon G ryhmä ja olkkoon sen laskutoimitus kertolaskunkaltainen. Olkkoot $a, b \in G$. Olkkoon nyt a vasemmanpuoleisesti kongruentti alkion b kanssa modulo H . Silloin a ja b poikkeavat toisistaan multiplikaatiivisesti aliryhmän H erään alkion määräämällä tavalla. Selvennetään tätä seuraavalla tavalla. Nyt $a \equiv_L b \pmod{H}$, jos ja vain jos $a^{-1}b \in H$. Jälkimmäinen relaatio on voimassa silloin ja vain silloin, kun on olemassa sellainen $h \in H$, että $a^{-1}b = h$. Tämä on yhtäpitävä ehdon $b = ah$ kanssa. Vastaava päättely pätee oikeanpuoleisen kongruenssin modulo H suhteen.

Olkkoon G Abelin ryhmä ja H sen aliryhmä. Silloin vasemmanpuoleisen ja oikeanpuoleisen kongruenssin modulo H välinen ero häviää, joten voidaan käyttää nimitystä *kongruenssi modulo H* . Jos $a, b \in G$ ovat kongruentteja modulo H , niin tällöin

$$a \equiv b \pmod{H} \Leftrightarrow a^{-1}b \in H \Leftrightarrow ab^{-1} \in H.$$

Oletetaan seuraavaksi, että Abelin ryhmän G laskutoimitus on yhteenlaskunkaltainen. Tällöin alkio $a, b \in G$ ovat kongruentteja modulo H , jos ja vain jos $a - b \in H$. Tämän kanssa yhtäpitävä on ehto $b - a \in H$.

Oletetaan jälleen, että ryhmän G laskutoimitus on kertolaskunkaltainen. Seuraava lause ilmaisee, miten vasemmanpuoleinen ja oikeanpuoleinen kongruenssi modulo H jakavat ryhmän G ekvivalenssiluokkiin.

Lause 2.28 *Olkoon G ryhmä ja olkoon H ryhmän G aliryhmä. Olkoon a ryhmän G mielivaltainen alkio. Silloin alkion a*

- (i) *vasemmanpuoleinen kongruenssiluokka modulo H on vasen sivuluokka aH ,*
- (ii) *oikeanpuoleinen kongruenssiluokka modulo H on oikea sivuluokka Ha .*

Todistus. (Ks. [9], s. 93.) (i) Olkoon $[a]$ alkion a vasemmanpuoleinen kongruenssiluokka (mod H). Olkoon $t \in G$. Nyt $t \in [a]$, jos ja vain jos $a \equiv_L t \pmod{H}$. Jälkimmäinen relaatio on voimassa silloin ja vain silloin, kun on olemassa sellainen $h \in H$, että $t = ah$. Tämä puolestaan pätee, jos ja vain jos $t \in aH = \{ah \mid h \in H\}$. Näin on osoitettu, että $[a] = aH$. Kohdan (ii) todistus on vastaavanlainen. \square

Lause 2.28 merkitsee sitä, että jokainen kongruenssiluokka on sivuluokka ja jokainen sivuluokka on kongruenssiluokka.

Olkoot $a, b \in G$ ja olkoon $aH = bH$. Koska $a^{-1} \in G$, niin nyt $a^{-1}(aH) = a^{-1}(bH)$, joten $H = a^{-1}bH$. Koska $a^{-1}bH$ on alkion $a^{-1}b$ vasen kongruenssiluokka (mod H), niin edellinen yhtälö on voimassa silloin ja vain silloin, kun $a^{-1}b \in H$. (Ks. [9], s. 91-95.)

Tarkastellaan vielä ekvivalenssiluokkien ja tekijäryhmien välistä yhteyttä. Olkoon G ryhmä ja olkoon H sen normaali aliryhmä. Tekijäryhmän G/H muodostaminen merkitsee ryhmäteoreettisesti kahta asiaa. Kuten edellä on todettu, ensinnäkin ryhmä G jaetaan ekvivalenssiluokkiin normaalin aliryhmänsä H avulla. Toisaalta tällöin samastetaan ryhmän G alkiot a ja b , jos ne toteuttavat relaation $b^{-1}a \in H$.

Otetaan esimerkiksi Abelin ryhmä $(\mathbf{Z}, +)$ ja sen normaali aliryhmä $5\mathbf{Z} = \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$. Tekijäryhmää $\mathbf{Z}/5\mathbf{Z}$ muodostettaessa samastetaan kaikki luvun 5 monikerrat luvun 0 kanssa, samastetaan joukon $\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}$ luvut luvun 1 kanssa ja niin edelleen.

Tekijäryhmässä $\mathbf{Z}/5\mathbf{Z}$ pätee esimerkiksi laskutoimitus $(6 + 5\mathbf{Z}) + (13 + 5\mathbf{Z}) = (1+3) + 5\mathbf{Z} = 4 + 5\mathbf{Z}$. Toisaalta esimerkiksi $(5 + 5\mathbf{Z}) + (10 + 5\mathbf{Z}) = (0+0) + 5\mathbf{Z} = 5\mathbf{Z}$. Nyt siis ryhmän $(\mathbf{Z}, +)$ alkioiden samastaminen on sopusoinnussa ryhmän $(\mathbf{Z}, +)$ yhteenlaskun kanssa, kun siirrytään tekijäryhmään $\mathbf{Z}/5\mathbf{Z}$. (Vrt. [5], s. 97.)

3 Ryhmähomomorfismit ja -isomorfismit

3.1 Ryhmähomomorfismit

Ryhmähomomorfismi on kuvaus, joka säilyttää kuvaukseen liittyvien ryhmien algebrallisen rakenteen. Homomorfismit ovat myös läheisessä yhteydessä tekijäryhmiin (tätä tarkastellaan lähemmin kappaleessa 3.2).

Määritelmä 3.1 *Olkoot $(G, *)$ ja $(G_1, *_1)$ ryhmiä ja olkoon f kuvaus ryhmältä G ryhmään G_1 . Kuvaus f on **homomorfismi**, jos*

$$f(a * b) = f(a) *_1 f(b)$$

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

Olkoon e_1 ryhmän G_1 neutraali-alkio. Olkoon $f : G \rightarrow G_1$, $f(a) = e_1$ aina, kun $a \in G$. Nyt $f(a * b) = e_1 = e_1 *_1 e_1 = f(a) *_1 f(b)$ aina, kun $a, b \in G$. Näin ollen

f on homomorfismi. Ryhmältä $(G, *)$ ryhmään $(G_1, *_1)$ on aina olemassa ainakin tämä **triviaali homomorfismi**. (Laskutoimitusten symbolit $*$ ja $*_1$ jätetään tästä lähtien yleensä merkitsemättä silloin, kun tulkintaongelmaa ei synny.)

Myös identiteettikuvaus $f : G \rightarrow G, f(a) = a$ on homomorfismi, sillä $f(ab) = ab = f(a)f(b)$ aina, kun $a, b \in G$.

Seuraavassa lauseessa esitetään eräitä homomorfismien perusominaisuuksia.

Lause 3.1 *Olkoon f homomorfismi ryhmältä G ryhmään G_1 . Silloin seuraavat ominaisuudet ovat voimassa.*

(i) $f(e) = e_1$.

(ii) $f(a^{-1}) = f(a)^{-1}$ aina, kun $a \in G$.

(iii) Jos H on ryhmän G aliryhmä, niin $f(H) = \{f(h) \mid h \in H\}$ on ryhmän G_1 aliryhmä.

(iv) Jos H_1 on ryhmän G_1 aliryhmä, niin $f^{-1}(H_1) = \{g \in G \mid f(g) \in H_1\}$ on ryhmän G aliryhmä. Jos lisäksi H_1 on normaali aliryhmä, niin $f^{-1}(H_1)$ on ryhmän G normaali aliryhmä.

(v) Jos G on Abelin ryhmä, niin $f(G)$ on Abelin ryhmä.

(vi) Jos alkion $a \in G$ kertaluku $o(a)$ on n , niin $o(f(a))$ jakaa luvun n .

Todistus. Ks. [7], s. 141.

Lause 3.2 *Olkoon f homomorfismi ryhmältä G ryhmään G_1 . Silloin*

$$f(a^n) = (f(a))^n$$

aina, kun $n \in \mathbf{N}$.

Todistus. (Vrt. [4], s. 172.) Kun $n = 1$, niin $f(a^1) = f(a) = (f(a))^1$. Kun $n = 2$, niin $f(a^2) = f(a * a) = f(a) *_1 f(a) = (f(a))^2$. Tehdään nyt induktio-oletus, että väite on tosi indeksillä n , toisin sanoen $f(a^n) = (f(a))^n$. Tästä seuraa, että $f(a^{n+1}) = f(a^n * a) = f(a^n) *_1 f(a) = (f(a))^n *_1 f(a) = (f(a))^{n+1}$. Induktioperiaatteen nojalla väite on nyt tosi aina, kun $n \in \mathbf{N}$. \square

Potenssimerkintä lauseessa 3.2 viittaa kummankin ryhmän omaan laskutoimitukseen.

Lause 3.3 *Olkoon f homomorfismi ryhmältä G ryhmään G_1 . Olkoon H ryhmän G normaali aliryhmä. Silloin $f(H)$ on ryhmän $f(G)$ normaali aliryhmä.*

Todistus. (Vrt. [4], s. 172.) Lauseen 3.1 mukaan $f(H)$ on ryhmän G_1 aliryhmä, joten myös $f(G)$ on ryhmän G_1 aliryhmä. Olkoon $a \in G$ ja $h \in H$. Nyt $f(a) \in f(G)$ ja $f(h) \in f(H)$. Tällöin $f(a)f(h)f(a)^{-1} = f(a)f(h)f(a^{-1}) = f(aha^{-1})$. Esimerkin 2.7 nojalla tässä $aha^{-1} \in H$, joten $f(aha^{-1}) \in f(H)$. Näin ollen $f(H)$ on ryhmän $f(G)$ normaali aliryhmä esimerkin 2.7 perusteella. \square

Määritelmä 3.2 *Olkoon f homomorfismi ryhmältä G ryhmään G_1 . Kuvauksen f ydin $\text{Ker } f$ on joukko*

$$\text{Ker } f = \{a \in G \mid f(a) = e_1\}.$$

Koska lauseen 3.1 mukaan $f(e) = e_1$, niin $e \in \text{Ker } f$.

Määritelmä 3.3 Olkoot G ja G_1 ryhmiä. Homomorfismia $f : G \rightarrow G_1$ kutsutaan **epimorfismiksi**, jos f on surjektio. Homomorfismia f kutsutaan **monomorfismiksi**, jos f on injektio. Jos on olemassa epimorfismi f ryhmältä G ryhmälle G_1 , niin ryhmää G_1 kutsutaan ryhmän G **homomorfiseksi kuvaksi**.

Esimerkki 3.1 Olkoon G syklinen ryhmä, jonka kertaluku on 8, ja G_1 syklinen ryhmä, jonka kertaluku on 4. Olkoon f epimorfismi ryhmältä G ryhmälle G_1 . Määritetään kuvauksen f ydin $\text{Ker } f$.

Ratkaisu. Koska f on homomorfismi, niin $e \in \text{Ker } f$. Olkoon a ryhmän G generaattori. Koska a generoi ryhmän G ja f on surjektio ryhmältä G ryhmälle G_1 , niin $f(a)$ generoi ryhmän G_1 . Alkion $f(a)$ kertaluku on näin ollen 4. Koska f on homomorfismi, niin $f(a^n) = (f(a))^n, n \in \mathbf{N}$. Siis $(f(a))^4 = f(a^4) = e_1$, joten $a^4 \in \text{Ker } f$. Näin on todettu, että $e, a^4 \in \text{Ker } f$.

Toisaalta $f(a^5) = f(a^4 a) = f(a^4) f(a) = e_1 f(a) = f(a)$. Vastaavasti $f(a^6) = f(a^4) f(a^2) = e_1 f(a^2) = f(a^2) = (f(a))^2$ ja $f(a^7) = f(a^4) f(a^3) = e_1 f(a^3) = f(a^3) = (f(a))^3$. Näin havaitaan, että f kuvaa alkion a ja a^5 alkion $f(a)$, alkion a^2 ja a^6 alkion $(f(a))^2$ sekä alkion a^3 ja a^7 alkion $(f(a))^3$. Alkion $f(a)$, $(f(a))^2$ ja $(f(a))^3$ eivät voi olla e_1 , koska alkion $f(a)$ kertaluku on 4. Todetaan siis, että ainoastaan alkion e ja a^4 kuvautuvat alkion e_1 , joten $\text{Ker } f = \{e, a^4\}$. ([7], tehtävä 11, s. 152)

Esimerkki 3.2 Määritetään kaikki epimorfismit ryhmältä $(\mathbf{Z}, +)$ ryhmälle $(\mathbf{Z}_6, +_6)$.

Ratkaisu. Olkoon $f : (\mathbf{Z}, +) \rightarrow (\mathbf{Z}_6, +_6)$ epimorfismi. Olkoon $a \in \mathbf{Z}$. Sekä ryhmä \mathbf{Z} että ryhmä \mathbf{Z}_6 ovat syklisiä; edellinen on ääretön, jälkimmäinen äärellinen. Ryhmän \mathbf{Z} generaattori on luku 1 (myös luku -1 on sen generaattori), ryhmän \mathbf{Z}_6 generaattoreita ovat alkion $[1]$ ja $[-1]$. Olkoon $a \in \mathbf{Z}, a \neq 0$. Koska f on homomorfismi, niin se täyttää nyt lauseen 3.2 nojalla ehdon

$$f(a) = f(\underbrace{1 + 1 + \dots + 1}_{|a| \text{ kpl}}) = \underbrace{f(1) +_6 f(1) +_6 \dots +_6 f(1)}_{|a| \text{ kpl}}.$$

Näin ollen koko epimorfismi tulee määritellyksi, kun $f(1)$ tunnetaan (ks. [4], s. 174). Koska \mathbf{Z}_6 on syklinen, niin $f(1)$ generoi ryhmän \mathbf{Z}_6 jonkin syklisen aliryhmän. Lagrangen lauseen perusteella nyt $|\langle f(1) \rangle| = o(f(1))$ jakaa luvun 6, joten $o(f(1))$ on 1, 2, 3 tai 6.

Jos $o(f(1)) = 1$, niin $f(1) = [0]$. Tällöin f on triviaali homomorfismi, joten se ei ole epimorfismi. Jos $o(f(1)) = 2$, niin $f(1) = [3]$. Tällöin $f(a) = [3a], a \in \mathbf{Z}$. Nyt $f(0) = [0] = \{0, \pm 6, \pm 12, \pm 18, \dots\}, f(1) = [3] = \{\pm 3, \pm 9, \pm 15, \dots\} = f(3) = f(5)$ ja $f(2) = [6] = [0] = f(0) = f(4)$. Havaitaan, että alkiolla $[1], [2], [4]$ ja $[5]$ ei ole alkukuvaa ryhmässä \mathbf{Z} , joten f ei ole epimorfismi.

Jos $o(f(1)) = 3$, niin $f(1) = [2]$. Tällöin $f(a) = [2a], a \in \mathbf{Z}$. Nyt $f(0) = [0] = \{0, \pm 6, \pm 12, \pm 18, \dots\}, f(1) = [2] = \{\dots, -16, -10, -4, 2, 8, 14, \dots\}$ ja $f(2) = [4] = \{\dots, -14, -8, -2, 4, 10, 16, \dots\}$. Havaitaan, että ”parittomilla” alkiolla $[1], [3]$ ja $[5]$ ei ole alkukuvaa ryhmässä \mathbf{Z} , joten tämäkään kuvaus ei ole epimorfismi.

Jos $o(f(1)) = 6$, niin $f(1) = [1]$ tai $f(1) = [-1]$. Tällöin selvästi sekä kuvaus $f(a) = [a], a \in \mathbf{Z}$, että kuvaus $f(a) = [-a], a \in \mathbf{Z}$, ovat epimorfismeja. Etsityt epimorfismit ovat siis $f(a) = [a]$ ja $f(a) = [-a], a \in \mathbf{Z}$. ([7], tehtävä 3, s. 151)

Lause 3.4 Olkoon f homomorfismi ryhmältä G ryhmään G_1 . Silloin f on injektio, jos ja vain jos $\text{Ker } f = \{e\}$.

Todistus. Ks. [7], s. 142-143.

Lause 3.5 Olkoon f homomorfismi ryhmältä G ryhmään G_1 . Silloin $\text{Ker } f$ on ryhmän G normaali aliryhmä.

Todistus. Ks. [7], s. 143.

Lause 3.6 Olkoon H ryhmän G normaali aliryhmä. Määritellään kuvaus g ryhmältä G tekijäryhmälle G/H seuraavasti: $g(a) = aH$ aina, kun $a \in G$. Silloin g on epimorfismi ryhmältä G ryhmälle G/H ja $\text{Ker } g = H$. (Homomorfismia g kutsutaan **luonnolliseksi homomorfismiksi** ryhmältä G ryhmälle G/H).

Todistus. (Vrt. [7], s. 144.) Kuvauksen g määritelmästä seuraa, että kuvaus g on surjektio ryhmältä G ryhmälle G/H . Osoitetaan nyt, että g on homomorfismi. Olkoot $a, b \in G$. Silloin $g(ab) = abH = aHbH = g(a)g(b)$. Täten g on homomorfismi ryhmältä G ryhmälle G/H . Koska siis g on surjektiivinen homomorfismi, niin se on epimorfismi.

Osoitetaan vielä, että $\text{Ker } g = H$. Nyt $a \in \text{Ker } g$ jos ja vain jos $g(a) = eH$. Nyt $g(a) = eH$ silloin ja vain silloin, kun $aH = eH$. Edelleen lauseen 2.13 nojalla $aH = eH$, jos ja vain jos $e^{-1}a = a \in H$. Näin on osoitettu, että $\text{Ker } g = H$. \square

Lause 3.6 merkitsee sitä, että ryhmän G jokainen tekijäryhmä G/H on ryhmän G homomorfinen kuva, koska lauseen kuvaus g on epimorfismi.

Määritellään nyt erityinen ryhmien välisen homomorfismin laji, **ryhmäisomorfismi**. Sen avulla voidaan kuvata sellaisten ryhmien välistä suhdetta, jotka ovat algebrallisesti katsoen samanlaiset.

Määritelmä 3.4 Homomorfismia f ryhmältä G ryhmään G_1 sanotaan **isomorfismiksi**, jos f on injektio ja surjektio. Tässä tapaksessa merkitään $G \simeq G_1$ ja sanotaan, että G ja G_1 ovat **isomorfiset**. Isomorfismia ryhmältä G ryhmälle G kutsutaan **automorfismiksi**.

Lause 3.7 Olkoon f isomorfismi ryhmältä G ryhmälle G_1 . Silloin seuraavat ominaisuudet ovat voimassa.

- (i) $f^{-1} : G_1 \rightarrow G$ on isomorfismi.
- (ii) G on kommutatiivinen, jos ja vain jos G_1 on kommutatiivinen.
- (iii) $o(a) = o(f(a))$ aina, kun $a \in G$.
- (iv) G on syklinen, jos ja vain jos G_1 on syklinen.

Todistus. Ks. [7], s. 145.

Esimerkki 3.3 Osoitetaan, että ryhmä $(\mathbf{Z}, +)$ ei ole isomorfinen ryhmän $(\mathbf{R}, +)$ kanssa.

Ratkaisu. Ryhmä $(\mathbf{Z}, +)$ on syklinen, sillä $(\mathbf{Z}, +) = \langle 1 \rangle$. Lauseen 3.7 (iv) perusteella ryhmä $(\mathbf{R}, +)$ on nyt syklinen, jos ryhmät $(\mathbf{Z}, +)$ ja $(\mathbf{R}, +)$ ovat isomorfiset. Esimerkissä 2.6 kuitenkin osoitettiin, että $(\mathbf{R}, +)$ ei ole syklinen. Siten ryhmät $(\mathbf{Z}, +)$ ja $(\mathbf{R}, +)$ eivät ole isomorfiset. ([7], tehtävä 7, s. 151)

Lause 3.8 Jokainen äärellinen, syklinen ryhmä on isomorfinen ryhmän $(\mathbf{Z}_n, +_n)$ kanssa. Jokainen ääretön, syklinen ryhmä on isomorfinen ryhmän $(\mathbf{Z}, +)$ kanssa.

Todistus. Ks. [7], s. 147.

3.2 Isomorfia- ja vastaavuuslauseet

Tässä kappaleessa todistetaan *homomorfismien peruslause*, eräitä *isomorfialauseita* sekä *vastaavuuslause*. Nämä lauseet osoittavat homomorfismien ja tekijäryhmien välisen suhteen.

Lause 3.9 *Olkoon f homomorfismi ryhmältä G ryhmälle G_1 . Olkoon H ryhmän G sellainen normaali aliryhmä, että $H \subseteq \text{Ker } f$, ja olkoon g luonnollinen homomorfismi ryhmältä G ryhmälle G/H . Silloin on olemassa sellainen yksikäsitteinen homomorfismi h ryhmältä G/H ryhmälle G_1 , että $f = h \circ g$. Lisäksi h on injektio, jos ja vain jos $H = \text{Ker } f$.*

$$\begin{array}{ccc} G & \xrightarrow{f} & G_1 \\ g \downarrow & h \nearrow & \\ G/H & & \end{array} \qquad \begin{array}{ccc} a & \xrightarrow{f} & f(a) \\ g \downarrow & h \nearrow & \\ aH & & \end{array}$$

Kuvio 2. Normaalin aliryhmän H synnyttämät homomorfismit g ja h

Todistus. (Vrt. [7], s. 153-154.) Tarkastellaan kuvausta $h : G/H \rightarrow G_1$, missä $h(aH) = f(a)$ aina, kun $aH \in G/H$. Ehdosta $aH = bH$ seuraa, että $b^{-1}a \in H \subseteq \text{Ker } f$ (lauseen 3.5 perusteella $\text{Ker } f$ on ryhmän G normaali aliryhmä). Näin ollen $f(b^{-1}a) = e_1$ eli $f(a) = f(b)$. Tällöin $h(aH) = h(bH)$, joten h on hyvin määritelty, toisin sanoen kukin lähtöjoukon alkio kuvautuu yhdelle arvojoukon alkioille. Olkoon $a \in G$. Silloin $(h \circ g)(a) = h(g(a)) = h(aH) = f(a)$. Siten $h \circ g = f$. Koska f kuvaa ryhmän G ryhmälle G_1 , niin kuvauksen h täytyy kuvata G/H ryhmälle G_1 . Nyt $h((aH)(bH)) = h((ab)H) = f(ab) = f(a)f(b) = h(aH)h(bH)$. Kuvaus h on siten homomorfismi ryhmältä G/H ryhmälle G_1 , ja se toteuttaa ehdon $f = h \circ g$. Yksikäsitteisyyden osoittamiseksi oletetaan, että $f = h' \circ g$ jollakin homomorfismilla h' ryhmältä G/H ryhmälle G_1 . Silloin $h(aH) = f(a) = (h' \circ g)(a) = h'(g(a)) = h'(aH)$ aina, kun $aH \in G/H$. Näin ollen $h = h'$, joten h on ainoa sellainen homomorfismi ryhmältä G/H ryhmälle G_1 , että $f = h \circ g$.

Oletetaan, että h on injektio. Osoitetaan, että $H = \text{Ker } f$. Olkoon $a \in \text{Ker } f$. Silloin $f(a) = e_1$ ja siten $h(aH) = e_1$. Koska $h(eH) = e_1$ ja h on injektio, niin $aH = eH$. Näin ollen $a \in H$ ja siten $\text{Ker } f \subseteq H$. Oletuksen perusteella $H \subseteq \text{Ker } f$, joten nyt $H = \text{Ker } f$.

Oletetaan kääntäen, että $H = \text{Ker } f$. Osoitetaan, että h on injektio. Olkoon $h(aH) = h(bH)$. Silloin $f(a) = f(b)$ eli $f(b^{-1}a) = e_1$. Siten $b^{-1}a \in \text{Ker } f = H$. Tästä seuraa, että $aH = bH$, joten h on injektio. \square

Lauseessa 3.9 oletetaan, että f on surjektio, toisin sanoen *koko* ryhmä G_1 on ryhmän G kuvajoukko.

Lauseesta 3.9 seuraa, että jos $H = \text{Ker } f$, niin h on isomorfismi ja täten $G/\text{Ker } f$ on isomorfinen ryhmän G_1 kanssa. Tämä merkitsee sitä, että jokainen epimorfismi ryhmältä G ryhmälle G_1 *indusoi isomorfismin* ryhmältä $G/\text{Ker } f$ ryhmälle G_1 . Tällä lauseella on keskeinen merkitys ryhmäteoriassa, ja se tunnetaan nimellä **ryhmähomomorfismien peruslause** (the fundamental theorem of homomorphisms for groups). Sitä kutsutaan myös ensimmäiseksi isomorfialauseeksi. Seuraavassa lause esitetään yleisessä muodossaan ja sille annetaan suora todistus.

Lause 3.10 (Ensimmäinen isomorfialause) *Olkoon f homomorfismi ryhmältä G ryhmään G_1 . Silloin $f(G)$ on ryhmän G_1 aliryhmä ja*

$$G/\text{Ker } f \simeq f(G).$$

Todistus. (Vrt. [7], s. 154.) Lauseen 3.1 nojalla $f(G)$ on ryhmän G_1 aliryhmä. Olkoon $H = \text{Ker } f$. Olkoon $h : G/H \rightarrow f(G)$, $h(aH) = f(a)$ aina, kun $aH \in G/H$. Olkoot $a, b \in G$. Nyt $aH = bH$, jos ja vain jos $b^{-1}a \in H = \text{Ker } f$. Tämä on voimassa silloin ja vain silloin, kun $f(b^{-1}a) = e_1$ eli $f(b^{-1})f(a) = e_1$. Tämä ehto on yhtäpitävä sen kanssa, että $f(a) = f(b)$, joten h on hyvin määritelty ja samalla injektio.

Olkoon $x \in f(G)$. Silloin on olemassa sellainen $b \in G$, että $x = f(b)$. Valitaan tällainen b . Siten $h(bH) = f(b) = x$. Tämä osoittaa, että h on surjektio.

Lopuksi todetaan, että $h(aHbH) = h(abH) = f(ab) = f(a)f(b) = h(aH)h(bH)$ aina, kun $aH, bH \in G/H$. Tämä osoittaa, että h on homomorfismi.

Näin on osoitettu, että kuvaus h ryhmältä G/H ryhmälle $f(G)$ on bijektiivinen homomorfismi eli isomorfismi, joten $G/\text{Ker } f \simeq f(G)$. \square

Lause 3.6 osoittaa, että ryhmän G jokainen tekijäryhmä G/H on ryhmän G homomorfinen kuva. Ensimmäinen isomorfialause todistaa käänteisen asian: ryhmän G jokainen homomorfinen kuva on isomorfinen ryhmän G jonkin tekijäryhmän kanssa. (Ks. [2], s. 97.)

Esimerkki 3.4 *Olkoot $(\mathbf{Z}, +)$ ja $(\mathbf{Z}_3, +_3)$ ryhmiä, ja olkoon $f : \mathbf{Z} \rightarrow \mathbf{Z}_3$, $f(n) = [n]$ aina, kun $n \in \mathbf{Z}$. Osoitetaan, että ryhmän $(\mathbf{Z}, +)$ aliryhmän $\langle 6 \rangle$ kautta syntyy homomorfia mutta ei isomorfiaa.*

Ratkaisu. Osoitetaan aluksi, että f on homomorfismi. Olkoot $a, b \in \mathbf{Z}$. Nyt $f(a + b) = [a + b] = [a] +_3 [b] = f(a) +_3 f(b)$, joten f on homomorfismi. Nyt f on myös epimorfismi, sillä selvästi $f(\mathbf{Z}) = \mathbf{Z}_3$. Nyt $\text{Ker } f = \{0, \pm 3, \pm 6, \dots\} = \langle 3 \rangle$, sillä $[0] = f(0) = f(\pm 3) = f(\pm 6) = \dots$. Näin ollen $\langle 6 \rangle \subset \langle 3 \rangle = \text{Ker } f$. Selvästi $H = \langle 6 \rangle$ on ryhmän $(\mathbf{Z}, +)$ normaali aliryhmä. Olkoon g luonnollinen homomorfismi $g : \mathbf{Z} \rightarrow \mathbf{Z}/\langle 6 \rangle$, $g(n) = n + \langle 6 \rangle$ aina, kun $n \in \mathbf{Z}$. Lauseen 3.9 mukaan on olemassa sellainen homomorfismi h ryhmältä $\mathbf{Z}/\langle 6 \rangle$ ryhmälle \mathbf{Z}_3 , että $f = h \circ g$. Kuvauksen h määrittelee nyt laskulaki $h(n + \langle 6 \rangle) = [n]$ aina, kun $n \in \mathbf{Z}$.

Koska $H \neq \text{Ker } f$, niin lauseen 3.9 perusteella h ei ole injektio. Tämä ilmenee siten, että h kuvaa kaksi ryhmän $\mathbf{Z}/\langle 6 \rangle$ alkiota ryhmän \mathbf{Z}_3 kullekin alkiolle. Nämä tapaukset ovat

$$\left. \begin{array}{l} 0 + \langle 6 \rangle \\ 3 + \langle 6 \rangle \end{array} \right\} \longrightarrow [0] = [3],$$

$$\left. \begin{array}{l} 1 + \langle 6 \rangle \\ 4 + \langle 6 \rangle \end{array} \right\} \longrightarrow [1] = [4],$$

$$\left. \begin{array}{l} 2 + \langle 6 \rangle \\ 5 + \langle 6 \rangle \end{array} \right\} \longrightarrow [2] = [5].$$

Lähteessä [7] esimerkki 3.4 esitetään ensimmäisen isomorfialauseen sovelluksena, mikä on virhe, sillä $H \neq \text{Ker } f$. Esimerkki 3.4 esittää kylläkin homomorfiaa, mutta ei isomorfiaa. Täydennetään siis esitystä esimerkillä 3.5, joka vastaa suoraan lauseen 3.10 sisältöä.

Esimerkki 3.5 Olkoon f homomorfismi ryhmältä $(\mathbf{Z}, +)$ ryhmälle $\mathbf{Z}/\langle 3 \rangle$, ja olkoon $f(n) = [n]$ aina, kun $n \in \mathbf{Z}$. Osoitetaan, että ryhmän $(\mathbf{Z}, +)$ aliryhmän $\langle 3 \rangle$ kautta syntyy isomorfia.

Ratkaisu. Esimerkissä 3.4 todettiin, että $f(\mathbf{Z}) = \mathbf{Z}_3$ ja $\langle 3 \rangle = \text{Ker } f$. Näin ollen lauseen 3.10 nojalla

$$\mathbf{Z}/\langle 3 \rangle \simeq \mathbf{Z}_3.$$

Se, että kysymyksessä on isomorfia, ilmenee tässä siten, että ensimmäisen isomorfialauseen määrittelemä kuvaus h kuvaa ryhmän $\mathbf{Z}/\langle 3 \rangle$ kunkin alkion yhdelle ja vain yhdelle ryhmän \mathbf{Z}_3 alkion. Nämä vastaavuudet ovat

$$\begin{aligned} 0 + \langle 3 \rangle &\longrightarrow [0], \\ 1 + \langle 3 \rangle &\longrightarrow [1], \\ 2 + \langle 3 \rangle &\longrightarrow [2]. \end{aligned}$$

Esimerkkejä 3.4 ja 3.5 vertailemalla käy havainnollisesti ilmi, mikä merkitys *indusoituvan homomorfismin* kannalta on sillä seikalla, valitaanko normaaliksi aliryhmäksi $\text{Ker } f$ vai sen aito aliryhmä. Edellisessä tapauksessa saadaan isomorfia, jälkimmäisessä tapauksessa tätä löyhempi yhteys ryhmien välille.

Esimerkki 3.6 Osoitetaan, että $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}_n$, kun $n > 0$.

Ratkaisu. Olkoon $n \in \mathbf{Z}^+$. Olkoon $f : \mathbf{Z} \rightarrow \mathbf{Z}_n, f(a) = [a]$ aina, kun $a \in \mathbf{Z}$. Nyt f on homomorfismi, sillä $f(a + b) = [a + b] = [a] +_n [b] = f(a) +_n f(b)$ aina, kun $a, b \in \mathbf{Z}$. Kuvauksen f määrittelystä nähdään selvästi, että ryhmän \mathbf{Z}_n jokaisella alkionolla on alkukuva ryhmässä \mathbf{Z} , joten f on epimorfismi. Siten \mathbf{Z}_n on ryhmän \mathbf{Z} homomorfinen kuva.

Tarkastellaan joukkoa $n\mathbf{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$. Tämä on sama kuin ryhmän \mathbf{Z}_n neutraalialkio $[0]$, joten $n\mathbf{Z} = [0]$. Koska $f(a) \in [0]$ aina, kun $a \in n\mathbf{Z}$, niin $n\mathbf{Z} = \text{Ker } f$. Neutraalialkiona $[0] = n\mathbf{Z}$ myös muodostaa ryhmän \mathbf{Z}_n triviaalin, normaalin aliryhmän. Siten voidaan muodostaa tekijäryhmä $\mathbf{Z}/n\mathbf{Z}$. Lauseen 3.10 nojalla nyt $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}_n$, kun $n > 0$. ([7], tehtävä 2, s. 164)

Ensimmäisen isomorfialauseen nojalla ryhmän G kaikki homomorfiset kuvat voidaan määrittää käyttämällä ryhmää G (ks. [4], s. 176). Havainnollistetaan tätä tärkeää asiaa itse laaditulla esimerkillä. (Vrt. [7], esimerkki 1, s. 162.)

Esimerkki 3.7 *Oma esimerkki.* Määritetään ryhmän $G = \{e^{i\frac{n\pi}{6}} \mid n \in \mathbf{Z}\} = \langle e^{i\frac{\pi}{6}} \rangle$ kaikki homomorfiset kuvat.

Ratkaisu. Esimerkissä 2.5 (s. 8) osoitettiin, että G on syklinen ryhmä, jonka kertaluku on 12. Olkoon H ryhmän G homomorfinen kuva. Tällöin on olemassa epimorfismi f ryhmältä G ryhmälle H . (Ainakin yksi homomorfinen kuva on olemassa, sillä identiteettikuvaus on epimorfismi. Tällöin $H = G$, joskin tapaus on triviaali.) Lauseen 3.5 nojalla $\text{Ker } f$ on ryhmän G normaali aliryhmä. Lauseen 3.10 perusteella $G/\text{Ker } f \simeq H$. Koska $\text{Ker } f$ on ryhmän G aliryhmä, niin etsitään seuraavaksi ryhmän G aliryhmät. Esimerkin 2.5 nojalla ryhmällä G on nyt syklinen aliryhmä K_r aina, kun $|K_r| = r \in \{1, 2, 3, 4, 6, 12\}$. Nyt voidaan määrittellä aliryhmä $K_r = \{(e^{i\frac{\pi}{6}})^k \mid k = n\frac{12}{|K_r|}, n = 0, 1, \dots, |K_r| - 1\}$. Esimerkiksi $K_3 = \{(e^{i\frac{\pi}{6}})^k \mid k = 4n, n = 0, 1, 2\}$. Tällöin siis k saa arvot 0, 4 ja 8,

joten $K_3 = \{1, e^{i\frac{2\pi}{3}}, e^{i\frac{4\pi}{3}}\}$. Nyt todetaan, että $\text{Ker } f = K_r$ jollakin indeksillä $r \in \{1, 2, 3, 4, 6, 12\}$. Näin ollen $H \simeq G/K_r$ jollakin indeksillä $r \in \{1, 2, 3, 4, 6, 12\}$.

Lauseen 2.25 mukaan K_r on normaali aliryhmä, joten on olemassa luonnollinen homomorfismi f ryhmältä G ryhmälle G/K_r . Nyt $f(a) = aK_r$ aina, kun $a \in G$. Tässä selvästi $\text{Ker } f = K_r$. Kuvauksen f määritelmästä nähdään selvästi, että f on epimorfismi, joten G/K_r on ryhmän G homomorfinen kuva aina, kun $r \in \{1, 2, 3, 4, 6, 12\}$.

Tiedetään, että äärellisen tekijäryhmän G/K_r kertaluku on $|G/K_r| = |G|/|K_r|$. Esimerkissä 2.14 osoitettiin, että syklisen ryhmän tekijäryhmä on syklinen. Näin voidaan päätellä, että ryhmän G homomorfisia kuvia ovat (isomorfian kannalta) sykliset ryhmät \mathbf{Z}_s , $s \in \{1, 2, 3, 4, 6, 12\}$. Tekijäryhmään G/K_r liittyy isomorfia

$$G/K_r \simeq \mathbf{Z}_{\frac{12}{r}}$$

aina, kun $r \in \{1, 2, 3, 4, 6, 12\}$.

Lause 3.11 (Toinen isomorfialause) *Olkkoon H ryhmän G aliryhmä, ja olkkoon K ryhmän G normaali aliryhmä. Silloin*

$$H/(H \cap K) \simeq (HK)/K.$$

Todistus. (Vrt. [7], s. 156.) Esimerkin 2.12 nojalla HK on ryhmän G aliryhmä. Selvästi $K \subseteq HK$. Koska K on normaali ryhmässä G ja $HK \subseteq G$, niin K on ryhmän HK normaali aliryhmä. Tällöin voidaan muodostaa tekijäryhmä $(HK)/K$. Olkkoon $f : H \rightarrow (HK)/K$, $f(h) = hK$ aina, kun $h \in H$. Nyt $f(h_1h_2) = h_1h_2K = h_1Kh_2K = f(h_1)f(h_2)$ aina, kun $h_1, h_2 \in H$. Näin ollen f on homomorfismi. Olkkoon $xK \in (HK)/K$. Silloin ovat olemassa sellaiset $h \in H$ ja $k \in K$, että $x = hk$. Siten $xK = (hk)K = (hK)(kK) = hK = f(h)$. Tämä osoittaa, että f on epimorfismi ja siten $f(H) = (HK)/K$. Ensimmäisen isomorfialauseen nojalla tästä seuraa, että

$$H/\text{Ker } f \simeq (HK)/K.$$

Osoitetaan vielä, että $\text{Ker } f = H \cap K$. Nyt

$$\begin{aligned} \text{Ker } f &= \{h \in H \mid f(h) = \text{ryhmän } (HK)/K \text{ neutraalialkio}\} \\ &= \{h \in H \mid f(h) = eK\} \\ &= \{h \in H \mid hK = K\} \\ &= \{h \in H \mid h \in K\} \\ &= H \cap K. \end{aligned}$$

Lauseen 3.5 nojalla $\text{Ker } f$ on ryhmän H normaali aliryhmä. Näin ollen tekijäryhmä $H/(H \cap K)$ voidaan muodostaa. Siten $H/(H \cap K) \simeq (HK)/K$. \square

Lauseen 3.11 todistuksessa määritelty kuvaus f voidaan tulkita luonnollisen homomorfismin $g : G \rightarrow G/K$ rajoittumaksi aliryhmään H (ks. [2], s. 99). Tämä toteamus selkiyttää toisen isomorfialauseen merkitystä.

Esimerkissä 5.2.7 ([7], s. 156-157) on kaksi painovirhettä; kuvauksen h isomorfisuus ilmenee seuraavasti: $h : 0 + \langle 6 \rangle \rightarrow 0 + \langle 3 \rangle$, $2 + \langle 6 \rangle \rightarrow 1 + \langle 3 \rangle$, $4 + \langle 6 \rangle \rightarrow 2 + \langle 3 \rangle$.

Lähteessä [7] ei ole toista isomorfialauseetta havainnollistavia harjoitustehtäviä. Täydennetään esitystä seuraavalla esimerkillä ([3], tehtävä 15.7, s. 150).

Esimerkki 3.8 Olkoon $G = (\mathbf{Z}_{24}, +_{24})$ ja olkoot $H = \langle [4] \rangle$ ja $K = \langle [6] \rangle$ ryhmän G aliryhmiä. Todetaan toisen isomorfialauseen ilmaisema isomorfia.

Ratkaisu. Ryhmän G kaikki aliryhmät ovat normaaleja lauseen 2.25 perusteella.

a) Luetellaan kaikki aliryhmien $H +_{24} K$ ja $H \cap K$ alkiot.

Nyt $H = \langle [4] \rangle = \{[0], [4], [8], [12], [16], [20]\}$ ja $K = \langle [6] \rangle = \{[0], [6], [12], [18]\}$, joten $H +_{24} K = \{[0], [2], [4], [6], [8], [10], [12], [14], [16], [18], [20], [22]\} = \langle [2] \rangle$ ja $H \cap K = \{[0], [12]\} = \langle [12] \rangle$.

b) Luetellaan tekijäryhmän $H/(H \cap K) = \langle 4 \rangle / \langle 12 \rangle$ sivuluokat alkioineen.

$$[0] +_{24} H \cap K = [0] +_{24} \{[0], [12]\} = \{[0], [12]\},$$

$$[4] +_{24} H \cap K = [4] +_{24} \{[0], [12]\} = \{[4], [16]\},$$

$$[8] +_{24} H \cap K = [8] +_{24} \{[0], [12]\} = \{[8], [20]\}.$$

c) Luetellaan tekijäryhmän $(H +_{24} K)/K = \langle 2 \rangle / \langle 6 \rangle$ sivuluokat alkioineen.

$$[0] +_{24} K = K = \{[0], [6], [12], [18]\},$$

$$[2] +_{24} K = [2] +_{24} \{[0], [6], [12], [18]\} = \{[2], [8], [14], [20]\},$$

$$[4] +_{24} K = [4] +_{24} \{[0], [6], [12], [18]\} = \{[4], [10], [16], [22]\}.$$

d) Esitetään toisen isomorfialauseen kuvaama ryhmien $H/(H \cap K)$ ja $(H +_{24} K)/K$ välinen vastaavuus.

Nyt siis $H/(H \cap K) = \langle [4] \rangle / \langle [12] \rangle = \{\{[0], [12]\}, \{[4], [16]\}, \{[8], [20]\}\}$ ja

$(H +_{24} K)/K = \langle [2] \rangle / \langle [6] \rangle = \{\{[0], [6], [12], [18]\}, \{[2], [8], [14], [20]\}, \{[4], [10], [16], [22]\}\}.$

Lauseen 3.11 todistuksessa määritelty epimorfismi $f : H \rightarrow (H +_{24} K)/K$ ilmaisee vastaavuudet

$$[0], [12] \rightarrow [0] +_{24} K = \{[0], [6], [12], [18]\},$$

$$[4], [16] \rightarrow [4] +_{24} K = \{[4], [10], [16], [22]\},$$

$$[8], [20] \rightarrow [2] +_{24} K = \{[2], [8], [14], [20]\}.$$

Luonnollinen homomorfismi $g : H \rightarrow H/(H \cap K)$ ilmaisee vastaavuudet

$$[0], [12] \rightarrow [0] +_{24} \{[0], [12]\} = \{[0], [12]\},$$

$$[4], [16] \rightarrow [4] +_{24} \{[0], [12]\} = \{[4], [16]\},$$

$$[8], [20] \rightarrow [8] +_{24} \{[0], [12]\} = \{[8], [20]\}.$$

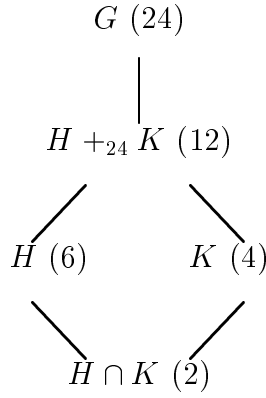
Epimorfismin f indusoima isomorfismi $h : H/(H \cap K) \rightarrow (H +_{24} K)/K$ ilmaisee nyt vastaavuudet

$$[0] +_{24} \{[0], [12]\} \rightarrow [0] +_{24} K = \{[0], [6], [12], [18]\},$$

$$[4] +_{24} \{[0], [12]\} \rightarrow [4] +_{24} K = \{[4], [10], [16], [22]\},$$

$$[8] +_{24} \{[0], [12]\} \rightarrow [2] +_{24} K = \{[2], [8], [14], [20]\}.$$

Esitetään vielä ryhmän $G = \mathbf{Z}_{24}$ ja sen aliryhmien suhteet seuraavalla hilakaa-
violla; liitetään siihen kunkin ryhmän kertaluku, joka merkitään sulkuihin.



Kuvio 3. Ryhmän \mathbf{Z}_{24} hilakaavio

Lauseen 3.11 määrittelemää isomorfiaa kutsutaan joskus *timantti-isomorfiaksi*; nimitys johtuu kuvion 3 rakenteesta (ks. [2], s. 99).

Lause 3.12 *Olkoon f homomorfismi ryhmältä G ryhmälle G_1 . Olkoon H ryhmän G sellainen normaali aliryhmä, että $H \supseteq \text{Ker } f$. Olkoon g luonnollinen homomorfismi ryhmältä G ryhmälle G/H , ja olkoon g' luonnollinen homomorfismi ryhmältä G_1 ryhmälle $G_1/f(H)$. Silloin on olemassa sellainen yksikäsitteinen isomorfismi h ryhmältä G/H ryhmälle $G_1/f(H)$, että $g' \circ f = h \circ g$.*

$$\begin{array}{ccc}
G & \xrightarrow{f} & G_1 \\
g \downarrow & & \downarrow g' \\
G/H & \xrightarrow{h} & G_1/f(H)
\end{array}$$

Kuvio 4. Oletuksen $H \supseteq \text{Ker } f$ nojalla syntyvä isomorfismi h

Todistus. (Vrt. [7], s. 157.) Jos osoitetaan, että $\text{Ker } g' \circ f = H$, niin lauseen 3.9 nojalla on olemassa yksikäsitteinen isomorfismi h ryhmältä G/H ryhmälle $G_1/f(H)$. Oletetaan aluksi, että $a \in H$. Osoitetaan, että $H \subseteq \text{Ker } g' \circ f$. Nyt $(g' \circ f)(a) = g'(f(a))$ on ryhmän $G_1/f(H)$ neutraalialkio, koska $f(a) \in f(H) = \text{Ker } g'$. Näin ollen $a \in \text{Ker } g' \circ f$, mistä seuraa, että $H \subseteq \text{Ker } g' \circ f$.

Kääntäen oletetaan, että $a \in \text{Ker } g' \circ f$. Osoitetaan, että $\text{Ker } g' \circ f \subseteq H$. Nyt $g'(f(a))$ on ryhmän $G_1/f(H)$ neutraalialkio ja siten $f(a) \in \text{Ker } g' = f(H)$. Sen vuoksi on olemassa sellainen $b \in H$, että $f(b) = f(a)$ eli $f(ab^{-1}) = e_1$. Tästä seuraa, että $ab^{-1} \in \text{Ker } f \subseteq H$ ja siten $a = (ab^{-1})b \in H$. Näin ollen $\text{Ker } g' \circ f \subseteq H$.

Koska siis $\text{Ker } g' \circ f = H$, niin väite on tosi. \square

Lause 3.13 (Kolmas isomorfialause) *Olkoot H_1 ja H_2 ryhmän G sellaisia normaaleja aliryhmiä, että $H_1 \subseteq H_2$. Silloin*

$$(G/H_1)/(H_2/H_1) \simeq G/H_2.$$

Todistus. (Ks. [7], s. 157.) Korvataan lauseessa 3.12 ryhmä G_1 ryhmällä G/H_1 , ryhmä H ryhmällä H_2 ja ryhmä $G_1/f(H)$ ryhmällä $(G/H_1)/(H_2/H_1)$. Tässä f on luonnollinen homomorfismi ryhmältä G ryhmälle G/H_1 . Koska $H_2 \subseteq G$, niin nyt $f(H_2) = H_2/H_1$. Ks. kuvio 5. \square

$$\begin{array}{ccc}
G & \xrightarrow{f} & G/H_1 \\
g \downarrow & & \downarrow g' \\
G/H_2 & \xrightarrow{h} & (G/H_1)/(H_2/H_1)
\end{array}$$

Kuvio 5. Tekijäryhmän tekijäryhmään $(G/H_1)/(H_2/H_1)$ liittyvä isomorfismi h

Lauseen 3.13 mukaan tekijäryhmän G/H_1 tekijäryhmä $(G/H_1)/(H_2/H_1)$ on isomorfinen yksinkertaisen tekijäryhmän G/H_2 kanssa.

Lähteessä [7] ei ole myöskään kolmatta isomorfialauseetta havainnollistavia harjoitustehtäviä. Täydennetään tässäkin esitystä ylimääräisellä esimerkillä (ks. [3], tehtävä 15.9, s. 150).

Esimerkki 3.9 Olkoon $G = (\mathbf{Z}_{24}, +_{24})$ ja olkoot $H_2 = \langle [4] \rangle$ ja $H_1 = \langle [8] \rangle$ ryhmän G aliryhmiä. Esitetään kolmannen isomorfialauseen määrittelemä ryhmien G/H_2 ja $(G/H_1)/(H_2/H_1)$ välinen vastaavuus.

Ratkaisu. Nyt $G = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23]\}$.

a) Luetellaan tekijäryhmän G/H_2 sisältämät sivuluokat alkioineen.

Nyt $H_2 = \langle [4] \rangle = \{[0], [4], [8], [12], [16], [20]\}$.

Nyt siis tekijäryhmän G/H_2 sivuluokat alkioineen ovat

$$\begin{aligned}
[0] +_{24} H_2 &= \{[0], [4], [8], [12], [16], [20]\}, \\
[1] +_{24} H_2 &= \{[1], [5], [9], [13], [17], [21]\}, \\
[2] +_{24} H_2 &= \{[2], [6], [10], [14], [18], [22]\}, \\
[3] +_{24} H_2 &= \{[3], [7], [11], [15], [19], [23]\}.
\end{aligned}$$

b) Nyt $H_1 = \langle [8] \rangle = \{[0], [8], [16]\}$, joten tekijäryhmän G/H_1 sivuluokat alkioineen ovat

$$\begin{aligned}
[0] +_{24} H_1 &= \{[0], [8], [16]\}, \\
[1] +_{24} H_1 &= \{[1], [9], [17]\}, \\
[2] +_{24} H_1 &= \{[2], [10], [18]\}, \\
[3] +_{24} H_1 &= \{[3], [11], [19]\}, \\
[4] +_{24} H_1 &= \{[4], [12], [20]\}, \\
[5] +_{24} H_1 &= \{[5], [13], [21]\}, \\
[6] +_{24} H_1 &= \{[6], [14], [22]\}, \\
[7] +_{24} H_1 &= \{[7], [15], [23]\}.
\end{aligned}$$

c) Tekijäryhmän H_2/H_1 sivuluokat alkioineen ovat

$$\begin{aligned}
[0] +_{24} H_1 &= [0] +_{24} \{[0], [8], [16]\} = \{[0], [8], [16]\}, \\
[4] +_{24} H_1 &= [4] +_{24} \{[0], [8], [16]\} = \{[4], [12], [20]\}.
\end{aligned}$$

(Huomataan helposti, että $\{[0], [8], [16]\}$ on tekijäryhmän H_2/H_1 neutraalialkio.)

d) Tekijäryhmän $(G/H_1)/(H_2/H_1)$ sivuluokat alkioineen ovat

$$\begin{aligned}
([0] +_{24} H_1) +_{24} (H_2/H_1) &= \{[0] +_{24} H_1, [4] +_{24} H_1\} = \{\{[0], [8], [16]\}, \{[4], [12], [20]\}\}, \\
([1] +_{24} H_1) +_{24} (H_2/H_1) &= \{[1] +_{24} H_1, [5] +_{24} H_1\} = \{\{[1], [9], [17]\}, \{[5], [13], [21]\}\}, \\
([2] +_{24} H_1) +_{24} (H_2/H_1) &= \{[2] +_{24} H_1, [6] +_{24} H_1\} = \{\{[2], [10], [18]\}, \{[6], [14], [22]\}\}, \\
([3] +_{24} H_1) +_{24} (H_2/H_1) &= \{[3] +_{24} H_1, [7] +_{24} H_1\} = \{\{[3], [11], [19]\}, \{[7], [15], [23]\}\}.
\end{aligned}$$

e) Esitetään kolmannen isomorfialauseen määrittelemä ryhmien G/H_2 ja $(G/H_1)/(H_2/H_1)$ välinen vastaavuus. Olkoon h lauseessa 3.12 määritelty isomorfismi. Ryhmien G/H_2 ja $(G/H_1)/(H_2/H_1)$ alkioiden välinen vastaavuus ilmenee nyt seuraavasti:

$$\begin{aligned} h([0] +_{24} H_2) &= \{\{[0], [8], [16]\}, \{[4], [12], [20]\}\}, \\ h([1] +_{24} H_2) &= \{\{[1], [9], [17]\}, \{[5], [13], [21]\}\}, \\ h([2] +_{24} H_2) &= \{\{[2], [10], [18]\}, \{[6], [14], [22]\}\}, \\ h([3] +_{24} H_2) &= \{\{[3], [11], [19]\}, \{[7], [15], [23]\}\}. \end{aligned}$$

Esitetään seuraavaksi vastaavuuslause (correspondence theorem), josta on eräissä tapauksissa hyötyä toisen ryhmän rakenteen selvittämisessä, kun toinen ryhmä tunnetaan.

Lause 3.14 (Vastaavuuslause) *Olkoon f epimorfismi ryhmältä G ryhmälle G_1 . Silloin f synnyttää injektiivisen inklusion (one-one inclusion), joka säilyttää vastaavuuden ryhmän G niiden aliryhmien, jotka sisältävät aliryhmän $\text{Ker } f$, ja ryhmän G_1 aliryhmien välillä. Tämä tarkoittaa sitä, että ryhmien välillä on injektio, joka säilyttää aliryhmien väliset suhteet siirryttäessä ryhmään G_1 . Jos H ja K ovat ryhmien G ja G_1 toisiaan vastaavat aliryhmät, niin H on ryhmän G normaali aliryhmä, jos ja vain jos K on ryhmän G_1 normaali aliryhmä.*

Todistus. (Vrt. [7], s. 158-159.) Olkoon $\mathcal{H} = \{H \mid H \text{ on ryhmän } G \text{ sellainen aliryhmä, että } \text{Ker } f \subseteq H\}$ ja olkoon $\mathcal{K} = \{K \mid K \text{ on ryhmän } G_1 \text{ aliryhmä}\}$.

Olkoon $f^* : \mathcal{H} \rightarrow \mathcal{K}$, $f^*(H) = \{f(h) \mid h \in H\}$ aina, kun $H \in \mathcal{H}$. Silloin $f^*(H) \in \mathcal{K}$ lauseen 3.1 perusteella. Näin ollen f^* on funktio, koska f on funktio. Olkoon $K \in \mathcal{K}$. Merkitään aliryhmän K alkukuvaa $f^{-1}(K)$ ryhmässä G symbolilla H . Olkoon $a \in \text{Ker } f$. Silloin $f(a) = e_1 \in K$ ja siis $a \in f^{-1}(K) = H$. Näin ollen $\text{Ker } f \subseteq H$. Olkoot nyt $a, b \in H$. Silloin $f(a), f(b) \in K$. Koska f on homomorfismi, niin $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in K$. Siksi $ab^{-1} \in H$ ja siten H on ryhmän G aliryhmä lauseen 2.1 nojalla. Koska H sisältää aliryhmän $\text{Ker } f$, niin $H \in \mathcal{H}$.

Edellä on osoitettu, että f^* kuvaa joukon \mathcal{H} joukolle \mathcal{K} , joten f^* on surjektio. Olkoot $H_1, H_2 \in \mathcal{H}$. Oletetaan nyt, että $f^*(H_1) = f^*(H_2)$. Olkoon $h_1 \in H_1$. Silloin on olemassa sellainen $h_2 \in H_2$, että $f(h_1) = f(h_2)$. Tästä seuraa, että $f(h_1 h_2^{-1}) = e_1$ ja siten $h_1 h_2^{-1} \in \text{Ker } f \subseteq H_2$. Täten $h_1 = (h_1 h_2^{-1}) h_2 \in H_2$, mistä seuraa, että $H_1 \subseteq H_2$. Vastaavasti voidaan osoittaa, että $H_2 \subseteq H_1$. Näin ollen $H_1 = H_2$ ja siten f^* on injektio. Koska siis f^* on surjektio ja injektio, niin se on bijektio. Selvästi $H_1 \subseteq H_2$, jos ja vain jos $f^*(H_1) \subseteq f^*(H_2)$. Lisäksi f^* on injektio, joten $H_1 \subset H_2$ silloin ja vain silloin, kun $f^*(H_1) \subset f^*(H_2)$.

Oletetaan nyt, että H on ryhmän G sellainen normaali aliryhmä, että $\text{Ker } f \subseteq H$. Olkoon $K = f^*(H)$. Osoitetaan, että K on ryhmän G_1 (lähteessä [7], s. 159, virheellisesti ”ryhmän G ”) normaali aliryhmä. Olkoon $f(a) \in G_1$ ja $f(h) \in K$. Nyt $aha^{-1} \in H$, sillä H on ryhmän G normaali aliryhmä. Siten $f(a)f(h)f(a)^{-1} = f(aha^{-1}) \in K$. Täten K on ryhmän G_1 normaali aliryhmä.

Oletetaan kääntäen, että J on ryhmän G_1 normaali aliryhmä ja että $L \in \mathcal{H}$ on sellainen, että $f^*(L) = J$. Osoitetaan, että L on ryhmän G normaali aliryhmä. Olkoon $a \in G$ ja $h \in L$. Silloin $f(aha^{-1}) = f(a)f(h)f(a)^{-1} \in J$ ja siten $aha^{-1} \in L$. Tämä osoittaa, että L on ryhmän G normaali aliryhmä. \square

Vastaavuuslause voidaan muotoilla erikseen *tekijäryhmiä* koskevaksi. Tämä tulos esitetään seuraavaksi. (Vrt. [1], s. 121.)

Lause 3.15 *Olkoon N ryhmän G normaali aliryhmä. Silloin ryhmän G/N jokainen aliryhmä on muotoa K/N , missä K on ryhmän G sellainen aliryhmä, joka sisältää aliryhmän N . Lisäksi K/N on ryhmän G/N normaali aliryhmä, jos ja vain jos K on ryhmän G normaali aliryhmä.*

Todistus. Ks. [7], s. 159.

Esimerkki 3.10 *Olkoon f epimorfismi äärelliseltä ryhmältä G ryhmälle \mathbf{Z}_{15} . Osoitetaan, että ryhmällä G on normaalit aliryhmät, joiden indeksit (erillisten vasempien sivuluokkien lukumäärät) ryhmässä G ovat 5 ja 3.*

Ratkaisu. Olkoon siis $f : G \rightarrow \mathbf{Z}_{15}$ epimorfismi. Ensimmäisen isomorfialauseen nojalla tällöin $G/\text{Ker } f \simeq \mathbf{Z}_{15}$. Koska \mathbf{Z}_{15} on syklinen ja sen kertaluku on 15, niin tekijäryhmä $G/\text{Ker } f$ on syklinen ja sen kertaluku on 15 lauseen 3.7 perusteella. Koska nyt $G/\text{Ker } f$ on äärellinen ja syklinen, sillä on lauseen 2.12 mukaan aliryhmä H_1 , jonka kertaluku on 5, sekä aliryhmä H_2 , jonka kertaluku on 3. Lauseen 2.10 nojalla aliryhmät H_1 ja H_2 ovat syklisiä, ja lauseen 2.25 mukaan nämä ovat normaaleja ryhmässä G . Lauseen 3.15 mukaan tällöin ovat olemassa sellaiset ryhmän G normaalit aliryhmät N_1 ja N_2 , että $\text{Ker } f \subseteq N_1$, $\text{Ker } f \subseteq N_2$, $N_1/\text{Ker } f = H_1$ ja $N_2/\text{Ker } f = H_2$. Täten voidaan kirjoittaa yhtälö

$$\begin{aligned} 15 &= |G/\text{Ker } f| = [G : \text{Ker } f] = \frac{|G|}{|\text{Ker } f|} = \frac{|G|}{|N_1|} \cdot \frac{|N_1|}{|\text{Ker } f|} \\ &= [G : N_1][N_1 : \text{Ker } f] = [G : N_1]|N_1/\text{Ker } f| = [G : N_1] \cdot 5. \end{aligned}$$

Tästä seuraa, että $[G : N_1] = 3$. Toiseksi voidaan muodostaa yhtälö

$$\begin{aligned} 15 &= |G/\text{Ker } f| = [G : \text{Ker } f] = \frac{|G|}{|\text{Ker } f|} = \frac{|G|}{|N_2|} \cdot \frac{|N_2|}{|\text{Ker } f|} \\ &= [G : N_2][N_2 : \text{Ker } f] = [G : N_2]|N_2/\text{Ker } f| = [G : N_2] \cdot 3. \end{aligned}$$

Tästä puolestaan seuraa, että $[G : N_2] = 5$. ([7], tehtävä 11, s. 164)

Näin tekijäryhmiä koskevan vastaavuuksilauseen avulla pystyttiin selvittämään ryhmän G rakennetta, kun ryhmän \mathbf{Z}_{15} rakenne tunnettiin; ratkaistussa esimerkissä 2 ([7], s. 162) viitataan harhaanjohtavasti lauseeseen 3.14.

4 Ryhmän vaikutukset

Ryhmäteoria käsitteli alunperin permutaatioryhmiä. Laajennetaan nyt joukon permutaatio joukkoon kohdistuvaa ryhmän vaikutusta koskevaksi. Määritellään johonkin joukkoon liittyvän *ryhmän vaikutuksen* käsite, jonka avulla voidaan selvittää tärkeitä äärellisten ryhmien ominaisuuksia. Käsite mahdollistaa tehokkaan, tarkoitukseen sopivan laskutekniikan.

Määritelmä 4.1 *Olkoon G ryhmä ja olkoon S epätyhjä joukko. Ryhmän G (vasen) vaikutus (action) joukkoon S on sellainen funktio $\cdot : G \times S \rightarrow S$ (merkitään $\cdot(g, x) \rightarrow g \cdot x$), että*

- (i) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ ja
- (ii) $e \cdot x = x$, missä e on ryhmän G neutraalialkio, aina, kun $x \in S$, $g_1, g_2 \in G$.

Jos epäselvyyttä ei synny, merkinnän $g \cdot x$ sijasta kirjoitetaan gx . Jos on olemassa ryhmän G vasen vaikutus joukkoon S , niin sanotaan, että G vaikuttaa joukkoon S vasemmalta ja että S on G -joukko.

Lause 4.1 *Olkoon S G -joukko, missä G on ryhmä ja S on epätyhjä joukko. Määritellään nyt relaatio \sim joukossa S seuraavasti:*

$$a \sim b, \text{ jos ja vain jos on olemassa sellainen } g \in G, \text{ että } g \cdot a = b.$$

Silloin \sim on ekvivalenssirelaatio joukossa S .

Todistus. (Vrt. [7], s. 173.) Kohdan (ii) mukaan $ea = a$ aina, kun $a \in S$, joten $a \sim a$. Siten \sim on refleksiivinen. Olkoot seuraavaksi $a, b, c \in S$. Oletetaan seuraavaksi, että $a \sim b$. Silloin on olemassa sellainen $g \in G$, että $ga = b$, mistä seuraa, että $g^{-1}b = g^{-1}(ga) = (g^{-1}g)a = ea = a$. Täten $b \sim a$, joten \sim on symmetrinen. Oletetaan lopuksi, että $a \sim b, b \sim c$. Silloin ovat olemassa sellaiset $g_1, g_2 \in G$, että $g_1a = b$ ja $g_2b = c$. Täten $(g_2g_1)a = g_2(g_1a) = g_2b = c$. Näin ollen $a \sim c$, joten \sim on transitiiivinen. Relaatio \sim täyttää siten kaikki ekvivalenssirelaation ehdot. \square

Määritelmä 4.2 *Olkoon G ryhmä, ja olkoon S (epätyhjä) G -joukko. Lauseen 4.1 ekvivalenssirelaation määrittelemiä ekvivalenssiluokkia kutsutaan ryhmän G **uriksi** (orbit) joukossa S .*

$$\text{Alkion } a \in S \text{ sisältävä ura on } [a] = \{ga \mid g \in G\}.$$

Lause 4.2 *Olkoon G ryhmä, ja olkoon S G -joukko. Osajoukko*

$$G_a = \{g \in G \mid ga = a\}$$

on ryhmän G aliryhmä.

Todistus. Ks. [7], s. 173. \square

Lauseen 4.2 aliryhmää G_a kutsutaan alkion a **stabiloijaksi** (stabilizer) tai alkion a **isotropiaryhmäksi** (isotropy group).

Lause 4.3 *Olkoon G ryhmä, ja olkoon S G -joukko. Silloin*

$$[G : G_a] = |[a]|$$

aina, kun $a \in S$.

Todistus. (Vrt. [7], s. 173-174.) Olkoon $a \in S$. Olkoon \mathcal{L} aliryhmän G_a kaikkien vasempien sivuluokkien joukko ryhmässä G . Nyt $[a] = \{b \in S \mid a \sim b\} = \{b \in S \mid ga = b \text{ jollakin alkiolla } g \in G\} = \{ga \mid g \in G\}$. Osoitetaan nyt, että on olemassa bijektio joukolta \mathcal{L} joukolle $[a]$. Määritellään kuvaus

$$f : \mathcal{L} \rightarrow [a], f(gG_a) = ga$$

aina, kun $gG_a \in \mathcal{L}$. Olkoot $g_1, g_2 \in G$. Tällöin $g_1G_a = g_2G_a$, jos ja vain jos $g_2^{-1}g_1 \in G_a$, jos ja vain jos $g_2^{-1}(g_1a) = (g_2^{-1}g_1)a = a$, jos ja vain jos $g_1a = g_2a$. Näin ollen f on injektio joukolta \mathcal{L} joukkoon $[a]$. Olkoon $b \in [a]$. Silloin on olemassa sellainen $g \in G$, että $ga = b$. Siten $f(gG_a) = ga = b$. Tästä seuraa, että f on surjektio. Näin on osoitettu, että f on bijektio, joten $[G : G_a] = |\mathcal{L}| = |[a]|$. \square

Lause 4.4 *Olkoon G ryhmä, ja olkoon S äärellinen G -joukko. Silloin*

$$|S| = \sum_{a \in A} [G : G_a],$$

missä A on joukon S osajoukko, joka sisältää täsmälleen yhden alkion kustakin urasta $[a]$.

Todistus. (Vrt. [7], s. 174.) Lauseen 4.1 mukaan joukko S voidaan osittaa unioniksi. Sen tähden

$$S = \bigcup_{a \in A} [a].$$

Nyt

$$|S| = \sum_{a \in A} |[a]| = \sum_{a \in A} [G : G_a]$$

lauseen 4.3 nojalla. \square

Esimerkissä 4.1 sovelletaan lausetta 4.4 tärkeässä erikoistapauksessa, jossa ryhmän G kertaluku on jokin alkuluvun p potenssi. Tulosta sovelletaan myöhemmin äärellisten ryhmien rakenteen analysoinnissa.

Esimerkki 4.1 (*Ks. [7], esimerkki 1, s. 176.*) *Olkoon S äärellinen G -joukko, missä G on ryhmä, jonka kertaluku on p^n , p alkuluku. Olkoon $S_0 = \{a \in S \mid ga = a \text{ aina, kun } g \in G\}$. Osoitetaan, että $|S| \equiv |S_0| \pmod{p}$, mistä käytetään myös lyhyempää merkintää $|S| \equiv_p |S_0|$.*

Ratkaisu. Lauseen 4.4 nojalla $|S| = \sum_{a \in A} [G : G_a]$, missä A on joukon S osajoukko, joka sisältää täsmälleen yhden alkion ryhmän G kustakin urasta $[a]$. Nyt $a \in S_0$, jos ja vain jos $ga = a$ aina, kun $g \in G$. Tämän kanssa yhtäpitävä on ehto $[a] = \{a\}$. Täten

$$|S| = |S_0| + \sum_{a \in A \setminus S_0} \frac{|G|}{|G_a|}.$$

Koska $|G_a| \neq |G|$ aina, kun $a \in A \setminus S_0$, niin $\frac{|G|}{|G_a|}$ on luvun p jokin potenssi aina, kun $a \in A \setminus S_0$. Täten $\frac{|G|}{|G_a|}$ on jaollinen luvulla p , mikä todistaa sen, että $|S| \equiv_p |S_0|$.

Jatkona esimerkille 4.1 seuraava esimerkki käsittelee ryhmän ja sen aliryhmien kertalukujen välisiä yhteyksiä.

Esimerkki 4.2 (*Vrt. [7], esimerkki 3 (i), s. 176-177.*) *Olkoon G äärellinen ryhmä ja olkoon H ryhmän G sellainen aliryhmä, että $|H| = p^k$, missä p on alkuluku ja k ei-negatiivinen kokonaisluku.*

(i) *Osoitetaan, että $[G : H] \equiv_p [N(H) : H]$, missä $N(H) = \{g \in G \mid gHg^{-1} = H\}$.*
(ii) *Osoitetaan, että jos p jakaa luvun $[G : H]$, niin $N(H) \neq H$.*

Ratkaisu. (i) Olkoon $S = \{xH \mid x \in G\}$. Selvästi S on epätyhjä. Olkoon ryhmän H vasen vaikutus joukkoon S $h(xH) = (hx)H$ aina, kun $h \in H, xH \in S$. Silloin S on H -joukko. Olkoon $S_0 = \{xH \in S \mid h(xH) = xH \text{ aina, kun } h \in H\}$. Esimerkin 4.1 nojalla $|S| \equiv_p |S_0|$. Nyt $xH \in S_0$, jos ja vain jos $h(xH) = xH$ aina, kun $h \in H$. Tämä pätee silloin ja vain silloin, kun $x^{-1}hx \in H$ aina, kun $h \in H$. Tämä on yhtäpitävää sen kanssa, että $x^{-1}Hx \subseteq H$. Nyt $|x^{-1}Hx| = |H|$. Näin ollen $xH \in S_0$,

jos ja vain jos $x^{-1}Hx \subseteq H$, mikä pätee silloin ja vain silloin, kun $x^{-1}Hx = H$ (sillä H on äärellinen ja $|x^{-1}Hx| = |H|$). Tämä on yhtäpitävää sen kanssa, että $x \in N(H)$. Tämä osoittaa, että S_0 on kaikkien aliryhmän H vasempien sivuluokkien joukko ryhmässä $N(H)$. Täten $|S_0| = [N(H) : H]$. Toisaalta $|S| = [G : H]$. Siten on voimassa relaatio $[G : H] \equiv_p [N(H) : H]$.

(ii) Edellisen kohdan perusteella $[G : H] \equiv_p [N(H) : H]$. Nyt oletuksen mukaan p jakaa luvun $[G : H]$, joten p jakaa luvun $[N(H) : H]$. Koska $[N(H) : H] \geq 1$, niin $N(H) \neq H$.

Ryhmän vaikutuksen käsitettä sovelletaan myöhemmin *Sylowin lauseiden* todistamiseen. Käsitteellä on kuitenkin muitakin sovelluksia. Esitetään tässä kiintoisaa *Burnsiden lause* ja kaksi esimerkkiä sen soveltamisesta.

Määritelmä 4.3 *Olkoon G ryhmä, ja olkoon S G -joukko. Olkoon $a \in S$ ja $g \in G$. Jos $ga = a$, niin sanotaan, että a on alkion g **kiinnittämä**. Jos on voimassa ehto $ga = a$ aina, kun $g \in G$, niin sanotaan, että a on ryhmän G kiinnittämä.*

Lause 4.5 (Burnside) *Olkoon S äärellinen epätyhjä joukko, ja olkoon G äärellinen ryhmä. Jos S on G -joukko, niin ryhmän G urien lukumäärä on*

$$\frac{1}{|G|} \sum_{g \in G} F(g),$$

missä $F(g)$ on alkion g kiinnittämien joukon S alkioden lukumäärä.

Todistus. (Vrt. [7], s. 175-176.) Olkoon $T = \{(g, a) \in G \times S \mid ga = a\}$. Koska $F(g)$ on sellaisten alkioden $a \in S$ lukumäärä, että $(g, a) \in T$, niin $|T| = \sum_{g \in G} F(g)$. Toisaalta $|G_a|$ on sellaisten alkioden $g \in G$ lukumäärä, että $(g, a) \in T$, joten $|T| = \sum_{a \in S} |G_a|$. Tässä laskettiin joukon T alkioden lukumäärän kahdella tavalla: ensin joukon S alkioden kannalta ja sitten ryhmän G alkioden kannalta.

Olkoon $S = [a_1] \cup [a_2] \cup \dots \cup [a_k]$, missä $\{[a_1], [a_2], \dots, [a_k]\}$ on ryhmän G kaikkien erillisten urien joukko joukossa S . Silloin

$$\sum_{g \in G} F(g) = \sum_{a \in [a_1]} |G_a| + \sum_{a \in [a_2]} |G_a| + \dots + \sum_{a \in [a_k]} |G_a|.$$

Olkoot a, b saman uran alkioita. Silloin $[a] = [b]$ ja $[G : G_a] = |[a]| = |[b]| = [G : G_b]$ lauseen 4.3 nojalla. Nyt G on äärellinen ja G_a on ryhmän G aliryhmä lauseen 4.2 perusteella. Tällöin $[G : G_a] = |G|/|G_a|$ Lagrangen lauseen 2.15 nojalla. Tästä seuraa edelleen, että

$$\frac{|G|}{|G_a|} = \frac{|G|}{|G_b|}$$

ja siten $|G_a| = |G_b|$. Näin ollen

$$\begin{aligned} \sum_{g \in G} F(g) &= |[a_1]| |G_{a_1}| + |[a_2]| |G_{a_2}| + \dots + |[a_k]| |G_{a_k}| \\ &= \frac{|G|}{|G_{a_1}|} |G_{a_1}| + \frac{|G|}{|G_{a_2}|} |G_{a_2}| + \dots + \frac{|G|}{|G_{a_k}|} |G_{a_k}| \\ &= k|G|, \end{aligned}$$

missä k on erillisten urien lukumäärä. Näin ollen

$$k = \frac{1}{|G|} \sum_{g \in G} F(g). \quad \square$$

(Vrt. [7], s. 175-176.)

Havainnollistetaan nyt lausetta 4.5 seuraavilla esimerkeillä ([3], s. 161-163).

Esimerkki 4.3 *Selvitetään ryhmän vaikutuksen käsitteen avulla, kuinka monella aidosti erilaisella tavalla tavallinen arpakuutio voidaan merkitä.*

Ratkaisu. Voidaan ensiksikin helposti todeta, että kuutio voidaan merkitä yhteensä $6! = 720$ tavalla niin, että jokainen taho on merkitty eri pistemäärällä $n_i \in \{1, 2, \dots, 6\}$. Olkoon S näiden merkintätapojen joukko. Osa näistä merkintätavoista tosin vastaa joitakin muita siinä mielessä, että toiseen merkintään päästään kuutiota kääntämällä. Korostetaan vielä, että joukon S alkio on yhdelmä, joka koostuu kuudesta eri tahoihin merkitystä pistemäärästä.

Arpakuutio voidaan asettaa 24 asentoon, ja mielivaltaisesta asennosta päästään mihin tahansa toiseen kuution pyörähdyksillä. Nämä pyörähdykset muodostavat erään ryhmän G , jonka kertaluku on 24 (todistus ohitetaan).

Pidetään kuution kahta merkintää samoina, jos toisesta päästään toiseen kuution pyörähdyksillä eli merkinnästä toiseen päästään ryhmän G alkion vaikutuksesta. Toisin sanoen katsotaan ryhmän G uran joukossa S vastaavan arpakuution yhtä merkintätapaa ja toisaalta eri urien vastaavan eri merkintätapoja. Arpakuutioiden erilaisten merkintätapojen määrittäminen johtaa näin siihen, että määritetään ryhmän G urien lukumäärä G -joukossa S . Nyt siis S on äärellinen G -joukko, jossa on 720 alkiota.

Olkoon arpakuutio merkitty millä tahansa tavalla siten, että kuhunkin tahoon on merkitty jokin pistemäärästä $n_i \in \{1, 2, \dots, 6\}$. Olkoon arpakuutio mielivaltaisessa asennossa. Olkoon $g \in G, g \neq e$. Koska $g \neq e$, niin ryhmän alkion g vaikutuksesta kuutio pyörähtää johonkin toiseen asentoon. Alkio $g \neq e$ ei siis kiinnitä kuutiota, joten kuution jokaisen tahon merkintä vaihtuu toiseksi. Koska kuution merkintä vaihtuu jokaisella erilaisella kuution merkintätavalla, niin $F(g) = 0$. Toisaalta neutraalialkio e ei käännä kuutiota, vaan kiinnittää kuution tahojen merkinnät. Koska kuution tahojen merkinnät säilyvät jokaisella erilaisella kuution merkintätavalla, niin $F(e) = 720$. Näin ollen urien lukumäärä on

$$k = \frac{1}{|G|} \sum_{g \in G} F(g) = \frac{1}{|G|} \left(\sum_{g \in G, g \neq e} F(g) + F(e) \right) = \frac{1}{24} \cdot (0 + 720) = 30$$

lauseen 4.5 nojalla. Todetaan siis, että arpakuutio voidaan merkitä 30:llä toisistaan poikkeavalla tavalla; sama tulos saadaan luonnollisesti myös ennestään tutuilla kombinatoriikan periaatteilla. ([3], esimerkki 17.1, s. 161)

Esimerkki 4.4 *Selvitetään, kuinka monella erilaisella tavalla tasasivuisen kolmion kulmat voidaan värjätä, kun käytettävissä on neljä väriä. Oletetaan lisäksi, että vain yhtä väriä käytetään yhteen kulmaan ja että samaa väriä voidaan käyttää samanaikaisesti myös eri kulmissa.*

Ratkaisu. Kukin kulma voidaan värjätä neljällä värillä, joten on yhteensä $4^3 = 64$ mahdollista värjättyä kolmiota. Olkoon S näiden värjättyjen kolmioiden joukko. Joukkoon S vaikuttava ryhmä G on *kolmion symmetrioiden ryhmä* (ks. s. 4). Ryhmän G alkioita ovat ne tavat, joilla kaksi samanlaista tasasivuista kolmiota voidaan asettaa päällekkäin. Ryhmä G on isomorfinen ryhmän S_3 kanssa (todistus sivuutetaan), minkä vuoksi ryhmässä G on kuusi alkioita. Lauseen 4.5 soveltamiseksi määritetään nyt jokaista $g \in G$ vastaava luku $F(g)$, mitä varten laaditaan seuraava taulukko.

Taulukko 2. Ryhmän G vaikutukset joukkoon S

alkio g	alkion g vaikutus	huomautus	$F(g)$
neutraalialkio e	kulmat paikoillaan		64
kierto, yksi askel	$1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1$	kaikki kulmat samanvärisiä	4
kierto, kaksi askelta	$1 \rightarrow 3, 2 \rightarrow 1, 3 \rightarrow 2$	kaikki kulmat samanvärisiä	4
kulmat 2 ja 3 vaihdetaan	$1 \rightarrow 1, 2 \rightarrow 3, 3 \rightarrow 2$	vaihdettavat samanvärisiä	16
kulmat 1 ja 3 vaihdetaan	$1 \rightarrow 3, 2 \rightarrow 2, 3 \rightarrow 1$	vaihdettavat samanvärisiä	16
kulmat 1 ja 2 vaihdetaan	$1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3$	vaihdettavat samanvärisiä	16

Näin ollen erillisten urien lukumäärä

$$k = \frac{1}{|G|} \sum_{g \in G} F(g) = \frac{1}{6} \cdot (64 + 4 + 4 + 16 + 16 + 16) = \frac{120}{6} = 20$$

lauseen 4.5 nojalla. Näin todetaan, että tasasivuisen kolmion kulmat voidaan värjätä 20 tavalla, kun käytettävissä on neljä väriä. (Vrt. [3], esimerkki 17.4, s. 162-163)

5 Ryhmien ulkoiset ja sisäiset suorat tulot

Suoran tulon määrittelyn avulla ryhmä voidaan kuvata pienempien ryhmien *tulo-na*. Jakamalla näin ryhmä tekijöihinsä päästään helpommin tarkastelemaan ryhmän rakennetta.

Olkoon $I_n = \{1, 2, \dots, n\}$. Olkoon $\{G_i \mid i \in I_n\}$ jokin ryhmien joukko. Olkoon G näiden tekijöiden tulojoukko eli karteeminen tulo; toisin sanoen

$$G = G_1 \times G_2 \times \dots \times G_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in G_i, i \in I_n\}.$$

Määritellään laskutoimitus $*$ joukossa G seuraavasti:

$$(a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$$

aina, kun $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in G$.

Lause 5.1 *Olkoon $\{G_i \mid i \in I_n\}$ ryhmien joukko ja olkoon $G = G_1 \times G_2 \times \dots \times G_n$. Olkoon e_i ryhmän G_i neutraalialkio aina, kun $i \in I_n$. Silloin $(G, *)$ on ryhmä, missä $*$ on yllä määritelty laskutoimitus. Ryhmän G neutraalialkio on $e = (e_1, e_2, \dots, e_n)$ ja mielivaltaisen alkion $(a_1, a_2, \dots, a_n) \in G$ käänteisalkio on*

$$(a_1, a_2, \dots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}).$$

Olkoon lisäksi $H_i = \{(e_1, e_2, \dots, e_{i-1}, a_i, e_{i+1}, \dots, e_n) \mid a_i \in G_i\}$ aina, kun $i \in I_n$. Silloin seuraavat ominaisuudet ovat voimassa.

- (i) H_i on ryhmän G normaali aliryhmä aina, kun $i \in I_n$.
- (ii) Jokainen $a \in G$ voidaan yksikäsitteisesti ilmaista muodossa $a = h_1 h_2 \cdots h_n$, missä $h_i \in H_i, i \in I_n$.
- (iii) $H_i \cap (H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$ aina, kun $i \in I_n$.
- (iv) $G = H_1 H_2 \cdots H_n$.

Todistus. Ks. [7], s. 181-183.

Määritelmä 5.1 Lauseen 5.1 ryhmä G on ryhmien $G_i, i = 1, 2, \dots, n$, **ulkoinen suora tulo** (external direct product).

Määritelmä 5.2 Olkoon G ryhmä ja $\{N_i | i \in I_n\}$ ryhmän G normaalien aliryhmien joukko. Silloin G on normaalien aliryhmiensä N_1, N_2, \dots, N_n **sisäinen suora tulo** (internal direct product), jos jokainen $a \in G$ voidaan yksikäsitteisesti ilmaista muodossa $a = a_1 a_2 \cdots a_n$, missä $a_i \in N_i$ aina, kun $i \in I_n$.

Olkoon $G = G_1 \times G_2 \times \cdots \times G_n$ ryhmien $G_i, i \in I_n$, ulkoinen suora tulo, ja olkoon H_i lauseessa 5.1 määritelty ryhmän G normaali aliryhmä. Silloin ryhmä G on aliryhmiensä H_1, H_2, \dots, H_n sisäinen suora tulo lauseen 5.1 (ii) nojalla.

Lause 5.2 Olkoon G ryhmä ja olkoon $\{N_i | i \in I_n\}$ ryhmän G normaalien aliryhmien joukko. Silloin G on aliryhmien $\{N_i | i \in I_n\}$ sisäinen suora tulo, jos ja vain jos $G = N_1 N_2 \cdots N_n$ ja $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_n) = \{e\}$ aina, kun $i \in I_n$.

Todistus. Ks. [7], s. 183-184.

Lause 5.3 Olkoon G normaalien aliryhmiensä $N_i, i \in I_n$, sisäinen suora tulo. Silloin

$$G \simeq N_1 \times N_2 \times \cdots \times N_n.$$

Todistus. Ks. [7], s. 184-185.

Lauseen 5.3 mukaan normaalien aliryhmiensä sisäisenä suorana tulona kuvattava ryhmä G on isomorfinen samojen aliryhmien ulkoisen suoran tulon kanssa. Näin ollen tästä lähtien käytetään merkintää $G = N_1 \times N_2 \times \cdots \times N_n$ silloin, kun G on normaalien aliryhmiensä $N_i, i \in I_n$, suora sisäinen tulo.

Esimerkki 5.1 (Vrt. [7], esimerkki 5, s. 186-187.) Olkoot A ja B syklisiä ryhmiä, joiden kertaluvuille m ja n pätee ehto $\text{sy}(m, n) = 1$. Osoitetaan, että tällöin $A \times B$ on syklinen ryhmä, jonka kertaluku on mn .

Ratkaisu. Olkoon $|A| = m$ ja $|B| = n$. Oletuksen perusteella on olemassa sellainen $a \in A$ ja sellainen $b \in B$, että $A = \langle a \rangle$ ja $B = \langle b \rangle$. Olkoon $g = (a, b)$. Selvästi $g \in A \times B$. Silloin $g^{mn} = (a, b)^{mn} = (a^{mn}, b^{mn}) = (e_A, e_B)$, missä e_A on ryhmän A ja e_B on ryhmän B neutraalialkio. Olkoon $o(g) = t$. Silloin $(a, b)^t = (e_A, e_B)$. Tästä seuraa, että $a^t = e_A$ ja $b^t = e_B$. Näin ollen $m | t$ ja $n | t$. Koska $\text{sy}(m, n) = 1$, niin $mn | t$. Täten mn on pienin sellainen positiivinen kokonaisluku, että $g^{mn} = e$. Näin ollen $o(g) = mn$. Nyt $|A \times B| = mn$ ja $A \times B$ sisältää alkion g , jonka kertaluku on mn . Näin on osoitettu, että $A \times B$ on syklinen ryhmä, jonka kertaluku on mn .

Esimerkki 5.2 Olkoon G äärellinen syklinen ryhmä, jonka kertaluku on mn , missä $\text{sy}(m, n) = 1$. Olkoot H ja K ryhmän G sellaisia aliryhmiä, että $|H| = m$ ja $|K| = n$. Osoitetaan, että tällöin $G = H \times K$.

Ratkaisu. Lauseen 2.25 nojalla H ja K ovat ryhmän G normaaleja aliryhmiä. Nyt $|H \cap K|$ jakaa luvun $|H| = m$ ja $|H \cap K|$ jakaa luvun $|K| = n$. Koska $\text{syt}(m, n) = 1$, niin $|H \cap K| = 1$. Täten lauseen 2.19 nojalla $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{mn}{1} = mn = |G|$.

Koska $HK \subseteq G$, $|HK| = |G|$ ja G on äärellinen, niin $G = HK$. Näin ollen $G = HK$, $H \cap K = \{e\}$ ja H ja K ovat ryhmän G normaaleja aliryhmiä. Täten G on aliryhmien H ja K suora sisäinen tulo lauseen 5.2 perusteella. Näin ollen $G = H \times K$ lauseen 5.3 nojalla. ([7], tehtävä 6, s. 188)

6 Sylowin lauseet

6.1 Konjugaattiluokat

Ryhmien analysoinnissa käytetään paljon käsitettä *ryhmän konjugaattirelaatio*. Sen avulla ryhmä voidaan jakaa erillisiin ekvivalenssiluokkiin. Äärellisen ryhmän kertaluku pyritään jakamaan tekijöihinsä; tähän jakoon käytetään *luokkayhtälöä*.

Määritelmä 6.1 *Olkoon G ryhmä ja olkoon $a \in G$. Alkion a keskittäjä (centralizer) eli normalisoija (normalizer) ryhmässä G on joukko $C(a)$, jonka kaikki alkiot kommutoivat alkion a kanssa; toisin sanoen*

$$C(a) = \{b \in G \mid ba = ab\}.$$

Huomataan välittömästi, että $C(a) = G$, jos ja vain jos $a \in Z(G)$.

Olkoon G ryhmä ja olkoon $a \in G$. Alkiota $b \in G$ kutsutaan alkion a **konjugaatiksi** ryhmässä G , jos on olemassa sellainen $c \in G$, että $b = cac^{-1}$.

Lause 6.1 *Olkoon G ryhmä ja $a \in G$.*

(i) *Silloin $C(a)$ on ryhmän G aliryhmä.*

(ii) *Ryhmässä G määritelty relaatio $\rho = \{(a, b) \in G \times G \mid b \text{ on alkion } a \text{ konjugaatti}\}$ on ekvivalenssirelaatio ryhmässä G . Relaatiota ρ kutsutaan **konjugaattirelaatioksi** (conjugacy). Relaation ρ ekvivalenssiluokkaa $[a]$ kutsutaan alkion a **konjugaattiluokaksi** ryhmässä G . Konjugaattiluokasta käytetään myös merkintää $C_l(a)$, joten $C_l(a) = [a] = \{xax^{-1} \mid x \in G\}$.*

(iii) *Alkion a konjugaattien lukumäärä on sama kuin aliryhmän $C(a)$ indeksi ryhmässä G , toisin sanoen $|C_l(a)| = [G : C(a)]$.*

Todistus. Ks. [7], s. 191. \square

Lause 6.2 *Olkoon G äärellinen ryhmä. Silloin*

$$|G| = \sum_a [G : C(a)],$$

missä yhteenlasku koskee täydellistä erillisten konjugaattiluokkien edustajien joukkoa.

Todistus. Ks. [7], s. 191. \square

Lause 6.3 Olkoon G äärellinen ryhmä. Silloin

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)],$$

missä $Z(G)$ on ryhmän G keskus ja yhteenlasku koskee täydellistä sellaisten erillisten konjugaattiluokkien edustajien (mahdollisesti tyhjää) joukkoa, jotka eivät kuulu joukkoon $Z(G)$.

Todistus. (Vrt. [7], s. 192.) Lauseen 6.2 nojalla $|G| = \sum_a [G : C(a)]$, missä yhteenlasku koskee täydellistä erillisten konjugaattiluokkien edustajien joukkoa. Näin ollen

$$|G| = \sum_{a \in Z(G)} [G : C(a)] + \sum_{a \notin Z(G)} [G : C(a)].$$

Alkio a kommutoi kaikkien ryhmän G alkioiden kanssa silloin ja vain silloin, kun $a \in Z(G)$. Tällöinhän $C(a) = G$ ja sen vuoksi $[G : C(a)] = 1$. Tästä seuraa, että $\sum_{a \in Z(G)} [G : C(a)] = |Z(G)|$. Nyt yllä esitetty yhtälö voidaan kirjoittaa muotoon

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)],$$

missä yhteenlasku koskee täydellistä sellaisten erillisten konjugaattiluokkien edustajien (mahdollisesti tyhjää) joukkoa, jotka eivät kuulu joukkoon $Z(G)$. \square

Lauseen 6.3 yhtälöä kutsutaan **konjugaattiluokkayhtälöksi**.

Konjugaattirelaatio on kiinnostava ei-kommutatiivisten ryhmien yhteydessä, mutta ei Abelin ryhmien kannalta. Olkoon G nyt Abelin ryhmä ja olkoot $a, b \in G$. Tällöin $Z(G) = G$. Nyt $ab = ba$, joten $b = aba^{-1}$. Näin ollen kaksi alkioita a ja b ovat konjugaatteja, jos ja vain jos ne ovat samat. (Ks. [5], s. 121.) Samalla havaitaan, että Abelin ryhmässä jokainen alkio a muodostaa oman konjugaattiluokkansa, toisin sanoen $C_l(a) = [a] = \{xax^{-1} \mid x \in G\} = \{a\}$.

Lause 6.4 Olkoon H ryhmän G aliryhmä, ja olkoon $a \in G$. Silloin aHa^{-1} on ryhmän G aliryhmä, jota kutsutaan aliryhmän H **konjugaatiksi** (conjugate). Lisäksi $H \simeq aHa^{-1}$.

Todistus. Ks. [7], s. 193. \square

Määritelmä 6.2 Olkoon H ryhmän G aliryhmä, ja olkoon $a \in G$. Jos pätee ehto $aHa^{-1} = H$, niin aliryhmää H kutsutaan **invariantiksi** alkion a suhteen.

Määritelmän 6.2 perusteella huomataan välittömästi, että jos aliryhmä H on invariantti ryhmän G kaikkien alkioiden suhteen, niin H on ryhmän G normaali aliryhmä.

Määritelmä 6.3 Olkoot H ja K ryhmän G aliryhmiä. Joukkoa

$$N_K(H) = \{k \in K \mid kHk^{-1} = H\}$$

kutsutaan aliryhmän H **normalisoijaksi** (normalizer) aliryhmässä K .

Selvästi $N_K(H) \subseteq K$. Määritelmästä 6.3 nähdään, että joukon $N_K(H)$ muodostavat aliryhmän K ne alkio, joiden suhteen H on invariantti.

Lause 6.5 *Olko H ja K ryhmän G aliryhmiä. Silloin $N_K(H)$ on ryhmän K aliryhmä.*

Todistus. Ks. [7], s. 193-194. \square

Kun $K = G$, niin $N_K(H) = N_G(H)$. Merkinnän $N_G(H)$ sijasta käytetään lyhyempää merkintää $N(H)$ ja nimitystä *aliryhmän H normalisoija*. Triviaalisti $N(H) = G$ silloin, kun H on ryhmän G normaali aliryhmä tai kun G on kommutatiivinen. Jos $K = G$, niin lauseen 6.5 mukaan $N(H)$ on ryhmän G aliryhmä.

Lause 6.6 *Olko H ryhmän G aliryhmä. Silloin H on ryhmän $N(H)$ normaali aliryhmä.*

Todistus. Olkoon $h \in H$. Selvästi $hHh^{-1} = H$, joten H on joukon $N(H)$ osajoukko. Koska H ja $N(H)$ ovat ryhmän G aliryhmiä ja $H \subseteq N(H)$, niin H on aliryhmän $N(H)$ aliryhmä. Nyt normalisoijan määritelmän mukaan $aHa^{-1} = H$ aina, kun $a \in N(H)$. Näin ollen H on ryhmän $N(H)$ normaali aliryhmä. \square

Lause 6.7 *Olko H ja K ryhmän G aliryhmiä. Aliryhmän K alkioiden indusoimien aliryhmän H erillisten konjugaattien lukumäärä on $[K : N_K(H)]$.*

Todistus. Ks. [7], s. 194. \square

Esimerkki 6.1 *Olko H ryhmän G aliryhmä. Osoitetaan, että H on normaali aliryhmä, jos ja vain jos H on konjugaattiluokkiensa yhdiste.*

Ratkaisu. Olkoon $a \in G$ ja $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Oletetaan ensin, että H on normaali aliryhmä. Osoitetaan, että H on konjugaattiluokkiensa yhdiste. Olkoon $h \in H$. Koska H on normaali aliryhmä, niin $aha^{-1} \in H$ aina, kun $a \in G$, esimerkin 2.7 nojalla. Nyt $C_l(h) = \{aha^{-1} \mid a \in G\}$, joten $C_l(h) \subseteq H$. Koska myös $h = ehe^{-1} \in C_l(h)$, niin huomataan, että $H = \cup_{h \in H} C_l(h)$.

Oletetaan kääntäen, että H on konjugaattiluokkiensa unioni. Osoitetaan, että H on normaali aliryhmä. Olkoon $h \in H$. Oletuksen mukaan $H = \cup_{h \in H} C_l(h)$, missä $C_l(h) = \{aha^{-1} \mid a \in G\}$. Tässä siis $aha^{-1} \in C_l(h) \subseteq H$ aina, kun $h \in H, a \in G$. Väite seuraa nyt esimerkistä 2.7.

Esimerkissä 6.1 käsitellyn tehtävän alkuperäinen määrittely (ks. [7], tehtävä 3, s. 195) on harhaanjohtava, sillä siinä puhutaan *ryhmän G konjugaattiluokkien unionista*. Jokainen joukkohan on *omien* ekvivalenssiluokkiensa (tässä konjugaattiluokkien) yhdiste, sillä joukon ekvivalenssiluokat muodostavat kyseisen joukon *osituksen* (ks. [7], s. 24). Tässä alkuperäinen tehtävä on korjattu mielekkääksi siten, että ryhmässä G määritelty konjugaattirelaatio liitetään *aliryhmään H* .

6.2 Cauchyn lause ja p -ryhmät

Tämän kappaleen pääsisältö on *Cauchyn lause*, joka on osittainen käänteinen tulos Lagrangen lauseeseen nähden. Väite todistetaan ensin äärellisille Abelin ryhmille ja sitten tämä lause yleistetään koskemaan kaikkia äärellisiä ryhmiä.

Lause 6.8 *Olkoon G äärellinen Abelin ryhmä, jonka kertaluku n on jaollinen alkuluvulla p . Silloin G sisältää alkion, jonka kertaluku on p , ja aliryhmän, jonka kertaluku on p .*

Todistus. (Vrt. [7], s. 196.) Induktiotodistus ryhmän kertaluvun $|G|$ suhteen. Kun $|G| = 1$, niin lause on triviaalisti tosi. Olkoon p alkuluku. Jos $|G| = p$, niin ryhmän G jokaisen alkion $\neq e$ kertaluku on p lauseen 2.18 nojalla. Silloin lause on erityisesti tosi, kun $|G| = 2$. Tehdään nyt induktio-oletus, että lause on tosi aina, kun $|G| = r$, missä $2 \leq r < n$. Olkoon G nyt ryhmä, jonka kertaluku on n . Olkoon $a \in G$, $a \neq e$, ja olkoon m alkion a kertaluku. Silloin joko $p \mid m$ tai $p \nmid m$. Jos $p \mid m$, niin $m = pk$ jollakin positiivisella kokonaisluvulla k . Tässä tapauksessa $(a^k)^p = a^m = e$, mistä seuraa ensinnäkin, että $a^k \neq e$, sillä $m = pk$ on alkion a pienin potenssi, joka on yhtä kuin e . Toiseksi havaitaan, että $a^k \in G$ on alkio, jonka kertaluku on p . Oletetaan nyt, että $p \nmid m$. Koska G on Abelin ryhmä, niin sen syklinen aliryhmä $H = \langle a \rangle$ on ryhmän G normaali aliryhmä lauseen 2.25 perusteella. Nyt tiedetään, että $|H| = |\langle a \rangle| = m$. Nyt $|G| = m \cdot [G : H]$ Lagrangen lauseen 2.15 perusteella. Koska tässä p ei jaa lukua m , niin p jakaa luvun $[G : H]$. Koska H on ryhmän G normaali aliryhmä, niin voidaan muodostaa tekijäryhmä G/H . Nyt p jakaa luvun $|G/H| = [G : H]$. Koska $|G/H| < n$, niin induktio-oletuksen nojalla on olemassa sellainen $bH \in G/H$, että $o(bH) = p$. Tässä b on eräs ryhmän G alkio. Nyt $b^p H = (bH)^p = eH = H$. Täten $b^p \in H$. Nyt $(b^m)^p = (b^p)^m = e$, joten joko $b^m = e$ tai alkion b^m kertaluku on p . Oletetaan nyt, että $b^m = e$. Tällöin $b^m H = (bH)^m = eH$, mistä seuraa, että $p \mid m$. Tämä on ristiriidassa oletuksen kanssa, joten $b^m \neq e$. Näin ollen alkion b^m kertaluku on p , ja siten b^m on etsitty ryhmän G alkio. Alkio, jonka kertaluku on p , generoi nyt ryhmän G syklisten aliryhmän, jonka kertaluku on p . Näin on induktioperiaatteen nojalla osoitettu lause todeksi, kun $|G| = n$. \square

Lause 6.9 (Cauchy) *Olkoon G äärellinen ryhmä, jonka kertaluku n on jaollinen alkuluvulla p . Silloin G sisältää alkion, jonka kertaluku on p , ja aliryhmän, jonka kertaluku on p .*

Todistus. (Vrt. [7], s. 196-197.) Induktiotodistus ryhmän kertaluvun $|G|$ suhteen. Kun $|G| = 1$, niin lause on triviaalisti tosi. Kun $|G| = n = 2$, niin G on syklinen ryhmä ja siten Abelin ryhmä. Väite seuraa tällöin lauseesta 6.8. Tehdään induktio-oletus, että väite on tosi aina, kun ryhmän kertaluku on m , missä $2 \leq m < n$. Tarkastellaan nyt ryhmän G luokkayhtälöä

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)].$$

Jos $G = Z(G)$, niin G on Abelin ryhmä ja tulos seuraa lauseesta 6.8. Jos $G \neq Z(G)$, niin on olemassa sellainen $a \in G$, että $a \notin Z(G)$. Valitaan tällainen a . Koska a ei kommutoi ryhmän G kaikkien alkuiden kanssa, niin $G \neq C(a)$. Tällöin $[G : C(a)] > 1$, joten Lagrangen lauseen nojalla $|G| = [G : C(a)] \cdot |C(a)| > |C(a)|$. Jos p jakaa luvun $|C(a)|$, niin induktio-oletuksen nojalla aliryhmällä $C(a)$ ja siten

myös ryhmällä G on alkio, jonka kertaluku on p . Jos p ei jaa lukua $|C(a)|$ aina, kun $a \notin Z(G)$, niin luvun p täytyy jakaa luku $[G : C(a)]$ aina, kun $a \notin Z(G)$. Oletuksen mukaan p jakaa luvun $|G|$, ja p jakaa nyt myös summan $\sum_{a \notin Z(G)} [G : C(a)]$ jokaisen tekijän. Näin ollen p jakaa luokkayhtälössä myös luvun $|Z(G)|$. Koska $Z(G)$ on Abelin ryhmä, niin lauseen 6.8 nojalla on olemassa sellainen aliryhmän $Z(G)$ ja samalla ryhmän G alkio a , jonka kertaluku on p . Näin on induktioperiaatteen nojalla osoitettu lause todeksi, kun $|G| = n$. \square

Cauchyn lauseen avulla voidaan nyt todistaa seuraava osittainen käänteinen tulos Lagrangen lauseeseen nähden.

Lause 6.10 *Olkoon G äärellinen Abelin ryhmä, jonka kertaluku on n . Jos n on jaollinen positiivisella kokonaisluvulla m , niin G sisältää aliryhmän, jonka kertaluku on m .*

Todistus. Ks. [7], s. 197.

Määritelmä 6.4 *Olkoon p alkuluku. Ryhmää G kutsutaan p -ryhmäksi, jos ryhmän G jokaisen alkion kertaluku on luvun p jokin potenssi. Ryhmän G aliryhmää H kutsutaan p -aliryhmäksi, jos H on p -ryhmä.*

Lause 6.11 *Olkoon G ei-triviaali ryhmä. Silloin G on äärellinen p -ryhmä, jos ja vain jos $|G| = p^k$ jollakin positiivisella kokonaisluvulla k .*

Todistus. Ks. [7], s. 198.

Seuraava lause on hyvin tärkeä äärellisten p -ryhmien tarkastelussa.

Lause 6.12 *Olkoon G sellainen äärellinen p -ryhmä, että $|G| > 1$. Silloin ryhmän G keskuksessa $Z(G)$ on enemmän kuin yksi alkio. Toisin sanoen: jos $|G| = p^k$, kun $k \geq 1$, niin $|Z(G)| > 1$.*

Todistus. (Vrt. [7], s. 198.) Olkoon G sellainen äärellinen p -ryhmä, että $|G| > 1$. Tarkastellaan ryhmän G luokkayhtälöä

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)].$$

Jos $G = Z(G)$, niin $|G| = |Z(G)| > 1$, joten lause on tosi. Oletetaan nyt, että $G \supset Z(G)$. Koska $Z(G)$ on nyt joukon G aito osajoukko, on olemassa sellainen $a \in G$, että $a \notin Z(G)$. Valitaan tällainen alkio a . Nyt $C(a)$ on ryhmän G aliryhmä lauseen 6.1 nojalla. Koska $a \notin Z(G)$, niin $C(a)$ on ryhmän G aito aliryhmä. Nyt siis $|C(a)| < |G|$. Koska G on p -ryhmä, niin $C(a)$ sen aliryhmänä on myös p -ryhmä. Lagrangen lauseen mukaan $[G : C(a)] = |G|/|C(a)| = p^m$, missä $m \geq 1$. Näin ollen p jakaa luvun $[G : C(a)]$ aina, kun $a \notin Z(G)$. Tästä seuraa, että p jakaa summan $\sum_{a \notin Z(G)} [G : C(a)]$. Koska p jakaa myös luvun $|G|$, niin luokkayhtälön perusteella p jakaa luvun $|Z(G)|$. Tästä seuraa, että $|Z(G)| > 1$. \square

Jos $k = 1$, niin lauseen 6.12 välittömänä seurauksena saadaan mielenkiintoinen tulos. Olkoon G sellainen äärellinen p -ryhmä, että $|G| = p$. Osoitetaan, että silloin G on Abelin ryhmä. Koska nyt G on p -ryhmä, niin $|Z(G)| > 1$ lauseen 6.12 perusteella. Koska $Z(G)$ on ryhmän G aliryhmä, niin Lagrangen lauseesta seuraa nyt, että $G = Z(G)$. Näin ollen G on Abelin ryhmä. Aiemminhan on jo osoitettu, että jos $|G| = p$, missä p on alkuluku, niin G on syklinen ja siten Abelin ryhmä.

Esimerkki 6.2 *Olkoon G Abelin ryhmä, jonka kertaluku on pq , missä p ja q ovat erisuuria alkulukuja. Osoitetaan, että G on syklinen. Osoitetaan lisäksi, että väite ei päde yleisesti, jos $p = q$.*

Ratkaisu. Oletetaan aluksi, että $p \neq q$. Cauchyn lauseen nojalla ryhmällä G on eräs aliryhmä H , jonka kertaluku on p , sekä eräs aliryhmä K , jonka kertaluku on q . Nyt $H \cap K$ on ryhmän G aliryhmä lauseen 2.3 perusteella. Lauseen 2.21 mukaan nyt $H \cap K = \{e\}$. Abelin ryhmän G aliryhminä H ja K ovat normaaleja aliryhmiä. Lauseen 2.24 perusteella HK on nyt ryhmän G normaali aliryhmä. Nyt $|H \cap K| = 1$, joten $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{pq}{1} = pq$. Koska G on äärellinen, $HK \subseteq G$ ja $|HK| = |G|$, niin $HK = G$.

Olkoon nyt $H = \langle h \rangle$ ja $K = \langle k \rangle$, missä $h \neq e \neq k$. Selvästi $\langle hk \rangle$ on ryhmän G eräs syklinen aliryhmä. Osoitetaan, että $\langle hk \rangle = G$. Lauseen 1.4 nojalla ensiksikin $(hk)^{pq} = h^{pq}k^{pq} = (h^p)^q(k^q)^p = ee = e$. Osoitetaan nyt, että $(hk)^m = h^m k^m \neq e$, kun $0 < m < pq$. Tehdään vasta oletus, että on olemassa sellainen positiivinen kokonaisluku m , että $h^m k^m = e$, kun $0 < m < pq$. Valitaan tällainen m . Vastaoletuksesta seuraa, että $h^m = (k^m)^{-1} = (k^{-1})^m$, joten $h^m \in K$ ja $(k^{-1})^m \in H$. Nyt selvästi $h^m, (k^{-1})^m \in H \cap K$, joten $h^m = (k^{-1})^m = e$. Oletuksen nojalla $o(h) = p$ ja $o(k) = o(k^{-1}) = q$, kun $k \neq e$. Tällöin $p \mid m$ ja $q \mid m$, mikä johtaa ristiriitaan oletuksen $0 < m < pq$ kanssa. Näin ollen vasta oletus on väärä, joten $m = pq$ on pienin sellainen positiivinen kokonaisluku, että $(hk)^m = e$. Näin on osoitettu, että $o(hk) = pq = |\langle hk \rangle|$. Koska tässä $\langle hk \rangle \subseteq G$ ja $|\langle hk \rangle| = |G|$, niin G on syklinen.

Oletetaan seuraavaksi, että $p = q$. Nyt siis $|G| = p^2$. Kleinin neliryhmä on eräs tämän ehdon täyttävä Abelin ryhmä; sen kertaluku on 2^2 . Kuitenkaan Kleinin neliryhmä ei ole syklinen (ks. [7], s. 111). Tämä vastaesimerkki osoittaa, että väite ei yleisesti ole voimassa, kun $p = q$. ([7], tehtävä 9, s. 200)

6.3 Sylowin lauseet

Jos äärellisellä ryhmällä G on aliryhmä, niin Lagrangen lauseen nojalla aliryhmän kertaluku jakaa ryhmän G kertaluvun. Sylowin lauseet antavat osittaisia vastauksia käänteiseen kysymykseen. Jotkut pitävät Sylowin lauseita Lagrangen lauseen jälkeen tärkeimpinä äärellisten ryhmien teoriassa ([4], s. 352). Kun Lagrangen lause ilmaisee välttämättömän ehdon äärellisen ryhmän G aliryhmän olemassaololle, niin Sylowin ensimmäinen lause ilmaisee riittävän ehdon (silloin, kun aliryhmän kertaluvussa on kysymys jonkin alkuluvun potenssista).

Lause 6.13 (Sylowin ensimmäinen lause) *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, r ja m ovat positiivisia kokonaislukuja, ja p ja m ovat keskenään jaottomia. Silloin ryhmällä G on aliryhmä, jonka kertaluku on p^k , aina, kun $0 \leq k \leq r$.*

Todistus. (Vrt. [7], s. 201-202.) Todetaan aluksi, että jokaisella ryhmällä G on triviaali aliryhmä $\{e\}$, joten lause on tosi, kun $k = 0$. Osoitetaan lause oikeaksi induktiotodistuksella, kun $1 \leq k \leq r$. Olkoon $k = 1$. Koska p jakaa luvun $|G|$, niin ryhmällä G on aliryhmä, jonka kertaluku on $p = p^k$ Cauchyn lauseen 6.9 perusteella. Lause on siis tosi, kun $k = 1$. Tehdään induktio-oletus, että ryhmällä G on aliryhmä H , jonka kertaluku on p^k , $1 \leq k < r$. Silloin H on ryhmän G aito aliryhmä. Lauseen 6.5 nojalla $N(H)$ on ryhmän G aliryhmä. Esimerkin 4.2 nojalla $[N(H) : H] \cong_p [G : H]$ ja $H \neq N(H)$. Koska $p \mid [G : H]$, niin $p \mid [N(H) : H]$.

Lauseen 6.6 nojalla H on ryhmän $N(H)$ normaali aliryhmä, joten tekijäryhmä $N(H)/H$ voidaan määritellä. Nyt $|N(H)/H| = [N(H) : H]$, joten p jakaa luvun $|N(H)/H|$. Täten tekijäryhmällä $N(H)/H$ on Cauchyn lauseen mukaan aliryhmä, jonka kertaluku on p . Tämä aliryhmä on lauseen 3.15 nojalla muotoa K/H , missä K on ryhmän $N(H)$ aliryhmä ja H on aliryhmän K normaali aliryhmä. Nyt Lagrangen lauseen perusteella $|K| = [K : H]|H| = |K/H||H| = pp^k = p^{k+1}$. Sen vuoksi K on ryhmän G aliryhmä, jonka kertaluku on p^{k+1} . Näin on osoitettu, että jos ryhmällä G on aliryhmä, jonka kertaluku on p^k , niin ryhmällä G on aliryhmä, jonka kertaluku on p^{k+1} , missä $1 \leq k < r$. Induktioperiaatteen nojalla ryhmällä G on tällöin aliryhmä, jonka kertaluku on p^k aina, kun $1 \leq k \leq r$. Näin on lause osoitettu oikeaksi aina, kun $0 \leq k \leq r$. \square

Lause 6.13 ilmaisee sen, että ryhmällä G on *ainakin* yksi aliryhmä, jonka kertaluku on p^k , aina, kun $0 \leq k \leq r$. Samaa kertalukua edustavia aliryhmiä voi olla useampiakin.

Määritelmä 6.5 *Olkoon G äärellinen ryhmä ja olkoon p alkuluku. Ryhmän G aliryhmää P kutsutaan ryhmän G **Sylowin p -aliryhmäksi**, jos P on p -aliryhmä eikä se sisälly aidosti mihinkään muuhun ryhmän G p -aliryhmään. Toisin sanoen P on ryhmän G maksimaalinen p -aliryhmä.*

Määritelmän 6.5 ja lauseen 6.13 nojalla kertalukua $p^r m$ edustavan ryhmän Sylowin p -aliryhmän kertaluku on p^r .

Lause 6.14 *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, r ja m ovat positiivisia kokonaislukuja, ja p ja m ovat keskenään jaottomia. Olkoon H ryhmän G sellainen aliryhmä, jonka kertaluku on p^i , $1 \leq i < r$. Silloin on olemassa sellainen ryhmän G aliryhmä K , että $|K| = p^{i+1}$ ja H on aliryhmän K normaali aliryhmä.*

Todistus. Ks. [7], s. 203.

Lause 6.15 (Sylowin toinen lause) *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, r ja m ovat positiivisia kokonaislukuja, ja p ja m ovat keskenään jaottomia. Silloin mitkä tahansa kaksi Sylowin p -aliryhmää ovat konjugaatteja, ja siten ne ovat isomorfiset.*

Todistus. (Vrt. [7], s. 204-205.) Olkoot H ja K ryhmän G Sylowin p -aliryhmiä ja olkoon S aliryhmän H kaikkien vasempien sivuluokkien joukko ryhmässä G , toisin sanoen $S = \{aH \mid a \in G\}$. Silloin $|S| = [G : H]$. Vaikuttakoon K joukkoon S siten, että aina kun $k \in K$, $aH \in S$, niin

$$k(aH) = (ka)H.$$

Siten S on K -joukko. Olkoon $S_0 = \{aH \in S \mid k(aH) = aH \text{ aina, kun } k \in K\}$. Esimerkin 4.1 nojalla $|S_0| \equiv_p |S|$. Koska H on ryhmän G Sylowin p -aliryhmä, niin $|S| = [G : H]$ ei ole jaollinen luvulla p . Täten $|S_0| \neq 0$. Olkoon $aH \in S_0$. Silloin $k(aH) = aH$ aina, kun $k \in K$. Tästä seuraa, että $a^{-1}kaH = H$ aina, kun $k \in K$, ja siten $a^{-1}ka \in H$ aina, kun $k \in K$. Siten $a^{-1}Ka \subseteq H$. Koska $|a^{-1}Ka| = |K| = |H|$, niin $a^{-1}Ka = H$. Näin ollen H ja K ovat konjugaatteja. \square

Seuraava lause on Sylowin toisen lauseen välitön seuraus.

Lause 6.16 *Olkoon G äärellinen ryhmä ja olkoon H sen Sylowin p -aliryhmä. Silloin H on yksikäsitteinen ryhmän G Sylowin p -aliryhmä, jos ja vain jos H on ryhmän G normaali aliryhmä.*

Todistus. Olkoon H ryhmän G Sylowin p -aliryhmä. Oletetaan aluksi, että H on yksikäsitteinen ryhmän G Sylowin p -aliryhmä. Osoitetaan, että H on ryhmän G normaali aliryhmä. Aliryhmän H jokainen konjugaatti P on muotoa $P = aHa^{-1}$, missä $a \in G$. Oletuksen mukaan $H = aHa^{-1}$ aina, kun $a \in G$. Tällöinhän H on ryhmän G normaali aliryhmä.

Oletetaan kääntäen, että H on ryhmän G normaali aliryhmä. Osoitetaan, että H on yksikäsitteinen ryhmän G Sylowin p -aliryhmä. Oletuksen mukaan $H = aHa^{-1}$ aina, kun $a \in G$. Tämä merkitsee samalla sitä, että aliryhmä H on itsensä ainoa konjugaatti, joten H on yksikäsitteinen ryhmän G Sylowin p -aliryhmä. \square

Lause 6.17 (Sylowin kolmas lause) *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^r m$, missä p on alkuluku, r ja m ovat positiivisia kokonaislukuja, ja p ja m ovat keskenään jaottomia. Silloin ryhmän G Sylowin p -aliryhmien lukumäärä n_p on $1 + kp$, missä k on ei-negatiivinen kokonaisluku ja n_p jakaa luvun $p^r m$.*

Todistus. (Vrt. [7], s. 205-206.) Olkoon S ryhmän G kaikkien Sylowin p -aliryhmien joukko ja olkoon $P \in S$. Vaikuttakoon P joukkoon S konjugoimalla, toisin sanoen $a \cdot Q = aQa^{-1}$ aina, kun $a \in P, Q \in S$. Nyt S on P -joukko. Olkoon $S_0 = \{Q \in S \mid a \cdot Q = Q \text{ aina, kun } a \in P\} = \{Q \in S \mid aQa^{-1} = Q \text{ aina, kun } a \in P\}$. Nyt siis S_0 on ryhmän G niiden Sylowin p -aliryhmien Q joukko, jotka ovat invariantteja aliryhmän P alkioden suhteen. Esimerkin 4.1 nojalla $|S| \equiv_p |S_0|$. Koska selvästi $P \in S_0$, niin $S_0 \neq \emptyset$. Olkoon $Q \in S_0$. Silloin $Q = aQa^{-1}$ aina, kun $a \in P$. Täten $P \subseteq N(Q)$. Toisaalta triviaalisti $Q \subseteq N(Q)$. Nyt P ja Q ovat ryhmän G aliryhmiä ja lauseen 6.5 perusteella $N(Q)$ on ryhmän G aliryhmä. Näin ollen P ja Q ovat ryhmän $N(Q)$ aliryhmiä. Koska lisäksi P ja Q ovat ryhmän G Sylowin p -aliryhmiä, niin ne ovat ryhmän $N(Q)$ Sylowin p -aliryhmiä. Nyt Sylowin toisen lauseen perusteella on olemassa sellainen $a \in N(Q)$, että $aQa^{-1} = P$; tässä P ja Q ovat konjugaatit, ja a on alkio, jonka suhteen Q on invariantti. Silloinhan $P = Q$, sillä Q on invariantti jokaisen alkion $a \in N(Q)$ suhteen. Täten $S_0 = \{P\}$ ja siis $|S_0| = 1$. Näin ollen $|S| \equiv_p 1$, joten $|S| = 1 + kp$, missä k on jokin ei-negatiivinen kokonaisluku. Tähän Sylowin p -aliryhmien lukumäärään liittyvään yhtälöön päädyttiin konjugaattirelaation pohjalta. Kyseessä on erikoistapaus esimerkin 4.1 tarkastelusta.

Vaikuttakoon G joukkoon S konjugoimalla. Sylowin toisen lauseen nojalla mitkä tahansa kaksi Sylowin p -aliryhmää ovat konjugaatteja. Siksi on vain yksi joukon S ura ryhmässä G ; toisin sanoen joukon S kaikki alkiot kuuluvat samaan uraan. Olkoon $P \in S$. Silloin $G_P = \{g \in G \mid g \cdot P = P\} = \{g \in G \mid gPg^{-1} = P\} = N(P)$. Täten lauseen 4.3 nojalla

$$|S| = \text{aliryhmän } P \text{ uran alkioden lukumäärä on } = [G : G_P].$$

Lauseen 4.2 nojalla G_P on äärellisen ryhmän G aliryhmä, joten Lagrangen lauseen 2.15 perusteella $[G : G_P]$ jakaa luvun $|G|$. Näin ollen ryhmän G Sylowin p -aliryhmien lukumäärä jakaa luvun $|G|$. \square

Esimerkki 6.3 *Olkoon G ryhmä, jonka kertaluku on 65. Osoitetaan, että G ei ole yksinkertainen.*

Ratkaisu. Nyt $|G| = 65 = 13 \cdot 5$. Sylowin ensimmäisen lauseen nojalla ryhmällä G on aliryhmät, joiden kertaluvut ovat 13 ja 5. Nyt Sylowin kolmannen lauseen mukaan $n_{13} = 1 + 13k$ ja $(1 + 13k) \mid 65$, missä k on ei-negatiivinen kokonaisluku. Jälkimmäinen ehto toteutuu vain silloin, kun $k = 0$, joten $n_{13} = 1$. Ryhmällä G on siten yksikäsitteinen Sylowin 13-aliryhmä, joka lauseen 6.16 perusteella on normaali. Koska ryhmällä G siis on ei-triviaali, normaali aliryhmä, niin G ei ole yksinkertainen. ([7], tehtävä 3, s. 219)

Esimerkki 6.4 *Tarkastellaan ryhmää G , jonka kertaluku on 70.*

Ratkaisu. Nyt $|G| = 70 = 7 \cdot 5 \cdot 2$. Sylowin ensimmäisen lauseen perusteella ryhmällä G on ainakin yksi kutakin kertalukua 7, 5 ja 2 edustava aliryhmä.

(i) Osoitetaan, että ryhmällä G on yksikäsitteinen Sylowin 7-aliryhmä. Sylowin kolmannen lauseen mukaan $n_7 = 1 + 7k$ ja $(1 + 7k) \mid 70$, missä k on ei-negatiivinen kokonaisluku. Jälkimmäinen ehto toteutuu vain silloin, kun $k = 0$, joten $n_7 = 1$. Ryhmällä G on siten yksikäsitteinen Sylowin 7-aliryhmä H , joka lauseen 6.16 perusteella on ryhmän G normaali aliryhmä.

(ii) Osoitetaan, että ryhmällä G on yksikäsitteinen Sylowin 5-aliryhmä. Sylowin kolmannen lauseen mukaan $n_5 = 1 + 5k$ ja $(1 + 5k) \mid 70$, missä k on ei-negatiivinen kokonaisluku. Jälkimmäinen ehto toteutuu vain silloin, kun $k = 0$, joten $n_5 = 1$. Ryhmällä G on siten yksikäsitteinen Sylowin 5-aliryhmä K , joka lauseen 6.16 perusteella on ryhmän G normaali aliryhmä.

(iii) Osoitetaan, että ryhmällä G on syklinen aliryhmä, jonka kertaluku on 35. Koska H ja K ovat ryhmän G normaaleja aliryhmiä, niin lauseen 2.24 perusteella $M = HK = KH$ on tällöin ryhmän G normaali aliryhmä. Lauseen 2.21 nojalla $H \cap K = \{e\}$. Lauseen 2.19 perusteella nyt $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{7 \cdot 5}{1} = 35$. Koska aliryhmien H ja K kertaluvut ovat alkulukuja, niin H ja K ovat syklisiä ryhmiä. Koska selvästi $H \subseteq HK$ ja $K \subseteq HK$, niin H ja K ovat ryhmän G normaalin aliryhmän M normaaleja aliryhmiä. On siis todettu, että $M = HK$ ja että $H \cap K = \{e\}$. Näin ollen M on normaalien aliryhmiensä H ja K sisäinen suora tulo lauseen 5.2 perusteella. Lauseen 5.3 nojalla nyt $M = HK = H \times K \simeq \mathbf{Z}_7 \times \mathbf{Z}_5$. Esimerkin 5.1 perusteella $\mathbf{Z}_7 \times \mathbf{Z}_5$ on syklinen ryhmä, jonka kertaluku on $7 \cdot 5 = 35$. Näin ollen $M = HK = H \times K \simeq \mathbf{Z}_7 \times \mathbf{Z}_5 \simeq \mathbf{Z}_{35}$, joten ryhmällä G on syklinen aliryhmä, jonka kertaluku on 35. ([7], tehtävä 11, s. 220)

Todistetaan lopuksi vielä yksi Sylowin p -aliryhmiin liittyvä tulos. Aluksi esitetään seuraava apulause.

Lause 6.18 *Olkoon P äärellisen ryhmän G Sylowin p -aliryhmä. Silloin aliryhmän P normalisoijan jokainen p -aliryhmä sisältyy aliryhmään P .*

Todistus. (Vrt. [6], s. 471.) Olkoon P on äärellisen ryhmän G Sylowin p -aliryhmä, jonka kertaluku on p^r , $r \geq 1$. Olkoon R normalisoijan $N(P)$ mielivaltainen p -aliryhmä, jonka kertaluku on p^k , $k \geq 1$. Koska P on lauseen 6.6 perusteella normalisoijansa $N(P)$ normaali aliryhmä ja $R \subseteq N(P)$, niin toisen isomorfialauseen 3.11 perusteella

$$R/(R \cap P) \simeq (RP)/P.$$

Tekijäryhmälle $R/(R \cap P)$ pätee yhtälö $|R/(R \cap P)| = [R : (R \cap P)]$. Toisaalta $[R : (R \cap P)] = |R|/|R \cap P|$ Lagrangen lauseen perusteella. Koska $|R \cap P|$ jakaa luvun $|R| = p^k$, niin $|R/(R \cap P)| = p^m$, missä $m \geq 0$. Koska tutkitaan äärellisen

ryhmän G aliryhmiä, niin nyt isomorfian tähden $|R/(R \cap P)| = |(RP)/P| = p^m$. Tarkastellaan seuraavaksi tekijäryhmää $(RP)/P$. Nyt $|(RP)/P| = [(RP) : P] = |RP|/|P|$, mistä seuraa, että $|RP| = p^m p^r$; toisin sanoen $|RP|$ on luvun p eräs potenssi. Nyt $P, R \subseteq G$, joten myös $RP \subseteq G$. Koska P on ryhmän G Sylowin p -aliryhmä, niin ryhmän P kertaluku on suurin mahdollinen luvun p potenssi. Näin ollen $|RP| = |P|$, joten $RP = P$. Tästä seuraa, että $R \subseteq P$. \square

Lause 6.19 *Olkoon G äärellinen ryhmä. Silloin ryhmän G jokainen p -aliryhmä sisältyy johonkin Sylowin p -aliryhmään.*

Todistus. (Vrt. [6], s. 472.) Olkoon S äärellisen ryhmän G kaikkien Sylowin p -aliryhmien joukko. Olkoon $P \in S$. Olkoon R ryhmän G mielivaltainen p -aliryhmä. Vaikuttakoon R joukkoon S konjugoimalla. Tällöin S on R -joukko. Nyt $|R| = p^m$, missä $m \geq 0$. Lauseen 4.3 nojalla $[R : R_P] = |R|/|R_P| = |[P]|$, missä R_P on alkion P isotropiaryhmä. Koska $|R|$ on jokin alkuluvun p potenssi, niin nyt $|[P]|$ on myös jokin luvun p potenssi. Kutakin alkioita $P \in S$ vastaavassa urassa $[P]$ on siten 1 alkio tai p^n alkioita, missä $n \geq 1$. Sylowin kolmannen lauseen mukaan $|S| = 1 + kp$, missä $k \geq 0$. Siten $|S|$ ei ole jaollinen luvulla p (> 1), joten ainakin yksi ryhmän R joukkoon S muodostamista urista sisältää vain yhden alkion. Tästä seuraa, että on olemassa sellainen $P_i \in S$, että $R \subseteq N(P_i)$. Lauseen 6.18 nojalla tällöin $R \subseteq P_i$. Täten ryhmän G p -aliryhmä R sisältyy johonkin Sylowin p -aliryhmään. ([7], tehtävä 11, s. 210) \square

Lähteessä [6] lause 6.19 esitetään Sylowin kolmantena lauseena. Lauseiden nimissä noudatetaan tässä lähteen [7] käytäntöä, mutta oleellisinta on, että lause 6.19 tarkentaa äärellisten ryhmien aliryhmärakennetta. Kolme aiemmin esitettyä Sylowin lausetta auttavat määrittämään maksimaalisia p -aliryhmiä; viimeksi esitetty lause liittyy kaikkiin p -aliryhmiin.

7 Ratkeavat ja nilpotentit ryhmät

7.1 Ratkeavat ryhmät

Tämän kappaleen pääsisältö on *Jordanin-Hölderin lause* ja *ratkeavan* ryhmän määrittely. Niiden pohjaksi tarkastellaan aluksi eräänlaisia ryhmän ja sen aliryhmien muodostamia ketjuja.

Määritelmä 7.1 *Olkoon G ryhmä ja olkoon*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}$$

*ryhmän G aliryhmien ketju, $n \geq 0$. Ketjua kutsutaan **alinnormaaliksi sarjaksi** tai **ketjuksi** (subnormal series), jos kukin aliryhmä H_i on normaali aliryhmässä H_{i-1} . Ketjua kutsutaan **normaaliksi sarjaksi** (normal series), jos kukin aliryhmä H_i on normaali ryhmässä G .*

*Ketjua kutsutaan **kompositiosarjaksi** (composition series), jos kukin aliryhmä on maksimaalinen ryhmän H_{i-1} normaali aliryhmä. Tämä tarkoittaa sitä, että $H_i \neq H_{i-1}$, ja jos $H_i \subset H \subseteq H_{i-1}$ ja H on normaali aliryhmässä H_{i-1} , niin $H = H_{i-1}$, $i = 1, 2, \dots, n$.*

*Ketjuun sisältyvien aitojen inklusioiden \supset lukumäärää kutsutaan ketjun **pi-tuudeksi**. Tekijäryhmiä H_{i-1}/H_i sanotaan ketjun **tekijöiksi** (factors of the chain).*

Huomattakoon, että määritelmän mukaan vain *äärellinen* aliryhmien ketju voi olla alinormaali tai normaali sarja tai kompositiosarja. Jos G on Abelin ryhmä, niin sen alinormaali ja normaali sarja yhtyvät, koska ryhmän G jokainen aliryhmä on normaali.

Jos $H_{i-1} = H_i$ yllä olevassa määritelmässä, niin tekijäryhmä H_{i-1}/H_i koostuu yhdestä ainoasta alkioista eH_i ja ryhmää kutsutaan ketjun **triviaaliksi tekijäksi**. Näin ollen ketjun pituus on ketjun ei-triviaalien tekijöiden H_{i-1}/H_i lukumäärä.

Ryhmän G kompositiosarjasta $G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \dots \supseteq H_n = \{e\}$ havaitaan, että tekijät H_{i-1}/H_i ovat yksinkertaisia ryhmiä. Tämä johtuu siitä, että tekijäryhmän H_{i-1}/H_i ainoat normaalit aliryhmät ovat triviaalit aliryhmät H_{i-1}/H_i ja eH_i . Tavallaan ryhmän G analysointi kiteytyy nyt sen kompositiotekijöiden tarkasteluksi.

Määritelmä 7.2 *Olkoon G ryhmä ja olkoon*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \dots \supseteq H_{n-1} \supseteq H_n = \{e\} \quad (7.1)$$

ryhmän G alinormaali sarja. Tämän sarjan yhden askeleen tarkennus (one-step refinement) on mikä tahansa muotoa

$$G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_{i-1} \supseteq H \supseteq H_i \supseteq \dots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

*oleva sarja, missä H on ryhmän H_{i-1} normaali aliryhmä ja H_i on ryhmän H normaali aliryhmä, $i = 1, 2, \dots, n$. Sarjan (7.1) **tarkennus** (refinement) on sellainen alinormaali sarja, joka on saatu sarjasta (7.1) äärellisellä määrällä yhden askeleen tarkennuksia. Sarjan (7.1) tarkennusta*

$$G = K_0 \supseteq K_1 \supseteq K_2 \supseteq \dots \supseteq K_{m-1} \supseteq K_m = \{e\} \quad (7.2)$$

*kutsutaan **aidoksi tarkennukseksi** (proper refinement), jos sarjassa (7.2) on olemassa sellainen aliryhmä K_j , joka eroaa sarjan (7.1) kustakin aliryhmästä H_i .*

Täten ryhmän G aliryhmien ketjua

$$G = K_0 \supseteq K_1 \supseteq K_2 \supseteq \dots \supseteq K_{m-1} \supseteq K_m = \{e\}$$

kutsutaan ryhmän G aliryhmien ketjun

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \dots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

tarkennukseksi, jos

$$\{H_0, H_1, H_2, \dots, H_n\} \subseteq \{K_0, K_1, K_2, \dots, K_m\}.$$

Vastaavasti käytetään ilmausta **aito tarkennus**, jos

$$\{H_0, H_1, H_2, \dots, H_n\} \subset \{K_0, K_1, K_2, \dots, K_m\}.$$

Lause 7.1 *Ryhmän G alinormaali sarja on kompositiosarja, jos ja vain jos sillä ei ole aitoa tarkennusta.*

Todistus. Ks. [7], s. 225-226.

Määritelmä 7.3 *Olkoot seuraavat ketjut ryhmän G alinormaaleja sarjoja:*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}, \quad (7.3)$$

$$G = K_0 \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{m-1} \supseteq K_m = \{e\}. \quad (7.4)$$

Sarjat (7.3) ja (7.4) ovat ekvivalentit, jos on olemassa sellainen yksikäsitteinen vastaavuus näiden sarjojen ei-triviaalien tekijöiden välillä, että toisiaan vastaavat tekijät ovat isomorfiset.

Jos sarjat ovat ekvivalentit, niin niiden pituudet ovat samat. Seuraavat kaksi lausetta luovat perustan Jordanin-Hölderin lauseelle. Esitetään ensin *Zassenhausin lemmän* melko tekninen todistus.

Lause 7.2 (Zassenhausin lemma) *Olkoot H', H, K' ja K ryhmän G aliryhmiä. Olkoon H' ryhmän H normaali aliryhmä ja K' ryhmän K normaali aliryhmä. Silloin $H'(H \cap K')$ on ryhmän $H'(H \cap K)$ normaali aliryhmä ja $K'(H' \cap K)$ on ryhmän $K'(H \cap K)$ normaali aliryhmä. Lisäksi*

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{K'(H \cap K)}{K'(H' \cap K)}.$$

Todistus. (Vrt. [7], s. 227.) Lauseen 2.3 nojalla $H \cap K$ ja $H \cap K'$ ovat ryhmän G aliryhmiä. Koska $K' \subseteq K$, niin $H \cap K' \subseteq H \cap K$. Oletuksen mukaan K' on ryhmän K normaali aliryhmä, joten myös $H \cap K' \subseteq K'$ on ryhmän K normaali aliryhmä. Toisaalta $H \cap K \subseteq K$, joten $H \cap K'$ on ryhmän $H \cap K$ normaali aliryhmä. Vastaavalla tavalla voidaan osoittaa, että $H' \cap K$ on ryhmän $H \cap K$ normaali aliryhmä. Täten $(H \cap K')(H' \cap K)$ on ryhmän $H \cap K$ normaali aliryhmä lauseen 2.24 perusteella.

Merkitään nyt $J = (H \cap K')(H' \cap K)$. Määritellään kuvaus $f : H'(H \cap K) \rightarrow (H \cap K)/J$ seuraavasti: Jos $a \in H'(H \cap K)$, niin $a = h'b$, missä $h' \in H'$ ja $b \in H \cap K$. Merkitään $f(a) = bJ = Jb$, missä otetaan huomioon se, että J on ryhmän $H \cap K$ normaali aliryhmä. Olkoot $a_1, a_2 \in H'(H \cap K)$. Silloin ovat olemassa sellaiset $h'_1, h'_2 \in H'$ ja $b_1, b_2 \in H \cap K$, että $a_1 = h'_1 b_1, a_2 = h'_2 b_2$. Valitaan tällaiset h'_1, h'_2, b_1, b_2 . Oletetaan nyt, että $a_1 = a_2$. Silloin $h'_1 b_1 = h'_2 b_2$. Täten $h_2^{-1} h'_1 = b_2 b_1^{-1} \in H' \cap (H \cap K) \subseteq H' \cap K \subseteq J$. Tällöin siis $b_2 b_1^{-1} \in J$, joten $J b_2 b_1^{-1} = J$. Tästä seuraa, että $J b_1 = J b_2$, joten $f(a_1) = f(a_2)$. Näin todetaan, että f on hyvin määritelty.

Koska $b_1 \in H \cap K \subseteq H$ ja H' on ryhmän H normaali aliryhmä, niin $b_1 h'_2 b_1^{-1} \in H'$ esimerkin 2.7 nojalla. Nyt $a_1 a_2 = h'_1 b_1 h'_2 b_2 = h'_1 b_1 h'_2 b_1^{-1} b_1 b_2 = h' b_1 b_2$, missä $h' = h'_1 b_1 h'_2 b_1^{-1} \in H'$. Täten $f(a_1 a_2) = J b_1 b_2 = J b_1 J b_2 = f(a_1) f(a_2)$, joten f on homomorfismi.

Kuvauksen f määritelmästä havaitaan, että f on surjektio.

Osoitetaan vielä, että $\text{Ker } f = H'(H \cap K')$. Jos $h' \in H'$ ja $x \in H \cap K$, niin $f(h'x) = xJ = J$, jos ja vain jos $x \in J$ eli jos ja vain jos $h'x \in H'J = H'(H' \cap K)(H \cap K') = H'(H \cap K')$; tässä selvästi $H'(H' \cap K) = H'$. Täten $\text{Ker } f = H'(H \cap K')$. (Vrt. [3], s. 147.) Nyt ensimmäisen isomorfialauseen 3.10 nojalla

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{(H \cap K)}{J}.$$

Symmetriasyistä on voimassa isomorfia

$$\frac{K'(H \cap K)}{K'(H' \cap K)} \simeq \frac{(H \cap K)}{J}.$$

Väitteen isomorfia seuraa näistä isomorfoista. \square

Lause 7.3 (Schreier) *Ryhmän G millä tahansa kahdella alinormaalilla sarjalla on ekvivalentit tarkennukset.*

Todistus. (Vrt. [7], s. 227-228.) Olkoot ryhmällä G alinormaalit sarjat (7.3) ja (7.4). Olkoon $0 \leq i \leq n-1$. Sijoitetaan aliryhmien H_i ja H_{i+1} väliin ryhmä $H_{i+1}(H_i \cap K_j)$, $j = 0, 1, 2, \dots, m$. Tämä sarjan (7.3) tarkennus on Zassenhausin lemmän edellyttämä alinormaali sarja, jossa on mn inklusiota, toisin sanoen $mn+1$ ryhmää (joista jotkin voivat olla samoja). Olkoon $0 \leq j \leq m-1$. Ryhmien K_j ja K_{j+1} väliin sijoitetaan puolestaan ryhmä $K_{j+1}(K_j \cap H_i)$, $i = 0, 1, 2, \dots, n$. Myös tämä sarjan (7.4) tarkennus on alinormaali sarja, jossa on mn inklusiota (eli $mn+1$ ryhmää). Lopulliset tarkennukset ovat

$$\begin{aligned} \cdots \supseteq H_{i+1}(H_i \cap K_j) \supseteq H_{i+1}(H_i \cap K_{j+1}) \supseteq \cdots, \\ \cdots \supseteq K_{j+1}(K_j \cap H_i) \supseteq K_{j+1}(K_j \cap H_{i+1}) \supseteq \cdots. \end{aligned}$$

Zassenhausin lemmän nojalla nyt

$$\frac{H_{i+1}(H_i \cap K_j)}{H_{i+1}(H_i \cap K_{j+1})} \simeq \frac{K_{j+1}(K_j \cap H_i)}{K_{j+1}(K_j \cap H_{i+1})}$$

aina, kun $0 \leq i \leq n-1$ ja $0 \leq j \leq m-1$. Näin on lause osoitettu oikeaksi. \square

Lause 7.4 (Jordan-Hölder) *Olkoon G ryhmä ja olkoot*

$$\begin{aligned} G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}, \\ G = K_0 \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{m-1} \supseteq K_m = \{e\} \end{aligned}$$

sen mielivaltaiset kompositiosarjat. Silloin nämä kompositiosarjat ovat ekvivalentit.

Todistus. (Vrt. [7], s. 228.) Kompositiosarjat ovat alinormaaleja sarjoja, joten valittujen kompositiosarjojen tarkennukset ovat ekvivalentit lauseen 7.3 nojalla. Kompositiosarjalla ei ole aitoja tarkennuksia, joten kompositiosarja on ekvivalentti itsensä jokaisen tarkennuksen kanssa. Näin ollen ryhmän G valitut, mielivaltaiset kompositiosarjat ovat ekvivalentit. \square

Jordanin-Hölderin lauseen nojalla havaitaan, että jos ryhmällä G on kompositiosarja, jonka pituus on n , niin ryhmän G minkä tahansa kompositiosarjan pituuden täytyy olla n . Lukua n kutsutaan ryhmän G **kompositiopituudeksi** (composition length). Huomataan helposti, että ryhmän G kompositiopituus on vähintään yhtä suuri kuin ryhmän G alinormaalien sarjan pituus.

Esimerkki 7.1 *Määritetään ryhmän \mathbf{Z}_{20} kompositiosarjat ja todetaan, että ne ovat keskenään ekvivalentit.*

Ratkaisu. Ryhmä \mathbf{Z}_{20} on syklinen, joten sen kaikki aliryhmät ovat normaaleja; selvästi aliryhmät ovat \mathbf{Z}_{20} , $\langle [2] \rangle$, $\langle [4] \rangle$, $\langle [5] \rangle$, $\langle [10] \rangle$ sekä $\langle [0] \rangle$. Aliryhmistä saadaan seuraavat kompositiosarjat:

$$\begin{aligned} \mathbf{Z}_{20} \supset \langle [5] \rangle \supset \langle [10] \rangle \supset \langle [0] \rangle, \\ \mathbf{Z}_{20} \supset \langle [2] \rangle \supset \langle [4] \rangle \supset \langle [0] \rangle. \end{aligned}$$

Kompositiopituus on 3. (Ketju $\mathbf{Z}_{20} \supset \langle [2] \rangle \supset \langle [10] \rangle \supset \langle [0] \rangle$ ei ole kompositiosarja, sillä $\langle [10] \rangle$ ei ole ryhmän $\langle [2] \rangle$ *maksimaalinen* normaali aliryhmä.) Nyt Jordanin-Hölderin lauseen mukaan nämä kompositiosarjat ovat ekvivalentit. Toisin $\mathbf{Z}_{20}/\langle [5] \rangle \not\cong \mathbf{Z}_{20}/\langle [2] \rangle$, mutta samalla havaitaan seuraavat kompositiosarjojen tekijöiden väliset isomorfiat:

$$\begin{aligned}\mathbf{Z}_{20}/\langle [5] \rangle &\cong \langle [4] \rangle/\langle [0] \rangle, \\ \mathbf{Z}_{20}/\langle [2] \rangle &\cong \langle [10] \rangle/\langle [0] \rangle, \\ \langle [5] \rangle/\langle [10] \rangle &\cong \langle [2] \rangle/\langle [4] \rangle.\end{aligned}$$

Tässä esimerkiksi $\mathbf{Z}_{20}/\langle [5] \rangle = \{[0], [1], [2], [3], [4]\}$. Helposti havaitaan, että eri veillä lueteltujen isomorfisten tekijöiden kertaluvut ovat 5, 2 ja 2 (tässä järjestyksessä). Näin on todettu, että kompositiosarjojen ei-triviaalien tekijöiden välillä on sellainen yksikäsitteinen vastaavuus, että vastaavat tekijät ovat isomorfiset. Siten sarjat ovat ekvivalentit. ([7], tehtävä 3, s. 237)

Määritelmä 7.4 *Ryhmää G sanotaan ratkeavaksi (solvable), jos sillä on sellainen alinormaali sarja*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\},$$

että H_i/H_{i+1} on kommutatiivinen, $i = 0, 1, \dots, n-1$. Sellainen alinormaali sarja on ryhmän G ratkeava sarja (a solvable series for G).

Nimitys *ratkeava* viittaa siihen, että *polynomi yhtälöitä* voidaan ratkaista käyttämällä osaltaan hyväksi ryhmäteorian käsitteitä (ohitetaan tässä työssä). Abelin ryhmä G on ratkeava, sillä $G = H_0 \supseteq H_1 = \{e\}$ täyttää yllä esitetyn määritelmän.

Esimerkki 7.2 *Olkoon G Abelin ryhmä. Osoitetaan, että ryhmällä G on kompositiosarja, jos ja vain jos G on äärellinen.*

Ratkaisu. Oletetaan aluksi, että G on äärellinen. Osoitetaan, että ryhmällä G on kompositiosarja. Oletuksen mukaan G on Abelin ryhmä, joten sen kaikki aliryhmät ovat normaaleja. Kun $|G| = 1$, niin $G = H_0 \supseteq H_1 = \{e\}$ on ryhmän G kompositiosarja. Olkoon nyt $|G| > 1$. Koska G on äärellinen, niin on olemassa maksimaalinen ryhmän G normaali aliryhmä H_1 ; siten G/H_1 on yksinkertainen. Jos $H_1 = \{e\}$, niin $G = H_0 \supseteq H_1 = \{e\}$ on ryhmän G kompositiosarja. Jos $H_1 \neq \{e\}$, niin ryhmällä H_1 on maksimaalinen normaali aliryhmä H_2 . Silloin H_1/H_2 on yksinkertainen. Jos $H_2 = \{e\}$, niin $G = H_0 \supseteq H_1 \supseteq H_2 = \{e\}$ on ryhmän G kompositiosarja. Jos $H_2 \neq \{e\}$, niin samalla tavalla jatkamalla saadaan sarja $G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}$, jonka jokainen tekijä on yksinkertainen. Koska G on äärellinen, niin sillä on äärellinen määrä aliryhmiä, joten sarja on äärellinen. Näin on muodostettu ryhmän G kompositiosarja.

Oletetaan kääntäen, että ryhmällä G on kompositiosarja

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}.$$

Osoitetaan, että G on äärellinen. Kompositiosarjan tekijäryhmät H_{i-1}/H_i ovat yksinkertaisia ryhmiä, ja esimerkin 2.13 nojalla tekijät ovat Abelin ryhmiä. Tekijät ovat myös syklisiä ryhmiä, joiden kertaluvut $|H_{i-1}/H_i|$ ovat alkulukuja p_i , missä $i = 1, 2, \dots, n$. Tämä voidaan osoittaa seuraavasti. Tehdään vasta oletus, että

$|H_{i-1}/H_i|$ ei ole alkuluku jollakin indeksillä i . Silloin lauseen 6.10 mukaan ryhmällä H_{i-1}/H_i on ei-triviaali aliryhmä, joten H_{i-1}/H_i ei ole yksinkertainen. Tämä on ristiriidassa oletuksen kanssa, joten vasta oletus on väärä. Nyt

$$|G| = |H_0/H_1| \cdot |H_1/H_2| \cdots |H_{n-1}/H_n| = p_1 p_2 \cdots p_n,$$

joten G on äärellinen.

Näin on koko väite osoitettu oikeaksi. ([7], tehtävä 6, s. 237)

Esitetään seuraava kiintoisa yhteys, jonka Sylowin ensimmäinen lause luo ratkeaviin ryhmiin. Tämä koskee tapausta, jossa ryhmän kertaluku on jokin alkuluvun p potenssi.

Lause 7.5 *Olkoon G äärellinen ryhmä, jonka kertaluku on p^r , missä p on alkuluku ja r on positiivinen kokonaisluku. Silloin G on ratkeava.*

Todistus. (Ks. [3], s. 172-173.) Jos ryhmän G kertaluku on p^r , niin Sylowin ensimmäisen lauseen nojalla ryhmällä G on aliryhmä H_i , jonka kertaluku on p^i , aina, kun $0 \leq i \leq r$. Lauseen 6.14 nojalla H_i on ryhmän H_{i+1} normaali aliryhmä aina, kun $1 \leq i < r$. Lisäksi $\{e\}$ on niistä jokaisen normaali aliryhmä. Nyt

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{r-1} \supset H_r = \{e\}$$

on kompositiosarja, missä tekijöiden kertaluku on p . Koska tekijöiden H_i/H_{i+1} kertaluku on alkuluku p , niin tekijät ovat syklisiä ja siten myös kommutatiivisia. Tällöin G on ratkeava ja edellä mainittu sarja on ryhmän G ratkeava sarja. \square

7.2 Nilpotentit ryhmät

Tässä kappaleessa määritellään *nilpotentti* (engl. nil=nolla; potent=mahtava) ryhmä. Päälähteen [7] esityksestä poiketen määritellään aluksi *nouseva keskussarja*.

Olkoon G ryhmä. Määritellään eräs ryhmän G normaalien aliryhmien ketju induktioperiaatetta käyttämällä. Olkoon $i = 1$. Määritellään $Z_{i-1}(G) = Z_0(G) = \{e\}$, $Z_i(G) = Z_1(G) = Z(G)$. Esimerkin 2.8 perusteella nyt $Z_1(G)$ on ryhmän G normaali aliryhmä. Vastaavasti $Z(G/Z_1(G))$ on ryhmän $G/Z_1(G)$ normaali aliryhmä esimerkin 2.8 nojalla. Täten on lauseen 3.15 perusteella olemassa sellainen yksikäsitteinen ryhmän G normaali aliryhmä $Z_2(G)$, että $Z_1(G) \subseteq Z_2(G)$ ja $Z_2(G)/Z_1(G) = Z(G/Z_1(G))$.

Olkoon nyt $i \geq 1$. Tehdään induktio-oletus, että $Z_i(G)$ on määritelty, toisin sanoen on olemassa sellainen ryhmän G normaali aliryhmä $Z_i(G)$, että

$$Z_{i-1}(G) \subseteq Z_i(G) \text{ ja } Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)).$$

Tällöin on induktioperiaatteen mukaan, lauseen 3.15 nojalla olemassa sellainen yksikäsitteinen ryhmän G normaali aliryhmä $Z_{i+1}(G)$, että

$$Z_i(G) \subseteq Z_{i+1}(G) \text{ ja } Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Ryhmää Z_{i+1} kutsutaan ryhmän G $i+1$:nneksi **keskukseksi** (ks. [6], s. 473). Peräkkäin saadut keskukset muodostavat (mahdollisesti) kasvavan, ryhmän G normaalien aliryhmien ketjun

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_i(G) \subseteq Z_{i+1}(G) \subseteq \cdots$$

ja $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$, $i \geq 0$. Tätä normaalien aliryhmien ketjua kutsutaan ryhmän G **nousevaksi keskussarjaksi** (ascending central series of G). Ketju ei aina koskaan saavuta koko ryhmää G . (Ks. [7], s. 240; vrt. [6], s. 473.)

Esitettyä tarkastelua voidaan luonnehtia niinkin, että yhtälö $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ indusoi keskusta $Z_i(G)$ seuraavan keskuksen $Z_{i+1}(G)$.

Nousevan keskussarjan erikoistapauksena määritellään nyt keskussarja.

Määritelmä 7.5 *Olkoon $G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots \subseteq G_n$ ryhmän G normaalien aliryhmien ketju. Ketjua kutsutaan **keskussarjaksi** (central series), jos $G_{i+1}/G_i \subseteq Z(G/G_i)$ aina, kun $i = 0, 1, \dots, n-1$.*

Määritelmä 7.6 *Ryhmää G kutsutaan **nilpotentiksi**, jos ryhmällä G on sellainen keskussarja*

$$G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots \subseteq G_n,$$

että $G_0 = \{e\}$ ja $G_n = G$.

On syytä korostaa, että ryhmä G on nilpotentti vain silloin, kun keskussarja saavuttaa koko ryhmän G äärellisellä määrällä peräkkäisiä normaaleja aliryhmiä. Nilpotentin ryhmän G keskussarja on normaali sarja, koska kaikki ryhmän G aliryhmät ovat normaaleja ryhmässä G .

Nilpotentin ryhmän määritelmä edellyttää, että keskussarjan tekijäryhmät ovat kommutatiivisia. Tästä seuraa, että *nilpotentti ryhmä on ratkeava*. Käänneväite ei kuitenkaan päde; tämän osoittaa esimerkiksi havainto, että symmetrinen ryhmä S_3 on ratkeava, mutta ei nilpotentti (ks. [7], esimerkit 8.1.15 ja 8.2.3).

Lähde [7] toteaa, että jokainen Abelin ryhmä on nilpotentti; osoitetaan tämä etsimällä Abelin ryhmän keskussarja. Olkoon G mielivaltainen (äärellinen tai ääretön) Abelin ryhmä. Tällöin ovat olemassa ryhmän G normaalit aliryhmät $Z_0(G) = \{e\}$ ja $Z_1(G) = Z(G) = G$, joten selvästi $G/\{e\} = Z_1(G)/Z_0(G) \subseteq Z(G/Z_0(G)) = G/\{e\}$. Näin saadaan keskussarja $\{e\} = Z_0(G) \subseteq Z_1(G) = G$, joten G on nilpotentti.

Äärelliset p -ryhmät ovat tärkein esimerkki nilpotenteista ryhmistä.

Lause 7.6 *Jokainen äärellinen p -ryhmä on nilpotentti.*

Todistus. (Vrt. [7], s. 239-240.) Olkoon G äärellinen p -ryhmä. Merkitään $|G| = p^k$, $k \geq 0$. Jos $|G| = p^0 = 1$, niin lause on triviaalisti tosi. Olkoon tästä lähtien $k \geq 1$. Esitetään nyt induktiotodistus indeksin k suhteen.

Olkoon $k = 1$. Tällöin $|G| = p^k = p$. Koska p on alkuluku, niin G on syklinen ryhmä ja siten myös Abelin ryhmä. Ryhmän G keskussarja on $\{e\} = G_0 \subset G_1 = G$, ja tässä $G/\{e\} \subseteq Z(G/\{e\}) = G/\{e\}$, sillä tekijäryhmä $G/\{e\}$ on Abelin ryhmä esimerkin 2.13 mukaan. Ryhmä G on siis nilpotentti.

Olkoon seuraavaksi $k = 2$, jolloin $|G| = p^2$. Lauseen 6.12 nojalla nyt $Z_1 = Z(G) \neq \{e\}$. Jos $G = Z_1$, niin G on Abelin ryhmä, jolloin G on nilpotentti. Oletetaan nyt, että $G \neq Z_1$. Tällöin $|Z_1| = p$. Esimerkin 2.8 perusteella $Z_1 = Z(G)$ on ryhmän G normaali aliryhmä. Tällöin voidaan muodostaa tekijäryhmä G/Z_1 . Nyt $|G/Z_1| = |G|/|Z_1| = p$, joten G/Z_1 on myös p -ryhmä, johon lausetta 6.12 voidaan soveltaa. Sen mukaan $|Z(G/Z_1)| > 1$, joten $Z(G/Z_1) = Z_2/Z_1 \neq Z_1/Z_1$. Tässä Z_2 on lauseen 3.15 mukaan ryhmän G sellainen normaali aliryhmä, että $Z_1 \subset Z_2$. Koska $\{e\} \neq Z_1 \neq G$, niin $Z_2 = G$. Nyt saadaan keskussarja $\{e\} =$

$Z_0 \subset Z_1 \subset Z_2 = G$, sillä $Z_1/\{e\} \subseteq Z(G/\{e\})$ ja $Z_2/Z_1 \subseteq Z(G/Z_1) = Z_2/Z_1$; tässä $|Z_2/Z_1| = p$, joten Z_2/Z_1 on Abelin ryhmä. (Edellä esitetyn päättelyn perusidea on seuraava: oletuksesta $G \neq Z_1$ seuraa, että on olemassa sellainen ryhmän G normaali aliryhmä Z_2 , että $Z_1 \subset Z_2$.) Näin todetaan, että G on nilpotentti.

Olkoon sitten $|G| = p^r$, $r > 2$. Tehdään induktio-oletus, että lause on tosi aina, kun $0 \leq k \leq r - 1$. Tällöin on olemassa keskussarja $\{e\} = Z_0 \subset Z_1 \subset \dots \subset Z_{r-1}$. Nyt $|G/Z_{r-1}| > 1$, joten induktioperiaatteen mukaan, lauseen 3.15 nojalla $Z(G/Z_{r-1}) = Z_r/Z_{r-1}$, missä Z_r on ryhmän G sellainen normaali aliryhmä, että $Z_{r-1} \subset Z_r$. Koska $Z_{r-1} \neq G$, niin $Z_r = G$. Nyt $Z_r/Z_{r-1} \subseteq Z(G/Z_{r-1})$, joten saadaan keskussarja $\{e\} = Z_0 \subset Z_1 \subset \dots \subset Z_{r-1} \subset Z_r = G$. Induktioperiaatteen mukaan lause on näin ollen tosi aina, kun $k = 0, 1, \dots, r$. Näin on lause kokonaan todistettu. \square

Lause 7.7 *Olkoon G sellainen ryhmä, että $Z_n(G) = G$ jollakin ei-negatiivisella kokonaisluvulla n . Silloin G on nilpotentti.*

Todistus. Ks. [7], s. 240.

Lause 7.8 *Olkoon G_i nilpotentti ryhmä, $i = 1, 2, \dots, n$. Silloin ryhmien suora tulo $G_1 \times G_2 \times \dots \times G_n$ on nilpotentti.*

Todistus. Ks. [7], s. 242-243.

Seuraava lause kokoaa nilpotentin ryhmän ominaisuuksia.

Lause 7.9 *Olkoon G äärellinen ryhmä. Silloin seuraavat ehdot ovat ekvivalentteja.*

(i) G on nilpotentti.

(ii) Jos H on ryhmän G aito aliryhmä, niin $H \subset N_G(H)$.

(iii) Jokainen ryhmän G maksimaalinen aliryhmä on ryhmän G normaali aliryhmä.

(iv) Jokainen ryhmän G Sylowin aliryhmä on ryhmän G normaali aliryhmä.

(v) G on isomorfinen p -ryhmien suoran tulon kanssa.

Todistus. Ks. [7], s. 243.

Esimerkki 7.3 *Osoitetaan, että nilpotentin ryhmän homomorfinen kuva on nilpotentti.*

Ratkaisu. (Vrt. [7], lauseen 8.1.17 todistus, s. 229-230.) Olkoon G nilpotentti ryhmä ja olkoon \bar{G} sen homomorfinen kuva. Oletuksen perusteella on olemassa epimorfismi f ryhmältä G ryhmälle \bar{G} . Koska G on nilpotentti, niin sillä on keskussarja, johon kuuluvat aliryhmät G_i , $i = 0, 1, \dots, n$, ovat normaaleja ryhmässä G . Lisäksi $G_0 = \{e\}$ ja $G_n = G$. Merkitään $\bar{G}_i = f(G_i)$, $i = 0, 1, \dots, n$. Lauseen 3.3 perusteella $f(G_i)$ on ryhmän \bar{G} normaali aliryhmä aina, kun $i = 0, 1, \dots, n$. Toisaalta oletuksesta $G_i \subseteq G_{i+1}$ seuraa, että $f(G_i) \subseteq f(G_{i+1})$ aina, kun $i = 0, 1, \dots, n-1$. Näin ollen $f(G_i)$ on ryhmän $f(G_{i+1})$ normaali aliryhmä aina, kun $i = 0, 1, \dots, n-1$. Täten

$$\bar{G}_0 \subseteq \bar{G}_1 \subseteq \bar{G}_2 \subseteq \dots \subseteq \bar{G}_n$$

on ryhmän \bar{G} normaalien aliryhmien ketju, jossa $\bar{G}_0 = \{\bar{e}\}$ ja $\bar{G}_n = \bar{G}$. Tässä \bar{e} on ryhmän \bar{G} neutraalialkio. Osoitetaan nyt, että $f(G_{i+1})/f(G_i) = \bar{G}_{i+1}/\bar{G}_i \subseteq Z(\bar{G}/\bar{G}_i)$ aina, kun $i = 0, 1, \dots, n-1$.

Olkoon $h : G_{i+1} \rightarrow \bar{G}_{i+1}/\bar{G}_i$, $h(g_{i+1}) = f(g_{i+1})\bar{G}_i$, $g_{i+1} \in G_{i+1}$, $0 \leq i \leq n-1$. Koska f on epimorfismi, niin h on epimorfismi ryhmältä G_{i+1} ryhmälle \bar{G}_{i+1}/\bar{G}_i . Huomataan, että aina, kun $g_i \in G_i \subseteq G_{i+1}$, niin $h(g_i) = f(g_i)\bar{G}_i = f(g_i)f(G_i)$. Koska $f(g_i) \in f(G_i)$, niin nyt $h(g_i) = f(G_i) = \bar{G}_i$. Täten $G_i \subseteq \text{Ker } h$.

Koska G_i ja G_{i+1} ovat ryhmän G normaaleja aliryhmiä ja $G_i \subseteq G_{i+1}$, niin G_i on ryhmän G_{i+1} normaali aliryhmä. Olkoon nyt k luonnollinen homomorfismi ryhmältä G_{i+1} ryhmälle G_{i+1}/G_i . Näin ollen lauseen 3.9 nojalla epimorfismi h indusoi erään epimorfismin h' ryhmältä G_{i+1}/G_i ryhmälle \bar{G}_{i+1}/\bar{G}_i . Havainnollistetaan homomorfismeja seuraavalla kuviolla.

$$\begin{array}{ccc} G_{i+1} & \xrightarrow{h} & \bar{G}_{i+1}/\bar{G}_i \\ k \downarrow & h' \nearrow & \\ G_{i+1}/G_i & & \end{array}$$

Kuvio 6. Aliryhmään G_{i+1} liittyvät homomorfismit

Koska G on nilpotentti, niin G_{i+1}/G_i on kommutatiivinen. Nyt h' on epimorfismi, joten myös \bar{G}_{i+1}/\bar{G}_i on kommutatiivinen lauseen 3.1 nojalla. Tästä seuraa, että $\bar{G}_{i+1}/\bar{G}_i \subseteq Z(\bar{G}/\bar{G}_i)$ aina, kun $i = 0, 1, \dots, n-1$. Näin todetaan, että edellä esitetty ryhmän \bar{G} normaalien aliryhmien ketju on keskussarja. Tämä merkitsee sitä, että \bar{G} on nilpotentti. ([7], tehtävä 1, s. 244)

8 Loppukommentit

Esityksessä on tarkasteltu ryhmäteorian peruskäsitteitä. Tärkeimpiä yksittäisiä käsitteitä ovat ilmeisesti normaalit aliryhmät ja ryhmähomomorfismit, sillä niitä on sovellettu jatkuvasti eri yhteyksissä.

Seuraavassa esitetään yhteenvedo työssä todistetuista lauseista sekä täydentävistä ja havainnollistavista esimerkeistä. Lisäksi kootaan yhteen päälähteestä [7] löydetyt virheet ja epäjohdonmukaisuudet.

Aiheen käsittelyn yhteydessä esitetyistä lauseista seuraavien todistukset ovat kirjoittajan laatimia: 2.6, 2.7, 2.8, 2.9, 2.18, 2.21, 2.25, 3.2 ja 6.16 (yhteensä yhdeksän kappaletta). Näistä lauseista neljä ensimmäistä on kokonaan formuloitukin syklisten ryhmien tarkastelun yhteydessä.

Havainnollistavat esimerkit ovat lähinnä päälähteessä [7] ilman ratkaisua annettuja harjoitustehtäviä. Näitä ovat esimerkit 2.1, 2.2, 2.3, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 3.1, 3.2, 3.3, 3.5, 3.6, 3.7, 3.10, 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2 ja 7.3 (yhteensä 29 kappaletta).

Lähteestä [7] löydetyt virheet on esitetty sivuilla 21, 23 ja 27. Lisäksi sivuilla 28 ja 37 kiinnitetään huomiota lähteen harhaanjohtaviin esitystapoihin. Sivuilla 49-50 on poikettu lähteen [7] esitysjärjestyksestä, joka vaikuttaa epäjohdonmukaiselta, sillä keskussarja on luontevaa määritellä nousevan keskussarjan erikoistapauksena.

Kirjallisuus

- [1] Baumslag, B. & Chandler, B., Theory and Problems of Group Theory. McGraw-Hill, 1968. 279 s.
- [2] Bhattacharya, P. B. & Jain, S. K. & Nagpaul, S. R., Basic Abstract Algebra. 2. p. Cambridge University Press, 1994. 487 s.
- [3] Fraleigh, J. B., A First Course in Abstract Algebra. 3. p. Addison-Wesley, 1982. 478 s.
- [4] Gallian, J. A., Contemporary Abstract Algebra. 3. p. D. C. Heath and Company, 1994. 525 s.
- [5] Herstein, I. N., Abstract Algebra. 2. p. Macmillan Publishing Company, 1990. 293 s.
- [6] Mac Lane, S. & Birkhoff, G., Algebra. 1. p. The Macmillan Company, 1967. 598 s.
- [7] Malik, D. S. & Mordeson, J. N. & Sen, M. K., Fundamentals of Abstract Algebra. McGraw-Hill, 1997. 636 s.
- [8] Myrberg, L., Algebra. Kirjayhtymä. Vaasa 1978. 127 s.
- [9] Whitelaw, T. A., Introduction to Abstract Algebra. 3. p. Chapman & Hall/CRC, 1995. 247 s.

Korjaukset

Seuraavassa esitetään esimerkki 3.2 (s. 18) korjattuna sekä loppukommentteihin (s. 52) liittyviä korjauksia.

Esimerkki 8.1 Määritetään kaikki epimorfismit ryhmältä $(\mathbf{Z}, +)$ ryhmälle $(\mathbf{Z}_6, +_6)$.

Ratkaisu. Olkoon $f : (\mathbf{Z}, +) \rightarrow (\mathbf{Z}_6, +_6)$ epimorfismi. Olkoon $a \in \mathbf{Z}$. Sekä ryhmä \mathbf{Z} että ryhmä \mathbf{Z}_6 ovat syklisiä; edellinen on ääretön, jälkimmäinen äärellinen. Ryhmän \mathbf{Z} generaattori on luku 1 (myös luku -1 on sen generaattori), ryhmän \mathbf{Z}_6 generaattoreita ovat alkiot $[1]$ ja $[-1]$. Olkoon $a \in \mathbf{Z}$. Koska f on homomorfismi, niin se täyttää nyt lauseen 3.2 nojalla ehdon

$$f(a) = f(\underbrace{1 + 1 + \cdots + 1}_{a \text{ kpl}}) = \underbrace{f(1) +_6 f(1) +_6 \cdots +_6 f(1)}_{a \text{ kpl}}, a > 0.$$

Kun $a = 0$, niin $f(a) = [0]$ lauseen 3.1 perusteella. Olkoon nyt $a < 0$. Tällöin luku a voidaan esittää sivulla 3 määritellyllä tavalla luvun 1 monikertana $a1 = (-a)(-1)$, joten $f(a) = f(a1) = f((-a)(-1))$. Lauseen 3.2 mukaan siis

$$f(a) = f(\underbrace{(-1) + (-1) + \cdots + (-1)}_{-a \text{ kpl}}) = \underbrace{f(-1) +_6 f(-1) +_6 \cdots +_6 f(-1)}_{-a \text{ kpl}}, a < 0.$$

Edellä esitetyn nojalla koko epimorfismi tulee määritellyksi, kun $f(1)$ ja $f(-1)$ tunnetaan (vrt. [4], s. 174). Seuraava päättely liittyy tapaukseen, jossa $a > 0$. Samat päätelmät voitaisiin tehdä tapauksessa, jossa $a < 0$. Koska \mathbf{Z}_6 on syklinen, niin $f(1)$ generoi ryhmän \mathbf{Z}_6 jonkin syklisen aliryhmän. Lagrangen lauseen perusteella nyt $|\langle f(1) \rangle| = o(f(1))$ jakaa luvun 6, joten $o(f(1))$ on 1, 2, 3 tai 6.

Jos $o(f(1)) = 1$, niin $f(1) = [0]$. Tällöin f on triviaali homomorfismi, joten se ei ole epimorfismi. Jos $o(f(1)) = 2$, niin $f(1) = [3]$. Tällöin $f(a) = [3a]$, $a \in \mathbf{Z}$. Nyt $f(0) = [0] = \{0, \pm 6, \pm 12, \pm 18, \dots\}$, $f(1) = [3] = \{\pm 3, \pm 9, \pm 15, \dots\} = f(3) = f(5)$ ja $f(2) = [6] = [0] = f(0) = f(4)$. Havaitaan, että alkioilla $[1]$, $[2]$, $[4]$ ja $[5]$ ei ole alkukuvaa ryhmässä \mathbf{Z} , joten f ei ole epimorfismi.

Jos $o(f(1)) = 3$, niin $f(1) = [2]$. Tällöin $f(a) = [2a]$, $a \in \mathbf{Z}$. Nyt $f(0) = [0] = \{0, \pm 6, \pm 12, \pm 18, \dots\}$, $f(1) = [2] = \{\dots, -16, -10, -4, 2, 8, 14, \dots\}$ ja $f(2) = [4] = \{\dots, -14, -8, -2, 4, 10, 16, \dots\}$. Havaitaan, että ”parittomilla” alkioilla $[1]$, $[3]$ ja $[5]$ ei ole alkukuvaa ryhmässä \mathbf{Z} , joten tämäkään kuvaus ei ole epimorfismi.

Jos $o(f(1)) = 6$, niin $f(1) = [1]$ tai $f(1) = [-1]$. Tällöin selvästi sekä kuvaus $f(a) = [a]$, $a \in \mathbf{Z}$, että kuvaus $f(a) = [-a]$, $a \in \mathbf{Z}$, ovat epimorfismeja. Etsityt epimorfismit ovat siis $f(a) = [a]$ ja $f(a) = [-a]$, $a \in \mathbf{Z}$. ([7], tehtävä 3, s. 151)

Loppukommentit

Havainnollistavat esimerkit ovat lähinnä päälähteessä [7] ilman ratkaisua annettuja harjoitustehtäviä. Näitä ovat esimerkit 2.1, 2.2, 2.3, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 3.1, 3.2, 3.3, 3.5, 3.6, 3.10, 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2 ja 7.3 (yhteensä 27 kappaletta). Tekijä on laatinut esimerkit 2.5 (s. 8-9) ja 3.7 (s. 22-23).