Äärellisten ryhmien luokittelu isomorfialla

Pro gradu -tutkielma
Jani Hämäläinen
283007
Fysiikan ja matematiikan laitos
Itä-Suomen yliopisto
10. toukokuuta 2021

Tiivistelmä

Tämän tutkielman tarkoituksena on esitellä lauseita, joiden avulla voidaan luokitella äärellisiä ryhmiä isomorfian mukaisesti. Eräänä lähtökohtana on luokitella kaikki ne ryhmät, joissa on 15 alkiota tai vähemmän. Tutkielma alkaa ryhmien määrittelystä sekä niiden perusominaisuuksien tarkastelusta. Kolmannessa luvussa käsitellään lukuteorian ja modulaariaritmetiikan perusteita, sillä modulaariaritmetiikalla on keskeinen rooli äärellisten ryhmien luokittelussa. Syklisiin ja normaaleihin aliryhmiin perehdytään luvussa neljä. Kyseisiin aliryhmiin liittyvät tulokset, erityisesti Lagrangen lause, ovat keskeisiä ryhmien luokittelussa. Vaihdannaisilla ryhmillä eli Abelin ryhmillä on erityisiä ominaisuuksia. Näihin ominaisuuksiin liittyviin tuloksiin ja Abelin ryhmien luokitteluun perehdytään luvussa viisi. Abelin ryhmien jälkeen tutustutaan kolmeen erilaiseen ryhmätyyppiin, jotka toimivat esimerkkeinä ryhmien luokittelussa. Seitsemännessä luvussa todistetaan norjalaisen matemaatikon Peter Ludwig Meidell Sylowin kehittämiä lauseita. Sylowin lauseiden antamat tulokset ovat tärkeitä äärellisten ryhmien rakenteiden tarkastelussa. Tutkielman lopuksi todistetaan ne lauseet, joiden avulla voidaan luokitella kaikki 15-alkioiset ja sitä pienemmät ryhmät. Näitä lauseita voidaan hyödyntää myös monien muidenkin äärellisten ryhmien luokittelussa.

Abstract

The purpose of this Master's thesis is to present how groups are classified up to isomorphism. A premise to this thesis was to classify all groups of order 15 or less up to isomorphism. This paper begins with the fundamentals of group theory and advances to more advanced theorems. Modular arithmetic serves an important role in group theory and in classification theory of finite groups. Applications of modular arithmetic are exhibited in Chapter 3, along with the principles of number theory. Subgroups and their attributes are presented in Chapter 4. Especially Lagrange's theorem has a significant role in the analysis of the structure of groups. Chapter 5 is dedicated to classifying of Abelian groups and their unique properties. Examples of how symmetries form a group are presented in Chapter 6, with two special classes of groups that have a notable role in classifying groups up to isomorphism. Sylow's theorems are proved in Chapter 7. They have a significant role in the analysis of the structure of groups. Theorems by which groups can be classified up to isomorphism are proved in the last chapter.

Sisällys

1 Johdanto

Ryhmäteoria on algebran osa-alue, jossa tutkitaan algebrallisia rakenteita eli ryhmiä. Ryhmän alkiot voivat olla numeroita, matriiseja, polynomeja, funktioita, symmetrioita tai melkein tahansa, kunhan ne täyttävät ryhmän neljä vaatimusta. Symmetrisyyttä esiintyy kaikkialla luonnossa. Monet tieteenalat tutkivat symmetrioita ja niihin liittyviä ominaisuuksia. Kemistit pyrkivät ennustamaan aineiden ominaisuuksia tutkimalla molekyylien symmetrioita ja biologit pyrkivät ymmärtämään DNA:n ominaisuuksia sen symmetrioiden avulla. Fyysikot puolestaan tutkivat aika-avaruuden tasojen symmetrioita. Matemaattisesti symmetriat määritellään ryhmäteorian avulla. Tämä tekee ryhmäteoriasta keskeisen matematiikan osa-alueen, ja sillä on tärkeitä sovelluksia muillakin tieteenaloilla.

Suurien ja monimutkaisten ryhmien tutkiminen on usein työlästä. Työläyden vuoksi ryhmäteoreetikot etsivät monimutkaisten ja yksinkertaisten ryhmien välille kuvauksia, jotka säilyttävät ryhmien ominaisuudet. Kahden ryhmän välistä kuvausta, joka ei muuta ryhmien ominaisuuksia kutsutaan isomorfiaksi. Isomorfiset ryhmät omaavat identtiset matemaattiset ominaisuudet, minkä johdosta niitä voidaan pitää samana ryhmänä. Tämän vuoksi ryhmäteorian tutkijat ovat halunneet luoda listan, jossa luokitellaan kaikki äärelliset ryhmät isomorfian mukaisesti. Ryhmäteoreetikot ovat onnistuneet todistamaan kaikkien äärellisten ryhmien rakenneosasten, eli yksinkertaisten ryhmien olemassaolon. Todistus koostuu noin sadan matemaatikon työstä, viideltä eri vuosikymmeneltä ja se on kymmeniä tuhansia sivuja pitkä.

Tässä tutkielmassa luokitellaan isomorfian mukaisesti kaikki ne ryhmät, joissa on 15 alkiota tai vähemmän. Abelin ryhmät ovat helppoja luokitella. Ei-Abelisten ryhmien luokittelu on kuitenkin vaikeampaa, sen vuoksi ne joudutaan yleensä luokittelemaan tapauskohtaisesti. 16 alkioisia ryhmiä on 14 erilaista, joista viisi on Abelin ryhmiä ja yhdeksän ei-Abelin ryhmiä. Tästä syystä tässä tutkielmassa luokittelu rajoitetaan 15 alkioisiin ja sitä pienempiin ryhmiin. Tutkielman vaativimmat tarkastelun kohteet ovat 12-alkioiset ryhmät. Näitä ryhmiä on kuusi erilaista, kolme Abelin ryhmää ja kolme ei-Abelin ryhmää.

Tutkielma alkaa ryhmän määritelmän sekä ryhmien perusominaisuuksien esittelyllä. Jäännösluokkien ja niiden muodostamien ryhmien ominaisuuksiin perehdytään luvussa kolme. Seuraavaksi tutkielmassa käsitellään keskeisempiä aliryhmiä, sekä niiden ominaisuuksia. Luvussa viisi keskitytään Abelin ryhmien ominaisuuksiin ja niiden luokittelemiseen. Kuudennessa luvussa esitellään erityisiä ryhmiä, joita käytetään ryhmien luokittelussa. Samalla tarkastellaan myös symmetrioihin liittyviä ryhmiä. Tämän jälkeen esitellään ja todistetaan äärellisten ryhmien luokitteluun käytettävät Sylowin lauseet se-

kä niiden todistamiseksi vaadittavat aputulokset. Lopuksi todistetaan luokittelulauseet, joiden avulla luokitellaan kaikki ne ryhmät, joissa on alle 16 alkiota.

2 Ryhmien peruominaisuuksia

Tässä luvussa esitetään ryhmäteorian peruskäsitteitä ja -tuloksia. Lukijalta odotetaan algebran perusteiden tuntemusta, ja siksi tämän luvun tuloksia ei todisteta.

Määritelmä 2.1. Olkoon $\circ$ epätyhjän joukon G laskutoimitus. Paria $(G, \circ)$ kutsutaan *ryhmäksi*, jos seuraavat ehdot toteutuvat:

(i) Kaikilla $a, b \in G$ pätee $a \circ b \in G$.

(ii) Kaikilla $a, b, c \in G$ pätee $(a \circ b) \circ c = a \circ (b \circ c)$.

(iii) On olemassa alkio $e \in G$ siten, että $e \circ a = a \circ e$ kaikilla $a \in G$.

(iv) Jokaiselle alkiolle $a \in G$ on olemassa alkio $a^{-1} \in G$ siten, että

$$a \circ a^{-1} = e = a^{-1} \circ a.$$

Alkiota e sanotaan neutraalialkioksi, ja alkiota a^{-1} sanotaan alkion a käänteisalkioksi. Jos lisäksi on voimassa

$$a \circ b = b \circ a$$

kaikilla $a, b \in G$, ryhmää $(G, \circ)$ sanotaan Abelin ryhmäksi.

Jatkossa ryhmästä käytetään merkintää G parin $(G, \circ)$ sijaan, kun joukossa G on määritelty Määritelmän 2.1 mukainen laskutoimitus $\circ$. Lisäksi merkitään lyhyesti ab merkinnän $a \circ b$ sijaan. Jatkossa alkio e tarkoittaa aina neutraalialkiota.

Määritelmä 2.2. Olkoon G ryhmä, jossa on n alkiota. Tällöin lukua n sanotaan ryhmän G *kertaluvuksi*, ja merkitään $|G| = n$.

Lemma 2.3. *Olkoon G ryhmä ja olkoot $a, x, y \in G$. Tällöin*

(1) Ryhmän G neutraalialkio on yksikäsitteinen.

(2) $ax = ay \Leftrightarrow x = y$ ja $xa = ya \Leftrightarrow x = y$.

(3) Jokaisen alkion a käänteisalkio a^{-1} on yksikäsitteinen.

Todistus. [4], s.197. □

Määritelmä 2.4. Olkoot $(A, \circ)$ ja $(B, \bullet)$ ryhmiä. Näiden kahden ryhmän välinen *suora tulo* $(A \times B, *)$ määritellään järjestettyjen parien joukkona

$$A \times B = \{(a, b) : a \in A \text{ ja } b \in B\},$$

kun laskutoimitus $*$ määritellään asettamalla

$$a * b := (a_1 \circ b_1, a_2 \bullet b_2)$$

kaikilla $a = (a_1, a_2), b = (b_1, b_2) \in A \times B$.
Ryhmien välinen suora tulo voidaan yleistää tapaukseen, jossa on n ryhmää.

Jos kahden ryhmän välisessä suorassa tulossa on määritelty laskutoimitus $+$, niin käytetään termin suora tulo sijaan termiä *suora summa* ja käytetään merkinnän $\times$ sijaan merkintää $\oplus$.
Määritellään seuraavaksi se kuvaus, jonka avulla ryhmiä luokitellaan.

Määritelmä 2.5. Olkoot $(G, \circ)$ ja $(G', *)$ ryhmiä. Kuvausta $f : G \to G'$ sanotaan *homomorfismiksi*, jos

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

kaikille $a, b \in G$. Jos f on lisäksi bijektio $G \to G'$, kuvausta f sanotaan *isomorfismiksi* ja merkitään $G \cong G'$.

Homomorfismi on kuvaus, joka säilyttää laskutoimituksen kahden ryhmän välillä. Koska isomorfismi on homomorfismin lisäksi bijektio, niin isomorfiassa säilyvät laskutoimituksen lisäksi alkioiden ominaisuudet. Jos ryhmien välillä on isomorfia, niin ryhmiä voidaan pitää samana ryhmänä, joilla on eri merkintä tavat.
Seuraavaksi määritellään aliryhmä. Aliryhmiä ja niiden ominaisuuksia tarkastellaan tarkemmin luvussa 4.

Määritelmä 2.6. Olkoon G ryhmä ja $H \subset G$ epätyhjä. Ryhmää H sanotaan ryhmän G *aliryhmäksi*, mikäli seuraavat ehdot toteutuvat

(1) Ryhmän G neutraalialkio e kuuluu joukkoon H,

(2) Jos $a, b \in H$, niin $ab \in H$,

(3) Jos $a \in H$, niin $a^{-1} \in H$.

Aliryhmä on ryhmän epätyhjä osajoukko, jossa on sama neutraali- ja käänteisalkio kuin laajemmassa ryhmässä. Määritelmän 2.6 ehdot voi tiivistää seuraavasti:

Lemma 2.7. *Ryhmän G epätyhjä osajoukko H on ryhmän G aliryhmä, jos ja vain jos $ab^{-1} \in H$, kaikilla $a, b \in G$.*

Todistus. [2], s.73. □

Lemma 2.8. *Olkoot G ja H ryhmiä, joiden neutraalialkiot ovat e_G ja e_H, ja olkoon kuvaus $f : G \to H$ on homomorfismi. Tällöin*

(1) $f(e_G) = e_H$,

(2) $f(a^n) = f(a)^n$ *kaikille* $a \in G$ *ja* $n \in \mathbb{N}$.

(3) $f(a^{-1}) = f(a)^{-1}$ *kaikille* $a \in G$,

(4) kuvauksen $f(G)$ kuvajoukko on ryhmän H aliryhmä,

(5) jos kuvaus f on injektio, niin G on isomorfinen kuvauksen f kuvajoukon $f(G)$ kanssa.

Todistus. [4], s.221. □

Määritelmä 2.9. Olkoon kuvaus $f : G \to H$ homomorfismi ryhmältä G ryhmälle H. Kuvauksen *ydin* $(Ker\ f)$ on joukko

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

Lemma 2.10. *Olkoot G ja H ryhmiä ja kuvaus $f : G \to H$ homomorfismi, jonka ydin on $Kerf$. Tällöin $Kerf = \langle e \rangle$, jos ja vain jos kuvaus f on injektio.*

Todistus. [4], s.254. □

3 Jäännösluokkaryhmät

Jäännösluokat ovat tärkeässä osassa algebrassa ja ryhmäteoriassa. Tässä luvussa tutustutaan jäännösluokkien muodostamiin joukkoihin sekä niiden muodostamiin ryhmiin. Lukijalta odotetaan tuntemusta lukuteorian alkeista ja siksi yksinkertaiset tulokset on jätetty todistamatta. Aloitetaan lukujen jaollisuudesta.

Lemma 3.1. *Olkoot $a, b \in \mathbb{Z}$, ja $b > 0$. Tällöin on olemassa yksikäsitteiset luvut $r, q \in \mathbb{Z}$ siten, että*

$$a = bq + r,$$

missä $0 \leqslant r < b$.

Todistus. [10], s.20. □

Määritelmä 3.2. Lukua n kutsutaan luvun a *tekijäksi*, jos $n \mid a$. Suurinta lukua n, jolle $n \mid a$ ja $n \mid b$, kutsutaan lukujen a ja b *suurimmaksi yhteiseksi tekijäksi*, ja merkitään $n = syt(a, b)$.

Määritelmä 3.3. Kokonaislukua $p > 1$ sanotaan *alkuluvuksi*, jos sen tekijät ovat ainoastaan luvut 1 ja p.

Lemma 3.4. *Jos $p > 1$ ja $p \mid ab$, niin luku p on alkuluku, jos ja vain jos $p \mid a$ tai $p \mid b$.*

Todistus. [4], s.18. □

Lause 3.5 (Aritmetiikan peruslause)**.** *Kaikki kokonaisluvut $n > 1$ voidaan esittää yksikäsitteisesti alkulukujen tulona.*

Todistus. [12], s.112-114. □

Lauseen 3.5 mukaista esitystä kutsutaan *alkutekijähajotelmaksi.*

Lemma 3.6. *Olkoon $a, b \in \mathbb{Z}/\{0\}$. Tällöin*

(1) on olemassa $d \in \mathbb{N}$ siten, että $d = syt(a, b)$

(2) on olemassa $m, n \in \mathbb{Z}$ siten, että $d = am + bn$.

(3) $syt(a, b) = 1$, jos ja vain jos on olemassa $m, n \in \mathbb{N}$ siten, että

$$1 = am + bn.$$

Todistus. [2], s.33. □

Lemma 3.7. *Jos $a, b, c \in N$, $syt(a, b) = 1$ ja $a \mid bc$, niin $a \mid c$.*

Todistus. [12], s.113. □

Lemma 3.8. *Olkoon $syt(a, b) = 1$. Jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$.*

Todistus. Koska $a \mid c$, niin voidaan kirjoittaa $c = ak$ jollekin $k \in \mathbb{Z}$. Nyt $b \mid ak$, joten Lemman 3.7 nojalla $b \mid k$, ja edelleen $ab \mid c$. □

Lemma 3.9. *Olkoon $a, b \in \mathbb{Z}$ ja $syt(a, b) = d$. Jos $d \nmid c$, niin yhtälöllä $ax + by = c$ ei ole kokonaislukuratkaisua. Jos taas $d \mid c$, niin yhtälöllä on äärettömästi kokonaislukuratkaisuja.*

Todistus. [12], s.137-138. □

Seuraavaksi siirrytään modulaariaritmetiikan tutkimiseen.

Määritelmä 3.10. Olkoon $m \in \mathbb{N}$ ja $a, b \in \mathbb{Z}$. Jos $m \mid (a - b)$, niin sanotaan että luku a on *kongruentti* luvun b kanssa *modulo* m. Tästä käytetään merkintää

$$a \equiv b \ (mod\ m).$$

Kongruenssi *mod* m hajottaa kokonaislukujen joukon $\mathbb{Z}$ muotoa

$$[a] = \{a + mk \mid k \in \mathbb{Z}\}.$$

oleviin pistevieraisiin joukkoihin. Joukkoa $[a]$ kutsutaan luvun a *jäännösluokaksi modulo* m, josta käytetään merkintää $[a]_m$. Jäännösluokkaan kuuluvat kaikki luvut, jotka antavat saman jäännöksen jaettaessa luvulla m. Käymällä läpi kaikki luvun m jäännökset saamme muodostettua luvun m jäännösluokkien edustajiston, jota merkitään joukolla

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m - 1]\}.$$

Määritellään jäännösluokkien yhteen- ja kertolasku seuraavasti

$$[a]_m + [b]_m = [a + b]_m, \quad [a]_m \cdot [b]_m = [ab]_m.$$

Lemma 3.11. *Olkoon $a, b, m \in \mathbb{Z}$ ja $m > 0$. Tällöin $a \equiv b \ (mod\ m)$, jos ja vain jos $[a]_m = [b]_m$.*

Todistus. [4], s.28. □

Osoitetaan esimerkeillä, että yhteen- ja kertolaskut ovat hyvin määriteltyjä. Toisin sanoen havainnollistetaan, että niiden tulokset eivät riipu jäännösluokan edustajasta.

Esimerkki 3.12. Jäännösluokkien *mod* 9 joukossa Lemman 3.11 nojalla $[7]_9 = [88]_9$ ja $[3]_9 = [48]_9$. Näin ollen $[10]_9 = [7]_9 + [3]_9 = [88]_9 + [48]_9 = [136]_9$ Lemman 3.11 nojalla $(136 = 14 \cdot 9 + 10)$.

Esimerkki 3.13. Jäännösluokkien *mod* 5 joukossa $[4]_5 = [9]_5$ Lemman 3.11 nojalla. Näin ollen $[12]_5 = [4]_5[3]_5 = [9]_5[3]_5 = [9 \cdot 3]_5 = [27]_5 = [2]_5$ Lemman 3.11 nojalla.

Kongruenssille on voimassa seuraavat laskusäännöt:

Lemma 3.14. *Olkoon a, b, c, d ja $m \in \mathbb{Z}$, ja $m > 0$, siten että $a \equiv b \ (mod\ m)$ ja $c \equiv d \ (mod\ m)$. Tällöin*

1. $a + c \equiv b + d \ (mod\ m)$,
2. $ab \equiv cd \ (mod\ m)$.

Todistus. [12], s.148. □

Lemma 3.15. *Jos a, b, c ja $m \in \mathbb{Z}$, $m > 0$, $d = syt(c, m)$, ja $ac \equiv bc \ (mod\ m)$. Tällöin $a \equiv b \ (mod\ m/d)$.*

Todistus. [12], s.149. □

Yhden muuttujan lineaariseksi kongruenssiksi kutsutaan kongruenssia, joka on muotoa

$$ax \equiv b \ (mod\ m),$$

missä x on tuntematon kokonaisluku.

Lause 3.16. *Olkoon $a, b, m \in \mathbb{Z}$, $m > 0$ ja $syt(a, m) = 1$. Tällöin lineaarisella kongruenssilla $ax \equiv b \ (mod\ m)$ on yksikäsitteinen ratkaisu.*

Todistus. Kongruenssin määritelmän nojalla $ax \equiv b \ (mod\ m)$, jos ja vain jos $m \mid (ax - b)$. Näin ollen luku x on kongruenssin ratkaisu, jos on olemassa kokonaisluku y, joka toteuttaa yhtälön $ax - my = b$. Lemman 3.9 nojalla yhtälöllä $ax - my = b$ on ratkaisu x, y.
Yksikäsitteisyyden todistamiseksi oletetaan, että x_1 ja x_2 toteuttavat kongruenssit

$$ax_1 \equiv b \ (mod\ m) \quad \text{ja} \quad ax_2 \equiv b \ (mod\ m).$$

Koska kongruenssi on ekvivalenssirelaatio ([12], s.146.), niin symmetrisyyden ja transitiivisuuden nojalla

$$ax_1 \equiv ax_2 \ (mod\ m).$$

Näin ollen Lemman 3.15 nojalla $x_1 \equiv x_2 \ (mod\, m)$, joten lineaarisen kongruenssin $ax \equiv b \ (mod\ m)$ ratkaisu on yksikäsitteinen. □

Tutkitaan seuraavaksi millaisia ryhmiä jäännösluokkien joukot muodostavat. Jäännösluokan *mod* m muodostama joukko $\mathbb{Z}_m$, muodostaa Abelin ryhmän

yhteenlaskun suhteen. On helppo todeta, että yhteenlasku on suljettu jäännösluokissa. Jäännösluokka $[0]_m$ on selvästi neutraalialkio ja kaikilla alkioilla on käänteisalkio. Lisäksi yhteenlasku on selvästi vaihdannainen. Kertolaskun suhteen $\mathbb{Z}_m$ ei muodosta ryhmää, sillä esimerkiksi alkiolla $[0]_m$ ei ole käänteisalkiota, sillä $[1]_m$ on neutraalialkio kertolaskun suhteen. Valitsemalla jäännösluokat sopivasti, saadaan muodostettua jäännösluokkaryhmä kertolaskun suhteen.

Lemma 3.17. *Jäännösluokkien joukko $\mathbb{Z}_m^*$ muodostaa Abelin ryhmän kertolaskun suhteen, kun*

$$\mathbb{Z}_m^* = \{[a] \in \mathbb{Z}_m \mid syt(a, m) = 1\}.$$

Todistus. Olkoon $[a], [b] \in \mathbb{Z}_m^*$. Nyt Lemman 3.6 (2) nojalla on olemassa $k, l, s, t \in \mathbb{Z}$ siten, että

$$ka + lm = 1 \quad \text{ja} \quad sb + tm = 1.$$

Tällöin

$$\begin{aligned} 1 = 1 \cdot 1 = (ka + lm)(sb + tm) &= kasb + katm + lmsb + ltm^2 \\ &= (ks)ab + (kat + lsb + ltm)m, \end{aligned}$$

joten Lemman 3.6 (2) nojalla $syt(ab, m) = 1$ ja edelleen $[ab] \in \mathbb{Z}_m^*$. Näin ollen $\mathbb{Z}_m^*$ on suljettu kertolaskun suhteen. Neutraalialkio on selvästi $[1]_m$. Toisaalta

$$[a]_m([b]_m[c]_m) = [abc]_m = ([a]_m[b]_m)[c]_m,$$

joten kertolasku on liitännäinen. Lauseen 3.16 nojalla kongruenssilla $ax \equiv 1 (mod\ m)$ on olemassa ratkaisu, ja siten Lemman 3.11 nojalla $[ax]_m = [a]_m[x]_m = [1]_m$, joten alkion $[a]_m$ käänteisalkio on jäännösluokka $[x]_m$. Näin ollen $\mathbb{Z}_m^*$ on ryhmä kertolaskun suhteen. Lisäksi

$$[a]_m[b]_m = [a \cdot b]_m = [b \cdot a]_m = [b]_m[a]_m,$$

joten $\mathbb{Z}_m^*$ on Abelin ryhmä kertolaskun suhteen. □

Jäännösluokkien joukkoa $\mathbb{Z}_m^*$ kutsutaan *vähennetyksi jäännösluokkien joukoksi mod m*.

Esimerkki 3.18. Lemman 3.17 nojalla vähennetty jäännösluokkien joukko $\mathbb{Z}_9^*$ muodostaa Abelin ryhmän kertolaskun suhteen, kun

$$\mathbb{Z}_9^* = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}.$$

Vähennettyjen jäännösluokkien joukkojen muodostamien ryhmien kertaluvut voidaan selvittää Eulerin funktiolla.

Määritelmä 3.19. *Eulerin funktioksi* kutsutaan kuvausta $\phi : \mathbb{Z}_+ \to \mathbb{Z}_+$, jolle $\phi(m) = n$, missä n on lukujen k, $1 \leq k < m$, määrä joille on voimassa $syt(k, m) = 1$.

Esimerkki 3.20. $\phi(15) = 8$, sillä luvuista $1, 2, \ldots, 14$ täsmälleen luvuille $1, 2, 4, 7, 8, 11, 13$ ja 14 on voimassa $syt(k, 15) = 1$.

Esimerkki 3.21. Olkoon $n = 12$. Tällöin jäännösluokkajoukon $\mathbb{Z}_{12}$ vähennetty jäännösluokkajoukko on

$$\mathbb{Z}_{12}^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\},$$

ja $|\mathbb{Z}_{12}^*| = 4 = \phi(12)$.

Huomautus 3.22. Alkuluvulle p on selvästi voimassa $\phi(p) = p - 1$.

Lause 3.23 (Eulerin lause)**.** *Olkoon $m \in \mathbb{Z}_+$ ja $a \in \mathbb{Z}$ siten, että $syt(a, m) = 1$. Tällöin*

$$a^{\phi(m)} \equiv 1 \ (mod\ m).$$

Eulerin lauseen todistaminen jätetään lukuun 4, katso Huomautus 4.34.

Lause 3.24. *Olkoon $n, m \in \mathbb{Z}_+$ ja $syt(n, m) = 1$. Tällöin kuvaus $f : [a]_{nm} \to ([a]_n, [a]_m)$ on hyvin määritelty isomorfismi joukolta $\mathbb{Z}_{nm}$ joukolle $\mathbb{Z}_n \oplus \mathbb{Z}_m$.*

Todistus. Oletetaan, että $[a]_{nm} = [b]_{nm}$. Tällöin Lemman 3.11 nojalla b on muotoa $a + mnt$. Koska $[nm]_n = [0]_n$ ja $[nm]_m = [0]_m$, niin tällöin

$$([b]_n, [b]_m) = ([a + mnt]_n, [a + mnt]_m) = ([a]_m, [a]_n).$$

Nyt kuvaus f ei riipu jäännösluokan edustajasta ja on siten hyvin määritelty. Kuvaus f on homomorfismi, sillä

$$f([a+b]_{nm}) = ([a+b]_n, [a+b]_m) = ([a]_n+[b]_n, [a]_m+[b]_m) = f([a]_{nm})+f([b]_{nm}).$$

Oletetaan, että $f([a]_{nm}) = f([b]_{nm})$, eli $([a]_n, [a]_m) = ([b]_n, [b]_m)$. Nyt Lemman 3.11 nojalla $a \equiv b \ (mod\ n)$ ja $a \equiv b \ (mod\ m)$, ja siten $(a-b)$ on jaollinen molemmilla luvuilla n sekä m. Koska $syt(n, m) = 1$, niin Lemman 3.8 nojalla $nm \mid (a - b)$. Tästä saadaan, että $[a]_{nm} = [b]_{nm}$, ja f on siten injektio. Lopuksi kuvaus f on selvästi surjektio, ja siten se on myös bijektio, ja edelleen f on isomorfismi. □

4 Tärkeitä ryhmiä

Tässä luvussa tutustutaan syklisiin ja normaaleihin aliryhmiin sekä tekijäryhmiin. Luvussa keskitytään tarkastelemaan näiden ryhmien keskeisimpiä ominaisuuksia tämän tutkielman kannalta. Yksinkertaisimmat tulokset jätetään todistamatta.

4.1 Sykliset ryhmät

Syklisten ryhmien tutkiminen alkaa ryhmän alkioiden potenssien määrittelyllä, sekä perustulosten esittelyllä.

Määritelmä 4.1. Olkoon G ryhmä ja $a \in G$. Määritellään ryhmän G *potenssit* asettamalla

(1) $a^0 = e$,

(2) $a^{n+1} = a^n \circ a$, kaikilla $n \geq 1$,

(3) $a^{-n} = (a^n)^{-1}$ kaikilla $n > 0$.

Lemma 4.2. *Olkoon G ryhmä ja $a \in G$, sekä $n, m \in \mathbb{Z}$. Tällöin*

(1) $a^n \circ a^m = a^{n+m}$,

(2) $(a^n)^m = a^{nm}$,

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

Todistus. [10], s.46. □

Huomautus 4.3. Olkoon G Abelin ryhmä ja $a, b \in G$. Tällöin kaikilla $n \in \mathbb{N}$

$$(ab)^n = a^n b^n.$$

Todistetaan väite induktiolla. Kun $n = 1$, niin $(ab) = ab$, joten väite pätee. Oletetaan, että väite pätee jollakin $n \in \mathbb{N}$. Näin ollen

$$(ab)^{n+1} = (ab)^n(ab) = a^n b^n ab = a^n ab^n b = a^{n+1} b^{n+1},$$

joten väite pätee induktio todistuksen nojalla.

Lemma 4.4. *Olkoon G ryhmä ja $a, b \in G$. Tällöin*

(1) $(ab)^{-1} = b^{-1}a^{-1}$;

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

Todistus. [4], s.197. □

Lemma 4.5. *Olkoon G ryhmä ja olkoon $g \in G$. Tällöin joukko*

$$\langle a \rangle = \{a^i | i \in \mathbb{Z}\}$$

ja ryhmän G laskutoimitus muodostavat ryhmän G aliryhmän.

Todistus. [6], s.89. □

Ryhmää $\langle a \rangle$ kutsutaan alkion a virittämäksi aliryhmäksi.

Määritelmä 4.6. Ryhmää G kutsutaan *sykliseksi ryhmäksi*, mikäli on olemassa alkio $a \in G$ siten, että alkion a virittämä syklinen aliryhmä $\langle a \rangle$ on koko ryhmä G; toisin sanoen

$$G = \{a^n | n \in \mathbb{Z}\}.$$

Alkiota a kutsutaan ryhmän G *virittäjäksi*.

Määritelmä 4.7. Olkoon G ryhmä ja $a \in G$.

(1) Jos $a^n \neq e$ kaikilla $n \geq 1$, sanotaan, että ryhmän G *kertaluku* on ääretön ja merkitään $|a| = \infty$.

(2) Jos (1) ei päde, niin pienintä kokonaislukua $n \geq 1$, jolle $a^n = e$, sanotaan alkion a kertaluvuksi. Merkitään $|a| = n$.

Lause 4.8. *Olkoon G ryhmä ja $a \in G$.*

(1) Jos alkion a kertaluku on ääretön, niin $a^i \neq a^j$ kaikilla $i, j \in \mathbb{Z}, i \neq j$.

(2) Jos $a^i = a^j$ joillekin $i, j \in \mathbb{Z}, i \neq j$, niin alkion a kertaluku on äärellinen.

Todistus. [4], s.199. □

Lause 4.9. *Olkoon G ryhmä ja $a \in G$ alkio, jonka kertaluku on n. Tällöin*

(1) $a^k = e$, jos ja vain jos $n \mid k$;

(2) $a^i = a^j$, jos ja vain jos $i \equiv j \pmod{n}$;

(3) Jos $n = td$, $d \geq 1$, niin alkion a^t kertaluku on d.

Todistus. [4], s.200. □

Huomautus 4.10. Olkoon G ryhmä, ja $a \in G$. Jos $|a| = n$, niin tällöin myös $|a^{-1}| = n$ Lemman 4.2 nojalla. Nimittäin

$$(a^{-1})^n = (a^n)^{-1} = e$$

ja kaikilla $1 \leq k \leq n$ pätee $(a^{-1})^k = (a^k)^{-1} \neq e$.

Lemma 4.11. *Jos ryhmän G kaikkien alkioiden $a \neq e$ kertaluku on 2, niin ryhmä G on Abelin ryhmä.*

Todistus. Olkoon kaikkien ryhmän G alkioiden $a \neq e$ kertaluku $|a| = 2$. Tällöin $a = a^{-1}$ kaikilla $a \in G$. Olkoot $a, b \in G$. Tällöin Lemman 4.4 nojalla

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

joten G on Abelin ryhmä. □

Lemma 4.12. *Olkoon kuvaus $f : G \to H$ isomorfismi ja alkion $a \in G$ kertaluku äärellinen. Tällöin $|f(a)| = |a|$.*

Todistus. Olkoon alkion a kertaluku $|a| = n$. Tällöin Lemman 2.8 nojalla

$$f(a)^n = f(a^n) = f(e_G) = e_H,$$

joten alkion $f(a)$ kertaluku $|f(a)|$ on jokin luku k, joka jakaa luvun n. Oletetaan seuraavaksi, että $|f(a)| = m$ jollekin $m < n$. Lemman 2.8 nojalla

$$f(a^m) = f(a)^m = f(e_G).$$

Koska kuvaus f on isomorfismi ja siten injektio, niin $a^m = e_G$. Näin ollen $|a| \leq m$, mikä on ristiriita, ja siten $|f(a)| = k = |a|$. □

Lause 4.13. *Olkoon G ryhmä ja olkoon $a \in G$.*

(1) Jos alkiolla a on ääretön kertaluku, niin

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

on ääretön aliryhmä, jonka potenssit ovat erilliset, eli $a^i \neq a^j$ kaikilla $i, j \in \mathbb{Z}, i \neq j$.

(2) Jos alkion a kertaluku on äärellinen $|a| = n$, niin $\langle a \rangle$ on aliryhmä, jonka kertaluku on n ja

$$\langle a \rangle = \{e = a^0, a, a^2, \ldots, a^{n-1}\}.$$

Todistus. [4], s.207. □

Koska kaikki sykliset ryhmät koostuvat yhden alkion potensseista, niin kaikki saman kertaluvun sykliset ryhmät ovat isomorfisia.

Lause 4.14. *Olkoon G syklinen ryhmä.*

(1) Jos $|G| = \infty$, niin G on isomorfinen ryhmän $(\mathbb{Z}, +)$ kanssa.

(2) Jos $|G| = n$, niin G on isomorfinen ryhmän $(\mathbb{Z}_n, +)$ kanssa.

Todistus. Todistetaan kohta (2). Oletetaan, että $G = \langle a \rangle$ ja alkion a kertaluku on n. Nyt Lauseen 4.13 nojalla

$$G = \{a^0, a^1, \ldots, a^{n-1}\}.$$

Määritellään kuvaus $f : G \to \mathbb{Z}_n$ asettamalla $f(a^i) = [i]$. Todetaan, että f on bijektio.
Kuvaus f on surjektio: Olkoon $i \in \{0, 1, \ldots, n-1\}$. Tällöin $a^i \in G$ on alkion $[i]$ alkukuva.
Kuvaus f on injektio: Oletetaan, että $f(a^i) = [i] = [j] = f(a^j)$ joillekin $i, j \in \mathbb{Z}$. Tällöin $i \equiv j \ (mod\ n)$ Lemman 3.11 nojalla, joten Lauseen 4.9 nojalla $a^i = a^j$. Kuvaus f on siten bijektio. Lisäksi

$$f(a^i a^j) = f(a^{i+j}) = [i + j] = [i] + [j] = f(a^i) + f(a^j),$$

joten kuvaus f on isomorfismi ja siten $G \cong \mathbb{Z}_n$. □

4.2 Normaalit aliryhmät

Aloitetaan määrittelemällä ryhmien kongruenssi.

Määritelmä 4.15. Olkoon H ryhmän G aliryhmä. Määritellään joukossa G relaatio $\equiv (mod\ H)$ asettamalla

$$a \equiv b \ (mod\ H) \Leftrightarrow ab^{-1} \in H.$$

Lemma 4.16. *Olkoon H ryhmän G aliryhmä. Tällöin kaikilla $a, b, c \in G$ pätee*

(1) $a \equiv a \ (mod\ H)$;

(2) Jos $a \equiv b \ (mod\ H)$, niin $b \equiv a \ (mod\ H)$;

(3) Jos $a \equiv b \ (mod\ H)$ ja $b \equiv c \ (mod\ H)$, niin $a \equiv c \ (mod\ H)$.

Todistus. [4], s.239. □

Määritelmä 4.17. Olkoon G ryhmä, $H \subseteq G$ sen aliryhmä ja $a \in G$. Joukkoa

$$Ha := \{ha \mid h \in H\}$$

sanotaan alkion a määräämäksi *oikeanpuoleiseksi sivuluokaksi* modulo H. Vastaavasti vasemmanpuoleinen sivuluokka modulo H on joukko

$$aH := \{ah \mid h \in H\}.$$

Lemma 4.18. *Olkoon G ryhmä ja H sen aliryhmä.*

(1) Tällöin G on oikeanpuoleisten H-sivuluokkien yhdiste eli, $G = \bigcup_{a \in G} Ha$.

(2) Jokaiselle $a \in G$ on olemassa bijektio $f : H \to Ha$. Toisin sanoen jos H on äärellinen, niin mitkä tahansa kaksi ryhmän H oikeanpuoleista sivuluokkaa sisältävät yhtä monta alkiota.

Todistus. (1) Koska kaikki oikeanpuoleiset sivuluokat sisältävät ryhmän G alkioita, on voimassa $\bigcup_{a \in G} Ha \subseteq G$. Jos $b \in G$, niin $b = eb \in Hb \subseteq \bigcup_{a \in G} Ha$. Näin ollen, $G = \bigcup_{a \in G} Ha$.

(2) Määritellään kuvaus $f : H \to Ha$ asettamalla $f(x) = xa$. Nyt sivuluokan Ha määritelmän mukaan f on surjektio. Jos $f(x) = f(y)$, niin $xa = ya$, joten $x = y$ Lemman 2.3 nojalla. Tällöin kuvaus f on injektio ja siten bijektio. Näin ollen jos H on äärellinen, niin jokaisella sivuluokalla Ha on yhtä monta alkioita kuin aliryhmällä H. □

Lemma 4.19. *Olkoon H ryhmän G aliryhmä ja $a, c \in G$. Tällöin $Ha = Hc$, jos ja vain jos $a \equiv c \pmod{H}$.*

Todistus. Oletetaan ensin, että $a \equiv c \pmod{H}$. Olkoon $b \in Ha$. Nyt määritelmän mukaan $b = ha$ jollekin $h \in H$, joten $ba^{-1} = haa^{-1} = h \in H$. Nyt $b \equiv a \pmod{H}$, ja Lemman 4.16 (3) nojalla $b \equiv c \pmod{H}$. Tällöin $bc^{-1} = h' \in H$, joten $b = h'c \in Hc$. Siten $Ha \subset Hc$. Vastaavasti voidaan osoittaa, että $Hc \subset Ha$ ja siten $Ha = Hc$.
Oletetaan seuraavaksi, että $Ha = Hc$. Koska $a = ae \in Ha = Hc$, niin $a = hc$ jollekin $h \in H$. Näin ollen $ac^{-1} = hcc^{-1} = h \in H$ eli $a \equiv c \pmod{H}$. □

Lause 4.20. *Olkoon H ryhmän G aliryhmä. Kaksi oikeanpuoleista H-sivuluokkaa ovat joko samat tai pistevieraat.*

Todistus. Olkoon $Ha \cap Hc$ epätyhjä. Nyt on olemassa alkio b siten, että $b \in Ha$ ja $b \in Hc$. Vastaavasti, kuin Lemman 4.19 todistuksessa, saadaan

$$b \equiv a \ (mod\ H) \text{ ja } b \equiv c \ (mod\ H),$$

ja edelleen Lemman 4.16 (3) nojalla $a \equiv c \ (mod\ H)$. Nyt Lemman 4.19 nojalla $Ha = Hc$. □

Määritelmä 4.21. Jos H on ryhmän G aliryhmä, niin eriävien sivuluokkien määrää kutsutaan aliryhmän H *indeksiksi* ryhmässä G. Olkoon luku n aliryhmän H indeksi ryhmässä G. Tällöin käytetään merkintää $[G : H] = n$.

Määritelmä 4.22. Ryhmän G aliryhmää H sanotaan *normaali aliryhmäksi*, jos kaikkien ryhmän G alkioiden määräämät oikean- ja vasemmanpuoleiset sivuluokat ovat samoja. Toisin sanoen

$$Ha = aH$$

kaikilla $a \in G$.

Lemma 4.23. *Olkoon G ja H ryhmiä joiden välinen kuvaus $f : G \to H$ on homomorfismi, jonka ydin on $\ker f$. Tällöin ydin $\ker f$ on ryhmän G normaali aliryhmä.*

Todistus. [4], s.264. □

Lause 4.24. *Olkoon H ryhmän G aliryhmä, jonka indeksi on 2. Tällöin H on normaali aliryhmä.*

Todistus. Koska aliryhmän H indeksi on 2, niin ryhmän G oikeanpuoleiset sivuluokat ovat H ja Hg jollekin $g \in G$. Vastaavasti vasemmanpuoleiset sivuluokat ovat H ja aH jollekin $a \in G$. Koska $[G : H] = 2$, niin saadaan $\{H, Hg\} = \{H, aH\}$. Koska $H \neq Hg, aH$, niin on oltava, että $Hg = aH$. Huomataan myös, että Ha on ryhmän G oikeanpuoleinen sivuluokka. Koska ryhmällä H on vain kaksi erillistä sivuluokkaa ja $a \notin H$, niin $Ha = Hg$, ja siten

$$Ha = aH.$$

□

Lemma 4.25. *Ryhmän G aliryhmän H seuraavat ominaisuudet ovat ekvivalentteja:*

(1) H on ryhmän G normaali aliryhmä,

(2) $a^{-1}Ha \subset H$ *kaikilla* $a \in G$*, missä* $a^{-1}Ha = \{a^{-1}ha | h \in H\}$,

(3) $aHa^{-1} \subset H$ *kaikilla* $a \in G$*, missä* $aHa^{-1} = \{aha^{-1} | h \in H\}$,

(4) $a^{-1}Ha = H$ *kaikilla* $a \in G$,

(5) $aHa^{-1} = H$ *kaikilla* $a \in G$.

Todistus. [4], s.251. □

Lemma 4.26. *Olkoon* N *ja* M *ryhmän* G *normaaleja aliryhmiä siten, että* $N \cap M = \langle e \rangle$*. Jos* $a \in M$ *ja* $b \in N$*, niin* $ab = ba$.

Todistus. Olkoot $a \in M$ ja $b \in N$. Tarkastellaan alkiota $a^{-1}b^{-1}ab$. Koska M on normaali aliryhmä, niin Lemman 4.25 (2) nojalla $b^{-1}ab \in M$. Koska M on suljettu laskutoimituksen suhteen tiedetään, että

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

Vastaavasti koska ryhmä N on normaali aliryhmä, niin $a^{-1}b^{-1}a \in N$ ja koska $b \in N$ saadaan

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

Näin ollen

$$a^{-1}b^{-1}ab \in M \cap N = \langle e \rangle .$$

Operoimalla puolittain vasemmalta alkiolla ba saadaan $ab = ba$. □

4.3 Tekijäryhmät

Lause 4.27. *Olkoon* N *ryhmän* G *normaali aliryhmä. Määritellään joukossa* G/N *laskutoimitus* $(Na)(Nc) = Nac$ *kaikilla* $a, c \in G$.

(1) Tällöin G/N *on ryhmä.*

(2) Jos G *on äärellinen ryhmä, niin ryhmän* G/N *kertaluku on* $|G|/|N|$.

(3) Jos G *on Abelin ryhmä, niin myös* G/N *on Abelin ryhmä.*

Todistus. (1) Koska $(Na)(Ne) = Na$ ja $(Ne)(Na) = Na$, niin sivuluokka Ne on neutraalialkio. Koska

$$(Na)(Na^{-1}) = Naa^{-1} = Ne = Na^{-1}a = Na^{-1}Na,$$

niin sivuluokan Na käänteisalkio on sivuluokka Na^{-1}. Koska

$$[(Na)(Nb)](Nc) = (Nab)(Nc) = Nabc = (Na)(Nbc) = (Na)[(Nb)(Nc)],$$

niin laskutoimitus on liitännäinen ja näin ollen N/G on ryhmä.
(2) ja (3) [4], s.256. □

Lemma 4.28. *Olkoon H ryhmän G normaali aliryhmä ja $a \in G$. Tällöin $(Ha)^n = Ha^n$ kaikilla $n \in \mathbb{Z}$.*

Todistus. Todistetaan väite induktiolla. Tapaus $n = 0$ on selvä, sillä nollapotenssin määritelmän ja Lauseen 4.27 nojalla $(Ha)^0 = He = Ha^0$. Oletetaan seuraavaksi, että väite $(Ha)^n = Ha^n$ pätee jollekin $n \in \mathbb{Z}_+$. Nyt

$$(Ha)^{n+1} = (Ha)^n(Ha) = (Ha^n)(Ha) = Ha^n a = Ha^{n+1},$$

joten väite pätee induktiotodistuksen nojalla kaikilla $n \geq 0$.
Lopuksi jos $n < 0$, niin $-n > 0$, joten potenssien määritelmän ja Lauseen 4.27 nojalla

$$(Ha)^n = ((Ha)^{-1})^{-n} = (Ha^{-1})^{-n} = H(a^{-1})^{-n} = Ha^n.$$

□

Määritelmä 4.29. Olkoon G ryhmä ja N sen normaali aliryhmä. Tällöin ryhmä G/N tarkoittaa ryhmän G *tekijäryhmää*. Ryhmä G/N muodostuu ryhmän G kaikkien oikeanpuoleisten sivuluokkien yhdisteestä.

Lause 4.30. *Olkoon N ryhmän G normaali aliryhmä. Jos K on ryhmän G/N mikä tahansa aliryhmä, niin $K = H/N$, missä H on ryhmän G aliryhmä, joka sisältää ryhmän N.*

Todistus. [4], s.268. □

Lause 4.31 (Lagrangen lause)**.** *Jos K on äärellisen ryhmän G aliryhmä, niin $|G| = |K|[G : H]$. Erityisesti ryhmän K kertaluku jakaa ryhmän G kertaluvun.*

Todistus. Jos A ja B ovat erillisiä äärellisiä joukkoja, niin $|A \cup B| = |A| + |B|$. Oletetaan, että ryhmän G oikeanpuoleisten K-sivuluokkien lukumäärä on n ja merkitään näitä erillisinä sivuluokkina $Kc_1, Kc_2, \ldots, Kc_n$. Tällöin

$$G = Kc_1 \cup Kc_2 \cup \cdots \cup Kc_n.$$

Koska Lauseen 4.20 nojalla sivuluokat ovat erillisiä, niin

$$|G| = |Kc_1| + |Kc_2| + \cdots + |Kc_n|.$$

Jokaiselle c_i on kuitenkin voimassa $|Kc_i| = |K|$ Lemman 4.18 nojalla. Näin ollen

$$|G| = \underbrace{|K| + |K| + \cdots + |K|}_{\text{n kpl}} = |K|n = |K|[G : K].$$

□

Lemma 4.32. *Olkoon G äärellinen ryhmä, jolle $|G| = k$.*

(1) Jos $a \in G$, niin alkion a kertaluku jakaa ryhmän G kertaluvun.

(2) Tällöin $a^k = e$ kaikilla $a \in G$.

Todistus. (1) Jos alkion $a \in G$ kertaluku on n, niin Lauseen 4.13 nojalla syklisen aliryhmän $\langle a \rangle$ kertaluku on n. Lauseen 4.31 nojalla n jakaa ryhmän G kertaluvun k.
(2) Jos alkion $a \in G$ kertaluku on n, niin tällöin kohdan (1) nojalla $n \mid k$, olkoon $k = nt$. Nyt $a^k = a^{nt} = (a^n)^t = e^t = e$. □

Huomautus 4.33. Lause 3.23, eli Eulerin lause saadaan Lemman 4.32 sivutuotteena seuraavasti:
Ryhmässä $\mathbb{Z}_m^*$ on $\phi(m)$ alkiota, joten $|\mathbb{Z}_m^*| = \phi(m)$. Olkoon $[a] \in \mathbb{Z}_m$ siten, että $syt(a, m) = 1$. Tällöin $[a] \in \mathbb{Z}_m^*$ ja nyt Lemman 4.32 kohdan (2) nojalla $[a^{\phi(m)}] = [1]$. Siten $[a^{\phi(m)}]_m = [1]_m$, joten Lemman 3.11 nojalla $a^{\phi(m)} \equiv 1 \ (mod\ m)$.

Huomautus 4.34. Lemman 3.17 seurauksena joukko $\mathbb{Z}_p \setminus [0]$, missä p on alkuluku, muodostaa aina hyvin määritellyn syklisen Abelin ryhmän, jonka kertaluku $|\mathbb{Z}_p| = \phi(p) = p - 1$, kertolaskun suhteen.

Lemma 4.35. *Olkoot H ja K kaksi erillistä äärellisen ryhmän G aliryhmää ja olkoon ryhmän H kertaluku jokin alkuluku p. Tällöin*

$$H \cap K = \langle e \rangle .$$

Todistus. Ryhmien H ja K muodostaman leikkauksen $H \cap K$ täytyy olla molempien ryhmien aliryhmä. Lagrangen lauseen nojalla $|H \cap K| \mid |H|$, joten $|H \cap K| = p$ tai 1. Koska ryhmät ovat eriävät, niin $H \cap K \neq H$, ja siten $H \cap K$ on joukon H aito osajoukko. Näin ollen $|H \cap K| < |H|$, joten $|H \cap K| = 1$, ja edelleen $H \cap K = \langle e \rangle$.

□

Lemma 4.36. *Jos ryhmän G aliryhmille H ja K pätee $H \cap K = \langle e \rangle$, niin tällöin $|HK| = |H||K|$, missä*

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

Todistus. Olkoot $h_1, h_2 \in H$ ja $k_1, k_2 \in K$ siten, että $h_1k_1 = h_2k_2$. Nyt operoimalla alkioilla h_1^{-1} ja k_2^{-1} saadaan

$$h_1^{-1}h_1k_1k_2^{-1} = h_1^{-1}h_2k_2k_2^{-1},$$

mistä saadaan $k_1k_2^{-1} = h_1^{-1}h_2$. Oletuksen nojalla kuitenkin $H \cap K = \langle e \rangle$, joten $k_1k_2^{-1} = e = h_1^{-1}h_2$. Edelleen saadaan, että $h_1 = h_2$ ja $k_1 = k_2$. Ryhmän HK jokainen alkio voidaan näin ollen kirjoittaa yksikäsitteisesti muodossa hk ja siten $|HK| = |H||K|$. □

5 Äärellisten Abelin ryhmien ominaisuuksia

Tässä luvussa perehdytään äärellisiin Abelin ryhmiin sekä niiden ominaisuuksiin. Tässä luvussa Abelin ryhmille käytetään laskutoimitusta + ja neutraalialkiota 0. Luvun tärkein tulos on Lause 5.11, jonka avulla kaikki äärelliset Abelin ryhmät voidaan luokitella isomorfian mukaisesti.

Lause 5.1. *Olkoot $N_1, N_2, \ldots, N_k$ Abelin ryhmän $(G, +)$ normaaleja aliryhmiä siten, että ryhmän G jokainen alkio voidaan kirjoittaa yksikäsitteisesti muodossa $a_1 + a_2 + \cdots + a_k$, kun $a_i \in N_i$. Tällöin G on isomorfinen suoran summan $N_1 \oplus N_2 \oplus \cdots \oplus N_k$ kanssa.*

Todistus. [4], s.283. Määritellään kuvaus $f : N_1 \oplus N_2 \oplus \cdots \oplus N_k \to G$ asettamalla

$$f(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k.$$

Koska jokainen ryhmän G alkio voidaan kirjoittaa muodossa $a_1+a_2+\cdots+a_k$, niin oletuksen nojalla f on surjektiivinen.
Jos $f(a_1, a_2, \ldots, a_k) = f(b_1, b_2, \ldots, b_k)$, niin $a_1+a_2+\cdots+a_k = b_1+b_2+\cdots+b_k$. Yksikäsitteisyyden nojalla $a_i = b_i$ jokaisella i $(1 \leq i \leq k)$. Näin ollen

$$(a_1, a_2, \ldots, a_k) = (b_1, b_2, \ldots, b_k) \in N_1 \oplus N_2 \oplus \cdots \oplus N_k,$$

ja f on injektiivinen.
Osoittaaksemme, että f on homomorfismi täytyy ensin osoittaa, että $N_i \cap N_j = \langle 0 \rangle$ kun $i \neq j$. Jos $a \in N_i \cap N_j$, niin a voidaan kirjoittaa kahtena eri tulona

$$\begin{array}{ccccccccccccccccc}
0 & + \cdots + & a & + \cdots + & 0 & + \cdots + & 0 & = a = & 0 & + \cdots + & 0 & + \cdots + & a & + \ldots + & 0 \\
\uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\
N_1 & & N_i & & N_j & & N_k & & N_1 & & N_i & & N_j & & N_k.
\end{array}$$

Yksikäsitteisyydestä seuraa, että aliryhmän N_i alkioiden täytyy olla samat, joten $a = 0$. Näin ollen, $N_i \cap N_j = \langle 0 \rangle$, kun $i \neq j$. Lemman 4.26 nojalla $a_i + b_j = b_j + a_i$ kaikille $a_i \in N_i$ ja $b_j \in N_j$, joten

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

Jatkamalla tätä operointia saamme siirrettyä kaikki alkiot $a_4, \ldots, a_k$ vasemmalle kunnes saamme

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

Näin ollen f on homomorfismi ja siten myös isomorfismi. □

Lause 5.2. *Olkoot N ja M ovat ryhmän $(G, +)$ normaaleja aliryhmiä siten, että $G = N + M$ ja $N \cap M = \langle e \rangle$. Tällöin $G \cong N \oplus M$.*

Todistus. [4], s.285. Oletuksen nojalla ryhmän G jokainen alkio voidaan kirjoittaa muodossa $n + m$, missä $n \in N$ ja $m \in M$. Oletetaan, että ryhmän G alkiolla $n + m$ on toinen esitystapa $n' + m'$, missä $n' \in N$ ja $m' \in M$. Lisäämällä yhtälöön

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

puolittain vasemmalta $-n'$ ja oikealta $-m$ saadaan

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

joten

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

Koska $-n' + n \in N$ ja $m' - m \in M$ ja $N \cap M = \langle 0 \rangle$, niin

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

Tällöin välttämättä $n = n'$ ja $m = m'$, eli jokainen ryhmän G alkio voidaan kirjoittaa yksikäsitteisesti muodossa $n + m$. Koska N ja M ovat ryhmän G normaaleja aliryhmiä, niin Lauseen 5.1 nojalla $G \cong N \oplus M$. □

Määritelmä 5.3. Jos G on Abelin ryhmä ja p on alkuluku, niin merkintä $G(p)$ tarkoittaa ryhmän G alkioiden joukkoa, joiden kertaluku on jokin luvun p potenssi. Toisin sanoen

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

Huomautus 5.4. Ryhmän $(G, \circ)$ alkioiden potenssit määriteltiin seuraavasti

$$a^n = \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ kpl}}.$$

Ryhmän $(G, +)$ potensseille käytetään seuraavaa monikertamerkintää

$$na = \underbrace{a + a + \cdots + a}_{n \text{ kpl}}.$$

Monikerta esityksellä Lemman 4.2 yhtälöt ovat seuraavat:

(1) $na + ma = (n + m)a$,

(2) $(na)m = nam$

(3) $(na)^{-1} = n(a^{-1}) = n \cdot (-a) = -na$.

Lemma 5.5. *Jos $(G, +)$ on Abelin ryhmä ja p on alkuluku, niin tällöin $G(p)$ on ryhmän G aliryhmä.*

Todistus. Joukko $G(p)$ on epätyhjä, sillä $|0| = p^0 \in G(p)$.
Olkoot $a, b \in G(p)$. Tällöin $|a| = p^n$ ja $|b| = p^m$ joillekin $n, m \geq 0$. Huomautuksen 4.10 nojalla $|-a| = |a| = p^n$, joten $-a \in G(p)$. Koska $G(p)$ on määrittelynsä nojalla vaihdannainen ja $p^n a = 0 = p^m b$, niin Lemman 4.2 ja Huomautuksen 4.3 nojalla saadaan

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

Näin ollen Lauseen 4.9 (1) nojalla $|a + b|$ jakaa luvun p^{n+m}. Alkio $|a + b|$ on siten luvun p ei negatiivinen potenssi ja siten $a + b \in G(p)$. □

Lause 5.6. *Olkoon G Abelin ryhmä ja alkion $a \in G$ kertaluku äärellinen. Tällöin*

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

kun $a_i \in G(p_i)$, missä $p_1, \ldots, p_t$ ovat ne erilliset alkuluvut, jotka jakavat alkion a kertaluvun.

Todistus. [4], s.290. Todistetaan väite induktiolla alkutekijöiden määrän suhteen. Jos $|a|$ on jaollinen vain ja ainoastaan alkuluvulla p_1, niin tällöin alkion a kertaluku on luvun p_1 potenssi, ja siten $a \in G(p_1)$. Näin ollen väite pätee, jos kertaluvulla $|a|$ on vain yksi alkutekijä p_1. Oletetaan induktiivisesti, että väite pätee kaikille alkioille, joiden kertaluku on jaollinen korkeintaan $k-1$ kappaleella eri alkulukuja ja oletetaan, että $|a|$ on jaollinen eri alkuluvuilla $p_1, \ldots, p_k$. Tällöin $|a| = p_1^{r_1} \cdots p_k^{r_k}$, missä $r_i > 0$. Olkoon $m = p_2^{r_2} \cdots p_k^{r_k}$ ja $n = p_1^{r_1}$, joten $|a| = mn$. Tällöin $\text{syt}(m, n) = 1$ ja Lemman 3.6 nojalla on olemassa luvut $u, v \in \mathbb{Z}$ siten, että $1 = mu + nv$. Tästä ja Lemmasta 4.2 seuraa, että

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

Mutta $mua \in G(p_1)$, koska alkion a kertaluku on mn ja siten

$$p_1^{r_1}(mua) = (nm)ua = u(mna) = u0 = 0.$$

Vastaavasti $m(nva) = 0$. Nyt Lauseen 4.9 nojalla alkion nva kertaluku jakaa luvun m. Koska luvulla m on $k-1$ kappaletta eriäviä alkulukutekijöitä, niin induktio-oletuksesta seuraa, että $nva = a_2 + a_3 + \cdots + a_k$, missä $a_i \in G(p_i)$. Merkitään $a_1 = mua$, tällöin

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

kun $a_i \in G(p_i)$. Näin ollen väite pätee induktio-oletuksen nojalla. □

Lause 5.7. *Jos $(G, +)$ on äärellinen Abelin ryhmä, niin*

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

missä $p_1, p_2, \ldots, p_t$ ovat erilliset alkuluvut, jotka jakavat ryhmän G kertaluvun.

Todistus. [4], s.291. Jos $a \in G$, niin Lemman 4.32 nojalla sen kertaluku jakaa ryhmän G kertaluvun. Näin ollen Lauseen 5.6 nojalla $a = a_1 + \cdots + a_t$, kun $a_i \in G(p_i)$. Todistetaan, että kyseessä on yksikäsitteinen esitys. Oletetaan, että

$$a_1 + a_2 + \cdots + a_t = b_1 + b_2 + \cdots + b_t,$$

missä $a_i, b_i \in G(p_i)$. Koska G on Abelin ryhmä, niin

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

Lemman 5.5 nojalla $b_i - a_i \in G(p_i)$ kaikille i, joten alkion $b_i - a_i$ kertaluku on luvun p_i potenssi $p_i^{r_i}$. Lisäksi koska $G(p)$ on vaihdannainen, niin Huomautuksen 4.3 nojalla $n(a+b) = na + nb$. Jos $m = p_2^{r_2} \ldots p_t^{r_t}$, niin $m(b_i - a_i) = 0$ kaikilla $i \geq 2$, joten

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

Myöskin alkion $(a_1 - b_1)$ kertaluvun täytyy jakaa luku m Lauseen 4.9 nojalla. Mutta $a_1 - b_1 \in G(p_1)$, joten sen kertaluku on luvun p_1 potenssi. Nyt ainoa luvun p_1 potenssi, joka jakaa luvun $m = p_2^{r_2} \dots p_t^{r_t}$ on $p_1^0 = 1$. Näin ollen $a_1 - b_1 = 0$ ja siten $a_1 = b_1$. Vastaavat argumentit osoittavat kaikille $i = 2, \dots, t$, että $a_i = b_i$. Näin ollen jokainen ryhmän G alkio voidaan kirjoittaa yksikäsitteisesti muodossa $a_1 + a_2 + \dots + a_t$, missä $a_i \in G(p_i)$ ja siten Lauseen 5.1 nojalla

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

□

Määritelmä 5.8. Jos p on alkuluku, niin ryhmää G, jonka jokaisen alkion kertaluku on jokin luvun p potenssi, kutsutaan *p-ryhmäksi*. Edelleen p-ryhmän G alkiota a sanotaan *suurimman kertaluvun alkioksi*, jos $|g| \leq |a|$ kaikilla $g \in G$.

Huomautus 5.9. Olkoon a ryhmän G suurimman kertaluvun alkio. Jos $|a| = p^n$ ja $g \in G$, niin tällöin alkiolla g on kertalukuna p^j, kun $j \leq n$. Koska $p^n = p^j p^{n-j}$, niin $p^n g = p^{n-j}(p^j g) = 0$. Näin ollen $p^n g = 0$ kaikille $g \in G$.

Lause 5.10. *Olkoon $(G, +)$ äärellinen Abelin p-ryhmä ja olkoon a ryhmän G suurimman kertaluvun alkio. Tällöin on olemassa ryhmän G aliryhmä K siten, että $G = \langle a \rangle \oplus K$.*

Todistus. [4], s.292 Olkoon H ryhmän G aliryhmä, jolle $\langle a \rangle \cap H = \langle 0 \rangle$ (ainakin $H = \langle 0 \rangle$ on tällainen). Koska G on äärellinen, niin on olemassa suurin aliryhmä K, jolle $\langle a \rangle \cap K = \langle 0 \rangle$. Lauseen 5.2 nojalla riittää osoittaa, että $G = \langle a \rangle + K$.
Oletetaan vastoin väitettä, että on olemassa $b \notin \langle a \rangle + K$. Nyt on olemassa pienin positiivinen kokonaisluku k, jolle $p^k b \in \langle a \rangle + K$, koska G on p-ryhmä, ja silloin $p^j b = 0 = 0 + 0 \in \langle a \rangle + K$ jollekin positiiviselle luvulle j.
Nyt

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

ja $pc = p^k b$ kuuluu joukkoon $\langle a \rangle + K$, olkoon

$$pc = ta + k \qquad (t \in \mathbb{Z}, k \in K). \tag{2}$$

Jos alkion a kertaluku on p^n, niin Huomautuksen 5.9 nojalla $p^n x = 0$ kaikille $x \in G$. Yhtälöstä (2) seuraa, että

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

Siten, $p^{n-1} ta = -p^{n-1} k \in \langle a \rangle \cap K = \langle 0 \rangle$ eli $p^{n-1} ta = 0$. Lauseen 4.9 nojalla p^n (alkion a kertaluku) jakaa luvun $p^{n-1} t$, joten $p \mid t$. Olkoon $t = pm$. Nyt

saadaan $pc = ta + k = pma + k$, ja edelleen $k = pc - pma = p(c - ma)$. Olkoon

$$d = c - ma. \tag{3}$$

Tällöin $pd = p(c - ma) = k \in K$, mutta $d \notin K$, koska jos $c - ma = k' \in K$, niin $c = ma + k' \in \langle a \rangle + K$. Tämä on ristiriidassa yhtälön (1) kanssa. Joukko $H = \{x + zd | x \in K,\ z \in \mathbb{Z}\}$ on epätyhjä ($0 + 0d = 0 \in H$) ja $H \subset G$. Toisaalta

$$(x_1 + z_1 d) - (x_2 + z_2 d) = (x_1 - x_2) + (z_1 - z_2)d \in H$$

kaikilla $x_1, x_2 \in K,\ z_1, z_2 \in \mathbb{Z}$, joten Lemman 2.7 nojalla H on ryhmän G aliryhmä. Lisäksi $K \subset H$ joukon H määrittelyn nojalla. Koska $d = 0 + 1d \in H$ ja $d \notin K$, H on suurempi joukko kuin K. Mutta K on laajin aliryhmä, jolle $\langle a \rangle \cap K = \langle 0 \rangle$, joten välttämättä $\langle a \rangle \cap H \neq \langle 0 \rangle$.
Olkoon $w \in \langle a \rangle \cap H$, $w \neq 0$. Tällöin

$$w = sa = k_1 + rd \qquad (k_1 \in K;\ r, s \in \mathbb{Z}). \tag{4}$$

Nyt $p \nmid r$, sillä jos $r = py$ jollakin $y \in \mathbb{Z}$, niin koska $pd \in K$, saadaan

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

mikä on ristiriita. Näin ollen $\text{syt}(p, r) = 1$ ja Lemman 3.6 nojalla voidaan muodostaa lineaarikombinaatio $pu + rv = 1,\ u, v \in \mathbb{Z}$. Nyt saadaan

$$\begin{aligned} c = 1c = (pu + rv)c &= u(pc) + v(rc) \\ &= u(ta + k) + v(r(d + ma)) \quad [(2) \text{ ja } (3)] \\ &= u(ta + k) + v(rd + rma) \\ &= u(ta + k) + v(sa - k_1 + rma) \quad [(4)] \\ &= (ut + vs + rm)a + (uk - vk_1) \in \langle a \rangle + K. \end{aligned}$$

Tämä on ristiriidassa ehdon (1) kanssa. Näin ollen, $G = \langle a \rangle + K$ ja Lauseen 5.2 nojalla $G \cong \langle a \rangle \oplus K$. □

Lause 5.11 (Äärellisten Abelin ryhmien peruslause)**.** *Olkoon $(G, +)$ äärellinen Abelin ryhmä. Tällöin*

$$G \cong K_1 \oplus K_2 \oplus \ldots \oplus K_n,$$

missä jokainen $K_i, i = 1, \ldots, n$, on syklinen ryhmä, jonka kertaluku on muotoa $p_i^{r_i}$, missä p_i on alkuluku.

Todistus. [4], s.293 Lauseen 5.7 nojalla G on aliryhmiensä $G(p_i)$ suora summa, missä jokainen alkuluku p_i jakaa ryhmän G kertaluvun. Koska jokainen $G(p_i)$ on p_i-ryhmä, niin osoitetaan, että jokainen äärellinen Abelin p_i-ryhmä H on syklisten ryhmien, joiden kertaluku on jokin luvun p_i potenssi, suora summa. Osoitetaan tämä induktiolla ryhmän H kertaluvun suhteen. Kun $|H| = 2$, niin alkion $h \neq 0 \in H$ kertaluvun täytyy olla 2. Tunnetusti jokainen kahden alkion ryhmä on isomorfinen ryhmän $\mathbb{Z}_2$ kanssa. Näin ollen väite pätee kun $|H| = 2$. Oletetaan seuraavaksi, että $|H| > 2$ ja väite pätee kaikille Abelin p_i-ryhmille, joiden kertaluku on pienempi kuin ryhmän H kertaluku. Olkoon ryhmän H suurimman kertaluvun alkion a kertaluku $|a| = p_i^r,\ r \in \mathbb{N}$. Tällöin Lauseen 5.10 nojalla H on isomorfinen ryhmän $\langle a \rangle \oplus K_i$ kanssa. Koska K_i on ryhmän H aliryhmä, niin K_i on p_i^r-ryhmä. Nyt induktio-oletuksen nojalla tiedetään, että K_i on isomorfinen syklisten aliryhmiensä suoran summan kanssa. Tällöin, koska $\langle a \rangle$ on syklinen ja $|a| = p_i^r$, väite pätee myös ryhmälle $H = \langle a \rangle \oplus K$. Väite seuraa induktiotodistuksen nojalla. □

Lause 5.12. *Jos* $syt(m, k) = 1$, *niin* $\mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}$.

Todistus. [4], s.293 Alkion $([1], [1]) \in \mathbb{Z}_m \oplus \mathbb{Z}_k$ kertaluku on pienin positiivinen kokonaisluku t, jolle $([0], [0]) = t([1], [1]) = ([t], [t])$. Näin ollen $t \equiv 0\ (mod\ m)$ ja $t \equiv 0\ (mod\ k)$. Nyt $m \mid t$ ja $k \mid t$, mutta koska $\text{syt}(m, k) = 1$, niin Lemman 3.8 nojalla $mk \mid t$, ja siten $mk \leq t$. Koska $mk([1], [1]) = ([mk], [mk]) = ([0], [0])$, ja t on pienin positiivinen kokonaisluku, jolle $([0], [0]) = t([1], [1]) = ([t], [t])$, niin välttämättä $t = mk$. Näin ollen $\mathbb{Z}_m \oplus \mathbb{Z}_k$ (ryhmä, jonka kertaluku on mk) on syklinen ryhmä, jonka virittää alkio $([1], [1])$, ja siten Lauseen 4.14 nojalla

$$\mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}.$$

□

Lause 5.13. *Jos* $n = p_1^{n_1} p_2^{n_2} \dots p_t^{n_t}$ *ja* $p_1, \dots, p_t$ *ovat eriäviä alkulukuja, niin*

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

Todistus. [4], s.294 Väite pitää paikkansa ryhmille, joiden kertaluku on 2. Oletetaan induktiivisesti, että

$$\mathbb{Z}_k \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{k_t}},$$

kaikille $k < n$. Valitaan $m = p_1^{n_1}$ ja $k = p_2^{n_2} \dots p_t^{n_t} < n$. Nyt Lauseen 5.12 nojalla $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_k$. Yhdistämällä tämä induktio-oletuksen kanssa saamme

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

□

Lemma 5.14. *Jos $(G,+)$ on Abelin ryhmä ja p on alkuluku, joka jakaa ryhmän G kertaluvun, niin ryhmässä G on alkio, jonka kertaluku on p.*

Todistus. [4], s.307. Olkoon p alkuluku, joka jakaa Abelin ryhmän G kertaluvun. Lauseen 5.11 nojalla ryhmällä G on syklinen aliryhmä, jonka kertaluku on muotoa p^k. Tällöin on olemassa $a \in G$ siten, että $|a| = p^k$. Nyt Lauseen 4.9 (3) nojalla $|a^{p^{k-1}}| = p$, joten ryhmä G sisältää alkion jonka kertaluku on p. □

6 Luokittelun apuryhmät

Tässä luvussa esitetään ne ei sykliset ryhmät, joiden avulla luvussa 8 luokittelemme ryhmiä isomorfian mukaisesti. Jokainen tässä luvussa esitetty ryhmä toteuttaa Määritelmän 2.1 mukaiset vaatimukset.

6.1 Permutaatioryhmät

Määritelmä 6.1. Olkoon $n \in \mathbb{N}$ ja $K = \{1, 2, \ldots, n\}$. Joukon K kaikkien permutaatioiden (kaikki bijektiot $K \to K$) ryhmää S_n, jonka laskutoimitus $\circ$ on kuvausten yhdistäminen, kutsutaan *symmetriaryhmäksi.*

Merkitään permutaatioita $2 \times n$ taulukoilla, joissa ensimmäisen rivin alkiot kuvataan niiden alapuolella oleville alkioille.

Esimerkki 6.2. Olkoon $K = \{1, 2, 3\}$. Tällöin

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Käytetään jatkossa ryhmän S_n alkioista syklistä merkintää $(a_1 a_2 a_3 \ldots a_k)$, $1 \leq k \leq n$, mikä tarkoittaa, että a_1 kuvautuu alkiolle a_2, a_2 kuvautuu alkiolle a_3,..., a_{k-1} kuvautuu alkiolle a_k ja a_k kuvautuu alkiolle a_1. Kaikki loput alkiot kuvautuvat itselleen. Tätä kuvausta kutsutaan *k-sykliksi.* Tällä merkinnällä ryhmä S_3 on

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

Määritelmä 6.3. Permutaatio $\tau \in S_n$ on *parillinen (pariton)*, jos se voidaan esittää parillisella (parittomalla) määrällä 2-syklejä, joita kutsutaan myös *transpositioiksi.*

Huomautus 6.4. Jokainen transpositio on itsensä käänteisalkio. Esimerkiksi $(ij)(ij) = (i)(j) = (1)$ kaikilla $i, j \in S_n$.

Määritelmä 6.5. Ryhmän S_n osajoukkoa A_n, joka on ryhmän S_n kaikkien parillisten permutaatioiden muodostama, kutsutaan *alternoivaksi ryhmäksi.*

Lause 6.6. *Alternoiva ryhmä A_n on ryhmän S_n normaali aliryhmä.*

Todistus. [9], s.202. Koska jokainen transpositio on itsensä käänteisalkio, niin neutraalialkio (1) voidaan esittää parillisella määrällä transpositioita, ja siten $(1) \in A_n$. Olkoon $\alpha, \beta \in A_n$. Tällöin α voidaan esittää parillisella määrällä, k, transpositioita. Vastaavasti β voidaan esittää parillisella määrällä, l, transpositioita. Nyt $\alpha\beta$ voidaan esittää $k + l$ määrällä transpositioita, joka on myös parillinen ja siten $\alpha\beta \in A_n$. Koska A_n on äärellinen ja $\alpha\alpha \in A_n$, niin välttämättä $\alpha^n = \alpha^m$ joillekin $0 < n < m$. Näin ollen $\alpha^{-1} = \alpha^{m-n-1}$. Koska $m-n-1 \geq 0$, niin α^{-1} on jokin alkion α positiivinen potenssi ja siten $\alpha^{-1} \in A_n$. Näin ollen A_n on ryhmän S_n aliryhmä.
Olkoon $\tau \in S_n$ jokin transpositio ja olkoon $\sigma \in S_n$ jokin permutaatio. Jos σ on parillinen, niin $\sigma \in A_n$. Jos taas σ on pariton, niin $\tau\sigma \in A_n$. Näin ollen $\sigma \in \tau^{-1}A_n$. Kuitenkin $\tau\tau = (1)$, ja edelleen $\tau = \tau^{-1}$, joten $\sigma \in \tau A_n$. Näin ollen $[S_n : A_n] = 2$, ja siten Lauseen 4.24 nojalla A_n on normaali aliryhmä.
□

Lemma 6.7. *Olkoon $r, s \in \{1, 2, \ldots, n\}, r \neq s$. Tällöin alternoiva ryhmä A_n, kun $n \geq 3$, on 3-syklien $\{(rsk) \mid 1 \leq k \leq n, k \neq r, s\}$ virittämä.*

Todistus. [5], s.49. □

Lause 6.8. *Alternoiva ryhmä A_n on ryhmän S_n ainoa aliryhmä, jonka indeksi on 2.*

Todistus. [15], s.70. Voidaan olettaa, että $n > 2$. Tällöin S_n sisältää jonkin 3-syklin α. Olkoon $H \subset S_n$ aliryhmä, siten että $[S_n : H] = 2$. Oletetaan, että $\alpha \notin H$. Koska α on 3-sykli, niin $|\alpha| = 3$. Jos $\alpha^{-1} \in H$, niin kaikki syklin α potenssit kuuluvat ryhmään H, mikä tarkoittaa, että $\alpha \in H$, joka on ristiriita, ja siten $\alpha^{-1} \notin H$. Koska ryhmän H indeksi on 2, niin alkiot α ja α^{-1} kuuluvat sivuluokkaan αH. Kuitenkin $H = \alpha H \alpha H = \alpha^2 H = \alpha^{-1} H = \alpha H$, joka on ristiriita, ja siten $\alpha \in H$ kaikille 3-sykleille $\alpha \in S_n$. Nyt kaikki 3-syklit kuuluvat ryhmään H, niin Lemman 6.7 nojalla $A_n \subset H$. Koska oletimme, että $[S_n : H] = 2$ ja Lauseen 6.6 nojalla $[S_n : A_n] = 2$, niin on oltava $H = A_n$, ja siten A_n on ainoa ryhmän S_n aliryhmä, jonka indeksi on 2.
□

Huomautus 6.9. Ryhmän S_n aliryhmän A_n kertaluku on $\frac{n!}{2}$. Lauseen 6.6 todistuksen nojalla $[S_n : A_n] = 2$ ja Lauseen 4.31 nojalla $|S_n| = |A_n|[S_n : A_n]$.

Huomautus 6.10. Koska $|A_4| = 4!/2 = 12$, ja vain $[S_4 : A_4] = 2$, niin alternoiva ryhmä A_4 on ainoa ryhmän S_4 aliryhmä, jonka kertaluku on 12.

Lause 6.11. *Ryhmässä A_4 ei ole alkiota, jonka kertaluku on 6.*

Todistus. [3], s.3. Olkoon H vastoin väitettä alternoivan ryhmän aliryhmä, jolle pätee $|H| = 6$. Tällöin Lauseen 4.31 nojalla $[A_4 : H] = 2$. Osoitetaan, että $x^2 \in H$ kaikilla $x \in A_4$. Olkoon $x \in A_4$. Jos $x \in H$, niin selvästi $x^2 \in H$. Jos $x \notin H$, niin tällöin xH on ryhmän A_4 vasemmanpuoleinen sivuluokka, ja $xH \neq H$. Koska sivuluokkia on vain kaksi niin täytyy olla, joko $x^2H = H$ tai $x^2H = xH$. Oletetaan, että $x^2H = xH$. Tällöin $x^2 \in xH$, joten $x^2 = xh$ jollekin $h \in H$. Tästä kuitenkin seuraa, että $x = h \in H$, mikä on ristiriita. Tällöin $x^2H = H$, joten $x^2 \in H$
Jokainen 3-sykli $(abc) \in A_4$, voidaan esittää neliöiden tulona, sillä jokaisen 3-syklin kertaluku on 3. Toisin sanoen $(abc) = (abc)^4 = ((abc)^2)^2$. Tästä seuraa, että jokainen ryhmän A_4 3-sykli sisältyy aliryhmään H. Ryhmä A_4 sisältää 3-syklit $(123), (132), (124), (142), (134), (143), (234)$ ja (243), mikä tarkoittaa, että $|H| \geq 8$, joka on vastoin oletusta $|H| = 6$. Näin ollen ryhmää H ei voi olla olemassa. Näin ollen ryhmässä A_4 ei voi olla alkiota, jonka kertaluku olisi 6. □

6.2 Disykliset ryhmät

Disykliset ryhmät ovat tietyn tyyppisiä ei Abelisia ryhmiä, joiden kertaluku on $4n, n > 1$. Ne ovat kertalukua 2 olevien syklisten ryhmien laajennuksia kertalukua $2n$ olevilla syklisillä ryhmillä.

Lause 6.12. *Disyklinen ryhmä T_n on ryhmä, jonka kertaluku on $4n$ ja se on alkioiden a ja b virittämä, kun pätee*

$$a^{2n} = e, b^2 = a^n, ba = a^{-1}b.$$

Lisäksi disyklisten ryhmien, jokainen alkio voidaan kirjoittaa yksikäsitteisesti muodossa

$$a^k b^j, \quad 0 < k < 2n, j = 0, 1.$$

Todistus. [11], s.347. □

Määritelmä 6.13. Yksikkökvaternioiden joukon $Q = \{1, -1, i, -i, j, -j, k, -k\}$ muodostamaa ryhmää, jonka laskutaulukko on

Q	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

kutsutaan *kvaterniooryhmäksi*. Taulukosta nähdään, että 1 on neutraalialkio. Lisäksi kvaternioryhmän alkioille pätee $a^4 = 1 = e$, $a^2 = -1$, $ba = a^{-1}b$, missä $a, b \in \{i, -i, j, -j, k, -k\}$. Kvaternioryhmä on disyklinen ryhmä, jolle $n = 2$.
Toinen tärkeä disyklinen ryhmä on T_3, joka muodostuu kun $n = 3$. Tällöin ryhmä T_3, $|T| = 12$, on alkioiden a ja b virittämä, joille on voimassa

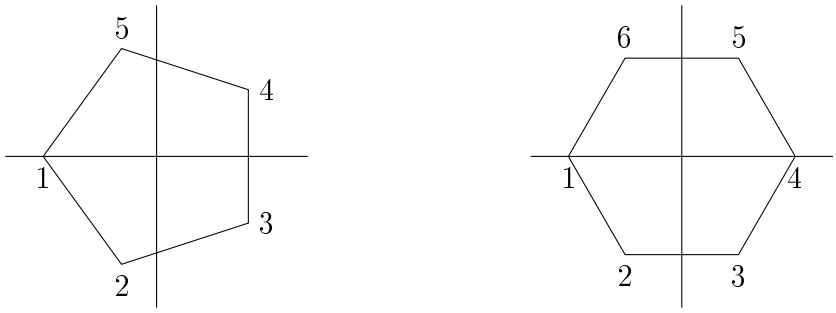
$$|a| = 6, b^2 = a^3, ba = a^{-1}b.$$

Ryhmän T_3 laskutaulukoksi saadaan

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

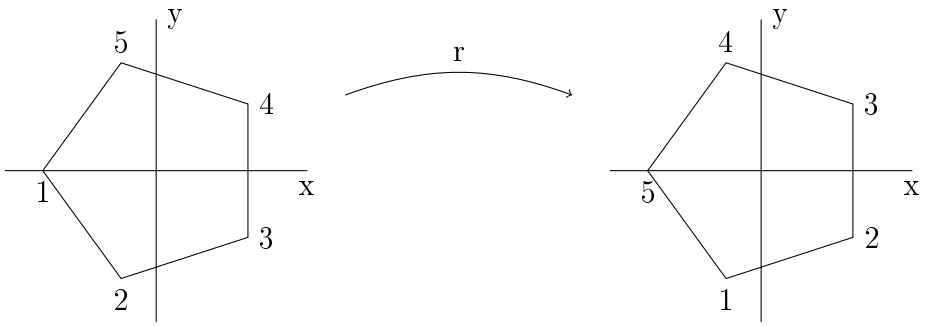
6.3 Diedriryhmät

Olkoon P_n säännöllinen monikulmio, jolla on $n \geq 3$ kylkeä. Havainnollistamiseksi sijoitetaan P_n siten, että sen keskipiste on origossa ja yksi kärjistä on negatiivisella x-akselilla. Kärjet nimetään vastapäivään kiertäen, aloittaen kärjestä, joka sijaitsee negatiivisella x-akselilla.



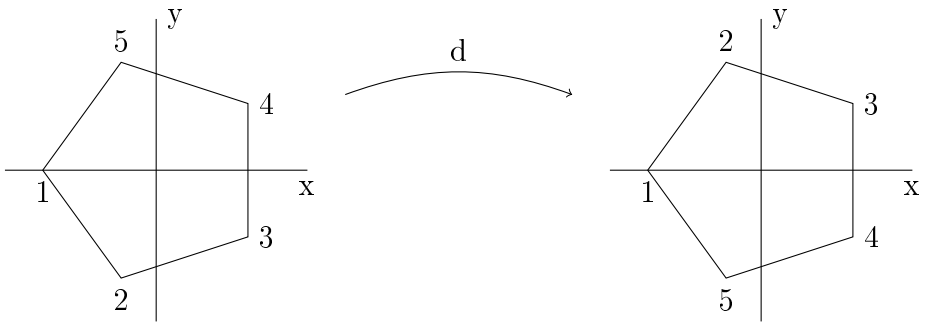
Kuva 1: Monikulmiot P_5 ja P_6

Säännöllisen monikulmion P_n *kierto* r määritellään siten, että monikulmiota P_n kierretään vastapäivään origon suhteen $360/n$ astetta, toisin sanoen kärjet liikkuvat yhden askeleen eteenpäin.



Kuva 2: Monikulmion P_5 kierto

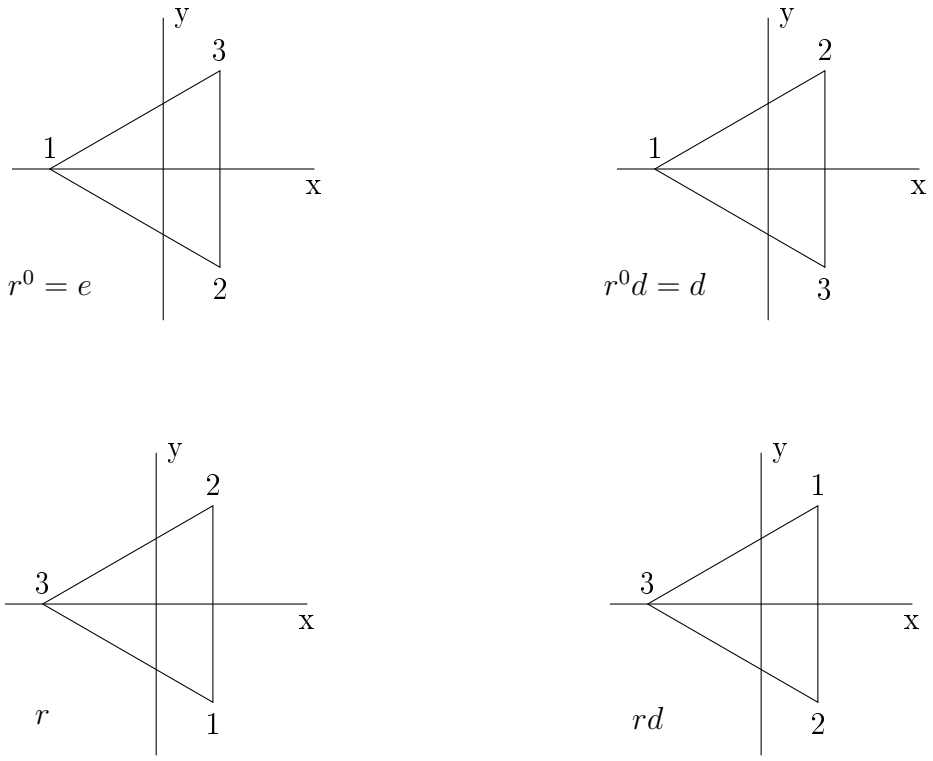
Säännöllisen monikulmion P_n *peilaus* d määritellään kärkien peilauksena x-akselin suhteen.

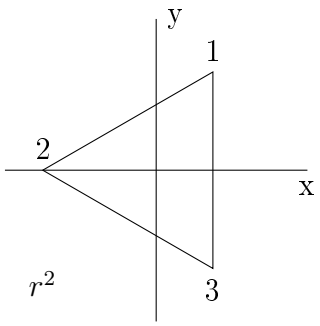


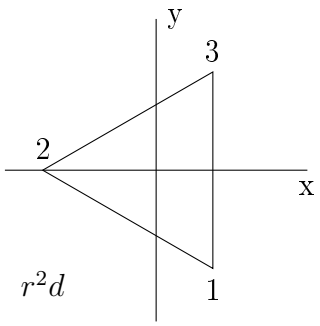
Kuva 3: Monikulmion P_5 peilaus

Määritelmä 6.14. *Diedriryhmät* D_n ovat ryhmiä, jotka muodostuvat säännöllisten monikulmioiden P_n kaikista kierroista ja peilauksista, sekä niiden yhdisteistä.

Esimerkki 6.15. Diedriryhmän D_3 muodostaa säännöllisen monikulmion P_3 kierrot $r^0 = e, r, r^2$, peilaus d, ja näiden yhdisteet rd, r^2d.







Huomataan, että $|d| = 2$, eli $d^2 = e$, ja edelleen $d = d^{-1}$. Lisäksi huomataan $r^2 = r^{-1} = drd$. Operoimalla $drd = r^{-1}$ puolittain alkiolla d saadaan

$$drdd = dr = r^{-1}d = r^2d.$$

Näin ollen $|D_3| = 6 = 2n$, $|r| = 3 = n$, ja siten

$$D_3 = \{r^0 = e, r, r^2, d = r^0d, rd, r^2d\}.$$

Lause 6.16. *Diedriryhmä D_n on ryhmä, jonka kertaluku on $2n$ ja sen virittää alkiot r ja d siten, että*

$$|r| = n, \quad |d| = 2, \quad dr = r^{-1}d.$$

Todistus. [4], s.315. □

Esimerkki 6.17. Olkoon $n = 6$. Lauseen 6.16 nojalla saadaan muodostettua

diedriryhmälle D_6 seuraava laskutaulukko

	e	r	r^2	r^3	r^4	r^5	d	rd	r^2d	r^3d	r^4d	r^5d
e	e	r	r^2	r^3	r^4	r^5	d	rd	r^2d	r^3d	r^4d	r^5d
r	r	r^2	r^3	r^4	r^5	e	rd	r^2d	r^3d	r^4d	r^5d	d
r^2	r^2	r^3	r^4	r^5	e	r	r^2d	r^3d	r^4d	r^5d	d	rd
r^3	r^3	r^4	r^5	e	r	r^2	r^3d	r^4d	r^5d	d	rd	r^2d
r^4	r^4	r^5	e	r	r^2	r^3	r^4d	r^5d	d	rd	r^2d	r^3d
r^5	r^5	e	r	r^2	r^3	r^4	r^5d	d	rd	r^2d	r^3d	r^4d
d	d	r^5d	r^4d	r^3d	r^2d	rd	e	r^5	r^4	r^3	r^2	r
rd	rd	d	r^5d	r^4d	r^3d	r^2d	r	e	r^5	r^4	r^3	r^2
r^2d	r^2d	rd	d	r^5d	r^4d	r^3d	r^2	r	e	r^5	r^4	r^3
r^3d	r^3d	r^2d	rd	d	r^5d	r^4d	r^3	r^2	r	e	r^5	r^4
r^4d	r^4d	r^3d	r^2d	rd	d	r^5d	r^4	r^3	r^2	r	e	r^5
r^5d	r^5d	r^4d	r^3d	r^2d	rd	d	r^5	r^4	r^3	r^2	r	e.

7 Sylowin lauseet

Tässä luvussa käsitellään norjalaisen matemaatikon Peter Ludvig Meidell Sylowin (1832-1918) kehittämiä lauseita, jotka antavat erittäin tärkeitä tuloksia ryhmien luokittelua varten. Määritellään aluksi muutamia aputuloksia, joita tarvitaan Sylowin lauseiden todistamisessa.

Määritelmä 7.1. Olkoon G ryhmä ja S jokin joukko. Kuvausta $G \times S \to S$ kutsutaan *ryhmän G toiminnaksi joukossa S*, jos kaikille $x \in S$ ja $g_1, g_2 \in G$ on voimassa

$$e_G x = x \text{ ja } (g_1 g_2)x = g_1(g_2 x).$$

Lause 7.2. *Jos ryhmä G toimii joukossa S, niin toiminta muodostaa homomorfismin $f : G \to A(S)$, missä $A(S)$ on joukon S kaikkien permutaatioiden muodostama ryhmä.*

Todistus. [5], s.90. Jos g inG, niin määritellään kuvaus $\tau_g : S \to S$ asettamalla $\tau_g(x) = gx$. Koska $x = g(g^{-1}x)$ kaikilla $x \in S$, niin τ_g on surjektio. Vastaavasti yhtälöstä $gx = gy$ seuraa

$$x = g^{-1}(gx) = g^{-1}(gy) = y,$$

joten τ_g on injektio. Näin ollen τ_g on bijektio ja siten $\tau_g \in A(G)$.
Määritellään seuraavaksi kuvaus $f : G \to A(S)$ asettamalla $f(g) = \tau_g$. Kaikille $g, g' \in G$ on $f(gg') = \tau_{gg'}$, kuvaus $S \to S$, joka määritellään asettamalla $\tau_{gg'}(x) = gg'x$. Toisaalta $f(g)f(g') = \tau_g\tau_{g'}$ on kuvaus $S \to S$, jolle

$$(\tau_g\tau_{g'})(x) = \tau_g(\tau_{g'}(x)) = \tau_g(g')(x) = gg'x.$$

Näin ollen $f(gg') = f(g)f(g')$, joten f on homomorfismi. □

Lause 7.3. *Olkoon G ryhmä ja olkoon joukko S ryhmän G aliryhmän H kaikkien vasemmanpuolisten sivuluokkien joukko. Jos G toimii yli joukon S, niin tällöin muodostuneen homomorfismin $f : G \to A(S)$ ydin kuuluu aliryhmään H.*

Todistus. [5], s.90. Kun ryhmä G toimii joukon S yli niin Lauseen 7.2 nojalla, muodostuu kuvaus $f : G \to A(S)$, jonka määrittelee kuvaus $f(g) = \tau_g$, missä $\tau_g : S \to S$ ja $\tau_g(xH) = gxH$. Olkoon $g \in Kerf$. Tällöin $\tau_g = e_S$ ja $gxH = xH$ kaikille $x \in G$. Erityisesti, kun $x = e$, niin $geH = eH = H$, mistä seuraa $g \in H$.

□

Seuraavaksi esitellään jatkon kannalta tärkeä ryhmätoiminto.

Määritelmä 7.4. Olkoon G ryhmä ja $a, b \in G$. Alkiota a kutsutaan alkion b *konjugaatiksi*, jos on olemassa $x \in G$ siten että $b = x^{-1}ax$.

Lause 7.5. *Konjugointi on ekvivalenssirelaatio ryhmässä G.*

Todistus. [4], s.304. Jos a on alkion b konjugaatti, eli $b = x^{-1}ax$, niin käytetään merkintää $a \sim b$. Reflektiivisyys $a \sim a$ pätee, sillä $a = eae = e^{-1}ae$.
Jos $a \sim b$, niin $b = x^{-1}ax$ jollekin $x \in G$. Kertomalla vasemmalta alkiolla x ja oikealta alkiolla x^{-1}, saadaan $a = xbx^{-1} = (x^{-1})^{-1}bx^{-1}$. Siten $b \sim a$, eli $\sim$ on symmetrinen.
Jos $a \sim b$ ja $b \sim c$, niin $b = x^{-1}ax$ ja $c = y^{-1}by$ joillekin $x, y \in G$. Edelleen

$$c = y^{-1}(x^{-1}ax)y = (y^{-1}x^{-1})a(xy) = (xy)^{-1}a(xy).$$

Näin ollen $a \sim c$ ja konjugointi on siten transitiivinen. Yhdistämällä kaikki saadaan, että konjugointi on ekvivalenssirelaatio ryhmässä G. □

Huomautus 7.6. Konjugaattirelaation muodostamia ekvivalenssiluokkia ryhmässä G kutsutaan konjugaattiluokiksi. Alkion a muodostama konjugaattiluokka sisältää kaikki ne ryhmän G alkiot, jotka ovat alkion a konjugaatteja. Koska kyse on ekvivalenssiluokista, niin konjugaattiluokat ovat joko identtiset tai pistevieraat ja G on sen erillisten konjugaattiluokkien yhdiste.

Yleistetään konjugointi myös aliryhmille:

Määritelmä 7.7. Olkoon H ryhmän G kiinnitetty aliryhmä ja olkoot A ja B mitkä hyvänsä kaksi muuta aliryhmää. Jos on olemassa $x \in H$ siten, että

$$B = x^{-1}Ax = \{x^{-1}ax \mid a \in A\},$$

niin sanotaan, että ryhmä A on *H-konjugaatti* ryhmän B kanssa. Erikoistapauksessa, jossa $H = G$ sanotaan, että A on ryhmän B konjugaatti tai toisin päin.

Huomautus 7.8. H-konjugointi on ekvivalenssirelaatio kaikkien aliryhmien joukossa. Tämä todistetaan vastaavasti kuin Lauseessa 7.5 käyttämällä aliryhmiä A, B, C alkioiden a, b, c sijaan.

Seuraavaksi esitellään kaksi tärkeää aliryhmää, sekä niiden olennaisimpia ominaisuuksia.

Määritelmä 7.9. Olkoon G ryhmä ja $a \in G$. Alkion a *keskittäjä* $C(a)$ koostuu kaikista ryhmän G alkioista, joille

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

Lemma 7.10. *Jos G ryhmä on ja $a \in G$, niin $C(A)$ on ryhmän G aliryhmä.*

Todistus. [4], s.305 Koska $ea = ae$, niin $e \in C(a)$, joten $C(a)$ ei ole tyhjä joukko. Jos $g, h \in C(a)$, niin

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

Siten $gh \in C(a)$, ja $C(a)$ on suljettu laskutoimituksen suhteen. Kertomalla $ga = ag$ puolittain vasemmalta ja oikealta alkiolla g^{-1} saadaan $ag^{-1} = g^{-1}a$, joten jos $g \in C(a)$, niin myös $g^{-1} \in C(a)$. Näin ollen Määritelmän 2.6 nojalla $C(a)$ on ryhmän G aliryhmä. □

Määritelmä 7.11. Jos G on ryhmä, niin sen osajoukkoa

$$Z(G) = \{a \in G \mid ag = ga \text{ kaikille } g \in G\}$$

kutsutaan ryhmän G *keskukseksi*.

Lause 7.12. *Olkoon G ryhmä. Tällöin keskus $Z(G)$ on ryhmän G normaali aliryhmä.*

Todistus. [4], s.206. Jokaiselle $g \in G$ on voimassa $eg = g = ge$. Näin ollen $e \in Z(G)$, ja keskus ei ole tyhjä. Jos $a, b \in Z(G)$, niin kaikille $g \in G$ on voimassa $ag = ga$ ja $bg = gb$. Nyt

$$ab^{-1}g = ab^{-1}ge = ab^{-1}gbb^{-1} = ab^{-1}bgb^{-1} = agb^{-1} = gab^{-1},$$

ja näin ollen $ab^{-1} \in Z(G)$, joten $Z(G)$ on ryhmän G aliryhmä Lemman 2.7 nojalla. Olkoon $x \in Z(G)$. Nyt kaikille $g \in G$ on voimassa

$$gxg^{-1} = gg^{-1}x = x \in Z(G),$$

joten $Z(G)$ on normaali aliryhmä. □

Lause 7.13. *Jos G on ryhmä ja sen tekijäryhmä $G/Z(G)$ on syklinen, niin tällöin G on Abelin ryhmä.*

Todistus. [4], s.260. Koska $G/Z(G)$ on syklinen, niin sillä on virittäjäalkio $Z(G)d$. Jokainen sivuluokka ryhmässä $G/Z(G)$ on Lemman 4.28 nojalla muotoa $(Z(G)d)^k = Z(G)d^k$ jollekin $k \in \mathbb{Z}$.
Olkoot $a, b \in G$. Koska $a = ea \in Z(G)a$, ja koska $Z(G)a = Z(G)d^i$ jollekin i, niin $a = z_1 d^i$ jollekin $z_1 \in Z(G)$. Vastaavasti $b = z_2 d^j$. Nyt $d^i d^j = d^{i+j} = d^{j+i} = d^j d^i$, ja keskuksen määritelmän nojalla z_1 sekä z_2 ovat vaihdannaisia jokaisen ryhmän G alkion kanssa. Saadaan

$$ab = (z_1 d^i)(z_2 d^j) = z_1 z_2 d^i d^j = z_2 z_1 d^j d^i = (z_2 d^j)(z_1 d^i) = ba,$$

joten G on Abelin ryhmä. □

Lause 7.14. *Olkoon G äärellinen ryhmä ja $a \in G$. Konjugaattiluokan a alkioiden määrä on aliryhmän $C(a)$ indeksi ryhmässä G ($[G : C(a)]$) ja se jakaa ryhmän G kertaluvun.*

Todistus. [4], s.305. Olkoon S ryhmän G keskittäjän $C(a)$ oikeanpuolisten sivuluokkien muodostama joukko. Olkoon $K(a)$ alkion $a \in G$ muodostama konjugaattiluokka. Määritellään kuvaus $f : S \to K(a)$ asettamalla $f(C(a)x) = x^{-1}ax$. Osoitetaan seuraavaksi, että f on bijektio. Koska konjugointi on symmetrinen, niin $f(C(a)x) \in K(a)$ kun $x \in G$.
Olkoon $x, y \in G$ siten että $C(a)x = C(a)y$. Tästä seuraa

$$\begin{aligned}
C(a)x = C(a)y &\Leftrightarrow xy^{-1} \in C(a) && \text{[Lemma 4.19]}\\
&\Leftrightarrow (xy^{-1})a = a(xy^{-1}) && \text{[Keskittäjän määritelmä]}\\
&\Leftrightarrow a = (xy^{-1})^{-1}a(xy^{-1}) && \text{[kerrotaan } (xy^{-1})^{-1} \text{ puolittain vasemmalle]}\\
&\Leftrightarrow a = yx^{-1}axy^{-1} && \text{[Lemma 4.4]}\\
&\Leftrightarrow y^{-1}ay = x^{-1}ax && \text{[kerrotaan puolittain } y^{-1} \text{ vasemmalle ja } y \text{ oikealle]}\\
&\Leftrightarrow f(C(a)y) = f(C(a)x). && \text{[kuvauksen } f \text{ määritelmä]}
\end{aligned}$$

Jos $f(C(a)x) = f(C(a)y)$, niin $C(a)x = C(a)y$, joten f on injektiivinen. Toisaalta f on surjektiivinen, koska mielivaltainen alkion a konjugaatti $u^{-1}au$ on sivuluokan $C(a)u$ kuva. Kuvaus f on siten bijektio, ja siksi joukon S alkioiden määrä on sama kuin konjugaattiluokan K alkioiden määrä. Lauseen 4.31 nojalla indeksi $[G : C(a)]$ jakaa kertaluvun $|G|$. □

Seuraavaksi esittelemme kolme tapaa esittää ryhmä G konjugaattiluokkiensa avulla.
Olkoon G ryhmä ja olkoot $C_1, C_2, \ldots, C_t$ ryhmän G erilliset konjugaattiluokat, eli $G = C_1 \cup C_2 \cup \cdots \cup C_t$. Koska erilliset konjugaatti luokat ovat pistevieraita, niin

$$|G| = |C_1 \cup C_2 \cup \cdots \cup C_t| = |C_1| + |C_2| + \cdots + |C_t|. \tag{5}$$

Valitaan yksi alkio a_i jokaisesta konjugaattiluokasta C_i. Lauseen 7.14 nojalla $|C_i| = [G : C(a_i)]$, joka jakaa ryhmän G kertaluvun. Nyt yhtälö (5) saadaan muotoon

$$|G| = |G : C(a_1)| + |G : C(a_2)| + \cdots + |G : C(a_t)|. \tag{6}$$

Jos $c, x \in G$, niin tällöin $cx = xc$ jos ja vain jos $x^{-1}cx = c$. Tällöin c kuuluu ryhmän G keskukseen, jos ja vain jos alkiolla c on ainoastaan yksi konjugaatti, se itse. Näin ollen ryhmän G keskus $Z(G)$ on ryhmän G yksialkioisten konjugaattiluokkien yhdiste. Nyt yhtälö (5) voidaan kirjoittaa muodossa

$$|G| = |Z(G)| + |C_1| + |C_2| + \cdots + |C_r|, \tag{7}$$

missä konjugaattiluokat $C_1, C_2, \ldots, C_r$ ovat ryhmän G konjugaattiluokkia, joiden kertaluku on suurempi kuin yksi, ja kertaluku jakaa ryhmän G kertaluvun.
Yhtälöitä (5), (6) ja (7) kutsutaan *luokkayhtälöiksi.*

Nyt olemme esittäneet tarvittavat aputulokset, jotta voimme todistaa Sylowin ensimmäisen lauseen.

Lause 7.15 (Sylowin ensimmäinen lause)**.** *Olkoon G ryhmä. Jos p on alkuluku ja p^k jakaa ryhmän G kertaluvun, niin ryhmällä G on aliryhmä, jonka kertaluku on p^k.*

Todistus. [4], s.307. Käytetään induktiotodistusta. Jos ryhmän G kertaluku on 1, tällöin p^0 on ainoa alkuluvun potenssi, joka jakaa ryhmän G kertaluvun, ja ryhmä G on itse aliryhmä, jonka kertaluku on p^0.
Olkoon G ryhmä, jolle $|G| > 1$. Oletetaan induktiivisesti, että lause on tosi

kaikille ryhmille, joiden kertaluku on pienempi kuin ryhmän G kertaluku. Yhdistämällä luokkayhtälöt (6) ja (7) ryhmälle G saadaan

$$|G| = |Z(G)| + |G : C(a_1)| + |G : C(a_2)| + \cdots + |G : C(a_t)|,$$

missä $[G : C(a_i)] > 1$ kaikille i. Huomioidaan, että $|Z(G)| \geq 1$ ja $|C(a_i)| < |G|$ (koska $[G : C(a_i)] \neq 1$).
Oletetaan ensin, että on olemassa indeksi j siten, että $[G : C(a_j)]$ ei ole jaollinen luvulla p. Nyt Lemman 3.7 nojalla luvun p^k täytyy jakaa kertaluku $|C(a_j)|$, koska oletuksen nojalla luku p^k jakaa ryhmän G kertaluvun, ja Lauseen 4.31 nojalla $|G| = |C(a_j)|[G : C(a_j)]$. Koska aliryhmän $C(a_j)$ kertaluku on pienempi kuin ryhmän G kertaluku, niin induktio-oletuksen nojalla aliryhmällä $C(a_j)$ on aliryhmä jonka kertaluku on p^k. Tästä seuraa, että ryhmällä G on aliryhmä, jonka kertaluku on p^k.
Jos taas p jakaa indeksin $[G : C(a_i)]$ kaikilla i, niin p jakaa myös luvun $|G| - [G : C(a_1)] - \cdots - [G : C(a_t)] = |Z(G)|$, sillä p jakaa ryhmän G kertaluvun $|G|$. Koska $Z(G)$ on Abelin ryhmä, niin Lemman 5.14 nojalla $Z(G)$ sisältää alkion c, jonka kertaluku on p.
Olkoon N alkion c virittämä syklinen ryhmä, tällöin syklisen ryhmän N kertaluku on p. Olkoon $n \in N$. Koska $N \subseteq Z(G)$, niin $g^{-1}ng = g^{-1}gn = n \in N$, ja siten Lemman 4.25 nojalla ryhmä N on ryhmän G normaali aliryhmä. Nyt tekijäryhmän G/N kertaluku $|G|/p$ on pienempi kuin ryhmän G kertaluku, ja jaollinen luvulla p^{k-1}. Induktio-oletuksen nojalla ryhmällä G/N on aliryhmä K, jonka kertaluku on p^{k-1}. Lauseen 4.30 nojalla on ryhmällä G on olemassa aliryhmä H, siten että $N \subseteq H$ ja $K = H/N$. Lauseen 4.31 nojalla saadaan

$$|H| = |N| \cdot |H/N| = |N| \cdot |K| = pp^{k-1} = p^k.$$

Näin ollen ryhmällä G on aliryhmä, jonka kertaluku on p^k. □

Havainnollistetaan Sylowin ensimmäistä lausetta esimerkillä.

Esimerkki 7.16. Olkoon G ryhmä, jonka kertaluku on $3600 = 2^4 \cdot 3^2 \cdot 5^2$. Sylowin ensimmäisen lauseen nojalla ryhmällä G on ainakin yksi aliryhmä kertaluvuilla $2, 4, 8$ ja 16 (kun $p = 2$). Tällaisia aliryhmiä voi kuitenkin olla useampia. Vastaavasti ryhmällä G on vähintään yhdet kertalukua $3, 5, 9$ ja 25 olevat aliryhmät.

Sylowin ensimmäinen lause antaa seuraavan erikoistapauksen.

Seuraus 7.17 (Cauchyn lause)**.** *Olkoon G ryhmä, jonka kertaluvun alkuluku p jakaa. Tällöin ryhmä G sisältää alkion, jonka kertaluku on p, toisin sanoen $a^p = e \in G$.*

Määritelmä 7.18. Olkoon G ryhmä ja p alkuluku. Olkoon p^n suurin luku, joka jakaa ryhmän G kertaluvun. Ryhmän G aliryhmää, jonka kertaluku on p^n kutsutaan *Sylowin p-ryhmäksi.*

Ennen kuin todistamme Sylowin toisen ja kolmannen lauseen tarvitsemme vielä muutamia aputuloksia.

Lemma 7.19. *Olkoon K ryhmän G aliryhmä ja $x \in G$. Tällöin ryhmä $x^{-1}Kx = \{x^{-1}kx \mid k \in K\}$ on isomorfinen ryhmän K kanssa.*

Todistus. [4], s.300. Määritellään kuvaus $f : G \to G$ asettamalla $f(a) = x^{-1}ax$. Todetaan f isomorfismiksi. Ensinnäkin

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

joten f on homomorfismi. Toisaalta kaikilla $a \in G$ pätee

$$f(xax^{-1}) = x^{-1}(xax^{-1})x = eae = a,$$

joten f on surjektiivinen.
Oletetaan, että $f(a) = f(b)$. Tällöin $x^{-1}ax = x^{-1}bx$, ja supistamalla puolittain saadaan $a = b$, joten f on injektiivinen. Näin ollen f on isomorfismi.
Nyt käyttämällä kuvausta f aliryhmään K saadaan

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

Näin ollen aliryhmä $x^{-1}Kx$ on isomorfinen aliryhmän K kanssa. □

Lemman 7.19 seurauksena on, että jos K on Sylowin p-ryhmä, niin myös $x^{-1}Kx$ on Sylowin p-ryhmä.

Määritelmä 7.20. Olkoon G ryhmä ja A sen aliryhmä. Joukkoa

$$N(A) = \{g \in G \mid g^{-1}Ag = A\}$$

kutsutaan ryhmän A *normalisoijaksi.*

Lause 7.21. *Jos A on ryhmän G aliryhmä, niin tällöin normalisoija $N(A)$ on ryhmän G aliryhmä ja A on ryhmän $N(A)$ normaali aliryhmä.*

Todistus. [4], s.309. Osoitetaan ensin, että $A \subset N(A)$. Olkoon $a \in A$. Koska A on aliryhmä, niin kaikilla $b \in A$ on voimassa $a^{-1}ba \in A$ ja siten $a^{-1}Aa \subset A$. Toisaalta kaikilla $b \in A$ on voimassa $b = a^{-1}(aba^{-1})a$ ja siten $A \subset a^{-1}Aa$. Näin ollen $A = a^{-1}Aa$ ja normalisoijan määritelmästä seuraa, että $A \subset N(A)$. Todistetaan seuraavaksi, että $g \in N(A)$ jos ja vain jos

$Ag = gA$. Oletetaan, että $g \in N(A)$. Tällöin normalisoijan määritelmän nojalla $g^{-1}Ag = A$. Kertomalla tämä puolittain alkiolla g saadaan $Ag = gA$. Oletetaan seuraavaksi, että $Ag = gA$. Nyt kertomalla tämä puolittain alkiolla g^{-1} saadaan $g^{-1}Ag = A$, joten $g \in N(A)$. Nyt normalisoijan määritelmästä seuraa, että A on ryhmän $N(A)$ normaali aliryhmä.
Osoitetaan seuraavaksi, että $N(A)$ on ryhmän G aliryhmä. Selvästi $e \in N(A)$, joten $N(A)$ ei ole tyhjä joukko. Jos $g, h \in N(A)$, niin

$$(gh)^{-1}Agh = h^{-1}g^{-1}Agh = h^{-1}Ah = A,$$

joten $gh \in N(A)$ ja $N(A)$ on suljettu laskutoimituksen suhteen. Nyt kertomalla yhtälöä $Ag = gA$ puolittain termillä g^{-1} saadaan $A = gAg^{-1}$ ja näin ollen $g^{-1} \in N(A)$. Näin ollen $N(A)$ on ryhmän G aliryhmä Määritelmän 2.6 nojalla.

□

Lause 7.22. *Olkoon A ja H ryhmän G aliryhmiä. Ryhmän A erillisten H-konjugaattien määrä (aliryhmien määrä, jotka kuuluvat ryhmän A H-konjugaatin muodostamaan ekvivalenssiluokkaan) on $[H : H \cap N(A)]$, ja se jakaa ryhmän H kertaluvun.*

Todistus. [4], s.309. Olkoon S ryhmän H aliryhmän $H \cap N(A)$ oikeanpuolisten sivuluokkien joukko ryhmässä H. Olkoon $K(A)$ ryhmän A H-konjugaattien muodostama joukko. Määritellään kuvaus $f : S \to K(A)$ asettamalla

$$f((H \cap N(A))x) = x^{-1}ax.$$

Osoitetaan seuraavaksi, että f on bijektio. Koska konjugointi on symmetrinen, niin $f((H \cap N(A))x) \in K(A)$ kun $x \in G$.
Olkoon $x, y \in H$, siten että $(H \cap N(A))x = (H \cap N(A))y$. Tästä seuraa

$$\begin{aligned}
&(H \cap N(A))x = (H \cap N(A))y \\
&\Leftrightarrow xy^{-1} \in H \cap N(A) && \text{[Lemma 4.19]} \\
&\Leftrightarrow (xy^{-1})^{-1}Axy^{-1} = A && \text{[normalisoijan määritelmä]} \\
&\Leftrightarrow A = yx^{-1}Axy^{-1} && \text{[Lemma 4.4]} \\
&\Leftrightarrow y^{-1}Ay = x^{-1}Ax && \text{[kerrotaan puolittain } y^{-1} \text{ vasemmalle ja } y \text{ oikealle]} \\
&\Leftrightarrow f(H \cap N(A)y) = f((H \cap N(A))x). && \text{[kuvauksen } f \text{ määritelmä]}
\end{aligned}$$

Jos $f((H \cap N(A))x) = f((H \cap N(A))y)$, niin $(H \cap N(A))x = (H \cap N(A))y$, ja kuvaus f on siten injektiivinen. Lisäksi f on surjektiivinen, koska mielivaltainen konjugaattiluokka $u^{-1}Au$ on sivuluokan $(H \cap N(A))u$ kuva. Näin ollen

kuvaus f on bijektio, ja siten joukon S alkioiden määrä on sama kuin konjugaattiluokkien $K(A)$ määrä. Lauseen 4.31 nojalla indeksi $[H : H \cap N(A)]$ jakaa kertaluvun $|H|$.

□

Lause 7.23. *Olkoon U ryhmän G Sylowin p-ryhmä. Jos alkiolla $x \in G$ on kertalukuna luvun p potenssi ja $x^{-1}Ux = U$, niin tällöin $x \in U$.*

Todistus. [4], s.309. Koska Lauseen 7.21 nojalla U on ryhmän $N(U)$ normaali aliryhmä, niin tekijäryhmä $N(U)/U$ on määritelty. Oletuksen $x^{-1}Ux = U$ nojalla $x \in N(U)$. Koska $|x|$ on jokin luvun p potenssi p^t, ja Lemman 4.28 nojalla

$$(Ux)^{p^t} = Ux^{p^t} = Ue,$$

ja Lauseen 4.9 nojalla seuraa, että $|x| = p^t$ on jaollinen kertaluvulla $|Ux|$. Näin ollen ryhmän $N(U)/U$ sivuluokalla Ux on kertalukuna luvun p potenssi p^m. Nyt Ux virittää ryhmän $N(U)/U$ syklisen aliryhmän K, jonka kertaluku on luvun p potenssi p^k. Lauseen 4.30 nojalla $K = H/U$, missä H on ryhmän G aliryhmä, joka sisältää ryhmän U. Koska ryhmien U ja K kertaluvut ovat luvun p potensseja, ja $|H| = |U||K|$ (Lause 4.31), niin ryhmän H kertaluvun täytyy olla jokin luvun p potenssi p^h. Mutta $U \subseteq H$, ja $|U|$ on Sylowin p-ryhmän määritelmän nojalla suurin luvun p potenssi, joka jakaa ryhmän G kertaluvun. Näin ollen $U = H$, ja siten $K = H/U = U/U$, joten alkion Ux täytyy olla Ue. Täten yhtäsuuruudesta $Ux = Ue$ seuraa, että $x \in U$.

□

Lause 7.24 (Sylowin toinen lause)**.** *Jos P ja K ovat ryhmän G Sylowin p-ryhmiä, niin tällöin on olemassa $x \in G$ siten, että $P = x^{-1}Kx$.*

Todistus. [4], s.309. Koska K on Sylowin p-ryhmä, niin ryhmällä K on kertalukuna p^n, kun $|G| = p^n m$ ja $p \nmid m$. Olkoot $K = K_1, K_2, \ldots, K_t$ erilliset ryhmän K konjugaatit ryhmässä G. Lauseen 7.22 nojalla $t = [G : N(K)]$. Nyt

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

jolloin $p \nmid t$, sillä $p^n \mid |N(K)|$, koska K on normalisoijan $N(K)$ aliryhmä. Koska konjugointi on transitiivinen, niin jokainen konjugaatti K_i on jonkin konjugaatin K_j konjugaatti. Konjugaatin K_i muodostama ekvivalenssiluokka P-konjugoinnin suhteen sisältää vain konjugaatteja K_j. Näin ollen kaikkien K konjugaattien joukko $S = \{K_1, K_2, \ldots, K_t\}$ on P-konjugoinnin muodostamien erillisten ekvivalenssiluokkien yhdiste. Aliryhmien määrä jokaisessa ekvivalenssiluokassa on jokin luvun p potenssi, sillä Lauseen 7.22

nojalla aliryhmien määrä, jotka ovat P-konjugaatteja konjugaatin K_i kanssa on $[P : P \cap N(K_i)]$. Edelleen Lauseen 4.31 nojalla $[P : P \cap N(K_i)]$ jakaa luvun $|P| = p^n$. Näin ollen $t = p^{n_1} + \cdots + p^{n_k}$, jossa jokainen p^{n_i} on jokin joukon S erillisen ekvivalenssiluokan alkioiden määrä. Koska $p \nmid t$, niin ainakin yksi toteuttaa ehdon $p^{n_i} = p^0 = 1$. Näin ollen jokin K_i on itsensä ekvivalenssiluokka, eli $x^{-1}K_i x = K_i$ jokaiselle $x \in P$. Lauseesta 7.23 seuraa, että $x \in K_i$ jokaiselle x siten, että $P \subseteq K_i$. Koska P ja K_i ovat molemmat Sylowin p-ryhmiä, niin niillä on sama kertaluku, ja siten $P = K_i$.

□

Seuraus 7.25. *Olkoon G ryhmä ja K Sylowin p-ryhmä jollekin alkuluvulle p. Tällöin K on ryhmän G normaali aliryhmä, jos ja vain jos se on ainoa Sylowin p-ryhmä ryhmässä G.*

Todistus. [4], s.300. Oletetaan, että K on ainoa Sylowin p-ryhmä. Lemman 7.19 nojalla $x^{-1}Kx$ on Sylowin p-ryhmä kaikilla $x \in G$. Koska K on ainoa Sylowin p-ryhmä, niin välttämättä $x^{-1}Kx = K$ kaikilla $x \in G$. Näin ollen Lemman 4.25 nojalla K on normaali aliryhmä.
Oletetaan käänteisesti, että K on normaali aliryhmä ja olkoon P mikä tahansa Sylowin p-ryhmä. Nyt Sylowin toisen lauseen nojalla on olemassa $x \in G$ siten, että $P = x^{-1}Kx$. Koska K on normaali aliryhmä, niin $P = x^{-1}Kx = K$ Lemman 4.25 nojalla. Näin ollen K on ainoa Sylowin p-ryhmä. □

Lause 7.26 (Sylowin kolmas lause)**.** *Ryhmän G Sylowin p-ryhmien määrä jakaa ryhmän G kertaluvun ja on muotoa $1 + pk$ jollekin positiiviselle kokonaisluvulle k.*

Todistus. [4], s.310. Olkoon joukko $S = \{K_1, \ldots, K_t\}$ ryhmän G kaikkien Sylowin p-ryhmien joukko. Sylowin toisen lauseen todistus osoittaa, että $t = [G : N(K_1)]$, ja että $t \mid |G|$. Olkoon P jokin joukon S alkioista K_i. Nyt ainoa P-konjugaatti ryhmän P kanssa on ryhmä P itse. Sylowin toisen lauseen todistus osoittaa, että ainoa yhden aliryhmän sisältävä ekvivalenssiluokka on se luokka, joka sisältää ryhmän P. Sylowin toisen lauseen todistus osoittaa myös, että joukko S on erillisten ekvivalenssiluokkien yhdiste. Edelleen nähdään, että aliryhmien määrä jokaisessa ekvivalenssiluokassa on jokin luvun p potenssi. Ryhmä P sisältyy vain yhteen näistä ekvivalessiluokista, joten kaikissa muissa ekvivalenssiluokissa aliryhmiä on jokin luvun p positiivinen potenssi. Näin ollen Sylowin p-ryhmien määrä t voidaan kirjoittaa summana $t = 1 + kp$ jollekin $k \in \mathbb{Z}$.

□

Esimerkki 7.27. Olkoon G ryhmä ja $|G| = 20 = 2^2 \cdot 5$. Tällöin jokaisella Sylowin 5-ryhmällä on kertaluku 5, ja näiden ryhmien määrä jakaa ryhmän G kertaluvun, sekä on muotoa $1 + 5k, k \in \mathbb{Z}$. Luku 20 on jaollinen luvuilla 1,2,4,5,10 ja 20. Luvut 1,6,11,16 ja 21 ovat muotoa $1 + 5k$. Koska luku 1 on ainoa, joka esiintyy molemmissa listoissa, niin ryhmällä G on 1 Sylowin 5-ryhmä, ja Seurauksen 7.25 nojalla se on normaali aliryhmä.

Esimerkki 7.28. Olkoon G ryhmä ja $|G| = 80 = 2^4 \cdot 5$. Tällöin jokaisella Sylowin 5-ryhmällä on kertalukuna 5 ja näiden ryhmien määrä jakaa luvun $|G|$ sekä on muotoa $1+5k$. Luku 80 on jaollinen luvuilla 1,2,4,5,8,16,20,40 ja 80. Luvut 1,6,11,16,$\ldots$, 81 ovat muotoa $1+5k$. Nyt vain luvut 1 ja 16 esiintyvät molemmissa listoissa, joten ryhmällä G on joko yksi Sylowin 5-ryhmä tai 16 sellaista. Jos Sylowin 5-ryhmiä on yksi kappale, niin se on Seurauksen 7.25 nojalla normaali aliryhmä. Jos Sylowin 5-ryhmiä on 16 kappaletta, niin Lemman 4.32 seurauksena jokaisessa 5-ryhmässä on neljä neutraalialkiosta poikkeavaa alkiota, joiden kertaluku on 5. Lemman 4.35 nojalla 5-ryhmien leikkaus on $\langle e \rangle$. Nyt ryhmässä G on $16 \cdot 4 = 64$ alkiota, joiden kertaluku on 5. Jokaisella Sylowin 2-ryhmällä on kertalukuna 16. Jokaisen Sylowin 2-ryhmän alkion täytyy jakaa luku 16, ja siten ne eivät voi kuulua aiemmin esitettyjen 64 alkion joukkoon. Näin ollen ryhmään G ei mahdu kuin yksi Sylowin 2-ryhmä, joka on ryhmän G normaali aliryhmä Seurauksen 7.25 nojalla.

8 Ryhmien luokittelu

Tässä luvussa esitellään ne lauseet, joita tarvitaan luokittelussa isomorfian mukaisesti . Jokaisen lauseen todistamisen jälkeen lausetta sovelletaan alle 16 alkoisten ryhmien luokittelussa. Tässä luvussa käytetään merkintää G_n ryhmästä, jonka kertaluku on n.

Lause 8.1. *Olkoon p alkuluku. Jokainen ryhmä, jonka kertaluku on p, on syklinen ja isomorfinen ryhmän $\mathbb{Z}_p$ kanssa.*

Todistus. [4], s.242. Olkoon ryhmän G kertaluku alkuluku p, ja $a \in G, a \neq e$. Syklinen aliryhmä $\langle a \rangle$ on ryhmä jonka kertaluku on suurempi kuin 1. Koska Lauseen 4.31 nojalla ryhmän $\langle a \rangle$ kertaluku jakaa luvun p ja p on alkuluku, niin aliryhmän $\langle a \rangle$ kertaluvun täytyy olla p. Näin ollen $\langle a \rangle = G$, eli G on syklinen ryhmä, jonka kertaluku on p. Näin ollen Lauseen 4.14 nojalla $G \cong \mathbb{Z}_p$. □

Näin saamme luokiteltua isomorfian mukaisesti kaikki ne ryhmät, joiden kertaluku on jokin alkuluku. Näin ollen alle 16 alkioisille ryhmille on voimassa

seuraavat isomorfiat $G_1 \cong \mathbb{Z}_1, G_2 \cong \mathbb{Z}_2, G_3 \cong \mathbb{Z}_3, G_5 \cong \mathbb{Z}_5, G_7 \cong \mathbb{Z}_7, G_{11} \cong \mathbb{Z}_{11}$ ja $G_{13} \cong \mathbb{Z}_{13}$.

Lause 8.2. *Olkoon G ryhmä, jonka kertaluku on $2p$, missä p on pariton alkuluku. Tällöin G on isomorfinen syklisen ryhmän $\mathbb{Z}_{2p}$ tai diedriryhmän D_p kanssa.*

Todistus. [4], s.316. Seurauksen 7.17 nojalla ryhmässä G on alkio a, jonka kertaluku on p, ja alkio b, jonka kertaluku on 2 ($b^2 = e$). Olkoon H alkion a virittämä syklinen ryhmä ($H = \langle a \rangle$). Koska $|G| = 2p$, niin ryhmän H indeksi on 2 ja siten se on ryhmän G normaali aliryhmä. Nyt $bab = bab^{-1} \in H$. Koska $H = \langle a \rangle$, niin $bab = a^t$ jollekin t. Nyt saadaan

$$a^{t^2} = (a^t)^t = (bab)^t = \underbrace{(bab)(bab)\dots(bab)}_{t \text{ kpl}} = ba^t b = b(bab)b = a.$$

Näin ollen Lauseen 4.9 (2) nojalla $t^2 \equiv 1 (mod\ p)$. Tästä seuraa, että p jakaa tulon $t^2 - 1 = (t-1)(t+1)$, joten Lemman 3.4 nojalla $p \mid (t-1)$ tai $p \mid (t+1)$. Näin ollen $t \equiv 1 (mod\ p)$ tai $t \equiv -1 (mod\ p)$.
Olkoon $t \equiv 1 (mod\ p)$. Nyt Lauseen 4.9 nojalla $bab = a^t = a$. Operoimalla edellistä yhtälöä puolittain alkiolla b saadaan $ab = ba$. Nyt $|ab| = 2p = |G|$, sillä

$$(ab)^{2p} = (abab)^p = (a^2b^2)^p = (a^2e)^p = a^{2p} = (a^p)^2 = e^2 = e.$$

Näin ollen G on syklinen ja siten Lauseen 4.14 nojalla isomorfinen ryhmän $\mathbb{Z}_{2p}$ kanssa.
Olkoon $t \equiv -1 (mod\ p)$. Nyt Lauseen 4.9 nojalla $bab = a^{-1}$, ja koska $b^2 = e$, niin myös $bab^{-1} = a^{-1}$ kaikilla $a \in G$. Näin ollen myös $ba^ib^{-1} = a^{-i}$. Nyt koska $b^2 = e$, niin $b^j a^i b^{-j} = a^{(-1)^j i}$ ja edelleen $b^j a^i = a^{(-1)^j i} b^j$. Määritellään kuvaus $f : D_p \to G$ asettamalla

$$f(r^i d^j) = a^i b^j.$$

Nyt kuvaus f on homomorfismi, sillä (muistetaan Lauseesta 6.16, että $|r| =$

$n, |d| = 2, drd^{-1} = r^{-1}$ ja edeltävän päättelyketjun nojalla $d^j r^i = r^{(-1)^j i} d^j$)

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

Valitaan $K = \langle b \rangle$. Lemman 4.35 nojalla $H \cap K = \langle e \rangle$, koska $|H| = p$ ja $|K| = 2$. Nyt G voidaan esittää muodossa (Lemma 4.36)

$$G = HK = \{ab \in G \mid a \in H, b \in K\}.$$

Nyt jos $ab = a_1 b_1$, niin saadaan $a_1^{-1} a = b_1 b^{-1}$. Mutta $H \cap K = \langle e \rangle$, joten

$$a_1^{-1} a = b_1 b^{-1} = e,$$

mistä seuraa, että $a = a_1$ ja $b = b_1$. Siten kaikki ryhmän G alkiot voidaan kirjoittaa yksikäsitteisesti muodossa $a^i b^j$, kun $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$. Koska $|D_p| = |G| = 2p$, sekä molempien alkiot voidaan kirjoittaa yksikäsitteisesti muodossa $x^i y^j$, kun $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$, niin f on sekä surjektio ja injektio, ja siten bijektio. Koska f on homomorfismi ja bijektio, niin f on isomorfismi, joten $G \cong D_p$. □

Nyt voimme luokitella isomorfian mukaisesti kaikki ne ryhmät, joiden kertaluku on $2p$. Alle 16 alkioisissa ryhmissä tällaisia ovat $G_6 \cong \mathbb{Z}_{2\cdot 3}$ tai $G_6 \cong D_6$, $G_{10} \cong \mathbb{Z}_{2\cdot 5}$ tai $G_{10} \cong D_{10}$ ja $G_{14} \cong \mathbb{Z}_{2\cdot 7}$ tai $G_{14} \cong D_{14}$.

Lause 8.3. *Olkoon G ryhmä, jonka kertaluku on pq, missä p ja q ovat parittomia alkulukuja, ja $p > q$. Jos $q \nmid (p-1)$, niin tällöin $G \cong \mathbb{Z}_{pq}$.*

Todistus. [4], s.302. Sylowin kolmannen lauseen nojalla ryhmän G Sylowin p-ryhmien määrän täytyy jakaa ryhmän G kertaluvun. Sylowin p-ryhmiä on tällöin $1, p, q$ tai pq kappaletta. Toisaalta p-ryhmien määrän täytyy kuitenkin olla muotoa $1+pk$ jollekin $k \in \mathbb{Z}_+$. Koska $p > q$, niin välttämättä $q \neq 1+pk$. Molemmista tilanteista $p = 1 + pk$ ja $pq = 1 + pk$ seuraisi, että $p \mid 1$, mikä on mahdotonta. Ryhmällä G on siten vain yksi kappale Sylowin p-ryhmiä H, joka on Seurauksen 7.25 nojalla normaali aliryhmä. Vastaavasti voidaan

todeta, että ryhmällä G on ainoastaan yksi Sylowin q-ryhmä K, ja sekin on normaali aliryhmä. Ryhmä $H \cap K$ on sekä ryhmän H että ryhmän K aliryhmä, joten Lauseen 4.31 nojalla sen kertaluvun täytyy jakaa molempien ryhmien H ja K kertaluvut $|H| = p$ ja $|K| = q$. Näin ollen ainoa vaihtoehto on $H \cap K = \langle e \rangle$. Nyt Lemma 4.36 osoittaa, että $G = HK$ ja Lauseen 5.2 nojalla $G = H \times K$. Kuitenkin Lauseen 8.1 nojalla $H \cong \mathbb{Z}_p$ ja $K \cong \mathbb{Z}_q$, joten Lauseen 5.12 nojalla $G = H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. □

Nyt voimme luokitella kaikki ryhmät, joiden kertaluvut on muotoa $pq, q \nmid (p-1)$. Alle 16 alkioisissa ryhmissä tällaisia on vai yksi $G_{15} \cong \mathbb{Z}_{5\cdot 3}$.

Seuraavaksi esittelemme aputuloksen, jonka avulla voimme muodostaa lisää luokittelulauseita.

Lause 8.4. *Jos ryhmän G kertaluku on p^n, missä p on alkuluku ja $n \geq 1$, niin tällöin keskuksen $Z(G)$ kertaluku on $|Z(G)| = p^k$, missä $1 \leq k \leq n$.*

Todistus. [4], s.312. Lauseen 4.31 nojalla $|Z(G)| = p^k$, missä $0 \leq k \leq n$. Osoitetaan, että $k \geq 1$, eli $|Z(G)| \geq p$. Luokkayhtälön (7) nojalla

$$|Z(G)| = |G| - |C_1| - |C_2| - \cdots - |C_r|,$$

missä jokainen $|C_i| > 1$ ja $|C_i|$ jakaa kertaluvun $|G|$ kaikilla $i = 1, \ldots, r$. Koska $|G| = p^n$, niin sen lukua 1 suurempien jakajien täytyy olla luvun p potensseja. Näin ollen jokainen $|C_i|$ on jaollinen luvulla p. Koska myös $|G|$ on jaollinen luvulla p, niin seuraa, että myös $|Z(G)|$ on jaollinen luvulla p. Näin ollen $|Z(G)| \geq p$. □

Lause 8.5. *Jos G on ryhmä, jonka kertaluku on p^2, kun p on alkuluku, niin G on Abelin ryhmä. Tällöin G on isomorfinen joko ryhmän $\mathbb{Z}_{p^2}$ tai ryhmän $\mathbb{Z}_p \times \mathbb{Z}_p$ kanssa.*

Todistus. [4], s.312. Lauseiden 4.31 ja 8.4 nojalla keskuksella $Z(G)$ on kertalukuna joko p tai p^2. Jos kertaluku on p^2, niin tällöin $Z(G) = G$, ja G on Abelin ryhmä. Jos $|Z(G)| = p$, niin tekijäryhmällä $G/Z(G)$ on Lauseen 4.27 nojalla kertalukuna $|G|/|Z(G)| = p^2/p = p$. Näin ollen Lauseen 8.1 nojalla $G/Z(G)$ on syklinen. Edelleen Lauseen 7.13 nojalla G on Abelin ryhmä. Lauseen 5.11 nojalla G on isomorfinen joko ryhmän $\mathbb{Z}_{p^2}$ tai ryhmän $\mathbb{Z}_p \times \mathbb{Z}_p$ kanssa. □

Nyt saamme luokiteltua kaikki ryhmät, joiden kertaluku on jonkin alkuluvun p neliö. Alle 16 alkioisissa ryhmissä tällaisia ovat $G_4 \cong \mathbb{Z}_4$ tai $G_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ ja $G_9 \cong \mathbb{Z}_9$ tai $G_9 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Nyt olemme saaneet luokiteltua kaikki muut alle 16 kertalukua olevat ryhmät paitsi ryhmät joiden kertaluku on G_8 ja G_{12}. Näiden kertalukujen luokittelussa käytetään luvussa 6 esiintyviä apuryhmiä. Aloitetaan kertalukua 8 olevista ryhmistä.

Huomautus 8.6. Luvussa 6 esitetyt ryhmät Q ja D_4 eivät ole isomorfisia keskenään Lemman 4.12 nojalla, sillä ryhmässä Q on kuusi alkiota $i, -i, j, -j, k, -k$, joiden kertaluku on 4 ja ryhmässä D_4 kertaluvun 4 alkioita on vain kaksi r, r^3.

Lause 8.7. *Olkoon G ryhmä, jonka kertaluku on 8. Tällöin G on isomorfinen, jonkin ryhmistä $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2, D_4$ tai Q kanssa.*

Todistus. [4], s.317. Olkoon G ryhmä, jonka kertaluku on 8. Jos G on Abelin ryhmä, niin Lauseen 5.11 nojalla G on isomorfinen, jonkin ryhmän $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ tai $\mathbb{Z}_4 \times \mathbb{Z}_2$ kanssa.
Oletetaan, että G ei ole Abelin ryhmä. Lauseen 7.15 nojalla ryhmällä on vähintään yksi aliryhmä kertalukuja 2,4 ja 8. Jos ryhmällä G on kertaluvun 8 aliryhmä, niin G olisi syklinen ryhmä ja siten Abelin ryhmä, joka on vastoin oletusta. Jos kaikkien ryhmän G alkioiden $a \neq e$ kertaluku on 2, niin G on Abelin ryhmä Lemman 4.11 nojalla.
Näin ollen ryhmässä G on alkio a, jonka kertaluku on 4. Olkoon $b \in G$ siten, että $b \notin \langle a \rangle$. Nyt jokainen ryhmän G alkio voidaan kirjoittaa muodossa $a^i b^j$ $(i = 0, 1, 2, 3, j = 0, 1)$, sillä yhtälöstä $a^i = a^j b$ seuraa $b = a^{i-j} \in \langle a \rangle$, joka on ristiriita. Koska $[G : \langle a \rangle] = 2$, niin $\langle a \rangle$ on Lauseen 4.24 nojalla normaali aliryhmä, ja siten Lemman 4.25 nojalla $bab^{-1} \in \langle a \rangle$. Nyt $|bab^{-1}| = 4$, sillä

$$(bab^{-1})^4 = bab^{-1}bab^{-1}bab^{-1}bab^{-1} = ba^4b^{-1} = bb^{-1} = e$$

ja oletukset $(bab^{-1})^2 = e$ ja $bab^{-1} = e$ johtavat yhtälöihin $a^2 = e$ ja $a = e$, jotka eivät ole mahdollisia. Näin ollen bab^{-1} on joko a tai a^3, sillä $|e| = 1$ ja $|a^2| = 2$. Jos $bab^{-1} = a$, niin $ba = ab$, jolloin G olisi Abelin ryhmä, mikä on vastoin oletusta. Siten $bab^{-1} = a^3$ ja tutkitaan seuraavaksi, mitä alkio b^2 on. Jos $b^2 = a^i b$, niin $b = a^i \in \langle a \rangle$, mikä on ristiriita. Näin ollen $b^2 \in \langle a \rangle$. Jos $b^2 = a$, niin $b^2 b = ab$ ja $bb^2 = ab$. Siten $ba = ab$ ja G olisi Abelin ryhmä, mikä on vastoin oletusta. Vastaavasti $b^2 \neq a^3$. Nyt jos $b^2 = e$, niin ryhmälle G alkioille on voimassa

$$|a| = 4, |b| = 2, ba = a^{-1}b,$$

joten ryhmä G on Lauseen 6.16 mukainen ryhmä, kun $n = 4$, ja siten $G \cong D_4$. Jos taas $b^2 = a^2$, niin ryhmän G alkioille on voimassa

$$|a| = 4, b^2 = a^2, ba = a^{-1}b,$$

joten ryhmä G on Lauseen 6.12 mukainen ryhmä, jolle $n = 2$. Näin ollen $G \cong Q$. □

Ennen kertalukua 12 olevien ryhmien luokittelua esitetään kaksi aputulosta.

Lemma 8.8. *Olkoon G ryhmä, jonka kertaluku on 12. Olkoon H ryhmän G Sylowin 2-ryhmä ja K Sylowin 3-ryhmä. Tällöin ainakin toinen ryhmistä H tai K on normaali aliryhmä.*

Todistus. [1], s.209. Lauseen 7.26 nojalla Sylowin 3-ryhmiä on joko 1 tai 4 kappaletta. Jos niitä on 1, niin tällöin Seurauksen 7.25 nojalla K on normaali aliryhmä. Oletetaan, että Sylowin 3-ryhmiä on 4 kappaletta K_1, K_2, K_3 ja K_4. Jokaisen Sylowin 3-ryhmän kertaluku on 3. Jos $K_i \neq K_j$, niin leikkaus $K_i \cap K_j$ koostuu vain neutraalialkiosta e Lauseen 4.31 nojalla. Näin ollen joukoissa K_1, K_2, K_3 ja K_4 on yhteensä 9 alkiota. Toisaalta Sylowin 2-ryhmän H kertaluku on 4. Jälleen Lauseen 4.31 nojalla $H \cap K_i = \langle e \rangle$ kaikilla $i = 1, 2, 3, 4$, joten H on joukko

$$H = (G \setminus (K_1 \cup K_2 \cup K_3 \cup K_4)) \cup \langle e \rangle .$$

Näin ollen ryhmällä G on vain yksi Sylowin 2-ryhmä, joten H on Seurauksen 7.25 nojalla normaali aliryhmä. □

Huomautus 8.9. Luvussa 6 esitetyt 12-alkioiset ryhmät A_4, D_6 ja T_3 eivät ole isomorfisia keskenään Lemman 4.12 nojalla. Ryhmissä D_6 ja T_3 on alkio, jonka kertaluku on 6 (r ja a), kun taas ryhmässä A_4 sellaista ei ole. Ryhmä D_6 ei sisällä kertaluvun 4 alkiota, kun taas ryhmässä T_3 on alkio b, jonka kertaluku on 4.

Lause 8.10. *Olkoon G ryhmä, jonka kertaluku on 12. Tällöin ryhmä G on isomorfinen, jonkin ryhmän $\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, A_4, D_6 tai T_3 kanssa.*

Todistus. [1], s.209, [5], s.98. Olkoon G ryhmä, jonka kertaluku on 12. Jos G on Abelin ryhmä, niin Lauseen 5.11 nojalla G on isomorfinen joko ryhmän $\mathbb{Z}_{12}, \mathbb{Z}_4 \times \mathbb{Z}_3, \mathbb{Z}_2 \times \mathbb{Z}_6$ tai ryhmän $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ kanssa. Lauseen 5.12 nojalla kuitenkin $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ ja $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$. Oletetaan seuraavaksi, että G ei ole Abelin ryhmä.
Olkoon H ryhmän G Sylowin 2-ryhmä ja K Sylowin 3-ryhmä. Nyt Lemman 8.8 nojalla joko H tai K on normaali aliryhmä. Olkoon H normaali aliryhmä. Lemman 8.8 todistuksen nojalla voidaan olettaa, että ryhmällä G on 4 Sylowin 3-ryhmää. Olkoon $S = \{K_1, K_2, K_3, K_4\}$ Sylowin 3-ryhmien muodostama joukko. Nyt $|K_i| = 3$ ja $[G : K_i] = 4$ kaikilla $i \in 1, 2, 3, 4$. Lauseen 7.3 nojalla on olemassa homomorfismi $f : G \to S_4$ ($A(S) = S_4$),

jonka ydin $Ker\ f$ kuuluu ryhmään K_i. Koska Lauseen 4.31 nojalla ryhmän ytimen kertaluku jakaa ryhmän K_i kertaluvun, ja $|K_i| = 3$, niin $Ker\ f = \langle e \rangle$ tai $Ker\ f = K_i$. Jos $Ker\ f = K_i$, niin K_i on normaali aliryhmä Lemman 4.23 nojalla ja siten Seurauksen 7.25 nojalla K_i on ainoa Sylowin 3-ryhmä, mikä on vastoin oletusta. Näin ollen $Ker\ f = \langle e \rangle$ ja Lemman 2.10 nojalla f on injektio, ja siten Lemman 2.8 nojalla G on isomorfinen ryhmän S_4 12 alkioisen aliryhmän kanssa. Näin ollen Huomautuksen 6.10 nojalla $G \cong A_4$.
Oletetaan seuraavaksi, että K on normaali aliryhmä. Seurauksen 7.25 nojalla Sylowin 3-ryhmiä on vain yksi. Näin ollen ryhmä G sisältää vain kaksi alkiota, joiden kertaluku on 3. Olkoon c toinen näistä alkioista. Nyt alkion c keskittäjän $C_G(c)$ indeksi $[G : C_G(c)] = 1$ tai 2, sillä Lauseen 7.14 nojalla $[G : C_G(c)]$ alkion c konjugaattien määrä, ja alkion c jokaisen konjugaatin kertaluku on 3. Näin ollen $|C_G(c)| = 12$ tai 6. Molemmissa tapauksissa Seurauksen 7.17 nojalla on olemassa alkio $d \in C_G(c)$, siten että $|d| = 2$. Nyt keskittäjän $C_G(c)$ määritelmän nojalla $cd = dc$ joten alkion cd kertaluku $|cd| = 6$, sillä $(cd)^6 = c^6d^6 = (c^2)^3(d^3)^2 = e^3e^2 = e$.
Olkoon $a = cd$, jolloin siis $|a| = 6$. Nyt alkio a virittää syklisen ryhmän $\langle a \rangle$, jonka kertaluku on 6 ja siten $[G : \langle a \rangle] = 2$. Näin ollen $\langle a \rangle$ on normaali aliryhmä Lauseen 4.24 nojalla. Olkoon $b \in G$ siten että $b \notin \langle a \rangle$. Näin ollen ryhmä G voidaan kirjoittaa muodossa $G = \{e, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$, missä alkiot ovat pareittain erilliset, sillä $|a| = 6$ ja $a^i = a^jb$ johtaa tilanteeseen $b = a^{i-j} \in \langle a \rangle$, mikä on vastoin oletusta. Koska $\langle a \rangle$ on normaali aliryhmä, niin Lemman 4.25 nojalla $bab^{-1} \in \langle a \rangle$, ja vastaavasti kuin Lauseen 8.7 todistuksessa nähdään, että $|bab^{-1}| = 6$. Nyt $bab^{-1} = a$ tai a^5, sillä $|a^2| = 3$, $|a^3| = 2$ ja $|a^4| = 3$. Vaihtoehdosta $bab^{-1} = a$ seuraa, että $ba = ab$, jolloin G olisi Abelin ryhmä, mikä on vastoin oletusta. Näin ollen on $bab^{-1} = a^5 = a^{-1}$, mistä seuraa $ba = a^{-1}b$. Nyt vastaavasti kuin Lauseen 8.7 todistuksessa saadaan $b^2 \in \langle a \rangle$. Jos $b^2 = a^2$, niin yhtälöstä $ba = a^{-1}b$ seuraa

$$a^2 = b^2 = ba^{-1}b = a^5,$$

mikä on ristiriita. Vastaavasti jos $b^2 = a^4$ niin yhtälöistä $ba = a^{-1}b$ seuraa

$$a^4 = b^2 = ba^{-1}b = a^5,$$

joka on myös ristiriita. Vaihtoehdoista $b^2 = a$ ja $b^2 = a^5$ seuraa, että $|b| = 12$, ja G olisi Abelin ryhmä, mikä on ristiriita. Nyt joko $b^2 = e$ tai $b^2 = a^3$.
Olkoon $b^2 = e$. Tällöin ryhmän G alkioille a ja b on voimassa

$$|a| = 6, b^2 = e, ba = a^{-1}b.$$

Nyt G on Lauseen 6.16 mukainen ryhmä kun $n = 6$, ja siten $G \cong D_6$.
Olkoon nyt $b^2 = a^3$. Tällöin ryhmän G alkioille a ja b on voimassa

$$|a| = 6, b^2 = a^3, ba = a^{-1}b.$$

Tällöin G on Lauseen 6.12 mukainen ryhmä, kun $n = 3$, ja siten $G \cong T_3$. $\square$

Olemme saaneet luokiteltua isomorfian mukaisesti kaikki ne ryhmät, joiden kertaluku on alle 16. Kertalukua 16 olevia Abelin ryhmiä on viisi $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ja $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Ei Abelisia kertaluvun 16 ryhmiä on yhdeksän kappaletta SD_8, $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$, D_8, T_4, $D_8 \times \mathbb{Z}_2$, $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_4$, $Q \times \mathbb{Z}_2$, $Q \rtimes \mathbb{Z}_2$ ja $\mathbb{Z}_4 \rtimes \mathbb{Z}_4$. Lisää kertalukua 16 olevista ryhmistä voi lukea lähteestä [14].
Esittelemme vielä yhden luokittelulauseen, joka on todistettavissa saamillamme tuloksilla. Tällä ei kuitenkaan ole sovellusta alle 16 alkioisissa ryhmissä.

Lause 8.11. *Olkoon p ja q alkulukuja, siten että $q \not\equiv 1 (mod\ p)$ ja $p^2 \not\equiv 1 (mod\ q)$. Jos G on ryhmä, jonka kertaluku on p^2q, niin tällöin G on isomorfinen joko ryhmän $\mathbb{Z}_{p^2q}$ tai ryhmän $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$ kanssa.*

Todistus. [4], s.313. Sylowin kolmannen lauseen nojalla ryhmän G Sylowin p-ryhmien määrä on kongruentti 1 modulo p, ja se jakaa ryhmän G kertaluvun. Koska ryhmän G kertaluvun jakajat ovat $1, p, p^2, q, pq$ ja p^2q, niin Sylowin p-ryhmien määrä on joko 1 tai q. Kuitenkin Sylowin p-ryhmiä ei voi olla q kappaletta, sillä oletuksen nojalla $q \not\equiv 1 (\mathrm{mod}\ p)$. Siten on olemassa vain 1 Sylowin p-ryhmä H, joka on Seurauksen 7.25 nojalla normaali aliryhmä. Vastaavasti voidaan oletuksen $p^2 \not\equiv 1 (\mathrm{mod}\ q)$ nojalla todeta, että ryhmällä G ei ole kuin 1 normaali aliryhmä Sylowin q-ryhmä K. Lauseen 4.31 nojalla aliryhmän $H \cap K$ kertaluvun täytyy jakaa sekä ryhmän H kertaluvun p^2 että ryhmän K kertaluvun q. Näin ollen $H \cap K = \langle e \rangle$. Edelleen Lemman 4.36 nojalla $G = HK$. Näin ollen Lauseen 5.2 nojalla $G = H \times K$. Lauseen 8.5 nojalla H on isomorfinen joko ryhmän $\mathbb{Z}_{p^2}$ tai ryhmän $\mathbb{Z}_p \times \mathbb{Z}_p$ kanssa, ja Lauseen 8.1 nojalla K on isomorfinen ryhmän $\mathbb{Z}_q$ kanssa. Nyt Lauseen 5.12 nojalla $G = H \times K \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_q \cong \mathbb{Z}_{p^2q}$ tai $G = H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$. $\square$

Näin saamme esimerkiksi ryhmälle G_{45} $(45 = 3^2 \cdot 5)$ seuraavat isomorfiat, $G_{45} \cong \mathbb{Z}_{3^2 \cdot 5}$ tai $G_{45} \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

Lähteet

[1] Artin, Michael. *Algebra*, Englewood Cliffs, N.J. : Prentice Hall, 1991.

[2] Bhattacharya, P. B., Nagpaul, S. R., & Jain, S. K. (1994). *Basic Abstract Algebra: Vol. 2nd ed.* Cambridge University Press.

[3] Conrad, Keith. *No subgroup of A_4 has index 2.* Haettu osoitteesta https://kconrad.math.uconn.edu/blurbs/grouptheory/A4noindex2.pdf

[4] Hungerford, Thomas W. *Abstract Algebra An introduction, 3ed.* BROOKS/COLE CENGAGE Learning, Boston USA, 2013.

[5] Hungerford, Thomas W. *Algebra.* Springer-Verlarg. New York. 1989.

[6] Häsä Jokke & Rämö Johanna. *Johdatus abstraktiin algebraan.* Gaudeamus Helsinki University Press. 2012.

[7] Judson, Thomas W. *Abstract Algebra Theory and Applications.* Stephen F. Austin State University. 2013.

[8] Kirtland, Joseph. *Complementation of Normal Subgroups : In Finite Groups.* De Gruyter, Berlin, 2017.

[9] McCoy, Neal H., Janusz, Gerarld J. *Introduction to abstract algebra*, 6th edition, Harcourt/Academic Press. 2001.

[10] Robinson, Derek John Scott. *Abstract Algebra : An Introduction with Applications.* 2003.

[11] Roman, Steven, *Fundamentals of Group Theory: An Advanced Approach.* Birkhäuser Basel. 2012.

[12] Rosen, Kenneth H. *Elemetary Number Theory*, 6th edition, Pearson, 2011.

[13] Thompson, Gerard, *Classifying Groups of Small Order.* Advances in Pure Mathematics, 6, 58-65. doi: 10.4236/apm.2016.62007.

[14] Wild, Marcel. *The Groups of Order Sixteen Made Easy.* The American Mathematical Monthly. 112. 20-31. 2005. 10.2307/30037381.

[15] Wilson, James. *Hungerford's Algebra Solutions Manual*, 2010. Haettu osoitteesta http://site.iugaza.edu.ps/mashker/files/2010/02/solmanual-hungeford.pdf