JYVÄSKYLÄN YLIOPISTO
MATEMATIIKAN JA TILASTO-
TIETEEN LAITOS

Pro gradu-sivututkielma

Äärellisten ryhmien luokittelusta

Elina Aittoniemi

6. huhtikuuta 2024

Tekijä
Elina Aittoniemi

Otsikko
Äärellisten ryhmien luokittelusta (engl. On the classification of finite groups)

Tutkinto-ohjelma
Luokanopettajan maisteriohjelma

Päivämäärä	**Sivumäärä**
6. huhtikuuta 2024	39

Tiivistelmä

Tämän sivututkielman tarkoituksena on luokitella äärellisiä ryhmiä isomorfialla kertalukuun 21 saakka. Luokittelussa hyödynnetään muun muassa Lagrangen ja Cauchyn lauseita sekä myöhemmin Sylowin lauseita. Nämä antavat pohjaa ryhmien rakenteiden hahmottamiseen.

Ensimmäiseksi työssä käydään läpi ryhmäteorialle ominaisia määritelmiä ja käsitteitä sekä Lagrangen lause ja isomorfia. Tämän jälkeen esitellään ryhmäperheet, joiden yhteydessä käydään läpi esimerkiksi kertaluvultaan alkuluvullisen ryhmän luokittelu sekä erikoistapauksen 8 käsittely.

Tämän jälkeen perehdytään ryhmän toimintaan, rataan, stabiloijaan sekä rata-stabiloijalauseeseen konjugaation näkökulmasta. Käydään läpi luokkayhtälö, keskus ja keskittäjä sekä Cauchyn lause, joiden yhteydessä tarkastellaan kertalukujen tapausten p^2 ja $2p$, missä p on alkuluku, todistukset.

Viimeiseksi esitellään p-aliryhmät sekä erityisesti Sylowin lauseet ja niiden todistukset. Nämä antavat pohjaa kertalukujen erikoistapauksen 12 sekä yleisen tapauksen pq, missä p ja q ovat eri alkulukuja, tarkempaan perehtymiseen. Näiden jälkeen määritellään puolisuora tulo sekä esitellään pintapuolisesti kertaluvun erikoistapaukset $16, 18$ ja 20 viitaten niitä syvemmin käsitteleviin teoksiin. Kertaluvun tapaukset $1 - 21$ on koottu työn loppuun liitteeksi.

Sisällys

1 Johdanto

Abstrakti algebra tutkii algebrallisten kappaleiden rakennetta. Yksi abstraktin algebran osioista on *ryhmäteoria*, joka tutkii erityisesti erilaisten kappaleiden symmetrioita ja säännönmukaisuuksia esimerkiksi isomorfialla. Symmetrioiden tarkastelua hyödynnetään käytännössä muun muassa eri esineiden ja asioiden tulkinnassa tieteissä, taiteessa ja matematiikassa, kun tarkastellaan esineiden säännönmukaisuuksien ja liikkeiden erilaisia mahdollisuuksia [4, luku 3].

Kertaluvultaan pieniä tai rakenteeltaan yksinkertaisia äärellisiä ryhmiä voidaan luokitella isomorfialla Lagrangen lauseen avulla. Lauseen mukaan ryhmän aliryhmän kertaluku jakaa ryhmän kertaluvun. Lause kuitenkin olettaa aliryhmän olemassaolon, mikä rajoittaa ryhmien rakenteiden tarkastelun kertaluvultaan pieniin ryhmiin. Sen sijaan Sylowin lauseilla voidaan ryhmän kertaluvun ominaisuuksilla todeta ryhmällä olevan olemassa aliryhmiä, joiden lukumäärä saadaan tarkastelemalla kertaluvun muodostavia alkulukuja. Sylowin lauseilla saadaan laajennettua ryhmien rakenteiden tarkastelu monimutkaisempiin ja kertaluvultaan hieman suurempiin tapauksiin.

Tässä työssä tarkastellaan kertaluvultaan $1-21$ olevien ryhmien luokittelua Sylowin lauseilla ja ilman. Ryhmät luokitellaan eri ryhmäperheiden mukaan, mitkä esitellään työn edetessä. Tapaukset, joissa hyödynnetään esimerkiksi Lagrangen ja Cauchyn lausetta ryhmien luokittelussa esitellään ennen lukua 5 sitä mukaan, kuinka paljon eri tietoja luokittelussa tarvitaan. Tämän jälkeen luokitteluissa hyödynnetään myös Sylowin lauseita. Työn loppuun liitteeseen on koottu kertaluvultaan $1-21$ olevien ryhmien yleiset tai erikoistapaukset, ja viitattu lauseisiin, jotka todistavat ryhmien luokittelut isomorfialla. Tapaukset $n = 16, n = 18$ ja $n = 20$ on jätetty käsittelemättä tarkemmin, sillä niiden tarkastelu vaatii tästä työstä poikkeavia välineitä. Nämä kolme tapausta on esitelty luvussa 5.3. Lukijalta odotetaan joukkoopin, abstraktin algebran ja ryhmäteorian perusteiden hallintaa.

Merkintöjä

$\mathbb{Z}$	Kokonaislukujen joukko
$x \in G$	x on joukon/ryhmän G alkio
x^{-1}	Alkion x käänteisalkio
$x \mid y, x \nmid y$	Luku x jakaa luvun y, ei jaa lukua y
$x \equiv y \pmod{n}$	x ja y ovat kongruentit modulo n
$\ker(\varphi)$	Homomorfismin φ ydin
$\lvert x\rvert, \lvert G\rvert$	Alkion x, ryhmän G kertaluku
$G \cong G'$	Ryhmät G ja G' ovat isomorfiset
$G_1 \cup G_2$	Ryhmien/joukkojen G_1 ja G_2 yhdiste
$G_1 \cap G_2$	Ryhmien/joukkojen G_1 ja G_2 leikkaus
$H \subseteq G, H \subset G$	H on ryhmän G (aito) aliryhmä
$H \trianglelefteq G, G \triangleleft G$	H on ryhmän G (aito) normaali aliryhmä
G/H	Ryhmän G tekijäryhmä
$[G : H]$	Ryhmän G aliryhmän H indeksi
n_p	Sylowin p-aliryhmien lukumäärä
HK	Ryhmien H ja K tulo
$H \times K$	Ryhmien H ja K suora tulo
$H \rtimes K$	Ryhmien H ja K puolisuora tulo, missä H on normaali
$\langle x \rangle$	Alkion x virittämä ryhmä, jonka kertaluku on $\lvert x\rvert$
C_n	Syklinen ryhmä, jonka kertaluku on n
D_n	Dihedraaliryhmä, jonka kertaluku on $2n$
S_X, S_n	Kaikkien joukon X permutaatioiden joukko, Symmetrinen ryhmä, jonka kertaluku on $n!$
A_n	Alternoiva ryhmä, jonka kertaluku on $\frac{n!}{2}$
Dic_n	Disyklinen ryhmä, jonka kertaluku on $4n$
Q_8	Kvaternioryhmä, jonka kertaluku on 8
$G(x)$	Alkion $x \in G$ rata
G_x	Alkion $x \in G$ stabiloija
$C(x)$	Alkion x konjugaattiluokka
$N_G(H)$	Ryhmän G aliryhmän H normalisoija
$Z(G)$	Ryhmän G keskus

2 Ryhmä ja homomorfismi

Tässä kappaleessa tutustutaan ryhmäteorian perusteisiin. Esitellään siten alussa ryhmäteorialle ominaisia esitietoja, joita hyödynnetään tämän jälkeisissä ryhmän määritelmissä ja ominaisuuksissa. Ryhmän määritelmien ja ominaisuuksien ohella esitellään esimerkiksi (normaali) aliryhmä, sivuluokat sekä Lagrangen lause. Näiden jälkeen jatketaan homomorfismin, isomorfismin ja ytimen tarkasteluun.

2.1 Esitiedot

Tässä alaluvussa tutustutaan muutamiin ryhmäteorian esitietoihin eli muutamiin käsitteisiin ja merkintöihin. Tämän alaluvun teoria perustuu lähteisiin [4, luku 8.3], [6, luku 0] ja [9, luku 1].

Määritelmä 2.1. Joukkoa X kutsutaan *epätyhjäksi*, jos sillä on ainakin yksi alkio.
Joukkoa X kutsutaan *äärelliseksi*, jos alkioiden lukumäärä voidaan ilmaista kokonaisluvulla $\mathbb{Z}$.

Vastaavat termit pätevät myös ryhmälle. Alkioiden lukumäärää kutsutaan tällöin kertaluvuksi, ja se esitellään luvussa 2.2. Jatkossa joukon alkioiden lukumäärää ei erotella ryhmän kertaluvun merkinnästä.

Määritelmä 2.2. Kuvausta $* : G \times G \to G$ kutsutaan epätyhjän joukon G *laskutoimitukseksi*

Laskutoimitus kuvaa jonkin ryhmän $G \times G$ alkioparin joksikin muuksi ryhmän G alkioksi. Kirjallisuudessa tähän viitataan multiplikatiivisena laskutoimituksena. Usein laskutoimitukseen $x * y$ viitataan yksinkertaisemmin merkinnällä xy. Tästä eteenpäin laskutoimituksen merkintää $*$ käytetään vain tarvittaessa.

Määritelmä 2.3. Ekvivalenssiluokkaa

$$[a] = \{a + kn : k \in \mathbb{Z}\}$$

kutsutaan alkion a *jäännösluokaksi* modulo n.
Kaksi alkiota x ja y ovat *kongruentit*, jos ne ovat samassa jäännösluokassa.

Jäännösluokat ovat erillisiä ja niiden yhdiste on kokonaislukujen joukko $\mathbb{Z}$. Jäännösluokkien joukkoon modulo n viitattaessa käytetään merkintää

$$\mathbb{Z}/n\mathbb{Z} = \{[a] : a \in \mathbb{Z}\}.$$

Huomioitavaa on, että tekijäryhmät muodostetaan jäännösluokkien ja laskutoimituksen avulla. Tekijäryhmät esitellään luvussa 2.2.

Määritelmä 2.4. Epätyhjän joukon X *permutaatio* järjestää joukon alkiot uudelleen eli on bijektio $\sigma : X \to X$ joukolta itselleen. Joukon X kaikkien permutaatioiden joukkoon viitataan merkinnällä S_X.

Permutaatioiden joukkoon S_X viitataan myöhemmin nimikkeellä *symmetrinen ryhmä* (merkintä S_n). Siihen tutustutaan tarkemmin kappaleessa 3.4.

2.2 Ryhmä ja aliryhmä

Määritellään sekä ryhmä ja aliryhmä että normaali aliryhmä ja tekijäryhmä. Esitellään lopussa Lagrangen lause, jota hyödynnetään paljon äärellisten ryhmien luokittelussa. Tämän alaluvun tiedot perustuvat pääasiassa Armstrongin [1] lukuihin 2 ja 15 sekä Dummit ja Footen [6] lukuihin 0, 2.1, 3.1 ja 3.2.

Määritelmä 2.5. Paria $(G, *)$, missä $|G| \geq 0$, kutsutaan *ryhmäksi*, jos seuraavat aksioomat pätevät:

1. laskutoimitus on *assosiatiivinen* eli kaikille alkioille $x, y, z \in G$ pätee $(x * y) * z = x * (y * z)$,
2. ryhmällä G on olemassa yksikäsitteinen *neutraalialkio* $e \in G$ eli alkio, jolle pätee $e * x = x = x * e$ kaikille $x \in G$, ja
3. jokaisella alkiolla $x \in G$ on olemassa yksikäsitteinen *käänteisalkio* $x^{-1} \in G$, jolle pätee $x * x^{-1} = e = x^{-1} * x$.

Ryhmän G alkioiden lukumäärää kutsutaan ryhmän *kertaluvuksi*, jonka merkintä on $|G|$.

Ryhmää, jonka laskutoimitus on *kommutatiivinen* eli jonka alkioille pätee $yx = xy$ (tai toisin kirjoitettuna $yxy^{-1} = x$) kaikille $x, y \in G$, kutsutaan kommutatiiviseksi (tai Abelin) ryhmäksi.

Propositio 2.6. *Olkoon G ryhmä ja $x, y \in G$ joitakin alkioita. Tällöin pätee*

1. $(x^{-1})^{-1} = x$, *ja*
2. $(xy)^{-1} = y^{-1}x^{-1}$.

Todistus. [6, s. 18 propositio 1] □

Määritelmä 2.7. Ryhmä G on *triviaali*, jos se sisältää vain neutraalialkion e. Triviaalin ryhmän G kertaluku $|G| = 1$.
Kahden ryhmän H ja K, joiden ainoa yhteinen alkio on neutraalialkio e, leikkausta $H \cap K = \{e\}$ kutsutaan *triviaaliksi leikkaukseksi*.

Määritelmä 2.8. Olkoon G ryhmä ja x, y ryhmän G alkioita. Ryhmän G osajoukko $H \subseteq G$ on ryhmän G *aliryhmä*, jos pätee

1. H on epätyhjä,
2. $x^{-1} \in H$, kun $x \in H$, ja
3. $xy \in H$, kun $x, y \in H$.

Lemma 2.9. *Olkoon G ryhmä, jonka kaikkien neutraalialkiosta poikkeavien alkioiden kertaluku on 2. Tällöin G on kommutatiivinen.*

Todistus. Olkoot $x, y \in G$, missä $x \neq y$, ja $|x| = |y| = 2$, jolloin $x = x^{-1}$ ja $y = y^{-1}$. Koska myös $xy \in G$, niin $|xy| = 2$ ja propositiota 2.6 hyödyntäen saadaan $yx = y^{-1}x^{-1} = (xy)^{-1} = xy$. Siispä $xy = yx$ pätee kaikille alkioille $x, y \in G$ ja siten G on kommutatiivinen. □

Määritelmä 2.10. Olkoot $H \subseteq G$ ryhmän G aliryhmä ja $g \in G$.
Joukkoa

$$gH = \{gh : h \in H\}$$

kutsutaan aliryhmän H *vasemmaksi sivuluokaksi* ja joukkoa

$$Hg = \{hg : h \in H\}$$

oikeaksi sivuluokaksi ryhmässä G.

Määritelmä 2.11. Olkoon G ryhmä ja $g, h \in G$. Kuvausta $l_g : G \to G$, $l_g(h) = gh$ kutsutaan *vasemmaksi siirroksi*.

Lause 2.12. *Vasen siirto l_g on bijektio.*

Todistus. Olkoot G ryhmä ja $g, g_1, g_2 \in G$. Kuvaus $l_g : G \to G$ on surjektio, sillä kaikille $h \in G$ pätee $l_g(g^{-1}h) = gg^{-1}h = h$.
Jos $l_g(g_1) = l_g(g_2)$, niin $gg_1 = l_g(g_1) = l_g(g_2) = gg_2$ ja l_g on injektio. □

Määritelmä 2.13. Ryhmän G aliryhmä H on *normaali* (merkitään $H \trianglelefteq G$), jos kaikille $x \in G$ pätee $xHx^{-1} = H$ (tai $xH = Hx$).

Määritelmä 2.14. Olkoon H ryhmän G aliryhmä. Määritellään aliryhmän H *vasempien sivuluokkien joukko*

$$G/H = \{xH : x \in G\}.$$

Lause 2.15. *Olkoon H ryhmän G normaali aliryhmä. Kun joukko G/H varustetaan laskutoimituksella asettamalla*

$$(xH)(yH) = (xy)H,$$

niin joukko G/H on ryhmä ja sitä kutsutaan ryhmän G tekijäryhmäksi.

Todistus. [6, s. 77, lause 3] □

Lause 2.16 (Lagrangen lause)**.** *Äärellisen ryhmän G aliryhmän kertaluku jakaa ryhmän G kertaluvun.*

Todistus. [6, s. 89 lause 8] □

Lagrangen lauseen yhteydessä usein puhutaan, että ryhmän G alkion kertaluku jakaa ryhmän G kertaluvun. Tämä on seuraus siitä, että ryhmän G alkio x virittää ryhmän G syklisen aliryhmän $\langle x \rangle$, jonka kertaluku on yhtä suuri alkion x kertaluvun kanssa (syklinen ryhmä käydään tarkemmin läpi seuraavassa luvussa 3.1). Ks. [2, s. 57 seuraus 2.8.10].

Määritelmä 2.17. Määritellään ryhmän G aliryhmien H ja K tulo:

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

Seuraus 2.18. *Ryhmä HK on ryhmän G aliryhmä, jos aliryhmä H tai K on normaali.*

Todistus. [6, s. 94 seuraus 15] □

Propositio 2.19. *Olkoon H ja K ryhmän G äärellisiä aliryhmä. Tällöin saadaan*

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

Todistus. [6, s. 93 propositio 13] □

Määritelmä 2.20. Aliryhmän H *indeksi*

$$[G : H] = \frac{|G|}{|H|}$$

ilmaisee aliryhmän H sivuluokkien lukumäärän ryhmässä G.

Aliryhmän H indeksi ilmaisee tekijäryhmän G/H koon, eli $|G/H| = [G : H]$.

2.3 Homomorfismi

Tässä kappaleessa esitellään homomorfismi ja automorfismi sekä erityisesti ryhmien luokittelussa olennaisesti hyödynnettävä isomorfismi. Lisäksi käydään läpi homomorfismin ydin, jota hyödynnetään esimerkiksi kertaluvun tapauksen 12 todistuksessa. Tämän kappaleen määritelmät ja tulokset perustuvat pääasiassa Armstrongin [1] lukuihin 7, 8, 16 ja 23 sekä Rotmanin [9] lukuihin 1 ja 3.

Määritelmä 2.21. Olkoot $(G, *)$ ja $(H, \circ)$ ryhmiä varustettuna vastaavilla laskutoimituksilla. Kuvaus $\varphi : G \to H$ on *homomorfismi*, jos kaikille $x, y \in G$ pätee

$$\varphi(x * y) = \varphi(x) \circ \varphi(y)$$

Kuvaus φ on *isomorfinen* ja ryhmä G tällöin *isomorfinen* ryhmän H kanssa (merkitään $G \cong H$), jos on olemassa bijektiivinen homomorfismi φ.

Isomorfista kuvausta $\varphi : G \to G$ ryhmältä G itselleen kutsutaan *automorfismiksi*.

Lause 2.22. *Olkoot $\varphi : G \to H$ homomorfismi, $x \in G$ jokin alkio sekä $e_G \in G$ ja $e_H \in H$ neutraalialkioita. Tällöin pätee*

1. $\varphi(e_G) = e_H$, *ja*

2. $\varphi(x^n) = \varphi(x)^n$ *jollekin* $n \in \mathbb{Z}$.

Todistus. [9, s. 17 lause 1.13] □

Määritelmä 2.23. Homomorfismin φ *ytimeksi* $\ker(\varphi)$ kutsutaan ryhmän G sellaisten alkioiden joukkoa, jossa alkiot kuvautuvat neutraalialkioksi, eli

$$\ker(\varphi) = \{x \in G : \varphi(x) = e\}.$$

Propositio 2.24. *Homomorfismi* φ *on injektio jos ja vain jos* $\ker(\varphi) = \{e\}$.

Todistus. Injektiiviselle φ vain neutraalialkio e kuvautuu itsekseen lausetta 2.22 mukaillen, jolloin ydin $\ker(\varphi) = \{e\}$ on triviaali.

Oletetaan siten, että $\ker(\varphi)$ on triviaali ja että $x, y \in G$. Jos $\varphi(x) = \varphi(y)$, niin saadaan

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(x)^{-1} = e$$

kuvauksen homomorfisuuden ja lauseen 2.22 nojalla. Siten $xy^{-1} \in \ker(\varphi)$ ja $xy^{-1} = e$, josta edelleen $x = y$. Siten φ on injektio. □

3 Ryhmäperheet

Tässä kappaleessa esitellään ryhmäteorialle tyypillisimmät ryhmäperheet: syklinen ryhmä C_n, dihedraaliryhmä D_n, symmetrinen ja alternoiva ryhmä S_n ja A_n sekä disyklinen ja kvaternioryhmä Dic_n ja Q_8. Esitellään ryhmäperheiden yhteydessä myös ryhmien suora tulo.

3.1 Syklinen ryhmä

Esitellään tämän kappaleen alussa syklisen ryhmän määritelmä ja sille tyypillisimpiä ominaisuuksia. Todistetaan kertaluvultaan alkuluvullisen ryhmän syklisyys. Tämän alaluvun tiedot perustuvat pääosin Armstrongin [1] lukuihin 5, 11 ja 15, Carterin [4] lukuun 5.1.

Määritelmä 3.1. Olkoon $x \in G$ alkio, jonka kertaluku on n ja joka virittää ryhmän $G = \langle x \rangle = \{x^n = e, x, x^2, \ldots, x^{n-1}\}$. Tällöin G on syklinen ja sen kertaluku $|C_n| = n$.

Syklisiin ryhmiin viitattaessa käytetään joko jäännösluokan merkintää $\mathbb{Z}/n\mathbb{Z}$ (tai lyhyemmin $\mathbb{Z}_n$) tai merkintää C_n. Edeltävä merkintä johtuu siitä, että sykliset ryhmät ovat isomorfisia jäännösluokkien kanssa ja niiden laskutoimitus kytkeytyy modulaariaritmetiikkaan. Tässä työssä syklisistä ryhmistä käytetään merkintää C_n, missä n viittaa ryhmän virittävän alkion kertalukuun.

Lemma 3.2. *Syklinen ryhmä C_n on kommutatiivinen.*

Todistus. Olkoon G alkion x virittämä syklinen ryhmä $G = \langle x \rangle$. Tällöin mille tahansa $x^i, x^j \in G$ pätee $x^i x^j = x^{i+j} = x^{j+i} = x^j x^i$, jolloin G on kommutatiivinen. □

Lause 3.3 (Tapaus $n = p$)**.** *Olkoon G ryhmä, jonka kertaluku on alkuluku p. Tällöin G on syklinen ryhmä.*

Todistus. Olkoon $x \in G$ neutraalialkiosta poikkeava alkio. Lagrangen lauseen 2.16 nojalla ryhmän G kertaluku on jaollinen alkion x kertaluvulla eli alkuluvulla p. Koska $x \neq e$, niin täytyy olla $|x| = p$. Tällöin alkio x virittää koko ryhmän G, jolloin G on syklinen. Siispä $G = \langle x \rangle \cong C_p$. □

Lause 3.4. *Jos ryhmän G aliryhmän H indeksi $[G : H] = 2$, niin H on normaali ja $G/H \cong C_2$.*

Todistus. Osoitetaan ensin, että H on normaali. Selvästi $xH = Hx$ ja H on normaali määritelmän 2.13 nojalla, kun $x \in H$, sillä aliryhmän H sivuluokkien lukumäärä on indeksi $[G : H] = 2$. Oletetaan siis, että $x \notin H$.
Sivuluokat H ja xH muodostavat ryhmän G osituksen, mutta toisaalta H ja Hx ovat ryhmän G osituksia. Siispä täytyy olla $xH = Hx$, jolloin H on normaali.

Koska lauseen 3.3 nojalla ryhmä, jonka kertaluku on alkuluku p, on isomorfinen syklisen ryhmän C_p kanssa, niin pätee myös $G/H \cong C_2$. □

3.2 Ryhmien suora tulo

Käydään läpi ryhmien suoran tulon määritelmä sekä muutamia ryhmien luokittelun todistuksissa käytettäviä tuloksia, kuten Äärellisten kommutatiivisten ryhmien peruslause. Tämän alaluvun tiedot perustuvat Carterin [4] lukuun 8.5 sekä Dummit ja Footen [6] lukuihin 5.1 ja 5.2.

Määritelmä 3.5. Olkoot $G_1, \ldots, C_n$ ryhmiä, joiden vastaavia laskutoimituksia merkitään $*_1, \ldots, *_n$, ja olkoot $x_i, y_i \in G_i$ joitakin alkioita. Joukkoa $G_1 \times \cdots \times G_n$ kutsutaan ryhmien *suoraksi tuloksi*, jossa laskutoimitus

$$(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 *_1 y_1, \ldots, x_n *_n y_n).$$

Propositio 3.6. *Ryhmien $G_1, \ldots, G_n$ suora tulo $G_1 \times \cdots \times G_n$ on ryhmä, jonka kertaluku on $|G_1| \cdots |G_n|$.*

Todistus. [6, s. 153, propositio 1] □

Lause 3.7 (Äärellisten kommutatiivisten ryhmien peruslause)**.** *Jokainen äärellinen kommutatiivinen ryhmä G on isomorfinen syklisten ryhmien suoran tulon kanssa. Siten on olemassa lista kokonaislukuja $n_1, \ldots, n_m \in \mathbb{Z}$ siten, että*

$$G \cong C_{n_1} \times \cdots \times C_{n_m}.$$

Todistus. [6, s. 196-197 luku 6.1] □

Propositio 3.8. *Olkoot x ja y lukuja, joiden suurimmalle yhteiselle tekijälle pätee* $\text{syt}(x, y) = 1$. *Tällöin syklinen ryhmä C_{xy} on isomorfinen syklisten ryhmien C_x ja C_y suoran tulon kanssa.*

Todistus. [1, s. 53, Lause 10.1] □

Lause 3.9. *Olkoot $H, K \trianglelefteq G$ ryhmän G normaaleja aliryhmiä. Leikkaus $H \cap K = \{e\}$ on triviaali ja pätee $HK = G$ jos ja vain jos on olemassa isomorfismi $H \times K = G$.*

Todistus. [2, s. 65 propositio 2.11.4(d)] □

3.3 Dihedraaliryhmä

Säännöllisiä monikulmioita voidaan tarkastella kaksiulotteisessa ympäristössä, jolloin niiden symmetriat ovat kiertoja tai peilauksia. Myöhemmässä määritelmässä kiertoa merkitään alkiolla x ja peilausta alkiolla y. Tällöin $|x| = n$, missä n viittaa monitahokkaan sivujen tai kulmien lukumärään, ja $|y| = 2$. Tällöin dihedraaliryhmän kertaluvuksi saadaan $|D_n| = 2n$. Tämän alaluvun tiedot pohjautuvat Armstrongin [1] kappaleeseen 4 ja Carterin [4] kappaleeseen 5.3. Aloitetaan dihedraaliryhmien tarkastelu esimerkillä.

Esimerkki 3.10. Tarkastellaan tasasivuisen kolmion kiertoja ja peilauksia kuvan 3.1 avulla merkitsemällä kolmioiden kulmat ja tarkastelemalla, kuinka kulmien paikat muuttuvat kierron ja peilauksen myötä.

Dihedraaliryhmän alkiot voidaan kirjoittaa muotoon

$$D_3 = \{x^3 = y^2 = e, x, x^2, y, xy = yx^2, x^2y = yx\},$$

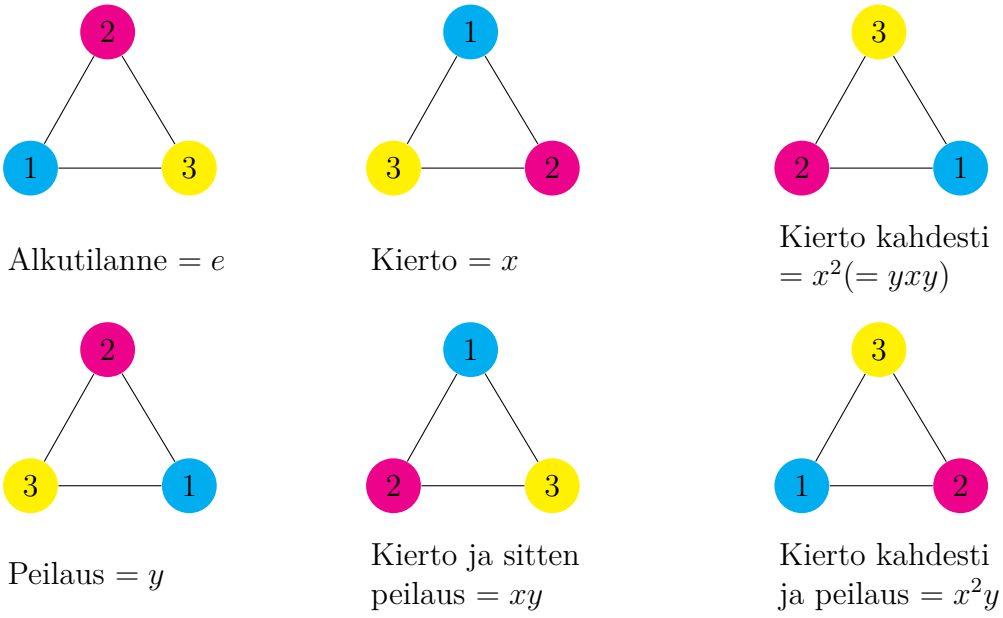
missä x viittaa kiertoon ja y peilaukseen, kuten kuvassa 3.1. Kuvasta huomataan, että tosiaan $yxy = x^2 = x^{-1}$, kuten olevassa määritelmässä 3.11.

Määritelmä 3.11. Olkoon D_n alkioiden x ja y virittämä aliryhmä, jonka kertaluku $|D_n| = 2n$. Jos sen alkioille x ja y pätee

$$x^n = e = y^2 \quad ja \quad yxy = x^{-1} = x^{n-1},$$

niin ryhmää G kutsutaan *dihedraaliryhmäksi.*

Lause 3.12. *Dihedraaliryhmä D_2 on isomorfinen Kleinin neliryhmän $C_2 \times C_2$ kanssa.*



Kuva 3.1: Dihedraaliryhmän D_3 kierrot ja peilaukset.

Todistus. Olkoot $x, y \in D_2$. Tällöin dihedraaliryhmän määritelmän 3.11 nojalla pätee $x^n = x^2 = e = y^2$ ja $(xy)^2 = x(yxy) = xx^{-1} = e$, niin lemman 2.9 nojalla D_2 on kommutatiivinen eli $D_2 = \{e, x, y, xy = yx\}$.

Koska kaikki ryhmän D_2 alkiot voidaan ilmaista alkioiden x ja y tulona, ja koska x ja y virittävät sykliset aliryhmät $\langle x \rangle$ ja $\langle y \rangle$, jotka ovat normaaleja ja isomorfisia syklisen ryhmän C_2 kanssa lauseen 3.4 nojalla, niin lauseen 3.9 nojalla $D_2 \cong \langle x \rangle \times \langle y \rangle \cong C_2 \times C_2$. □

3.4 Symmetrinen ja alternoiva ryhmä

Esitiedoissa sivuttiin symmetristen ryhmien S_n sisältävän jonkin n-alkioisen joukon kaikki permutaatioesitykset. Määritellään tässä kappaleessa ryhmä tarkemmin ja käydään läpi muutamia sille olennaisia ominaisuuksia. Tässä alaluvussa käsiteltävä aihe perustuu Armstrongin [1] lukuun 6 ja Carterin [4] lukuun 5.4.

Määritelmä 3.13. Olkoon joukon X permutaatio bijektio $\sigma : X \to X$

joukolta itselleen, ja $|X| = n$. Kaikkien joukon X alkioiden permutaatioiden joukkoa kutsutaan *symmetriseksi ryhmäksi* S_n.

Symmetrisen ryhmän S_n kertaluku on muotoa $|S_n| = n!$.

Seuraavissa tuloksissa tarkastelun apuna käytetään syklejä, joissa on kaksi alkiota. Näitä kutsutaan *2-sykleiksi.*

Lause 3.14. *2-syklit virittävät symmetrisen ryhmän S_n.*

Todistus. [1, s. 28 lause 6.1] □

Propositio 3.15. *Olkoot $\sigma \in S_n, \sigma = m_1$ ja $\sigma = m_2$, missä m_1 on 2-syklien tulo ja m_2 on 2-syklien tulo.*
Tällöin molemmissa m_1 ja m_2 2-syklejä on parillinen määrä tai molemmissa pariton määrä.

Todistus. [1, s. 28 lause 6.2 ja s. 29] □

Määritelmä 3.16. Symmetrisen ryhmän S_n permutaatiota σ kutsutaan *parilliseksi*, jos 2-syklejä on pariton määrä, tai *parittomaksi*, jos 2-syklejä on parillinen määrä.

Lause 3.17. *Symmetrisen ryhmän S_n parilliset permutaatiot muodostavat aliryhmän, alternoivan ryhmän A_n, jonka kertaluku $|A_n| = n!/2$.*

Todistus. [1, s. 29-30 lause 6.4] □

3.5 Disyklinen ryhmä

Disykliset ryhmät ovat syklisten ryhmien C_2 laajennuksia syklisillä ryhmillä C_{2n}, joiden kertaluvut vastaavasti ovat 2 ja $2n$. Disykliset ryhmät voidaan esitellä eri tavoin, joten aloitetaan disyklisten ryhmien käsittely matriisien avulla ja sitten siirrytään yleisempään määritelmään. Disyklisiä ryhmiä tarkastellessa tarkastellaan neutraalialkioa $e = 1$. Ryhmien esittelyn jälkeen käydään tapauksen $n = 8$ todistus läpi. Tämän kappaleen tiedot perustuvat osakseen Armstrongin [1] lukuun 13, Artinin [2] lukuihin 2.4 ja 7.8 sekä Dummit ja Footen [6] lukuun 1.

Määritelmä 3.18. Olkoot x ja y sellaisia alkioita, jotka virittävät ryhmän, jonka kertaluku on $4n$. Olkoot

$$x = \begin{bmatrix} \cos\frac{\pi}{n} + i\sin\frac{\pi}{n} & 0 \\ 0 & \cos\frac{\pi}{n} - i\sin\frac{\pi}{n} \end{bmatrix} \quad \text{ja} \quad y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \text{ jolloin}$$

$$x^n = y^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \text{ ja } x^{2n} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e,$$

missä $n \geq 2$. Näiden alkioiden sanotaan virittävän *disyklisen ryhmän* Dic_n.

Abstraktimmin disyklinen ryhmä määrittelemällä ryhmä, jonka kertaluku on $4n$ ja jonka virittää alkiot x ja y asettamalla

$$Dic_n = \{x, y : x^{2n} = x^n y^{-2} = xyxy^{-1} = e\}.$$

Määritelmä 3.19. *Kvaternioryhmäksi* kutsutaan ryhmää

$$Q_8 = \{\pm\,\mathbf{1}, \pm\,\mathbf{i}, \pm\,\mathbf{j}, \pm\,\mathbf{k}\}, \text{ missä}$$

$$\pm\,\mathbf{1} = \pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \pm\,\mathbf{i} = \pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \ \pm\,\mathbf{j} = \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \ \pm\,\mathbf{k} = \pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

ja missä laskutoimitus on matriisien kertolasku. Näille pätee

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{1}, \ \ \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \ \text{ ja } \ \mathbf{ki} = \mathbf{j}.$$

Huomautus 3.20. Kvaternioryhmän alkioiden $\pm\mathbf{i}$, $\pm\mathbf{j}$ ja $\pm\mathbf{k}$ kertaluku on 4 ja näistä millä tahansa kahdella alkoilla saadaan viritettyä koko kvaternioryhmä Q_8.

Lause 3.21. *Kvaternioryhmä Q_8 on isomorfinen disyklisen ryhmän Dic_2 kanssa.*

Todistus. Tarkastellaan kvaternioryhmän Q_8 alkioita disyklisen ryhmän Dic_2 tapauksessa. Todistettaessa voidaan asettaa x ja y miksi tahansa kahdeksi kvaternioryhmän alkioksi $\mathbf{i}, \mathbf{j}$ tai $\mathbf{k}$, koska määritelmän 3.19 nojalla ryhmä voidaan virittää millä tahansa kahdella alkiolla. Olkoot siten $x = \mathbf{i}$ ja $y = \mathbf{j}$,

jolloin $x^n = \mathbf{i}^2 = -\mathbf{1}$ ja $y^{-1} = \mathbf{j}^{-1} = -\mathbf{j}$ määritelmän 3.19 nojalla. Siispä saadaan

$$\begin{aligned} x^{2\cdot 2} &= \mathbf{i}^2\mathbf{i}^2 = (-\mathbf{1})(-\mathbf{1}) = \mathbf{1}, \\ x^n y^{-2} &= \mathbf{i}^2(\mathbf{j}^{-\mathbf{1}})^2 = -\mathbf{1}(-\mathbf{j})(-\mathbf{j}) = -\mathbf{1}(-\mathbf{1}) = \mathbf{1} \quad \text{ja} \\ xyxy^{-1} &= \mathbf{ijij}^{-1} = (\mathbf{ij})(\mathbf{\text{-}ij}) = \mathbf{k}(-\mathbf{k}) = \mathbf{1}, \end{aligned}$$

jolloin kvaternioryhmän Q_8 rakenne vastaa disyklisen ryhmän Dic_2 rakennetta määritelmän 3.18 nojalla eli $Q_8 \cong Dic_2$. □

Tähän asti ollaan nyt saatu esiteltyä tarpeeksi tietoja määrittelemään kertaluvun $|G| = 8$ erikoistapaus. Todistetaan siispä seuraavaksi sellaiset kommutatiiviset ja ei-kommutatiiviset ryhmät, jotka ovat isomorfisia tällaisen ryhmän G kanssa:

Lause 3.22 (Tapaus $n = 8$)**.** *Olkoon G ryhmä, jonka kertaluku on 8. Tällöin ryhmä G on isomorfinen syklisen ryhmän C_8, syklisten ryhmien tulon $C_2 \times C_4$ tai $C_2 \times C_2 \times C_2$, dihedraaliryhmän D_4 tai kvaternioryhmän Q_8 kanssa.*

Todistus. Olkoon G ryhmä, jolle $|G| = 8 = 2\cdot 4 = 2\cdot 2\cdot 2$. Oletetaan ensin, että ryhmä G on kommutatiivinen. Tällöin Äärellisten kommutatiivisten ryhmien peruslauseen 3.7 nojalla

$$G \cong C_8, \quad G \cong C_2 \times C_4, \quad \text{tai} \quad G \cong C_2 \times C_2 \times C_2.$$

Siispä oletetaan, että G ei ole kommutatiivinen ryhmä. Olkoon H ryhmän G aliryhmä ja x neutraalialkiosta poikkeava alkio, joka virittää aliryhmän H (eli $H = \langle x \rangle$). Lagrangen lauseen 2.16 nojalla $|x| \in \{2, 4, 8\}$.

Jos $|x| = 8$, niin alkio x virittää koko ryhmän G, jolloin $G \cong C_8$ on kommutatiivinen. Jos taas kaikille $x_i \in G$ pätee $|x_i| = 2$, niin lemman 2.9 nojalla G on kommutatiivinen. Siispä täytyy olla ainakin yksi alkio $x \in G$ siten, että $|x| = 4$.

Olkoon $y \in G \backslash H$. Tällöin vasen sivuluokka $yH = \{y, yx, yx^2, yx^3\} = G \backslash H$ ja aliryhmän H indeksi $[G : H] = 2$, jolloin H on normaali ja $G/H \cong C_2$ lauseen 3.3 nojalla. Siispä $yxy^{-1} \in \langle x \rangle$ ja $|yxy^{-1}| = 4$. Tapaus $yxy^{-1} = x$ johtaisi kommutatiiviseen tapaukseen, mikä vastoin oletusta. Koska tapauksissa $yxy^{-1} = e$ tai $yxy^{-1} = x^2$ kertaluku $|yxy^{-1}| \neq 4$, niin täytyy olla $yxy^{-1} = x^3$.

Koska G/H on kahden alkion ryhmä, saadaan $(y\langle x \rangle)^2 = y^2\langle x \rangle = e\langle x \rangle = \langle x \rangle$, jolloin pätee $y^2 \in \langle x \rangle$. Nyt jos $y^2 = x$ tai $y^2 = x^3$, saataisiin $(y^2)^4 = y^8 = e$,

jolloin alkion y kertaluku olisi 8 ja pätisi $G \cong \langle y \rangle \cong C_8$. Siispä täytyy olla $y^2 \in \{e, x^2\}$. Tarkastellaan nämä tapaukset erikseen.

Jos $y^2 = e$, niin $|y| = 2$ ja tarkastelemalla lukua $n = 4$ saadaan

$$x^n = x^4 = e, \quad y^2 = e \quad \text{ja} \quad yxy^{-1} = x^3 = x^{n-1},$$

jolloin kyseessä on dihedraaliryhmän D_4 määritelmän 3.11 nojalla, joten pätee $G \cong D_4$.

Jos $y^2 = x^2$, niin tarkastelemalla lukua $n = 2$ saadaan

$$\begin{aligned} x^{2n} &= x^4 = e \\ x^2y^{-2} = x^2(y^2)^{-1} &= x^2x^{-2} = e \\ \text{ja} \quad xyxy^{-1} &= xx^3 = x^4 = e, \end{aligned}$$

jolloin disyklisen ryhmän Dic_2 määritelmän 3.18 ja kvaternioryhmän Q_8 isomorfisuuden 3.21 nojalla $G \cong Dic_2 \cong Q_8$.

Huomioidaan vielä, että $Q_8 \ncong D_4$. Huomautuksen 3.20 nojalla kvaternioryhmällä Q_8 on kuusi alkiota $\pm\,\mathbf{i}$, $\pm\,\mathbf{j}$ ja $\pm\,\mathbf{k}$, joiden kertaluku on 4. Sen sijaan dihedraaliryhmällä D_4 on vain kolme alkiota, joiden kertaluvut on 4: kierrot x, x^2 ja x^3. Siispä $Q_8 \ncong D_4$. □

4 Rata-stabiloijalause

Tässä kappaleessa esitellään ryhmän toiminta, rata, stabiloija sekä rata-stabiloijalause. Näitä tarvitaan ryhmien rakenteiden tarkastelussa. Aloitetaan kappale esittelemällä teoriat abstraktilla tasolla, ja siirrytään sitten siitä konjugaation ja keskuksen tarkasteluihin. Esitellään lopuksi Cauchyn lause.

4.1 Ryhmän toiminta, rata ja stabiloija

Määritellään ryhmän toiminta, rata ja stabiloija sekä rata-stabiloijalause ensin abstraktilla tasolla. Määritelmät ja tulokset perustuvat Armstrongin [1] lukuun 17, Artinin [2] lukuun 6.9 sekä Dummit ja Footen [6] lukuihin 1.7 ja 2.2.

Määritelmä 4.1. Olkoot $g \in G$ ja $x \in X$. Ryhmän G *toiminnaksi* joukossa X kutsutaan kuvausta $\phi : (G, X) \to X$, missä $(g, x) \mapsto \phi(g, x) = g \cdot x$. Ryhmän toiminnalle pätee seuraavat aksioomat

1. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$, missä $g_1, g_2 \in G$, ja
2. $e \cdot x = x$.

Huomautus 4.2. Olkoon ϕ ryhmän G toiminta joukossa X. Tällöin kaikille $g \in G$ on olemassa permutaatio $\sigma_g \in S_X$, missä $\sigma_g(x) = g \cdot x = \phi(g, x)$.

Todistus. [6, s. 42 kpl 1.7] □

Määritelmä 4.3. Olkoot G ryhmä ja X joukko, jossa ryhmä G toimii, sekä $g \in G$ ja $x \in X$. Alkion x *radaksi* kutsutaan joukkoa

$$G(x) = \{g(x) = g \cdot x : g \in G\}.$$

Huomautus 4.4. Erilliset radat $G(x)$ osittavat joukon X.

Todistus. Olkoon $x, y \in X$, $g_1, g_2 \in G$ ja X joukko, jossa ryhmä G toimii. Ryhmän toiminnan määritelmällä 4.1 tiedetään, että kaikille $x \in X$ pätee

$$x = e \cdot x = e(x) \in G(x).$$

Olkoon $z \in G(x) \cap G(y)$. Tällöin $g_1(x) = z = g_2(y)$, josta edelleen saadaan $y = g_2^{-1}g_1(x)$, jolloin $y \in G(x)$. Vastaavasti voidaan saada $x \in G(y)$.

Siten täytyy olla $G(x) = G(y)$, jolloin ratojen leikkaus on joko tyhjä tai radat ovat täysin samat. Tällöin erilliset radat osittavat joukon X. □

Määritelmä 4.5. Olkoot G ryhmä, joka toimii joukossa X ja $x \in X$ jokin kiinnitetty alkio. Tällöin alkion x *stabiloija* ryhmässä G on joukko

$$G_x = \{\varphi \in G : \varphi(x) = x\}.$$

Lause 4.6 (Rata-stabiloijalause)**.** *Olkoon X äärellinen joukko, jossa äärellinen ryhmä G toimii sekä olkoot $G(x)$ alkion $x \in X$ rata ja G_x alkion x stabiloija. Tällöin saadaan*

$$|G| = |G(x)||G_x|.$$

Todistus. [1, s. 94 seuraus 17.3] □

Määritelmä 4.7. Olkoon G ryhmä, joka toimii joukossa X. Määritellään alkioiden $x \in X$ erillisten ratojen joukko

$$X/G = \{G(x) : x \in X\}.$$

Lemma 4.8. *Olkoot G ryhmä, joka toimii joukossa X, $x \in X$ ja X/G erillisten ratojen joukko. Tällöin*

$$|X| = \sum_{G(x) \in X/G} |G(x)|.$$

Todistus. Tulos seuraa huomautuksesta 4.4. Koska alkioiden $x \in X$ radat osittavat joukon X, niin niiden yhdiste on erillinen ja siten

$$|X| = \Big| \bigcup_{G(x) \in X/G} G(x) \Big| = \sum_{G(x) \in X/G} |G(x)|.$$

□

4.2 Konjugaatio, konjugaattiluokka ja normalisoija

Konjugaation tapauksessa huomataan, että konjugaatio on eräs ryhmän toiminta. Tällöin konjugaattiluokka toimii ryhmän ratana ja normalisoija ryhmän stabiloijana. Nämä huomataan vertaamalla määritelmiä toisiinsa. Luvun tulokset perustuvat Artinin [2] lukuun 7.2, Dummit ja Footen [6] lukuihin 2.2 ja 4.3 sekä Rotmanin [9] lukuihin 2 ja 3.

Määritelmä 4.9. Olkoot G ryhmä ja $x, y \in G$. Olkoon $\phi : G \to S_G$ toiminta konjugoinnilla, missä $\phi(y) = \varphi_y$, $\varphi_y : G \to G$ on bijektio ja $\varphi_y(x) = yxy^{-1}$. Tällöin kuvausta φ_y kutsutaan *konjugoinniksi* ja sanotaan, että x on *konjugaatti* alkion $\varphi_y(x)$ kanssa.

Huomautus 4.10. Konjugointi on toiminta.

Todistus. Osoitetaan konjugoinnin olevan toiminta tarkastelemalla ryhmän toiminnan määritelmän 4.1 aksioomia konjugoinnilla, missä merkintä $y \cdot x$ viittaa konjugoinnissa merkintään $\varphi_y(x) = yxy^{-1}$.

1. Selvästi kaikille $x, y, z \in G$ pätee

$$(\varphi_z)(\varphi_y(x)) = \varphi_z(yxy^{-1}) = zyxy^{-1}z^{-1} = (zy)x(zy)^{-1} = \varphi_{zy}(x), \text{ ja}$$

2. $exe^{-1} = x$ kaikille $x \in G$.

□

Määritelmä 4.11. Kaikki ne alkiot $\varphi_y(x)$, jotka ovat konjugaatteja alkion x kanssa, muodostavat joukon, jota kutsutaan alkion x *konjugaattiluokaksi*:

$$C(x) = \{\varphi_y(x) \in G : \varphi_y(x) = yxy^{-1} \text{ jollekin } y \in G\}.$$

Määritelmä 4.12. Ryhmän G aliryhmän H *normalisoijaksi* kutsutaan joukkoa

$$N_G(H) = \{y \in G : yHy^{-1} = H\}.$$

Koska konjugaattiluokat ovat konjugaatiolle ratoja, niin ne osittavat ryhmän lemman 4.8 nojalla. Tällöin rata-stabiloijalauseen sovelluksena saadaan aikaiseksi äärellisten ryhmien luokkayhtälö:

Määritelmä 4.13. Olkoot $C(x_j)$ ryhmän G alkioiden x_j konjugaattiluokkia siten, että jokainen x_j on eri konjugaattiluokassa. Merkitään näiden konjugaattiluokkien lukumäärää kirjaimella m. *Konjugaattiluokan luokkayhtälöksi* kutsutaan yhtälöä

$$|G| = \Big| \bigcup_{j=1}^{m} C(x_j) \Big| = \sum_{j=1}^{m} |C(x_j)|.$$

4.3 Keskus ja keskittäjä

Ryhmille voidaan määrittää keskus, joka tuo esille alkiot, jotka kommutoivat kaikkien ryhmän G alkioiden kanssa. Keskus on sen alkioiden erillisten ratojen yhdiste ja keskittäjä $Z(x)$ ryhmän G alkion x stabiloija, kun tarkastellaan ryhmän G toimintaa konjugaatiolla. Tässä alaluvussa esitellään yhteys konjugaatioon sekä tulokset, jotka pohjautuvat Armstrongin [1] lukuun 14, Dummit ja Footen [6] lukuihin 4.1−4.3 sekä Rotmanin [9] lukuihin 3 ja 4.

Määritelmä 4.14. Ryhmän G *keskus* $Z(G)$ koostuu kaikista niistä alkioista $y \in G$, jotka kommutoivat kaikkien ryhmän G alkioiden kanssa:

$$Z(G) = \{y \in G : yxy^{-1} = x \text{ kaikille } x \in G\}.$$

Lause 4.15. *Kommutatiivisen ryhmän G keskus on ryhmä itse eli $Z(G) = G$.*

Todistus. Keskuksen määritelmän 4.14 nojalla keskus $Z(G)$ koostuu kaikista sellaisista alkioista $y \in G$, jotka kommutoivat kaikkien ryhmän G alkioiden $x \in G$ kanssa. Koska tämä pätee kaikille $y \in G$, niin $Z(G) = G$. □

Lause 4.16. *Keskus $Z(G)$ koostuu sellaisista konjugaattiluokista, joissa on yksi alkio.*

Todistus. [1, s. 77 lause 14.1] □

Lause 4.17. *Keskus $Z(G)$ on ryhmän G normaali aliryhmä.*

Todistus. Olkoon $y, z \in Z(G) \subseteq G$. Osoitetaan ensin, että keskus $Z(G)$ on ryhmän G aliryhmä määritelmän 2.8 avulla:

1. $Z(G)$ on epätyhjä, koska se sisältää aina neutraalialkion e ryhmän määritelmän 2.5 kohdan 2 nojalla.

2. Osoitetaan, että $y^{-1} \in Z(G)$ mille tahansa $y \in Z(G)$. Koska $y \in Z(G)$, niin pätee $yxy^{-1} = x \in Z(G)$. Tästä saadaan kertomalla puolittain

   $$yxy^{-1} = x, \text{ josta saadaan } x = y^{-1}xy, \text{ ja edelleen } x = y^{-1}x(y^{-1})^{-1},$$

   jolloin $y^{-1} \in Z(G)$.

3. Osoitetaan, että $yz \in Z(G)$. Koska $y, z \in Z(G)$, niin niiden käänteisalkioille pätee $y^{-1}xy = x$ ja $z^{-1}xz = x$. Tällöin

$$(yz)x(yz)^{-1} = y(zxz^{-1})y^{-1} = x.$$

Tällöin $yz \in Z(G)$.

Siispä $Z(G)$ on ryhmän G aliryhmä. Koska kaikille $x \in G$ ja $y \in Z(G)$ pätee $yxy^{-1} = x$, niin kertomalla puolittain saadaan

$$yxy^{-1} = x, \text{ ja edelleen } y = xyx^{-1},$$

jolloin kaikille $y \in Z(G)$ pätee $xyx^{-1} \in Z(G)$ eli $xZ(G)z^{-1} = Z(G)$ ja määritelmän 2.13 nojalla $Z(G)$ on normaali.

□

Määritelmä 4.18. Ryhmän G alkion x *keskittäjäksi* kutsutaan joukkoa

$$Z(x) = \{y \in G : yxy^{-1} = x\}.$$

Lause 4.19. *Keskittäjä $Z(x)$ on ryhmän G aliryhmä.*

Todistus. Olkoon $x \in G$ mikä tahansa alkio. Todistetaan, että alkion x keskittäjä $Z(x)$ on ryhmän G aliryhmä määritelmän 2.8 aksioomien avulla:

1. $Z(x)$ on epätyhjä: Koska $xxx^{-1} = xe = x$, niin $x \in Z(x)$.
2. $y^{-1} \in Z(x)$, kun $y \in Z(x)$: Koska alkiot x ja y kommutoivat, pätee $yx = xy$, josta edelleen $y^{-1}xy = x$ ja $y^{-1} \in Z(x)$.
3. $yz \in Z(x)$, kun $y, z \in Z(x)$: Tällöin saadaan proposition 2.6 avulla

$$(yz)x(yz)^{-1} = yzxz^{-1}y^{-1} = yxy^{-1} = x,$$

jolloin $yz \in Z(x)$.

□

Lemma 4.20. *Keskittäjälle $Z(x)$ pätee $x \in Z(x)$ ja $Z(G) \subseteq Z(x)$.*

Todistus. Tapaus $x \in Z(x)$ todistettiin lauseen 4.19 todistuksessa.

Määritelmistä 4.14 ja 4.18 huomataan helposti tulos $Z(G) \subseteq Z(x)$: Jos $y \in Z(G)$ eli kaikille $x \in G$ pätee $yxy^{-1} = x$, niin $y \in Z(x)$. □

Lause 4.21. *Olkoon H ryhmän G aliryhmä ja $h \in G$. Tällöin aliryhmän H konjugaattien lukumäärä on yhtä suuri indeksin $[G : N_G(H)]$ kanssa.*
Alkion h konjugaattien lukumäärä on yhtä suuri keskittäjän $Z(h)$ indeksin $[G : Z(h)]$ kanssa. Tällöin

$$|G| = |N_G(H)|[G : N_G(H)] = |Z(h)|[G : Z(h)].$$

Todistus. [9, s. 44-45 lauseet 3.2 ja 3.3] □

Lause 4.22. *Luokkayhtälö voidaan ilmaista myös muodossa*

$$|G| = |Z(G)| + \sum_{|C_i|>1} |C_i|$$

Todistus. Määritellään kuvaus $\varphi : G \to G$, missä $\varphi(x_j) = yx_jy^{-1} \in G$, jossa ryhmä G toimii itsellään konjugaatiolla. Tällöin alkion x_j rata on yhtä suuri sen konjugaattiluokan kanssa eli $G(x_j) = C(x_j)$.

Tarkastellaan luokkayhtälöä 4.13. Lauseen 4.16 nojalla keskus koostuu sellaisista alkioista, joiden konjugaattiluokka sisältää vain tämän alkion itse. Tällöin luokkayhtälö 4.13 saadaan muotoon

$$|G| = \sum_{j=1}^{m} |C(x_j)| = |Z(G)| + \sum_{|C_i|>1} |C_i|$$

□

Lemma 4.23. *Olkoon p alkuluku ja k jokin positiivinen kokonaisluku. Ryhmän G, jonka kertaluku on p^k, keskus $Z(G)$ ei ole triviaali eli $Z(G) \neq \{e\}$.*

Todistus. Tarkastellaan ryhmää G, joka toimii keskuksessa $Z(G)$ konjugaatiolla.

Olkoon C_i konjugaattiluokkia, jotka osittavat joukon $G \backslash Z(G)$. Tällöin luokkayhtälön 4.22 nojalla

$$|G| = |Z(G)| + \sum_{|C_i|>1} |C_i|.$$

Koska konjugaattiluokka on ryhmän G rata, niin rata-stabiloijalauseella 4.6 tiedetään, että sen kertaluku jakaa ryhmän G kertaluvun eli $|C_i| \mid p^k$, kun $|C_i| > 1$.

Jotta kertaluku $|G|$ olisi jaollinen alkuluvulla p, niin keskuksen kertaluvun $|Z(G)|$ on oltava jaollinen luvulla p. Koska $p \nmid 1$, niin $|Z(G)| \neq 1$ eli $Z(G) \neq \{e\}$, jolloin keskus ei ole triviaali. □

Lause 4.24 (Tapaus $n = p^2$)**.** *Olkoon G ryhmä, jonka kertaluku on p^2, missä p on alkuluku. Tällöin G on isomorfinen syklisen ryhmän C_{p^2} tai syklisten ryhmien tulon $C_p \times C_p$ kanssa.*

Todistus. Lemman 4.23 nojalla tiedetään, että ryhmän G keskus on epätriviaali, kun ryhmän G kertaluku $|G| = p^k$. Siispä $|Z(G)| \in \{p, p^2\}$. Jälkimmäinen viittaa siihen, että keskus on yhtä suuri koko ryhmän kanssa, jolloin ryhmä G on kommutatiivinen lauseen 4.15 nojalla.

Oletetaan, että $|Z(G)| = p$. Olkoon $x \in G$ alkio, jolle pätee $x \notin Z(G)$. Lemman 4.20 nojalla x on sen keskittäjässä eli $x \in Z(x)$ ja lisäksi pätee $Z(G) \subseteq Z(x)$. Siispä $Z(G) \subset Z(x)$, sillä myös $x \in Z(x)$, eli $|Z(x)| \geq p + 1$. Koska $Z(x) \subseteq G$ lauseen 4.19 nojalla, niin Lagrangen lauseella 2.16 tiedetään, että $|Z(x)| = p^2$. Siispä $Z(x) = G$, jolloin pätisi $x \in Z(G)$, mikä on ristiriidassa alun oletuksen kanssa. Siten $|Z(G)| \neq p$, eli $|Z(G)| = p^2 = |G|$, jolloin G on kommutatiivinen lauseen 4.15 nojalla.

Koska $|G| = p \times p = p^2$, niin Äärellisten kommutatiivisten peruslauseen 3.7 nojalla $G \cong p \times p$ tai $G \cong C_{p^2}$. □

4.4 Cauchyn lause

Tässä kappaleessa käydään läpi ensin Cauchyn lause, jota hyödynnetään paljon ryhmien luokittelussa. Lisäksi käydään läpi kertaluvun tapaus $2p$, missä p on alkuluku. Tämän kappaleen asiat perustuvat Armstrongin [1] lukuihin 13 ja 15 sekä Rotmanin [9] lukuun 4.

Lause 4.25 (Cauchyn lause)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on jaollinen alkuluvulla p. Tällöin ryhmällä G on olemassa aliryhmä, jonka kertaluku on p.*

Todistus. Määritellään joukko X:

$$X = \{(x_1, \ldots, x_p) \in G^p : x_1 x_2 \cdots x_p = e\}.$$

Joukon X alkion komponentit ovat vapaasti valittavissa lukuunottamatta viimeistä, kun asetetaan $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$. Tällöin erilaisia mahdollisuuksia järjestellä muut komponentit x_i on yhteensä $|G|^{p-1}$. Tässä $|G| = kp$ on jaollinen alkuluvulla p oletuksen mukaisesti. Siispä saadaan

$$|X| = |G|^{p-1} = (kp)^{p-1}, \tag{4.1}$$

jolloin joukon X kertaluku on jaollinen alkuluvulla p.

Nyt mikä tahansa joukon X alkion komponenttien x_i syklinen permutaatio tuottaa alkion, joka myös sisältyy joukkoon X, niin voidaan määritellä syklisen ryhmän $C_p = \langle (1\ \ 2\ \ \cdots\ \ p) \rangle$ toiminta asettamalla jokaisella $\sigma \in C_p$ joukossa X:

$$\sigma \cdot (x_1, \ldots, x_p) = (x_{\sigma_{(1)}}, \ldots, x_{\sigma_{(p)}}).$$

Koska p on alkuluku, niin se on jaollinen vain luvulla 1 ja itsellään. Siispä myös alkion x radan $C_p(x)$ tai stabiloijan $C_{p,x}$ tulee jakaa luku p eli $|C_p(x)| \in \{1, p\}$ tai $C_{p,x} \in \{1, p\}$ rata-stabiloijalauseen 4.6 nojalla. Selvästi tapaus $|C_p(x)| = 1$ pätee neutraalialkiolle, sillä
$(x_1, \ldots, x_p) = (x, \ldots, x) = (e, \ldots, e) = e$.

Jos $|C_p(x)| = p$ kaikille $x \in X - \{e\}$, niin rata-stabiloijalauseen seurauksesta 4.8 saadaan

$$|X| = \sum_{x \in X} |C_{p,x}| = |C_{p,e}| + \sum_{y \in X - \{e\}} |C_{p,y}| = 1 + mp, \tag{4.2}$$

missä mp on alkuluvun p monikerta.

Yhtälöt (4.1) ja (4.2) aiheuttavat ristiriidan. Siispä on olemassa ainakin yksi rata $C_p(x_0)$ siten, että $|C_p(x_0)| = 1$ jollekin $x_0 \in X - \{e\}$. Siispä tälle neutraalialkiosta poikkeavalle alkiolle $x_0 = (x, \ldots, x)$ pätee $x \cdots x = x^p = e$, jolloin ryhmällä G on olemassa alkion x virittämä ei-triviaali aliryhmä, jonka kertaluku on p. □

Huomautus 4.26. Jos $p \mid |G|$. niin on olemassa alkio $x \in G$, jonka kertaluku $|x| = p$.

Todistus. Seuraa alkuluvullisen ryhmän syklisyydestä 3.3 sekä Cauchyn lauseesta 4.25. □

Lause 4.27 (Tapaus $n = 2p$)**.** *Olkoon G ryhmä, jonka kertaluku on $2p$ ja $p \geq 3$. Tällöin G on isomorfinen syklisen ryhmän C_{2p} tai dihedraaliryhmän D_p kanssa.*

Todistus. Olkoot $x, y \in G$ alkioita, jotka virittävät ryhmän G aliryhmät $\langle x \rangle$ ja $\langle y \rangle$, jotka leikkaavat triviaalisti eli $\langle x \rangle \cap \langle y \rangle = \{e\}$. Cauchyn lauseeseen 4.25 nojautuen olkoot $|x| = p$ ja $|y| = 2$.

Aliryhmä $\langle x \rangle$ on normaali lauseen 3.4 nojalla, sillä sen indeksi $[G : \langle x \rangle] = 2$.

Nyt Lagrangen lauseen nojalla alkion $xy \in G$ kertaluku jakaa ryhmän G kertaluvun, eli $|xy| \in \{2, p, 2p\}$.

Jos $|xy| = 2$, niin $(xy)^2 = xyxy = e$ josta edelleen $yxy = x^{-1} = x^{n-1} = x^{p-1}$, missä $n = p$. Siispä dihedraaliryhmän määritelmän 3.11 nojalla $G \cong D_p$.

Jos $|xy| = 2p$, niin $G \cong C_{2p}$.

Jos $|xy| = p$, niin pätisi $(xy)^p = e$ ja siten

$$\langle x \rangle = \langle x \rangle e = \langle x \rangle (xy)^p \overset{1}{=} (\langle x \rangle xy)^p \overset{2}{=} \langle x \rangle y^p \overset{3}{=} \langle x \rangle y,$$

jolloin pätisi $y \in \langle x \rangle$, mikä ei voi pitää paikkaansa, sillä aluksi oletettiin, että ryhmille $\langle x \rangle$ ja $\langle y \rangle$ pätee $\langle x \rangle \cap \langle y \rangle = \{e\}$.

Siispä ryhmä G on isomorfinen ryhmän D_p tai C_{2p} kanssa. □

[1] Tekijäryhmässä $\langle x \rangle / G\langle x \rangle$ alkio $\langle x \rangle = e$, jolloin pätee $\langle x \rangle (xy)^p = (\langle x \rangle xy)^p$.
[2] $\langle x \rangle x = \{ex, x^2, \ldots, x^{p-1}x\} = \{x, x^2, \ldots, x^p = e\} = \langle x \rangle$.
[3] $y^p = y^{2k+1} = y^{2k}y = ey = y$.

5 Sylowin lauseet

Tässä kappaleessa esitellään Sylowin lauseet ja niitä hyödyntävät todistukset tapauksista $n = 12, n = 16, n = 18$ ja $n = 20$. Kolmen viimeisen tapauksen todistukset käydään läpi tässä työssä pintapuolisesti listaamalla ryhmät, jotka ovat isomorfisia käsiteltävää kertalukua olevan ryhmän kanssa.

5.1 Sylowin p-aliryhmä ja Sylowin lauseet

Tässä kappaleessa esitellään Sylowin lauseet. Luvun tulokset perustuvat Armstrongin [1] lukuun 20, Artinin [2] lukuun 7.7, Dummit ja Footen [6] lukuun 4.5 ja Rotmanin [9] lukuun 4.

Määritelmä 5.1. Olkoon p jokin alkuluku ja $i \geq 1$ kokonaisluku. Ryhmää, jonka kaikkien neutraalialkiosta poikkeavien alkioiden kertaluku on muotoa p^i, kutsutaan *p-ryhmäksi*.

Ryhmän G aliryhmiä, jotka ovat p-ryhmiä, kutsutaan *p-aliryhmiksi*.

Esimerkki 5.2. Esimerkkejä 2-ryhmistä ovat Q_8 ja D_4.

Huomautuksesta 3.20 tiedetään, että kvaternioryhmän Q_8 neutraalialkiosta poikkeavien alkioiden $\pm$ **i**, $\pm$ **j** ja $\pm$ **k** kertaluvut ovat muotoa $4 = 2^2$, ja määritelmästä huomataan, että alkion -**1** kertaluku on 2.

Vastaavasti ryhmän D_4 kiertojen x, x^2 ja x^3 kertaluvut ovat muotoa $4 = 2^2$, ja peilauksen y kertaluku on 2.

Sen sijaan ryhmä D_3 (joka esiteltiin esimerkissä 3.10) ei ole p-aliryhmä, sillä sen alkioille pätee $|x| = 3$ ja $|y| = 2$, jolloin kertaluvut eivät ole saman alkuluvun potensseja.

Määritelmä 5.3. Olkoot p jokin alkuluku ja m jokin kokonaisluku siten, että $p \nmid m$. Olkoot G ryhmä, jonka kertaluku on muotoa $|G| = p^k m$, ja $H \subseteq G$ aliryhmä, jonka kertaluku on p^k.
Tällöin aliryhmää H kutsutaan ryhmän G *Sylowin p-aliryhmäksi*. Sylowin p-aliryhmien lukumäärää merkitään symbolilla n_p.

Huomautus 5.4. Sylowin p-aliryhmien lukumäärä n_p on yhtä suuri ryhmän G aliryhmän H konjugaattien lukumäärän kanssa.

Todistus. Sylowin 3. lauseen 5.10 yhteydessä. □

Lemma 5.5. *Olkoon P äärellisen ryhmän G Sylowin p-aliryhmä. Tällöin jos alkion $a \in G$ kertaluku on muotoa $|a| = p^k$ ja $aPa^{-1} = P$, niin pätee $a \in P$ ja $P \subseteq G$.*

Todistus. Rotmanin [9, s. 78 lemma 4.11] todistuksessa hyödynnetään neljättä isomorfismilausetta, vastaavuuslausetta (Correspondence Theorem), joka vaatii tästä teoksesta syvällisempää tietämystä. □

Lemma 5.6. *Binomikerroin $\binom{p^k m}{p^k}$ ei ole jaollinen alkuluvulla p.*

Todistus. [2, s. 206 lemma 7.7.10] □

Seuraavaksi perehdytään Sylowin lauseisiin ja niiden todistuksiin hyödyntämällä pääosin Armstrongin [1] luvun 20 ja Rotmanin [9] luvun 4 todistuksia.

Lause 5.7 (Sylowin 1. lause)**.** *Ryhmällä, jonka kertaluku on jaollinen alkuluvulla p, on olemassa Sylowin p-aliryhmä.*

Todistus. Olkoot p^k suurin alkuluvun p potenssi, joka jakaa ryhmän G kertaluvun $|G| = p^k m$ ja X joukko, jossa on kaikki sellaiset ryhmän G osajoukot, joiden kertaluku on p^k. Tällöin $|X| = \binom{p^k m}{p^k}$, joka ei lemman 5.6 nojalla ole jaollinen alkuluvulla p.

Määritellään ryhmän G toiminta joukossa X vasemmalla siirrolla, jossa $(g, A) \mapsto gA$, missä $g \in G$ ja $gA = \{ga : a \in A\} \in X$.

Koska $p \nmid |X|$, niin on olemassa rata $G(A) \in X$ siten, että $p \nmid |G(A)|$ huomautuksen 4.4 nojalla. Tällöin myös $p^k \nmid |G(A)|$ ja rata-stabiloijalauseen 4.6 nojalla

$$|G| = p^k m = |G_A||G(A)|,$$

jolloin täytyy olla $p^k \mid |G_A|$. Tällöin $|G_A| \geq p^k$.

Toisaalta, jos $g \in G_A$ ja $a \in A$, niin myös $ga \in A$, jolloin koko oikea sivuluokka $G_A a \subseteq A$, joten $|G_A| \leq |A| = p^k$.

Siten G_A on ryhmän G aliryhmä, jolle $|G_A| = p^k$. □

Lause 5.8 (Sylowin 2. lause)**.** *Mitkä tahansa kaksi Sylowin p-aliryhmää ovat konjugaatit.*

Todistus. Sylowin 3. lauseen 5.10 yhteydessä. □

Huomautus 5.9. [2, s. 204] Ryhmällä G on olemassa yksi Sylowin p-aliryhmä H jos ja vain jos H on normaali.

Todistus. Jos ryhmällä G on vain yksi Sylowin p-aliryhmä P, niin $P \trianglelefteq G$, sillä mikä tahansa ryhmän P konjugaatti on myös Sylowin p-aliryhmä. Vastaavasti jos P on ryhmän G normaali Sylowin p-aliryhmä, niin Sylowin p-aliryhmien konjugaatiosta seuraa lauseen 5.8 nojalla, että p-aliryhmiä on vain yksi. □

Lause 5.10 (Sylowin 3. lause)**.** *Sylowin p-aliryhmien lukumäärä n_p jakaa ryhmän G kertaluvun $|G| = p^k m$ ja lisäksi pätee*

$$n_p = 1 + lp \equiv 1 \pmod{p}$$

jollekin kokonaisluvulle l.

Todistus. Olkoon P_1 ryhmän G Sylowin p-aliryhmä ja $X = \{P_1, \dots P_t\}$ aliryhmän P_1 konjugaattien joukko. Tällöin ryhmä G toimii konjugaatiolla joukossa X ja voidaan määritellä huomautusta 4.2 mukaillen homomorfismi $\varphi : G \to S_X$, missä $a \mapsto \varphi_a \in S_X$ jollekin $a \in G$ ja $\varphi_a(P_i) = aP_ia^{-1}$ ja missä $1 \leq i \leq t$.

Olkoon Q jokin ryhmän G Sylowin p-aliryhmä, jolloin $Q \subset G$ ja siten myös ryhmä Q toimii joukossa X. Lauseen 4.21 nojalla toiminnan jokaisen radan koko jakaa ryhmän Q kertaluvun $|Q|$, jolloin radan koko on alkuluvun p potenssi ($\in \{p^0, p^1, \dots, |Q|\}$).

1. Jos jossain radassa on yksi alkio P_i, niin pätee $\varphi_q(P_i) = qP_iq^{-1}$ kaikille $q \in Q$. Lemman 5.5 nojalla tällöin $P_i \subseteq Q$. Koska $|P_i| = |Q|$ ja koska Q on Sylowin p-aliryhmä, niin $P_i = Q$.

   Koska konjugaatit P_i ovat eri ryhmiä, niin muiden joukon X alkioiden ratojen koko on oltava alkuluvun p aito potenssi ($p^l, 0 < l \leq k$). Tällöin $|X| \equiv 1 \pmod{p}$.

2. Oletetaan, että $Q \notin X$. Tällöin edellisen tapauksen nojalla ei ole olemassa sellaista rataa, jossa olisi vain 1 alkio. Siispä joukon X alkioiden ratojen koko on oltava alkuluvun p aito potenssi ($p^l, 0 < l \leq k$), jolloin $|X| \equiv 0 \pmod{p}$.

Tämä saa aikaan ristiriidan aiemman kanssa, joten ei ole olemassa Sylowin aliryhmää Q siten, että $Q \notin X$. Siispä X sisältää kaikki ryhmän G Sylowin p-aliryhmät, jotka ovat konjugaatteja Sylowin p-aliryhmän P_1 kanssa.

Lauseen 4.21 nojalla konjugaattien lukumäärä $n_p = [G : P_1]$ on ryhmän G kertaluvun tekijä eli $n_p \mid |G| = p^k m$. □

5.2 Luokittelua Sylowin lauseilla

Tässä kappaleessa hyödynnetään Sylowin lauseita kertaluvun erikoistapauksen 12 ja yleisen tapauksen pq todistuksissa. Myös tämän kappaleen asiat perustuvat Armstrongin [1] lukuun 20 ja Rotmanin [9] lukuun 4.

Lause 5.11 (Tapaus $n = 12$)**.** *Olkoon G ryhmä, jonka kertaluku on 12. Tällöin G on isomorfinen syklisen ryhmän C_{12}, kommutatiivisen ryhmän $C_2 \times C_2 \times C_3$, alternoivan ryhmän A_4, dihedraaliryhmän D_6 tai disyklisen ryhmän Dic_3 kanssa.*

Todistus. Olkoon G ryhmä, jonka kertaluku on $|G| = 12 = 2^2 \cdot 3$. Sylowin 1. lauseen 5.7 nojalla ryhmällä G on siten olemassa Sylowin 2-aliryhmä H ja Sylowin 3-aliryhmä K, joille $|H| = 4, |K| = 3$ ja $|H \cap K| = \{e\}$. Koska $|H| = 4$, niin tapauksen 4.24 nojalla $H \cong C_4$ tai $H \cong C_2 \times C_2$. Sylowin 3. lauseella tiedetään, että $n_2 \in \{1, 3\}$ ja $n_3 \in \{1, 4\}$. Käsitellään nämä tapaukset erikseen.

1. $n_2 = 3$ ja $n_3 = 4$:

   Tapaus $n_3 = 4$ tarkoittaa, että ryhmällä G on 4 aliryhmää K_i, joiden kertaluku on 3. Jos neutraalialkiota e ei huomioida, niin nämä aliryhmät sisältävät $4 \cdot 2 = 8$ ryhmän G alkiota. Koska $H \cap K = \{e\}$, niin jäljelle jää 3 neutraalialkiosta poikkeavaa alkiota, jotka kuuluvat aliryhmään H. Koska $|H| = 4$, niin aliryhmiä H ei voi olla kuin yksi.

2. $n_2 = 1$ ja $n_3 = 1$:

   Tällöin huomautuksen 5.9 nojalla H ja K ovat normaaleja aliryhmiä. Koska $H \cap K = \{e\}$ ja $|HK| = \frac{|H||K|}{|H \cap K|} = 12 = |G|$, niin lauseen 3.9 nojalla ja propositiota 3.8 hyödyntäen saadaan aikaiseksi isomorfiat $G \cong H \times K \cong C_4 \times C_3 \cong C_{12}$ tai $G \cong H \times K \cong C_2 \times C_2 \times C_3 \cong C_2 \times C_6$.

3. $n_2 = 1$ ja $n_3 = 4$:

   Tällöin huomautuksen 5.9 nojalla H on normaali. Merkitään Sylowin 3-aliryhmien joukkoa $\mathcal{K} = \{K_1, K_2, K_3, K_4\}$. Määritellään ryhmän G toiminta joukossa $\mathcal{K}$ konjugaatiolla asettamalla

   $$\varphi : G \to S_4, \text{ missä } (\varphi(g))(K_i) = gK_ig^{-1}$$

   kaikille $i \in \{1, 2, 3, 4\}$ ja $g \in G$.

   Koska nyt $K_i \subseteq N_G(K_i)$ ja lauseen 4.21 nojalla aliryhmän K_i konjugaattien lukumäärä on yhtä suuri aliryhmän K_i indeksin kanssa eli

   $$[G : N_G(K_i)] = [G : K_i] = 4 = n_3,$$

   niin pätee $K_i = N_G(K_i)$ kaikille i. Tästä seuraa, että kuvauksen φ ydin $\ker(\varphi) = \{e\}$ on triviaali, jolloin proposition 2.24 nojalla φ on injektio.

   Tällöin $|\varphi(G)| = 12 = |G|$ ja $\varphi(G)$ sisältää yhteensä 8 kertaluvun 3 alkiota, jotka ovat 3-syklejä tapauksen $n = p$ 3.3 nojalla ja jotka ovat parillisia syklejä määritelmän 3.16 nojalla. Tällöin lauseen 3.17 nojalla G on alternoivan ryhmän A_4 aliryhmä. Koska $|G| = 12 = \frac{4!}{2} = |A_4|$, niin $G \cong A_4$.

4. $n_2 = 3$ ja $n_3 = 1$:

   Olkoon $K = \langle x \rangle$. Koska K on normaali huomautuksen 5.9 nojalla, niin pätee $yxy^{-1} = x'$, missä $y \in G$ ja $x' \in K$. Aiemmin saatujen kommutatiivisten tapausten seurauksena voidaan olettaa, että G ei ole kommutatiivinen. Koska lisäksi alkion x kertaluku on 3, täytyy päteä $yxy^{-1} = x^2$ ja edelleen $yx = x^2y$. Tästä puolestaan saadaan

   $$y^2x = yx^2y = x^2yxy = x^4y^2 = xy^2,$$

   jolloin alkiot x ja y^2 kommutoivat.

   (a) Jos $H = \langle y \rangle \cong C_4$:

   Ryhmän G virittäviksi alkioiksi voidaan valita alkiot $y^2x = xy^2$ ja y. Koska alkion x kertaluku on 3 ja alkion y^2 kertaluku on 2 (koska $(y^2)^2 = y^4 = e$), niin saadaan $|y^2x| = |xy^2| = 6$ eli $(y^2x)^6 = e$. Tämä saadaan helposti myös hyödyntämällä tietoa $yx = x^2y$. Koska alkiot y^2 ja x kommutoivat, niin

   $$(y^2x)^3 = (xy^2)^3 = xy^2xy^2xy^2 = xxy^2y^2xy^2 = \cdots = x^3y^6 = y^2.$$

   Lisäksi saadaan

$$(y^2x)y(y^2x)y^{-1} = xy^5xy^{-1} = \cdots = x^3y^4 = e$$

tiedolla $yx = x^2y$ sekä alkioiden y^2 ja x kommutoinnilla.

Siispä virittäjille $y^2x = xy^2$ sekä y pätee $(y^2x)^6 = (y^2x)^{2\cdot 3} = e$, $(y^2x)^3y^{-2} = y^2y^{-2} = e$ sekä $(y^2x)y(y^2x)y^{-1} = e$, ja korvaamalla disyklisen ryhmän abstraktin määritelmän 3.18 alkio x alkiolla $y^2x = xy^2$ ja tarkastelemalla tapausta tilanteessa $n = 3$ huomataan, että $G \cong Dic_3$.

(b) Jos $H = \{e, y, z, yz\} \cong C_2 \times C_2$, missä $y^2 = e = z^2 = (yz)^2$ ja $yz = zy$:

Oletuksen nojalla $K = \langle x \rangle$, missä $|x| = 3$, on normaali, jolloin pätee

$$yxy^{-1} = yxy = x^a, zxz^{-1} = zxz = z^b \text{ ja}$$
$$(yz)x(yz)^{-1} = (yz)x(zy) = yx^ay = x^{ab},$$

missä $a, b \in \{\pm 1\}$. Jos pätee $a = b = 1$, niin nähdään, että kaikki ryhmän H alkiot kommutoivat ryhmän K kanssa, jolloin G on kommutatiivinen.

Siispä voidaan olettaa esimerkiksi, että $a = 1$ ja $b = ab = -1$. Tällöin alkiot y ja x kommutoivat, jolloin ne virittävät syklisten ryhmien tulon $\langle x \rangle \times \langle y \rangle \cong C_3 \times C_2 \cong C_6$ ja jolloin kertaluku $|xy| = 6$.

Alkio z ei ole mikään alkion xy potensseista, joten alkiot xy ja z virittävät ryhmän G. Aiemmin huomattiin, että $(xy)^6 = e = z^2$, ja $(yz)x(yz) = x^{-1}$, josta saadaan $z(xy)z = (xy)^{-1}$. Tällöin ryhmän G rakenne on sama dihedraaliryhmän D_6 kanssa määritelmän 3.11 nojalla eli $G \cong D_6$.

Siispä $G \cong C_{12}, G \cong C_3 \times C_2 \times C_2, G \cong A_4, G \cong Dic_3$ tai $G \cong D_6$. □

Lause 5.12 (Tapaus $n = pq$)**.** *Olkoon G ryhmä, jonka kertaluku on pq, missä p ja q ovat eri alkulukuja ja $p < q$. Jos $p \mid (q-1)$, niin G on syklinen tai isomorfinen sellaisen ryhmän $\langle x, y \rangle$ kanssa, jossa pätee*

$$x^q = e = y^p \quad ja \quad yxy^{-1} = x^k,$$

missä $k^p \equiv 1 \pmod q$, mutta $k \not\equiv 1 \pmod q$. Jos $p \nmid (q-1)$, niin G on syklinen.

Todistus. Olkoon $|G| = pq$, missä p ja q ovat alkulukuja ja $p < q$. Sylowin 1. lauseen 5.7 nojalla on olemassa Sylowin p-aliryhmä P ja Sylowin q-aliryhmä Q.

Sylowin 3. lauseen 5.10 nojalla $n_q \in \{1, q+1\}$. Jälkimmäinen ei kuitenkaan ole mahdollinen, sillä $q+1$ ei jaa lukua p oletuksen $p < q$ vuoksi, vaikka Sylowin 3. lause tämän vaatii. Siispä $n_q = 1$ ja Q on normaali huomautuksen 5.9 nojalla.

Vastaavasti $n_p \equiv 1 \pmod{p}$ ja $n_p \mid q$, missä q on alkuluku. Siispä saadaan $n_p \in \{1, q = 1+tp\}$ jollekin kokonaisluvulle t. Jos $p \nmid (q-1)$, niin pätee $t = 0$ ja siten $q = 1$ eli $n_p = 1$. Käydään tapaukset $n_p = 1$ ja $n_p = q$ läpi erikseen.

Jos $n_p = 1$, niin myös P on normaali huomautuksen 5.9 nojalla. Koska pätee $P \cap Q = \{e\}$ ja $|PQ| = pq = Q$, niin lauseen 3.9 nojalla ja propositiota 3.8 hyödyntäen saadaan $G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$.

Tarkastellaan tapausta $n_p = q$. Koska Q on normaali, niin $yxy^{-1} = x^k$ kiinnitetyillä virittäjillä $y \in P$ ja $x \in Q$, jolloin erityisesti $y^p = e$. Oletetaan, että $k \not\equiv 1 \pmod{q}$, sillä muutoin $k = 1$ ja palataan kommutatiiviseen tapaukseen. Induktiolla saadaan osoitettua, $y^p x y^{-p} = x^{k^p}$ ja siten se, että pätee $k^p \equiv 1 \pmod{q}$:

1. Tapaus $i = 1$: Tämä pätee, sillä aliryhmän Q normaalius johtaa tulokseen $yxy^{-1} = x^k$.

2. Induktio-oletus: Oletetaan, että kaikille $i = p-1$ pätee

$$y^{p-1} x y^{1-p} = x^{k^{p-1}}.$$

3. Tapaus $i = p$: Tällöin saadaan

$$x = y^p x y^{-p} = y y^{p-1} x y^{1-p} y = y x^{k^{p-1}} y^{-1} = (x^{k^{p-1}})^k = x^{(k^{p-1})k} = x^{k^p}.$$

Tulos menettelee induktiolla, ja siten pätee $x = x^{k^p}$ eli $e = x^{k^p - 1}$, jolloin $k^p \equiv 1 \pmod{q}$.

□

Esimerkki 5.13. Käydään tässä esimerkissä läpi muutama sellainen tapaus, jossa kertaluvulle pätee $|G| = pq$.

Aiemmista tapauksista voidaan huomata, että kaikille tapauksille $2p$, missä p on jokin pariton alkuluku, pätee $2 \mid (p-1)$. Lauseen 4.27 avulla huomataan, että tosiaan tällöin kyseinen ryhmä on isomorfinen syklisen ryhmän C_{2p} ja dihedraaliryhmän D_p kanssa. Siten tämän tapauksen ryhmälle pätee lauseen 5.12 ehdot.

Ryhmässä, jonka kertaluku muotoa $|G| = 21 = 3 \cdot 7$, missä $3 \mid (7-1) = 6$, ei-kommutatiiviselle tapaukselle pätee $x^7 = e = y^3$ ja $yxy^{-1} = x^2$.

Näiden sijaan esimerkiksi ryhmä, jonka kertaluku on $|G| = 15 = 3 \cdot 5$, missä $3 \nmid (5-1) = 4$, on syklinen. Muiden tällaisten ryhmien kertalukuja ovat esimerkiksi $33 = 3 \cdot 11$, $35 = 5 \cdot 7$, $51 = 3 \cdot 17$ ja $91 = 7 \cdot 13$.

5.3 Ryhmien puolisuora tulo

Tässä alaluvussa käydään läpi ryhmien puolisuoran tulon määritelmä pinnallisesti erikoistapausten $n = 16, n = 18, n = 20$ isomorfisten ryhmien esittelyä varten. Tässä kappaleessa tapauksia ei todisteta perusteellisesti, vaan niiden todistuksiin tai esityksiin viitataan lyhyesti. Alaluvun tiedot perustuvat Dummit ja Footen [6] lukuun 5.5, ja lisäksi erikoistapauksissa viitataan Deopurkarin [5], Finottin [7], Lapuyade-Lahorgue [8], Tschinkelin [10], Ulmerin [11] sekä Wilden [12] tuotoksiin. Osan ryhmien nimeämisessä on hyödynnetty Carter ja Ellisin [3] nettisivustoa.

Määritelmä 5.14. Olkoot H ja K ryhmän G aliryhmiä, ja H normaali. Jos $H \cap K = \{e\}$ ja $HK = G$, niin ryhmää G kutsutaan aliryhmien H ja K *puolisuoraksi tuloksi* ja merkitään $H \rtimes K$ (tai $H \ltimes K$).

Lause 5.15 (Tapaus $n = 16$, kommutatiiviset)**.** *Olkoon G kommutatiivinen ryhmä, jonka kertaluku on 16. Tällöin G on isomorfinen syklisen ryhmän C_{16} tai jonkin syklisten ryhmien suoran tulon $C_2 \times C_2 \times C_2 \times C_2$, $C_4 \times C_4$, $C_2 \times C_8$ tai $C_2 \times C_2 \times C_4$ kanssa.*

Todistus. Äärellisten kommutatiivisten ryhmien peruslauseella 3.7, kun tiedetään, että $|G| = 16 = 2 \cdot 2 \cdot 2 \cdot 2 = 4 \cdot 4 = 2 \cdot 8 = 2 \cdot 2 \cdot 4$. □

Lause 5.16 (Tapaus $n = 16$, ei-kommutatiiviset)**.** *Olkoon G ei-kommutatiivinen ryhmä, jonka kertaluku on 16. Tällöin G on isomorfinen jonkin seuraavan ryhmän kanssa:*

1. *suora tulo $C_2 \times D_4$,*

2. *suora tulo* $C_2 \times Q_8$

3. *dihedraaliryhmä* D_8

4. *semidihedraaliryhmä* SD_8*, missä*

$$\langle x, y : x^2 = y^2 = e, y^{-1}xy = a^3 \rangle,$$

5. *modulaarinen maksimaali-syklinen ryhmä* M_{16}*, missä*

$$\langle x, y : x^8 = y^2 = e, y^{-1}xy = x^5 \rangle,$$

6. *ei-triviaalinen puolisuora tulo* $C_4 \rtimes C_4$*, missä*

$$\langle x, y : x^4 = y^4 = e, yx = x^3 y \rangle,$$

7. *ryhmä, missä*

$$\langle x, y : x^4 = y^4 = (yx)^2 = (y^{-1}x)^2 = e \rangle,$$

8. *puolisuora tulo* $(C_4 \times C_2) \rtimes C_2$ *("Paulin ryhmä"), missä*

$$\langle x, y, z : x^2 = y^2 = z^2 = e, xyz = yzx = zxy \rangle, \quad ja$$

9. *yleistetty kvaterniooryhmä* Q_{16}*, missä*

$$\langle x, y : x^4 = y^2 = (xy)^2 \rangle$$

Todistus. [8, luku 4.2], [12] □

Lause 5.17 (Tapaus $n = 18$)**.** *Olkoon* G *ryhmä, jonka kertaluku on* 18*. Tällöin ryhmä* G *on isomorfinen jonkin seuraavan ryhmän kanssa:*

1. *syklinen ryhmä* C_{18}*,*

2. *syklisten ryhmien suora tulo* $C_3 \times C_6$*,*

3. *dihedraaliryhmä* D_9*,*

4. *syklisen ja symmetrisen ryhmän suora tulo* $C_3 \times S_3$*, missä*

$$\langle x, y, z : x^3 = y^2 = z^3 = e, yxy = x^{-1}, xz = zx, yz = zy \rangle, \quad ja$$

5. *puolisuora tulo* $(C_3 \times C_3) \rtimes C_2$, *missä*

$$\langle x, y, z : x^2 = y^3 = z^3 = e, yxy = x, zxz = x, yz = zy \rangle.$$

Todistus. [11, Corrigé 10.5] □

Ryhmät, joiden kertaluku on 18 todistetaan Sylowin lauseilla Ulmerin [11] oppikirjan harjoitustehtävän ratkaisussa. Lisäksi esimerkiksi Finottin [7] ja Tschinkelin [10] kurssin harjoitustehtävissä käydään tapaukset läpi jollakin tasolla.

Lause 5.18. *Olkoon G ryhmä, jonka kertaluku on 20. Tällöin ryhmä G on isomorfinen seuraavien ryhmien kanssa:*

1. *syklinen ryhmä C_{20},*
2. *syklisten ryhmien suora tulo $C_2 \times C_{10}$,*
3. *dihedraaliryhmä D_{10},*
4. *puolisuora tulo $C_5 \rtimes C_4$, missä*

$$\langle x, y : x^4 = y^5 = e, yxy = x \rangle, \quad \textit{ja}$$

5. *Frobeniuksen ryhmä Fr_{20}, missä*

$$\langle x, y : x^4 = y^5 = e, yx = xy^2 \rangle.$$

Kertaluvultaan 20 olevat ryhmät pyydetään luettelemaan esimerkiksi Dummit ja Footen [6] teoksessa sivun 186 harjoitustehtävässä 12. Deopurkar [5] käy läpi ryhmät lyhykäisesti.

Viitteet

[1] M. A. Armstrong: *Groups and Symmetry*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1988.

[2] Michael Artin: *Algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[3] Nathan Carter, Ray Ellis: *Group Explorer*. Viitattu 29.2.2024. https://nathancarter.github.io/group-explorer/

[4] Nathan C. Carter: *Visual group theory*. Classroom Resource Materials Series. Mathematical Association of America, Washington, DC, 2009.

[5] Anand Deopurkar: *Modern Algebra 1: Classification of Groups of Order up to 30 (with some exceptions)*, The Australian National University.

[6] David S. Dummit, Richard M. Foote: *Abstract Algebra*, John Wiley and Sons Inc, 3. painos, 2004.

[7] Luis Finotti: *Groups of order 18* (harjoitustehtävien ratkaisut), University of Tennessee - Knoxville.

[8] Jérôme Lapuyade-Lahorgue: *Groups of order 8 and 16.*, Cornell University, arxiv.1807.10004, 2018.

[9] Joseph J. Rotman: *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 4. painos, 1995.

[10] Yuri Tschinkel: *Algebra: Homework 3* (harjoitustehtävien ratkaisut), University of New York - Courant Institute of Mathematical Sciences.

[11] Felix Ulmer: *Théorie des groupes*, Editions Ellipses, 2. laitos, 2021.

[12] Marcel Wild: *The Groups of Order Sixteen Made Easy*, The American Mathematical Monthly, Vol. 112, No. 1 (Jan. 2005), pp. 20-31.

Liite

Alla olevaa taulukkoa lukiessa on hyvä huomioida, että ”lause”-sarake viittaa tekstissä ilmenevään lauseeseen, joka todistaa halutun rivin tapauksen. Numeroinnista saa selville, missä luvussa todistus käydään läpi. Taulukossa ilmenevä värikoodaus kytkeytyy tekstissä ilmenevään värikoodaukseen.

$\lvert G\rvert = n$	tapaus	lause	$\cong$ lkm
$n = 1$	$n = p$	3.3	1
$n = 2$	$n = p$	3.3	1
$n = 3$	$n = p$	3.3	1
$n = 4$	$n = p^2$	4.24	2
$n = 5$	$n = p$	3.3	1
$n = 6$	$n = 2p$	4.27	2
$n = 7$	$n = p$	3.3	1
$n = 8$	erikoistapaus	3.22	5
$n = 9$	$n = p^2$	4.24	2
$n = 10$	$n = 2p$	4.27	2
$n = 11$	$n = p$	3.3	1
$n = 12$	erikoistapaus	5.11	5
$n = 13$	$n = p$	3.3	1
$n = 14$	$n = 2p$	4.27	2
$n = 15$	$n = pq, p \nmid (q-1)$	5.12	1
$n = 16$	erikoistapaus	5.15, 5.16	14
$n = 17$	$n = p$	3.3	1
$n = 18$	p^2q	5.17	5
$n = 19$	$n = p$	3.3	1
$n = 20$	p^2q	5.18	5
$n = 21$	$n = pq, p \mid (q-1)$	5.12	2

Äärellisten ryhmien luokittelua.
Kertaluvun tapaukset 1-21.