Oulun yliopisto **TIIVISTELMÄ OPINNÄYTETYÖSTÄ (liite FM-tutkielmaan)**
Luonnontieteellinen tiedekunta **Maisterintutkinnon kypsyysnäyte**

Laitos: Matemaattisten tieteiden laitos **Pääaine:** Matematiikka

Tekijä (Sukunimi ja etunimet)	**Tutkielman sivumäärä**
Isopahkala Joel Viljami	34

Työn nimi

Äärellisten ryhmien teorian peruslauseita

Asiasanat: Ryhmäteoria, äärelliset ryhmät, algebra

Tutkimus käsittelee pääasiassa äärellisiä ryhmiä ja muutamaa tärkeää lausetta, jotka liittyvät nimenomaan äärellisiin ryhmiin. Tärkein kysymys tutkielmassa on, että miten ryhmän kertaluku vaikuttaa ryhmän rakenteeseen. Tässä tutkielmassa tähän kysymykseen vastataan Cauchyn ja Sylowin lauseilla. Tutkimus on luonteeltaan teoreettinen ja tärkeimmät lähteet, joita apuna käyttäen Cauchyn ja Sylowin lauseet on todistettu, ovat teokset I.N. Herstein: Abstract Algebra- 3rd edition, Prentice Hall, New Jersey, 1990 ja I.N. Herstein: Topics in Algebra- 2nd edition, John Wiley & Sons, New York, 1975.

Tutkielma alkaa toisessa luvussa perusasioiden läpikäymisellä, eli käydään läpi melko tarkasti alusta asti määritelmät, lauseet ja apulauseet, joiden avulla sitten voidaan todistaa tärkeät lauseet. Kolmannessa luvussa käydään läpi Cauchyn lause, joka kertoo, että jos ryhmän kertaluku on jaollinen jollain alkuluvulla, niin tällöin ryhmä sisältää alkion, jonka kertaluku on tämä kyseinen alkuluku. Tämä lause ei vielä kovin selkeästi kerro, miten ryhmän kertaluku vaikuttaa rakenteeseen, mutta on hyvänä apuna Sylowin lauseiden todistuksissa.

Neljäs luku käsittelee Sylowin lauseita, joita on kolme kappaletta. Ensimmäinen Sylowin lause kertoo, että jos ryhmän kertaluku on muotoa $p^n m$, missä p on alkuluku, niin tälle ryhmälle on olemassa aliryhmä, jonka kertaluku on p^n. Seuraavat kaksi Sylowin lausetta vielä hieman syventävät tätä tietoa ja antavat esimerkiksi tällaisten aliryhmien lukumäärän. Näiden lauseiden avulla saadaan usein melko helposti paljon tietoa ryhmän rakenteesta, ja voidaan tutkia esimerkiksi, onko ryhmä yksinkertainen tai Abelin ryhmä. Lopussa olevat kaksi esimerkkiä käsittelevät nimenomaan näitä kahta tapausta.

Tämä tutkielma on vasta pieni raapaisu siitä, miten ryhmän kertaluvun vaikutusta rakenteeseen voidaan tutkia ja pelkästään Sylowin lauseiden sovelluksia voidaan laajentaa vielä todella paljon. Usein, kun tutkitaan esimerkiksi ryhmien yksinkertaisuutta, ei päästä lopputulokseen noin helposti kuin tässä tutkielmassa. Tämän tutkielman avulla lukija kuitenkin oppii tärkeitä äärellisten ryhmien ominaisuuksia ja saa hyvää pohjatietoa ryhmän kertaluvun vaikutuksesta ryhmän rakenteeseen.

Muita tietoja

Äärellisten ryhmien teorian peruslauseita

Pro Gradu-tutkielma

Viljami Isopahkala

Matemaattisten tieteiden laitos

Oulun yliopisto

2015

Sisältö

Luku 1

Johdanto

Tämä tutkielma käsittelee pääasiassa äärellisiä ryhmiä, kuten otsikkokin kertoo. Pohjatietona oletetaan, että lukijalla on jonkinlaista matemaattista pohjaa, erityisesti matemaattiset merkinnät, lukujoukot yms. tulisi olla hallussa. Lukijalla olisi hyvä olla myös jonkinlaista pohjatietoa lukuteoriaan ja ryhmiin liittyen, mutta tässä tutkielmassa on luvussa 2 käyty perusasiat aika hyvin läpi todistuksineen. Kaikki tuon luvun esitiedot, jotka tässä on käyty läpi, liittyvät suoraan tärkeisiin tuloksiin, joten yhtään sellaista määritelmää tai lausetta ei tässä tutkielmassa käydä läpi, jota ei hyödynnettäisi myöhemmin.

Tärkein kysymys tässä tutkielmassa on, että miten ryhmän kertaluku vaikuttaa ryhmän rakenteeseen. Vähänkin ryhmäteoriaa lukenut todennäköisesti tietää Lagrangen lauseen, jonka mukaan äärellisen ryhmän jokaisen aliryhmän kertaluku jakaa ryhmän kertaluvun. Sittemmin vuonna 1845 Cauchy todisti lauseen, jonka mukaan jokaista ryhmän kertaluvun alkulukutekijää p kohden löytyy aliryhmä, jonka kertaluku on p. Tämän tutkielman luvussa 3 todistetaan Cauchyn lause, joka on tosin vähän eri muodossa kuin juuri esitetty.

Vuonna 1872, norjalainen ryhmäteoreetikko Peter Ludwig Mejdell Sylow

(1832-1918) syvensi Cauchyn lausetta osoittamalla, että jokaista p:n potenssia kohti, joka jakaa ryhmän kertaluvun, löytyy aliryhmä vastaavalla kertaluvulla. Luvussa 4 on käyty läpi Sylowin 3 lausetta, joissa käsitellään aihetta tarkemmin ja nimenomaan nämä Sylowin kehittämät lauseet ovat tämän tutkielman pääosassa. Cauchyn lause on kuitenkin hyödyllinen siinäkin mielessä, että sitä on hyödynnetty erään Sylowin lauseen todistuksessa. Luvussa 4 on käyty myös läpi pari esimerkkiä siitä, miten voidaan soveltaa Sylowin lauseita ja miten ryhmän kertaluvusta voidaan tehdä päätelmiä ryhmän rakenteesta.

Pääasiassa tärkeät lauseet, eli kaksi ensimmäistä Sylowin lausetta ja Cauchyn lause (sekä useita luvun 2 tuloksia) on todistettu käyttäen lähdettä [1]. Sylowin 3. lause on todistettu käyttäen lähdettä [2]. Esitieto- luvussa on käytetty pääosin lähteitä [3] ja [4].

Luku 2

Esitiedot

2.1 Funktioista

Määritelmä 2.1.1. Funktio $f : A \to B$ on sääntö tai kuvaus, joka liittää jokaiseen joukon A alkioon täsmälleen yhden joukon B alkion. Joukkoa A kutsutaan lähtö- tai määrittelyjoukoksi ja joukkoa B kutsutaan maalijoukoksi. Jos määrittelyjoukon alkio $x \in A$ kuvautuu maalijoukon alkioksi $y \in B$, niin merkitään $y = f(x)$.

Määritelmä 2.1.2. Kuvaus $f : A \to B$ on surjektio, jos jokaista maalijoukon alkiota $b \in B$ kohden on olemassa lähtöjoukon alkio $a \in A$ siten, että $f(a) = b$. Ts. jokaiseen lähtöjoukon alkioon voidaan liittää jokin maalijoukon alkio.

Määritelmä 2.1.3. Kuvaus $f : A \to B$ on injektio, jos kaikille $a_1, a_2 \in A, a_1 \neq a_2$ pätee $f(a_1) \neq f(a_2)$. Ts. mitkään kaksi lähtöjoukon alkiota eivät kuvaudu samalle maalijoukon alkiolle.

Määritelmä 2.1.4. Kuvaus $f : A \to B$ on bijektio, jos kuvaus on sekä surjektio, että injektio.

Määritelmä 2.1.5. Olkoon A Joukko. Nyt kuvausta $Id : A \to A$ sanotaan identiteettikuvaukseksi, jos $\forall x \in A$ pätee, että $Id(x) = x$.

2.2 Lukuteoriaa

Määritelmä 2.2.1. Olkoot $a, b \in \mathbb{Z}$. Tällöin b jakaa a:n eli $b|a$, jos on olemassa sellainen $c \in \mathbb{Z}$, että

$$a = bc.$$

Kun $b|a$, niin b on a:n tekijä ja a on b:n monikerta.

Määritelmä 2.2.2. Olkoot $a, b \in \mathbb{Z}$, joista ainakin toinen ei ole nolla. Nyt luku c on lukujen a ja b suurin yhteinen tekijä, jos

1. $c \mid a$ ja $c \mid b$,
2. $d \mid a$ ja $d \mid b \Rightarrow d \leq c$.

Suurinta yhteistä tekijää merkitään $syt(a, b) = c$.

2.3 Ekvivalenssirelaatiosta

Määritelmä 2.3.1. Olkoon A epätyhjä joukko. Tällöin joukkoa

$$A \times A = \{(a_1, a_2) | a_1, a_2 \in A\}$$

kutsutaan joukon A karteesiseksi tuloksi itsensä kanssa.

Määritelmä 2.3.2. Joukon $A \times A$ osajoukkoa R sanotaan binääriseksi relaatioksi joukossa A. Jos pari $(x, y) \in R$, niin merkitään xRy ja sanotaan, että alkio x on relaatiossa R alkion y kanssa.

Huomautus. Tästä eteenpäin käytetään relaatiosta R merkintää $\sim$, eli esimerkiksi $xRy = x \sim y$.

Määritelmä 2.3.3. Joukon A binäärinen relaatio $\sim$ on ekvivalenssirelaatio, mikäli

1. $x \sim x$ aina, kun $x \in A$;
2. $x \sim y \Rightarrow y \sim x$ aina, kun $x, y \in A$;
3. $x \sim y$ ja $y \sim z \Rightarrow x \sim z$ aina, kun $x, y, z \in A$.

Jos $\sim$ on ekvivalenssirelaatio ja $a \in A$, niin joukkoa

$$[a] = \{x \in A | x \sim a\}$$

sanotaan alkion a määräämäksi ekvivalenssiluokaksi.

Lause 2.3.4. *Jos $\sim$ on ekvivalenssirelaatio ja $a \sim b$, niin $[a] = [b]$.*

Todistus. Jos $x \in [a]$, niin $x \sim a$. Koska $a \sim b$, niin $x \sim b$. Siten $x \in [b]$. Näin ollen $[a] \subset [b]$. Jos $y \in [b]$, niin $y \sim b$. Koska $a \sim b$, niin $b \sim a$ ja siten $y \sim a$, eli $y \in [a]$. Näin ollen $[b] \subset [a]$. Eli saadaan, että $[a] = [b]$. □

Lause 2.3.5. *Jos $\sim$ on joukon A ekvivalenssirelaatio, niin kaikkien ekvivalenssiluokkien yhdiste (unioni) on koko joukko A. Lisäksi, jos $[a] \neq [b]$, niin $[a] \cap [b] = \emptyset$.*

Todistus. Jos $a \in A$, niin $a \sim a$, eli $a \in [a]$. Nyt $\bigcup_{a \in A} [a] = A$. Jos $x \in [a] \cap [b]$, niin $x \sim a$ ja $x \sim b$. Eli $a \sim x$ ja $x \sim b$ ja siten $a \sim b$ ja tästä seuraa lauseen 2.3.4 mukaan, että $[a] = [b]$. Jos siis $[a] \neq [b]$, niin $[a] \cap [b] = \emptyset$. □

2.4 Ryhmistä

Määritelmä 2.4.1. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G binäärinen operaatio. Pari $(G, *)$ on ryhmä, mikäli seuraavat kolme ehtoa toteutuvat:

1. $(*)$ on assosiatiivinen eli

   $$(a * b) * c = a * (b * c)$$

   aina, kun $a, b, c \in G$;

2. Joukossa G on sellainen alkio e, että

   $$a * e = e * a = a$$

   aina, kun $a \in G$. Alkiota e kutsutaan ykkös- tai neutraalialkioksi;

3. Aina, kun $a \in G$, on olemassa sellainen alkio $a^{-1} \in G$, että

   $$a * a^{-1} = a^{-1} * a = c.$$

   Alkiota a^{-1} kutsutaan alkion a käänteisalkioksi. Jos lisäksi $(G, *)$ toteuttaa ehdon

4. $a * b = b * a$ aina, kun $a, b \in G$ eli $(*)$ on kommutatiivinen,

niin kyseessä on Abelin ryhmä eli kommutatiivinen ryhmä.

Jatkossa ryhmästä $(G, *)$ käytetään pelkästään merkintää G, kun operaatiosta $(*)$ ei ole epäselvyyttä ja merkitään operaatiota $a * b$ lyhyemmin ab.

Ryhmän G kertaluku tarkoittaa, kuinka monta alkiota on ryhmässä G ja sitä merkitään $|G|$.

2.4.1 Aliryhmä

Määritelmä 2.4.2. Olkoon G ryhmä ja $H \subseteq G$, $H \neq \emptyset$. Jos H on ryhmä, sitä sanotaan ryhmän G aliryhmäksi ja merkitään $H \leq G$.

Lause 2.4.3. *(Aliryhmäkriteeri). Olkoot G ryhmä ja $H \subseteq G$, $H \neq \emptyset$. Nyt $H \leq G$ jos ja vain jos seuraavat ehdot toteutuvat:*

1. $a, b \in H \Rightarrow ab \in H$;
2. $a \in H \Rightarrow a^{-1} \in H$.

Todistus. 1. Jos $H \leq G$, niin H on ryhmä ja siten ehdot toteutuvat.

2. Ehdosta 1 seuraa, että kyseessä on binäärinen operaatio joukossa H. Ehdosta 2 seuraa, että jokaisella joukon H alkiolla on käänteisalkio H:ssa. Koska operaatio on assosiatiivinen ryhmässä G, niin on se sitä myös G:n osajoukossa H. Tarkastetaan vielä, onko $e \in H$. Jos $a \in H$, niin ehdon 2 nojalla on olemassa $a^{-1} \in H$. Ehdon 1 nojalla $aa^{-1} \in H$, eli $e \in H$. Siis H on ryhmä, eli $H \leq G$.

□

Huomautus. Aliryhmäkriteerin kaksi ehtoa voidaan yhdistää. Eli $H \leq G$, jos ja vain jos ehto

$$a, b \in H \Rightarrow ab^{-1} \in H$$

on voimassa.

Määritelmä 2.4.4. Olkoon $H \leq G$ ja $a \in G$. Joukkoa $aH = \{ah | h \in H\}$ sanotaan alkion a määräämäksi aliryhmän H vasemmaksi sivuluokaksi.

Huomautus.

- Koska $eH = H$, niin H itse on eräs vasen sivuluokka.

- Kuvaus $f : H \to aH, f(h) = ah$ on bijektio, joten sivuluokassa aH on yhtä monta alkiota, kuin aliryhmässä H.

- Vasenta sivuluokkaa vastaavalla tavalla voidaan määritellä myös ryhmän G alkion a määräämä aliryhmän H oikea sivuluokka

$$Ha = \{ha | h \in H\},$$

missä $a \in G$.

Lause 2.4.5. *(Lagrangen lause). Olkoot G äärellinen ryhmä, $H \leq G$ ja n aliryhmän H vasempien sivuluokkien lukumäärä ryhmässä G. Tällöin*

$$|G| = n|H|,$$

ts. äärellisessä ryhmässä aliryhmän kertaluku jakaa ryhmän kertaluvun.

Todistus. Olkoot $a_1H, a_2H, ..., a_nH$ aliryhmän H vasemmat sivuluokat. Lauseesta 2.3.5 saadaan, että ryhmä G voidaan muodostaa näiden ekvivalenssiluokkien unionina. Eli tällöin $G = \bigcup_{k=1}^{n} a_kH$ ja $a_1H \cap a_iH = \emptyset$, kun $2 \leq i \leq n$. Nyt $|a_iH| = |H|$, mistä saadaan, että $|G| = n|H|$. □

2.4.2 Syklinen ryhmä

Olkoon G ryhmä ja $a \in G$. Nyt joukko $H = \left\{a^k | k \in \mathbb{Z}\right\}$ on joukon G osajoukko. Jos $x, y \in H$, niin $x = a^m$ ja $y = a^n$ joillakin $m, n \in \mathbb{Z}$ sekä

$$xy^{-1} = a^m a^{-n} = a^{m-n} \in H.$$

Nyt H on ryhmän G aliryhmä.
Perustelu (aliryhmäkriteeri):

1. $xy = a^m a^n = a^{m+n} \in H$, sillä $m + n \in \mathbb{Z}$.

2. $x^{-1} = (a^m)^{-1} = a^{-m} \in H$, sillä $-m \in \mathbb{Z}$.

Määritelmä 2.4.6. Yllä määriteltyä ryhmää H sanotaan alkion a generoimaksi sykliseksi ryhmäksi ja merkitään $H = \langle a \rangle$. Alkio a on generoija.

Lause 2.4.7. *Jos ryhmän G kertaluku on alkuluku, niin ryhmä G on syklinen.*

Todistus. Kun ryhmän G kertaluku on alkuluku, niin lagrangen lauseen nojalla ryhmän G ainoat aliryhmät ovat vain neutraalialkion sisältävä ryhmä $\{e\}$ tai koko ryhmä G. Olk. alkio $x \in G$, jolle $x \neq e$. Tällöin alkion x generoima syklinen ryhmä $\langle x \rangle$ on ryhmän G aliryhmä. Nyt $\langle x \rangle$ ei selvästikään voi olla vain neutraalialkion sisältämä ryhmä, joten täytyy päteä $\langle x \rangle = G$. Ryhmä G on siis syklinen. □

Määritelmä 2.4.8. Olkoon G ryhmä ja $g \in G$. Jos $\exists n \in \mathbb{N}$ siten, että $g^n = e$, niin pienin tällainen n on alkion g kertaluku ja merkitään $|g| = n$. Jos $g^n \neq e \ \forall n \in \mathbb{N}$, niin $|g| = \infty$.

Lause 2.4.9. *Olkoon G ryhmä. Nyt $\forall x \in G: \ |x| = |x^{-1}|$, eli alkion ja sen käänteisalkion kertaluvut ovat samat.*

Todistus. Ryhmissä pätee: $(x^k)^{-1} = x^{-k} = (x^{-1})^k$ Olkoon nyt

$$x^k = e \Rightarrow (x^{-1})^k = e^{-1} = e$$

ja tästä saamme, että $|x^{-1}| \leq |x|$. Toisaalta

$$(x^{-1})^k = e \Rightarrow ((x^{-1})^{-1})^k = e^{-1} \Rightarrow x^k = e^{-1} = e,$$

joten $|x| \leq |x^{-1}|$. □

Lause 2.4.10. *Olkoon G ryhmä ja $x \in G$. Nyt $x = x^{-1} \Leftrightarrow |x| = 2$.*

Todistus. Olkoon $x \in G$ ja $x \neq e$. Nyt

$$|x| = 2$$

$$\Leftrightarrow xx = e$$

$$\Leftrightarrow x = x^{-1}.$$

□

2.4.3 Normaali aliryhmä ja tekijäryhmä

Määritelmä 2.4.11. Olkoon $N \leq G$. Aliryhmää N sanotaan normaaliksi, jos $aN = Na$ aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.

Huomautus.

1. $\{e\} \trianglelefteq G$ ja $G \trianglelefteq G$.

2. Jos G on Abelin ryhmä ja $N \leq G$, niin

$$aN = \{an | n \in N\} = \{na | n \in N\} = Na.$$

Siis Abelin ryhmän jokainen aliryhmä on normaali.

Lause 2.4.12. *Olkoon G ryhmä ja $N \leq G$. Nyt $N \trianglelefteq G$ jos ja vain jos*

$$ana^{-1} \in N \ \forall a \in G, \ n \in N.$$

Todistus. Oletetaan ensin, että $N \trianglelefteq G$. Valitaan nyt mielivaltaiset sivuluokkien alkiot $an = ma$, missä $n, m \in N$. Kerrotaan tämä oikealta a^{-1}:llä ja saadaan $ana^{-1} = m \in N$.

Oletetaan sitten, että $ana^{-1} \subseteq N \ \forall a \in G$ ja $n \in N$. Pyritään osoittamaan, että $aN = Na$. Olkoon nyt $n \in N$ ja merkitään $ana^{-1} = n_1$. Oletuksen

mukaan $n_1 \in N$. Operoidaan yhtälöä nyt oikealta a:lla ja saadaan $an = n_1 a$. Nyt siis $n_1 a \in Na \Rightarrow aN \subseteq Na$. Merkitään nyt, että $a^{-1}na = n_2$, missä $n_2 \in N$. Operoidaan tätä yhtälöä vasemmalta a:lla ja saadaan $na = an_2$. Nyt siis $an_2 \in aN \Rightarrow Na \subseteq aN$.

Näin ollen $aN = Na$. □

Olkoon $N \leq G$. Määritellään Sivuluokkien joukossa $\{aN|a \in G\}$ tulo $(\cdot)$ seuraavasti:

$$aN \cdot bN = abN.$$

Todistetaan, että sivuluokkien joukko $\{aN|a \in G\}$ yhdessä edellä esitellyn tulo-operaation kanssa muodostaa ryhmän.

Lause 2.4.13. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin $(\{aN|a \in G, \cdot\})$ on ryhmä.*

Todistus. Nyt $aN \cdot bN = abN$, eli kyseessä on binäärinen operaatio. Todistetaan ensin assosiatiivisuus:
$(aN \cdot bN) \cdot cN = abN \cdot cN = (ab)cN = a(bc)N = aN \cdot bcN = aN \cdot (bN \cdot cN)$.
Neutraalialkio on eN, sillä $eN \cdot aN = eaN = aN$ ja $aN \cdot eN = aeN = aN$.
Alkion aN käänteisalkio on $a^{-1}N$, sillä $aN \cdot a^{-1}N = aa^{-1}N = eN$ ja $a^{-1}N \cdot aN = a^{-1}aN = eN$. □

Määritelmä 2.4.14. Lauseessa 2.4.13 esiteltyä paria $(\{aN|a \in G, \cdot\})$ kutsutaan ryhmän G tekijäryhmäksi normaalin aliryhmän N suhteen. Kyseisestä ryhmästä käytetään merkintää G/N.

Huomautus.

$$|G/N| = \frac{|G|}{|N|},$$

mikäli ryhmä G on äärellinen.

2.4.4 Ryhmähomomorfismi

Määritelmä 2.4.15. Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä. Kuvausta $f : G \to H$ sanotaan ryhmähomomorfismiksi ryhmältä G ryhmälle H, mikäli

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

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

Lause 2.4.16. *Olkoon $f : G \to H$ homomorfismi ja olkoot e_G ja e_H ryhmien G ja H neutraalialkiot. Tällöin*

$$f(e_G) = e_H \qquad ja \qquad f(a^{-1}) = f(a)^{-1}$$

aina, kun $a \in G$.

Todistus. Koska kuvaus on homomorfismi, niin

$$f(e_G) * f(e_G) = f(e_G \cdot e_G) = f(e_G) = f(e_G) * e_H.$$

Nyt siis

$$f(e_G) * f(e_G) = f(e_G) * e_H$$

ja kun molemmat puolet kerrotaan vasemmalta $f(e_G)^{-1}$:llä, niin saadaan

$$f(e_G) = e_H.$$

Olkoon $a \in G$. Nyt

$$f(a^{-1}) * f(a) = f(a^{-1} \cdot a) = f(e_G) = e_H$$

ja

$$f(a) * f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H.$$

Täytyy siis pitää paikkaansa, että $f(a^{-1}) = f(a)^{-1}$. □

Määritelmä 2.4.17. Olkoon $f : G \to H$ homomorfismi. Joukkoa

$$Im(f) = f(G) = \{f(x) | x \in G\}$$

sanotaan homomorfismin f kuvaksi ja joukkoa

$$Ker(f) = \{x \in G | f(x) = e_H\}$$

sanotaan homomorfismin f ytimeksi.

Lause 2.4.18. *Olkoon kuvaus $f : (G, \cdot) \to (H, *)$ homomorfismi. Tällöin*

$$Ker(f) \trianglelefteq G.$$

Todistus. Todistetaan ensin, että $Ker(f) \leq G$. Nyt lauseen 2.4.16 mukaan $f(e_G) = e_H$, eli $e_G \in Ker(f)$ ja näin ollen ydin on epätyhjä. Olkoon $a, b \in Ker(f)$. Edelleen Lauseen 2.4.16 mukaan tiedetään, että $f(a^{-1}) = f(a)^{-1}$, eli saadaan

$$f(a \cdot b^{-1}) = f(a) * f(b^{-1}) = f(a) * f(b)^{-1} = e_H * (e_H)^{-1} = e_H.$$

Näin ollen $a \cdot b^{-1} \in Ker(f)$, eli aliryhmäkriteerin nojalla $Ker(f) \leq G$.
Olkoon $x \in G$ ja $n \in Ker(f)$. Nyt

$$f(x \cdot n \cdot x^{-1}) = f(x) * f(n) * f(x^{-1}) = f(x) * e_H * f(x)^{-1} = f(x) * f(x)^{-1} = e_H,$$

joten $x \cdot n \cdot x^{-1} \in Ker(f)$ ja normaalisuuskriteerin nojalla (lause 2.4.12) $Ker(f) \trianglelefteq G$. □

Lause 2.4.19. *Homomorfismi $f : G \to H$ on injektio, jos ja vain jos $Ker(f) = \{e_G\}$.*

Todistus. Oletetaan ensin, että f on injektio. Nyt lauseen 2.4.16 nojalla $f(e_G) = e_H$. Jos on olemassa jokin muu alkio, olkoon vaikka $x \in G$, jolle

$f(x) = e_H$, niin injektiivisyydestä seuraa, että $x = e_G$. Eli siis $Ker(f) = \{e_G\}$.

Olkoon nyt $Ker(f) = \{e_G\}$ ja olkoot $a, b \in G$. Nyt ehdosta $f(a) = f(b)$ seuraa, että $f(a) * f(b)^{-1} = e_H$ ja edelleen lauseen 2.4.16 nojalla $f(a) * f(b^{-1}) = e_H$. Ja koska kuvaus oli homomorfismi, niin saadaan $f(a \cdot b^{-1}) = e_H$, eli $a \cdot b^{-1} \in Ker(f)$. Nyt koska oletuksen mukaan $Ker(f) = \{e_G\}$, niin $a \cdot b^{-1} = e_G$ ja tästä nähdään lopulta, että $a = b$. Kuvaus siis on injektio. □

Määritelmä 2.4.20. Ryhmät $(G, \cdot)$ ja $(H, *)$ ovat isomorfiset eli rakenneyhtäläiset, mikäli on olemassa bijektio $f : G \to H$, joka toteuttaa ehdon $f(a \cdot b) = f(a) * f(b)$ aina, kun $a, b \in G$ (ts. f on bijektiivinen homomorfismi). Tällöin merkitään $G \cong H$ ja sanotaan, että f on ryhmäisomorfismi.

Lause 2.4.21. *(Homomorfismien peruslause). Olkoon $f : G \to H$ homomorfismi. Tällöin*

$$G/Ker(f) \cong Im(f).$$

Todistus. Heti aluksi kannattaa huomata, että ainakin $Ker(f) \trianglelefteq G$, kuten aiemmin todistettiin lauseessa 2.4.18, eli tekijäryhmän $G/Ker(f)$ muodostaminen on ainakin mahdollista. Merkitään nyt $Ker(f) = K$ ja määritellään kuvaus $F : G/K \to Im(f)$ siten, että kaikilla $a \in G$ pätee $F(aK) = f(a)$. Tehdään todistus tästä eteenpäin kolmessa osassa.

1. Tutkitaan ensin, onko kuvaus F hyvin määritelty. Olkoon $b \in G$. Jos $aK = bK$, niin $a \in bK$, eli $a = bk$, missä $k \in K$. Nyt

   $$F(aK) = f(a) = f(bk) = f(b)f(k) = f(b)e_H = f(b) = F(bK).$$

   Nyt siis F on riippumaton sivuluokan määrääjän a valinnasta, joten F on hyvin määritelty.

2. Tutkitaan, onko F bijektio. Ainakin se on surjektio, mikä seuraa suoraan F:n määritelmästä. Entä onko kuvaus injektio? Jos $F(aK) = e_H$, niin $f(a) = e_H$, eli $a \in K$. Tällöin $aK = K =$ ryhmän G/K ykkösalkio. Nyt siis lauseen 2.4.19 nojalla F on injektio.

3. Osoitetaan vielä, että F on homomorfismi. Olkoot $aK, bK \in G/K$. Nyt

$$F(aK \cdot bK) = F(abK) = f(ab) = f(a) * f(b) = F(aK) * F(bK).$$

Nyt on siis osoitettu, että F on bijektiivinen homomorfismi, eli isomorfismi, eli $G/Ker(f) \cong Im(f)$. □

Määritelmä 2.4.22. Olkoon G ryhmä. Jos $f : G \to G$ on homomorfismi ja bijektio, niin f on G:n automorfismi. Lisäksi kuvaus $f_a : G \to G,\ f(x) = a^{-1}xa$, missä $a \in G$, on alkion a indusoima G:n sisäinen automorfismi ja merkitään $I(G) = \{f_a | a \in G\}$.

2.5 Yleistä ryhmäteoriaa

Määritelmä 2.5.1. Olkoon $X = \{1, 2, ..., n\}$. Jos $\alpha : X \to X$ on bijektio, niin α on joukon X permutaatio. Merkitään $S_n = \{$joukon X kaikki permutaatiot$\}$ ja kutsutaan tätä symmetriseksi ryhmäksi astetta n (voit osoittaa itse, että $(S_n, \circ)$ on ryhmä). Lisäksi, jos $G \leq S_n$, niin G on astetta n oleva permutaatioryhmä.

Määritelmä 2.5.2. Olkoon G ryhmä ja $X = \{1, 2, ..., n\}$. Määritetään joukossa X seuraavanlainen ekvivalenssirelaatio:

$$i \sim j \Leftrightarrow \exists g \in G : g(i) = j.$$

Siis

$$X = \bigcup_{i=1}^{r} T_i, \text{missä } T_i : \text{t ovat ekvivalenssiluokkia.}$$

Nyt

$$|X| = \sum_{i=1}^{r} |T_i| = n.$$

Näitä ekvivalenssiluokkia $T_1, ..., T_r$ sanotaan permutaatioryhmän G radoiksi.

Määritelmä 2.5.3. Olkoon G ryhmä ja $A \leq G$ sekä $B \leq G$. Tällöin joukosta $AB = \{ab | a \in A, b \in B\}$ käytetään nimitystä kompleksi.

Huomautus. Yleensä AB ei ole G:n aliryhmä.

Lemma 2.5.4. *Olkoot $A \leq G$ ja $B \leq G$ äärellisiä. Tällöin*

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Todistus. Tulo ab, missä $a \in A$ ja $b \in B$, voidaan kirjoittaa $|A \times B| = |A| \cdot |B|$ tavalla. Osa näistä tuloista on kuitenkin keskenään identtisiä. Tutkitaan tarkemmin tuloa ab ja merkitään $E = \{(c, d) \in A \times B | cd = ab\}$ ja $T = \{(ax^{-1}, xb) | x \in A \cap B\}$. Osoitetaan, että $E = T$.

1. Nyt selvästi $ax^{-1} \in A, xb \in B$ ja $ax^{-1}xb = ab \Rightarrow T \subseteq E$.

2. Jos $(c, d) \in E$, niin $cd = ab$. Siis $c^{-1}a = db^{-1} \in A \cap B$. Merkitään nyt, että $x = c^{-1}a = db^{-1} \in A \cap B$. Siis $c = ax^{-1}$ ja $d = xb$, joten $E \subseteq T$.

Nyt on siis osoitettu, että $E = T$ ja $|E| = |T| = |A \cap B|$. Ja täten siis

$$|AB| = \frac{|A \times B|}{|A \cap B|} = \frac{|A||B|}{|A \cap B|}.$$

□

Määritelmä 2.5.5. Olkoon G ryhmä ja $a, g \in G$. Alkio $g^a = a^{-1}ga$ on alkion g konjugaatti. Lisäksi, jos $\emptyset \neq M \subseteq G$, niin $M^g = \{m^g | m \in M\}$ on joukon M konjugaatti G:ssä.

Huomautus. Jos $H \leq G$, niin $H^g \leq G$.

Todistus. Kuvaus $f_g : x \to x^g$ on G:n automorfismi. Siis $f_g(H) \leq G$ eli $H^g \leq G$. □

Määritellään ryhmässä G relaatio:

$$x \sim y \Leftrightarrow \exists a \in G : x^a = y.$$

Tämä relaatio on ekvivalenssirelaatio (helppo osoittaa itse). Näin muodostettuja ekvivalenssiluokkia sanotaan myös konjugointiluokiksi. Eli jos $x \in G$, niin $\{x^g | g \in G\}$ on eräs konjugointiluokka.

Huomautus. Olkoon G ryhmä. Lauseen 2.3.5 nojalla voimme todeta, että ryhmä G voidaan esittää G:n kaikkien konjugointiluokkien unionina.

Määritelmä 2.5.6. Olkoon G ryhmä ja joukko M epätyhjä ja lisäksi $M \subseteq G$. Nyt joukko $N_G(M) = \{g \in G | M^g = M\}$ on joukon M normalisoija G:ssä.

Määritelmä 2.5.7. Olkoon G ryhmä ja joukko M epätyhjä ja lisäksi $M \subseteq G$. Nyt joukko $C_G(M) = \{g \in G | gm = mg \ \forall m \in G\}$ on M:n sentralisoija G:ssä.

Huomautus. Alkion $a \in G$ sentralisoija G:ssä on joukko $C_G(a) = \{x \in G | xa = ax\}$.

Määritelmä 2.5.8. Olkoon G ryhmä. Nyt joukko $Z(G) = C_G(G) = \{g \in G | gx = xg \ \forall x \in G\}$ on ryhmän G keskus.

Määritelmä 2.5.9. Olkoon $A \leq G$, $B \leq G$ ja $g \in G$. Nyt

$$AgB = \{agb | a \in A, \ b \in B\}$$

on aliryhmien A ja B muodostama kaksoissivuluokka.

Määritelmä 2.5.10. Olkoon G äärellinen ryhmä ja $H \leq G$. Nyt $[G : H]$ on H:n indeksi G:ssä ja $[G : H] = H$:n sivuluokkien lukumäärä G:ssä. Lisäksi $[G : H] = |G|/|H|$.

Lause 2.5.11. *Olkoon G äärellinen ryhmä ja $\emptyset \neq M \subseteq G$. Indeksi $[G : N_G(M)]$ = joukon M konjugaattien lukumäärä G:ssä.*

Todistus. Osoitetaan, että

$$\sigma : \{gN_G(M)|g \in G\} \to \{M^g|g \in G\},\ \sigma(tN_G(M)) = M^{t^{-1}}$$

on bijektio.

1. Tarkistetaan ensin, että tämä ylipäätään on kuvaus. $tN_G(M) = sN_G(M) \Rightarrow t \in sN_G(M) \Rightarrow t = sn$ $(n \in N_G(M))$. Siis $M^{t^{-1}} = M^{(sn)^{-1}} = M^{n^{-1}s^{-1}} = (M^{n^{-1}})^{s^{-1}} = M^{s^{-1}}$.

2. Kuvaus on surjektio, sillä $\sigma(g^{-1}N_G(M)) = M^g$.

3. Onko kuvaus injektio? Nyt $\sigma(tN_G(M)) = \sigma(sN_G(M)) \Rightarrow M^{t^{-1}} = M^{s^{-1}} \Rightarrow (M^{t^{-1}})^s = (M^{s^{-1}})^s = M^{t^{-1}s} = M \Rightarrow t^{-1}s \in N_G(M) \Rightarrow s \in tN_G(M) \Rightarrow sN_G(M) = tN_G(M)$.

Näin ollen kuvaus σ on bijektio ja $[G : N_G(M)] = |\{M^g|g \in G\}|$. □

Huomautus. Jos $M = \{g\}$, niin $N_G(M) = N_G(\{g\}) = C_G(g)$. Siis alkion g konjugointiluokkien lukumäärä G:ssä

$$= [G : C_G(g)] = \frac{|G|}{|C_G(g)|}.$$

Lause 2.5.12. *Olkoon G ryhmä ja $a \in G$. Nyt $C_G(a) \leq G$.*

Todistus. 1. $e \in C_G(a)$, koska $ea = e = ae$.

2. Olkoon $x \in C_G(a)$. Nyt

$$\begin{aligned} & xa = ax \\ \Leftrightarrow\ & x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} \\ \Leftrightarrow\ & (x^{-1}x)ax^{-1} = x^{-1}a(xx^{-1}) \\ \Leftrightarrow\ & ax^{-1} = x^{-1}a. \end{aligned}$$

   Eli $x^{-1} \in C_G(a)$.

3. Olkoon $x, y \in C_G(a)$. Nyt

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$

   Eli $xy \in C_G(a)$.

□

Luku 3

Cauchyn lause

Ennen varsinaista Cauchyn lausetta todistetaan apulause, joka auttaa myöhemmin todistamaan Cauchyn lauseen. Määritellään lemmaa varten joukko S ja $f \in A(S)$. Määritellään S:ssä seuraava relaatio: $s \sim t$, jos $t = f^i(s)$ jollekin kokonaisluvulle i (i voi olla positiivinen, negatiivinen tai nolla). Tämä relaatio on ekvivalenssirelaatio S:ssä. Alkion s ekvivalenssiluokka $[s]$ on nimeltään s:n rata f:ssä.

Lemma 3.0.13. *Jos $f \in A(S)$, $|f| = p$ ja p on alkuluku, niin tällöin minkä tahansa S:n alkion radalla f:ssä on 1 tai p alkiota.*

Todistus. Olkoon $s \in S$; jos $f(s) = s$, niin s:n rata f:ssä sisältää ainoastaan s:n itse, eli vain yhden alkion. Oletetaan sitten, että $f(s) \neq s$. Tarkastellaan alkioita $s, f(s), f^2(s), ..., f^{p-1}(s)$; väitämme, että nämä p alkiota ovat erillisiä ja muodostavat s:n radan f:ssä. Jos näin ei ole, niin $f^i(s) = f^j(s)$ jollekin $0 \leq i < j \leq p-1$, mistä saamme, että $f^{j-i}(s) = s$. Olkoon $m = j - i$; tällöin $0 < m \leq p-1$ ja $f^m(s) = s$. Mutta $f^p(s) = s$ ja koska $p \nmid m, ap + bm = 1$ joillekin kokonaisluvuille a ja b. Siispä $f^1(s) = f^{ap+bm}(s) = f^{ap}(f^{bm}(s)) = f^{ap}(s) = s$, koska $f^m(s) = f^p(s) = s$. Tämä on ristiriidassa alkuoletuksen

$f(s) \neq s$ kanssa. Niinpä s:n rata f:ssä sisältää alkiot $s, f(s), f^2(s), ..., f^{p-1}(s)$, joita on siis p kappaletta. □

Todistetaan vielä ryhmän kertalukuun liittyvä lause, jonka jälkeen pääsemme käsiksi varsinaiseen cauchyn lauseeseen.

Lause 3.0.14. *Olkoon G ryhmä ja olkoon ryhmän G kertaluku parillinen. Nyt $\exists x \in G : \ |x| = 2$.*

Todistus. Jokaisessa ryhmässä vain neutraalialkiolle pätee $e = e^{-1}$ kertaluvulla 1. Nyt meille jää siis pariton määrä alkioita. Lauseen 2.4.9 mukaan jokaiselle $x \in G : \ |x| > 2$ löytyy käänteisalkiopari siten, että $|x| = |x^{-1}|$. Nyt koska alkioita on pariton määrä, niin jäljelle jääneelle alkiolle, olkoon vaikka a, täytyy päteä $a = a^{-1}$ ja lauseen 2.4.10 nojalla tälle alkiolle pätee myös $|a| = 2$. □

Lause 3.0.15. *(Cauchy) Jos p on alkuluku ja p jakaa ryhmän G kertaluvun, niin G sisältää kertalukua p olevan alkion.*

Todistus. Jos $p = 2$, niin ollaan lauseen 3.0.14 tilanteessa, jolloin lause pätee. Olkoon nyt $p \neq 2$. Nyt joukko S pitää sisällään kaikki järjestetyt alkiot $(a_1, a_2, ..., a_{p-1}, a_p)$, missä $a_1, ..., a_p \in G$ ja $a_1 a_2 \cdots a_p = e$. Nyt väitämme, että S sisältää n^{p-1} alkiota, missä $n = |G|$. Todistetaan väite seuraavaksi.

Voimme valita alkiot $a_1, ..., a_{p-1}$ G:stä n:llä eri tavalla, joten nyt meillä on kasassa n^{p-1} alkiota. Muistetaan nyt, että $a_1, ..., a_{p-1}, a_p = e$ ja tästä saadaan, että $a_p = (a_1, ..., a_{p-1})^{-1}$. Nyt siis

$$a_1 a_2 \cdots a_{p-1}, a_p = a_1 a_2 \cdots a_{p-1}(a_1, ..., a_{p-1})^{-1} = e,$$

eli siis $|S| = n^{p-1}$.

Huomataan, että jos $a_1a_2 \cdots a_{p-1}a_p = e$, niin $a_pa_1a_2 \cdots a_{p-1} = e$, joten voidaan määritellä kuvaus $f : S \to S,\ f(a_1, ..., a_p) = (a_p, a_1, ..., a_{p-1})$. Huomioidaan nyt, että $f \neq i$ (ei ole identiteettikuvaus S:ssä) ja $f^p = i$, joten kuvauksen f kertaluku on p.

Jos alkion $s \in S$ radalla f:ssä on yksi alkio, niin $f(s) = s$. Toisaalta, jos $f(s) \neq s$, niin lemman 3.0.13 nojalla s:n radalla on tällöin tasan p erillistä alkiota. Mutta milloin $f(s) \neq s$? Tehdään väite, että $f(s) \neq s$, jos ja vain jos $s = (a_1, a_2, ..., a_p)$ siten, että $a_i \neq a_j$ joillakin $i \neq j$. Tällöin myös $f(s) = s$ jos, ja vain jos $s = (a, a, ..., a)$ jollekin $a \in G$. Tämä väite on aika selvä, kun muistetaan, että $f(a_1, ..., a_p) = (a_p, a_1, ..., a_{p-1})$ ja kun ainakin yhdessä kohdassa $a_i \neq a_j$, niin $f(s) \neq s$.

Olkoon m niiden alkioiden lukumäärä s:ssä joille $f(s) = s$. Kun $s = (e, e, ..., e)$, niin $f(s) = s$, eli tiedetään, että $m \geq 1$. Toisaalta, jos $f(s) \neq s$, niin s:n rata f:ssä sisältää p alkiota ja nämä radat ovat erillisiä, eli radoista muodostuu p kappaletta erillisiä ekvivalenssiluokkia. Jos on olemassa k kappaletta ratoja, joille siis $f(s) \neq s$, niin saamme, että $|S| = n^{p-1} = m + kp$.

Nyt alkuoletuksen mukaan $p|n$ ja $p|(kp)$. Niimpä täytyy $p|m$, koska $m = n^{p-1} - kp$. Koska $m \neq 0$ ja $p|m$ saamme, että $m > 1$. Tällöin siis on olemassa sellainen $s \in G$, että $s = (a, a, ..., a) \neq (e, e, ..., e)$. Ja S:n määritelmästä saamme, että $a^p = e$, eli tämän alkion a kertaluku on p ja olemme siis löytäneet haluamamme alkion. □

Huomaa, että Cauchyn lause kertoo, että ratkaisujen lukumäärä ryhmässä G yhtälölle $x^p = e$ on aina alkuluvun p kerrannainen.

Luku 4

Sylowin lauseet

Tämä luku on jaettu kappaleisiin kunkin Sylowin lauseen mukaan, joita on kolme kappaletta. Jokaisessa kappaleessa on käyty läpi joitain lauseita, joiden todistuksia on suoraan käytetty apuna Sylowin lauseiden todistuksessa.

4.1 Sylowin 1. lause

Lause 4.1.1. *Olkoon G ryhmä ja $|G| = p^n$, missä p on alkuluku. Tällöin $Z(G)$ ei ole triviaali (eli $\exists a \neq e \in G : \ ax = xa \ \forall x \in G$).*

Todistus. Kuten totesimme huomautuksessa sivulla 18, ryhmä G voidaan esittää erillisten konjugointiluokkien unionina. Käytetään nyt tätä tietoa hyväksi, sekä lausetta 2.5.11. Eli siis

$$|G| = \sum_a \textit{alkion } a \textit{ konjugointiluokan koko} = \sum_a \frac{|G|}{|C_G(a)|}.$$

Nyt summassa käydään läpi yksi alkio a jokaisesta erillisestä konjugointiluokasta. Muistutuksena vielä, että $C_G(a) = \{x \in G | xa = ax\}$.

Olkoon nyt $z = |Z(G)|$, eli z on niiden alkioiden lukumäärä G:ssä, joiden konjugointiluokassa on vain yksi alkio. Koska $e \in Z(G)$, niin $z \geq 1$. Mille

tahansa $Z(G)$:n ulkopuoliselle alkiolle b pätee, että sen konjugointiluokassa on enemmän kuin yksi alkio ja $|C_G(b)| < |G|$. Lisäksi, koska lauseen 2.5.12 mukaan $C_G(b) \leq G$ ja $|C_G(b)|$ jakaa $|G|$:n lagrangen lauseen mukaan (lause 2.4.5), niin $|C_G(b)| = p^{n(b)}$, missä $1 \leq n(b) < n$.Nyt

$$p^n = |G| = \sum_a \frac{|G|}{|C_G(a)|} = z + \sum_{b \notin Z(G)} \frac{|G|}{|C_G(b)|} = z + \sum_{n(b)<n} \frac{p^n}{p^{n(b)}} = z + \sum_{n(b)<n} p^{n-n(b)}.$$

Selvästi p jakaa p^n:n ja summan $\sum_{n(b)<n} p^{n-n(b)}$. Näin ollen $p|z$ ja koska $z \geq 1$, niin saamme, että $z \geq p$. Täten $z = |Z(G)|$ ja täytyy olla olemassa alkio $a \neq e \in Z(G)$. □

Lause 4.1.2. *Olkoon kuvaus $f : G \to G'$ homomorfismi, jonka ydin on $Ker(f) = K$. Jos $H' \leq G'$ ja jos*

$$H = \{a \in G | f(a) \in H'\},$$

niin $H \leq G$, $H \supset K$ ja $H/K \cong H'$. Lisäksi, jos $H' \trianglelefteq G'$, niin $H \trianglelefteq G$.

Todistus. Tutkitaan ensin, onko $H \leq G$. Nyt $H \neq \emptyset$, sillä $e \in H$. Jos $a, b \in H$, niin $f(a), f(b) \in H'$, joten $f(ab) = f(a)f(b)$, koska H' on aliryhmä. Täten $ab \in H$. Tutkitaan vielä käänteisalkio. Jos $a \in H$, niin $f(a) \in H'$, joten $f(a^{-1}) = f(a)^{-1}$, koska edelleen H' on aliryhmä. Nyt siis $a^{-1} \in H$ ja näin ollen aliryhmäkriteerin nojalla $H \leq G$.

Koska $f(K) = \{e'\} \subset H'$, missä e' on G':n neutraalialkio, saamme että $K \subset H$. Koska $K \trianglelefteq G$ (lause 2.4.18) ja $K \subset H$, niin tästä seuraa, että $K \trianglelefteq H$. Nyt siis on mahdollista muodostaa tekijäryhmä H/K ja homomorfismin peruslauseesta (lause 2.4.21) saamme, että

$$H/K \cong H'.$$

Nyt, jos $H' \trianglelefteq G'$ ja jos $a \in G$, niin $f(a)^{-1}H'f(a) \subset H'$, eli $f(a^{-1}Ha) \subset H'$ ja niinpä $a^{-1}Ha \subset H$. Ja täten siis $H \trianglelefteq G$. □

Lause 4.1.3. *(Sylowin 1.lause) Olkoon G ryhmä, jonka kertaluku on $p^n m$, missä p on alkuluku ja $p \nmid m$. Tällöin G:llä on aliryhmä, jonka kertaluku on p^n.*

Todistus. Todistetaan lause induktiolla.

1. Kun $n = 0$, niin $p^n = p^0 = 1$ ja $\{e\} \leq G$. Oletetaan tästä eteenpäin, että $n \geq 1$.

2. Tehdään induktio-oletus, että lause pätee kaikille ryhmille H, joille $|H| < |G|$.

3. Oletetaan, että lause ei päde ryhmälle G. Nyt induktio-oletuksen nojalla p^n ei voi jakaa $|H|$:ta millään $H \leq G$, jos $H \neq G$. Erityisesti, jos $a \notin Z(G)$, niin $C_G(a) \neq G$, joten $p^n \nmid |C_G(a)|$. Nyt

$$[G : C_G(a)] = \frac{|G|}{|C_G(a)|} = \frac{p^n m}{p^j k}, \text{ missä } 0 \leq j < n \text{ ja } 0 \leq k \leq m,$$

joten $p|[G : C_G(a)]$, missä $a \notin Z(G)$. Käytetään seuraavaksi hyväksi lausetta 4.1.1, eli jos $z = |Z(G)|$, niin $z \geq 1$ ja

$$p^n m = |G| = z + \sum_{a \notin Z(G)} [G : C_G(a)].$$

Nyt $p|[G : C_G(a)]$, jos $a \notin Z(G)$, eli $p| \sum_{a \notin Z(G)} [G : C_G(a)]$. Lisäksi tiedetään, että $p|p^n m$, joten myös $p|z$. Cauchyn lauseen 3.0.15 mukaan on olemassa alkio $a \in Z(G)$ siten, että $|a| = p$, tai toisin kirjoitettuna $a^p = e$. Olkoon A alkion a generoima aliryhmä ja tällöin $|A| = p$ ja koska $a \in Z(G)$, niin myös $A \trianglelefteq G$. Olkoon $\Gamma = G/A$, eli $|\Gamma| = |G|/|A| = p^n m/p = p^{n-1} m$. Nyt koska $|\Gamma| < |G|$, niin induktio-oletuksen nojalla on olemassa aliryhmä $M \leq \Gamma$, jolle $|M| = p^{n-1}$.

Nyt voidaan soveltaa lausetta 4.1.2, sillä kuvaus $f : \Gamma \to G,\ f(g) = gA$ on homomorfismi ja $Ker(f) = A$. Eli lauseen 4.1.2 mukaan on olemassa

aliryhmä $P \leq G$ siten, että $P \supset A$ ja $P/A = M$. Edelleen, $|P| = |M||A| = p^{n-1}p = p^n$. Eli P on siis G:n kertalukua p^n oleva aliryhmä ja tämä on ristiriita vastaoletuksemme kanssa, että G:llä ei ole tällaista aliryhmää. Tämä ristiriita osoittaa lauseen paikkaansapitävyyden.

□

4.2 Sylowin 2. lause

Lause 4.2.1. *Jos $AgB \cap AhB \neq \emptyset$, niin $AgB = AhB$. Jos G äärellinen ryhmä, niin $G = \bigcup_{i=1}^{n} Ag_iB$, $Ag_jB \cap Ag_rB \neq \emptyset$ aina, kun $j \neq r$ sekä*

$$|G| = \sum_{i=1}^{n} \frac{|A||B|}{|A^{g_i} \cap B|}.$$

Todistus. Jos $AgB \cap AhB \neq \emptyset$, niin $a_1gb_1 = a_2hb_2$, missä siis $a_i \in A$ ja $b_i \in B$. Eli $g = a_1^{-1}a_2hb_2b_1^{-1}$, joten $AgB = (Aa_1^{-1}a_2)h(b_2b_1^{-1}) = AhB$. Siis

$$G = \bigcup Ag_iB.$$

Jos G on äärellinen, niin $G = \bigcup_{i=1}^{n} Ag_iB$ ja $|G| = \sum_{i=1}^{n} |Ag_iB|$. Nyt $|Ag_iB| = |g_i^{-1}Ag_iB| = |A^{g_i}B|$. Nyt lemman 2.5.4 nojalla $|A^{g_i}B| = \frac{|A^{g_i}||B|}{|A^{g_i} \cap B|} = \frac{|A||B|}{|A^{g_i} \cap B|}$. Siis

$$|G| = \sum_{i=1}^{n} \frac{|A||B|}{|A^{g_i} \cap B|}.$$

□

Määritellään ennen Sylowin 2. lausetta tärkeä käsite, eli Sylowin p-aliryhmät.

Määritelmä 4.2.2. Olkoon G ryhmä ja $|G| = p^a n$, missä p on alkuluku, $a \in \mathbb{N}$ ja $p \nmid n$. Jos ryhmässä G on sellainen aliryhmä P, että $|P| = p^a$, niin P on G:n Sylowin p-aliryhmä.

Huomautus. Jos G:llä on vain yksi Sylowin p-aliryhmä P, niin $P \trianglelefteq G$.

Perustelu: Nyt $P^g \leq G$ ja $|P^g| = p^a = |P| \Rightarrow P^g$ on G:n Sylowin p-aliryhmä $\Rightarrow p^g = p \; \forall y \in G \Rightarrow P \trianglelefteq G$.

Lause 4.2.3. *(Sylowin 2. lause) Olkoon P ryhmän G Sylowin p-aliryhmä.*

a) Jos $U \leq G$ ja $|U| = p^l$ $(l \in \mathbb{N})$, niin $\exists g \in G : \; U \leq P^g$.

b) Kaikki Sylowin p-aliryhmät konjugoivat G:ssä ja niiden lukumäärä on $[G : N_G(P)]$.

Todistus. a) Lauseesta 4.2.1 saadaan, että

$$G = \bigcup_{i=1}^{r} Pg_iU \quad \text{ja} \quad |G| = \sum_{i=1}^{r} \frac{|P||U|}{|P^{g_i} \cap U|}.$$

Jos $P^{g_i} \cap U < U \; \forall i \in \{1, ..., r\}$, niin $\frac{|U|}{|P^{g_i} \cap U} = p^{a_i}$, missä $a_i \geq 1 \; \forall i \in \{1, ..., r\}$. Nyt

$$\frac{|G|}{|P|} = \sum_{i=1}^{r} \frac{|U|}{|P^{g_i} \cap U|} = \sum_{i=1}^{r} p^{a_i}.$$

Nyt nähdään selvästi, että

$$p \mid \sum_{i=1}^{r} p^{a_i} \Rightarrow p \mid \frac{|G|}{|P|},$$

mikä on tietenkin ristiriita, sillä kyseinen p ei voi jakaa tätä osamäärää. Siispä $\exists j \in \{1, ..., r\} : \; P^{g_j} \cap U = U$ ja tällöin $U \leq P^{g_j}$.

1. Jos P ja Q ovat G:n Sylowin p-aliryhmiä, niin a)- kohdan nojalla $\exists g \in G : \; Q \leq P^g$. Koska $|Q| = |P| = |P^g|$, niin $Q = P^g$.

   Toinen väite, että Sylowin p-aliryhmien lukumäärä on $[G : N_G(P)]$ on seuraus lauseesta 2.5.11.

□

Huomautus. $[G : P] = |G|/|P| = |G|/|N_G(P)| \cdot |N_G(P)|/|P| = [G : N_G(P)] \cdot [N_G(P) : P] \Rightarrow [G : N_G(P)] \mid [G : P]$. Eli siis Sylowin p-aliryhmien lukumäärä jakaa P:n indeksin G:ssä.

4.3 Sylowin 3. lause

Lemma 4.3.1. *Olkoon G ryhmä ja $\emptyset \neq M \subseteq G$. Nyt $N_G(M) \leq G$.*

Todistus. 1. Selvästi $N_G(M) \subseteq G$. Nyt $M^e = M$ ja $e \in G \Rightarrow e \in N_G(M) \neq \emptyset$.

2. Olkoon $a, b \in N_G(M) \Rightarrow M^a = M$ ja $M^b = M$. Nyt $M^{ab} = (M^a)^b = M^b = M \Rightarrow ab \in N_G(M)$.

3. $M^a = a^{-1}Ma = M \; || a \cdot \; || \cdot a^{-1} \Leftrightarrow M = aMa^{-1} = (a^{-1})^{-1}Ma^{-1} = M^{a^{-1}} \Rightarrow a^{-1} \in N_G(M)$.

Aliryhmäkriteerin (lause 2.4.3) nojalla siis $N_G(M) \leq G$. □

Lause 4.3.2. *(Sylowin 3. lause) Olkoon G ryhmä ja p on alkuluku. Nyt Sylowin p-aliryhmien lukumäärä ryhmässä G on aina muotoa $1 + kp$.*

Todistus. Olkoon P G:n Sylowin p-aliryhmä, jolloin $|P| = p^n$. Muodostetaan nyt ryhmä G käyttämällä kaksoissivuluokkia P:stä, eli $G = \bigcup PxP$. Kysymme nyt, että kuinka monta alkiota on joukossa PxP. Lemmasta 2.5.4 saadaan, että

$$|PxP| = \frac{|P||P|}{|P \cap xPx^{-1}|}.$$

Tällöin, jos $P \cap xPx^{-1} \neq P$, niin $p^{n+1} \mid |PxP|$, missä siis $p^n = |P|$. Eli toisin sanoen: jos $x \notin N_G(P)$, niin $p^{n+1} \mid |PxP|$. Ja myös, jos $x \in N_G(P)$, niin $PxP = P(Px) = P^2x = Px$, eli tässä tapauksessa $|PxP| = p^n$. Eli saadaan, että

$$|G| = \sum_{x \in N_G(P)} |PxP| + \sum_{x \notin N_G(P)} |PxP|,$$

missä jokainen summa käy läpi yhden alkion jokaisesta kaksoissivuluokasta. Huomataan, että kun $x \in N_G(P)$, niin $\sum_{x \in N_G(P)} |PxP| = \sum_{x \in N_G(P)} |Px|$. Eli

lasketaan yhteen oikeanpuoleisia erillisiä sivuluokkia. On helppo osoittaa, että $P \leq N_G(P)$ ja lagrangen lauseesta 2.4.5 saamme, että $|N_G(P)| = n|Px|$, missä n =sivuluokkien lkm. Näin ollen $\sum_{x \in N_G(P)} |PxP| = |N_G(P)|$. Entä toinen summalauseke? Äsken näimme, että jokainen termi on jaollinen p^{n+1}:llä, joten

$$p^{n+1} \mid \sum_{x \notin N_G(P)} |PxP|.$$

Voimme siis kirjoittaa summan hieman eri tavalla, kuten

$$\sum_{x \notin N_G(P)} |PxP| = p^{n+1}u.$$

Näin ollen $|G| = |N_G(P)| + p^{n+1}u$, eli

$$\frac{|G|}{|N_G(P)|} = 1 + \frac{p^{n+1}u}{|N_G(P)|}.$$

Nyt koska lemman 4.3.1 mukaan $N_G(P) \leq G$, niin $|N_G(P)| \mid |G|$ ja tällöin $\frac{p^{n+1}u}{|N_G(P)|}$ on kokonaisluku. Myös, koska $p^{n+1} \nmid |G|$, niin $p^{n+1} \nmid |N_G(P)|$. Mutta nyt täytyy päteä, että $p \mid \frac{p^{n+1}u}{|N_G(P)|}$, eli voimme kirjoittaa, että $\frac{p^{n+1}u}{|N_G(P)|} = kp$. Katsotaan nyt äsken saamaamme yhtälöä uudelleen ja saamme, että

$$\frac{|G|}{|N_G(P)|} = 1 + \frac{p^{n+1}u}{|N_G(P)|} = 1 + kp.$$

Nyt Sylowin 2. lauseen mukaan (lause 4.2.3) indeksi $[G : N_G(P)]$ antaa meille Sylowin p-aliryhmien lukumäärän, joten lause on todistettu. □

4.4 Sovelluksia

Nyt onkin hyvä aika kysyä, että mihin Sylowin lauseita voidaan käyttää. Tässä osiossa käydään läpi pari kohtalaisen yksinkertaista esimerkkiä siitä, miten ryhmän kertaluvusta voidaan Sylowin lauseiden avulla saada tietoa ryhmän rakenteesta. Ennen esimerkkejä täytyy käydä läpi pari aputulosta sovelluksia varten ja määritellä yksinkertainen ryhmä.

Lemma 4.4.1. *Olkoon G ryhmä. Nyt $Z(G) \trianglelefteq G$.*

Todistus. Kuvaus $F : G \to I(G),\ F(a) = f_{a^{-1}}$ on surjektio. Nyt $F(ab)(x) = f_{(ab)^{-1}}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1} = f_{a^{-1}}(f_{b^{-1}}(x)) = (f_{a^{-1}} \circ f_{b^{-1}})(x) = [F(a) \circ F(b)](x) \Rightarrow F(ab) = F(a) \circ F(b)$, eli kuvaus on homomorfismi.

Nyt $Ker(f) = \{a \in G | F(a) = Id_G\} = \{a \in G | axa^{-1} = x\ \forall x \in G\} = \{a \in G | ax = xa\ \forall x \in G\} = Z(G)$. Näin ollen lauseen 2.4.18 nojalla $Z(G) \trianglelefteq G$. □

Lemma 4.4.2. *Olkoon G ryhmä ja $G/Z(G)$ syklinen. Nyt G on Abelin ryhmä.*

Todistus. Nyt $G/Z(G) = \{gZ | g \in G\} = \langle aZ \rangle$. Olkoon $x, y \in G \Rightarrow xZ, yZ \in G/Z(G) = \langle aZ \rangle$. Saamme, että $xZ = (aZ)^m = a^m Z$ ja $yZ = (aZ)^n = a^n$, missä $m, n \in \mathbb{Z}$.

Ajatellaan tekijäryhmät joukkoina, eli esim. $xZ = \{xz | z \in Z\}$ ja $e \in Z(G) \Rightarrow xe \in xZ$. Nyt $xZ \ni xe = x = a^m z_1 \in a^m Z,\ yZ \ni ye = y = a^n z_2 \in a^n Z$, missä $z_1, z_2 \in Z$. Nyt siis $xy = (a^m z_1)(a^n z_2) = (a^m a^n) z_2 z_1 = a^{m+n} z_2 z_1 = a^{n+m} z_2 z_1 = a^n a^m z_2 z_1 = (a^n z_2)(a^m z_1) = yx$. Nyt siis G on Abelin ryhmä. □

Lause 4.4.3. *Olkoon G ryhmä ja $|G| = p^2$, missä p on alkuluku. Nyt G on Abelin ryhmä.*

Todistus. Lauseesta 4.1.1 saadaan, että $Z(G) > \{e\} \Rightarrow |Z(G)| = p$ tai $|Z(G)| = p^2$. Jos $|Z(G)| = p$, niin lemman 4.4.1 mukaan $Z(G) \trianglelefteq G$ ja voidaan muodostaa tekijäryhmä $G/Z(G)$. Nyt $|G/Z(G)| = |G|/|Z(G)| = p^2/p = p \Rightarrow G/Z(G)$ on syklinen ja lemman 4.4.2 nojalla G on Abelin ryhmä.

Jos $|Z(G)| = p^2$, niin $Z(G) = G$ ja keskuksen määritelmän nojalla G on Abelin ryhmä. □

Määritelmä 4.4.4. Olkoon G ryhmä. Nyt G on yksinkertainen ryhmä, jos sillä on vain triviaalit normaalit aliryhmät, eli $\{e\}$ ja G itse.

Tutkitaan nyt paria esimerkkiä ja käytetään esimerkeissä merkintää $N(p) =$ Sylowin p-aliryhmien lukumäärä.

Esimerkki 4.4.5. *Olkoon G ryhmä ja $|G| = 42$. Onko G yksinkertainen ryhmä?*

Ratkaisu:
Nyt $|G| = 42 = 2 \cdot 3 \cdot 7$. Eli G:llä on Sylowin 2-aliryhmiä, Sylowin 3-aliryhmiä ja Sylowin 7-aliryhmiä. Tutkitaan Sylowin 7-aliryhmiä. Nyt Sylowin 3. lauseen mukaan $N(7) = 1 + 7k$, missä $k \in \mathbb{Z}$. Sylowin 2. lauseen jälkeinen huomautus kertoo, että $1 + 7k \mid 2 \cdot 3 = 6$, mistä saamme, että $N(7) = 1$. Merkitään tätä Sylowin 7-aliryhmää P:llä. Nyt koska P on ainoa Sylowin 7-aliryhmä G:ssä, niin $P \trianglelefteq G$ (määritelmän 4.2.2 huomautus). Nyt myös $|P| = 7^1 = 7$, joten $P \neq \{e\}$ ja erityisesti $P \neq G$. Joten siis G sisältää ei-triviaalin normaalin aliryhmän ja näin ollen G ei ole yksinkertainen ryhmä.

Esimerkki 4.4.6. *Olkoon G ryhmä ja $|G| = 1225$. Onko G Abelin ryhmä?*

Ratkaisu:
Nyt $|G| = 5^2 \cdot 7^2$. Tarkastellaan Sylowin p-aliryhmiä aloittaen 5-aliryhmistä. Sylowin lauseiden mukaan $N(5) = 1 + 5k$ ja $1 + 5k \mid 7^2 = 49 \Rightarrow N(5) = 1$. Merkitään tätä Sylowin 5-aliryhmää P:llä. Nyt koska P on ainoa Sylowin 5-aliryhmä, niin $P \trianglelefteq G$.

Sama pätee Sylowin 7-aliryhmille, eli $N(7) = 1+7h$ ja $1+7h \mid 5^2 = 25 \Rightarrow N(7) = 1$. Olkoon Sylowin 7-aliryhmä Q. Nyt myös $Q \trianglelefteq G$.

Nyt lauseen 4.4.3 mukaan P ja Q ovat molemmat Abelin ryhmiä. Olkoon $x \in P$ ja $y \in Q$. Koska P ja Q ovat molemmat normaaleja, niin $xyx^{-1}y^{-1} \in$

$P \cap Q = \{e\}$ (koska $syt(25, 49) = 1$), eli $xyx^{-1}y^{-1} = e \Rightarrow xy = yx$. Nyt siis kaikki alkiot kommutoivat PQ:ssa ja lisäksi $|PQ| = |P||Q|/|P \cap Q| = 5^2 \cdot 7^2 = |G|$ (lause 2.5.4), joten $PQ = G$ ja näin ollen G on Abelin ryhmä.

Kirjallisuutta

[1] I.N. Herstein: *Abstract Algebra- 3rd edition*, Prentice-Hall, New Jersey, 1990.

[2] I.N. Herstein: *Topics in Algebra- 2nd edition*, John Wiley & Sons, New York, 1975.

[3] M. Niemenmaa, Kari Myllylä, Juha-Matti Tirilä: *Lukuteoria ja ryhmät*, luentomoniste, Oulun yliopisto, kevät 2011.

[4] M. Niemenmaa, *Ryhmäteoria*, luennot ja muistiinpanot, Oulun yliopisto, syksy 2009.