Helsingin Yliopisto
Matemaattis-luonnontieteellinen tiedekunta
Matematiikan ja tilastotieteen osasto

Kandidaatintutkielma

Sylowin lauseet

Kalle Heinonen

Ohjaaja: Erik Elfving

22.5.2023

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen tiedekunta	Matematiikan ja tilastotieteen osasto

Tekijä — Författare — Author
Kalle Heinonen

Työn nimi — Arbetets titel — Title

Sylowin lauseet

Oppiaine — Läroämne — Subject
Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Kandidaatintutkielma	22.5.2023	28 sivua

Tiivistelmä — Referat — Abstract

Tutkielma käsittelee Sylowin lauseita, jotka ovat osa abstraktia algebraa ja erityisesti ryhmäteoriaa. Jo todella alkeellisella ryhmäteorialla voimme todistaa Lagrangen lauseen, joka kertoo meille minkälaisia aliryhmiä äärellisellä ryhmällä ei voi olla. On kuitenkin luonnollista kysyä minkälaisia aliryhmiä on olemassa. Koska Lagrangen lause antaa vain mahdollisen olemassaolon ehdon, niin Sylowin ensimmäinen lause kertoo erityistapauksen milloin käänteinen Lagrangen lause pätee. Sen antamat aliryhmät ja miten ne käyttäytyvät on osoittaunut hyödylliseksi työkaluksi, kun halutaan informaatiota ryhmän rakenteesta.

Ensimmäisessä kappaleessa johdatetaan lukija suoraan pääaiheeseen. Pienen motivoivan ja historiallisen kattauksen jälkeen siirrymme suoraan asiaan. Toisessa kappaleessa käymme läpi kaikki äärellisten ryhmien perustulokset. Esimerkiksi ryhmä, aliryhmä, permutaatioryhmät, isomorfia, virittäminen, lukuteoriaa, sykliset ryhmät, sivuluokat, Lagrangen lause, homomorfismi, normaali aliryhmä, ositus ja tekijäryhmä. Koska oletuksena tutkielmaa lukevalla on Algebra I kurssin käyminen, niin todistukset sivuutetaan viitaten alan kirjallisuuteen.

Kolmannessa kappaleessa tulee esille ryhmän toiminta. Lähdemme yleisestä ryhmän toiminnan käsitteestä keskittyen lopuksi konjugointiin. Käymme tämän läpi todistusteknillisistä syistä Sylowin lauseiden todistuksiin. Ryhmän toimintoja käytetään usein myös määrittelemättä niitä. Varsinkin konjugointi ja ryhmän esitys ovat kuuluisia tapauksia. Määrittelemme siksi ensin mikä on ryhmän toiminta, esittelemme esimerkkejä ja tutkielmaan vaadittavat toimintaan liittyvät tulokset. Kappaleen päätavoite on päästä luokkayhtälöön asti.

Viimeisessä kappaleessa todistetaan kaikki kolme Sylowin lausetta. Sylowin ensimmäisestä lauseesta seuraa Sylowin $p-$*aliryhmien* olemassaolo. Ensimmäinen lause on yleistys kuuluisasta Cauchyn lauseesta. Tästä saadaan helppo laskennallinen tapa löytää Sylowin $p-$aliryhmiä katsomalla äärellisen ryhmän kertaluvun alkulukuhajotelmaa. Sylowin toinen lause kertoo, että Sylowin p-aliryhmät ovat konjugaatteja keskenään. Sylowin kolmas lause kertoo tärkeää informaatiota Sylowin $p-$aliryhmien määrän suhteesta kertalukuun. Tästä seuraa vielä korollaarina, että jokainen yksikäsitteinen Sylow $p-$aliryhmä on normaali. Kappaleen lopuksi näytämme esimerkkejä, missä Sylowin lauseita voi hyödyntää.

Avainsanat — Nyckelord — Keywords
Abstrakti algebra, Ryhmäteoria

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

Sisällys

1 Johdanto

Ryhmäteoria on yksi olennainen abstraktin algebran ja matematiikan osa-ala. Ryhmä on luonnollisesti yksi matematiikassa yleisimmin esiintyvistä rakenteista. Niitä esiintyy kaikkialla matematiikassa ja luonnossa. Esimerkiksi kemiassa ja fysiikassa erilaisten geometristen objektien symmetriaa mallintaa ryhmä. Siksi ryhmien rakenteen ymmärtäminen on erityisen tärkeää. Ryhmäteorian pointti on tutkia ryhmän rakennetta ja yksi tärkeimmistä niistä on ryhmän aliryhmät, tässä tutkielmassa erityisesti äärellisten ryhmien aliryhmät. Näiden aliryhmien käyttäytyminen kertoo usein jo paljon ryhmän rakenteesta.

Jo hyvin alkeellisella ryhmäteorialla voidaan todistaa kuuluisa Lagrangen lause. Se kertoo minkälaisia aliryhmiä äärellisellä ryhmällä ei voi olla olemassa sen kertaluvun perusteella. Kuitenkin tästä seuraava luonnollinen jälkikysymys on, että minkälaisia aliryhmiä ryhmällä on olemassa. Tässä tutkielmassa käsittelemme lauseita nimeltään Sylowin lauseet. Ne todisti alun perin norjalainen Peter Ludvig Mejdell Sylow vuonna 1862 [1, s.149] jo ennen modernin abstraktin algebran syntyä.

Sylowin ensimmäinen lause (Sylow I) takaa Sylowin $p-$aliryhmien olemassaolon tutkimalla äärellisen ryhmän kertalukua. Tämä on yleistys kuuluisasta Cauchyn lauseesta. Lisäksi Sylowin muut lauseet (Sylow II), (Sylow III) ja näiden kolmen lauseen suorat korollaarit antavat vielä tarkempaa informaatiota Sylowin $p-$aliryhmien rakenteesta. Esimerkiksi niiden lukumäärästä, normaaliudesta ja suhteista toisiinsa. Lauseiden tärkeät sovellukset keskittyvät pääosin äärellisten yksinkertaisten ryhmien luokitteluun ja Galois'n teoriaan. Nämä ovatkin yksiä matematiikan suurimpia saavutuksia. Muita sovelluksia löytyy muun muassa koodausteoriasta, kryptografiasta, teoreettisesta tietojenkäsittelytieteestä ja ylipäätään kaikkialta, missä äärellisiä ryhmiä saattaa tulla vastaan.

2 Ryhmäteorian peruskäsitteitä

Määrittelemme ensiksi ryhmäteorian peruskäsitteitä ja tuloksia. Algebralliset rakenteet 1 ja 2 kurssien todistuksia ei käydä läpi, vaan ne löytyvät aihetta käsittelevistä teoksista. Kappale seuraa pääosin teoksen Rämö, Häsä *Johdatus abstraktiin algebraan* [3] todistuksia ja notaatiota. Joissakin kohdissa viitataan Joseph. A. Gallianin teokseen *Contemporary Abstract algebra* [1] ja Häsän *Algebra II* kurssimateriaaliin [2].

2.1 Ryhmä

Määritelmä 2.1. Joukko G varustettuna laskutoimituksella $\cdot$ on *ryhmä*, jos seuraavat ehdot ovat voimassa:

(G1): Kaikilla $x, y \in G$ pätee $x \cdot y \in G$.

(G2): Laskutoimitus on liitännäinen.

(G3): Joukossa G on neutraalialkio e laskutoimituksen suhteen.

(G4): Kaikilla $x \in G$ on olemassa käänteisalkio $x^{-1} \in G$ laskutoimituksen suhteen.

Parista $(G, \cdot)$ käytetään usein vain merkintää G.

Määritelmä 2.2. Ryhmää G kutsutaan *Abelin ryhmäks*i, jos kaikilla $g, h \in G$

$$gh = hg.$$

Määritelmä 2.3. Ryhmän G *kertaluku* $|G|$ on sen alkioiden lukumäärä.

Lause 2.1. *Olkoon G ryhmä ja $a, b \in G$. Tällöin yhtälöillä $a \cdot x = b$ ja $x \cdot a = b$ on olemassa yksikäsitteiset ratkaisut ryhmässä G.*

Todistus. [3, Lause 3.2.]. □

Ryhmän G alkion potenssi voidaan hyvin määritellä olemaan

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kertaa}}$$

ja myös alkion x^n käänteisalkio $x^{-n} = \underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{n \text{ kertaa}}$.
Jos kyseessä on erityisesti yhteenlasku, niin alkion potenssi merkitään

$$nx = \underbrace{x + x + \ldots + x}_{n\text{-kertaa}}.$$

Lause 2.2. *Olkoon G ryhmä ja x sen alkio. Kaikilla kokonaisluvuilla m ja n pätee:*

a) $(x^n)^{-1} = (x^{-1})^n$ *b)* $x^m \cdot x^n = x^{m+n}$ *c)* $(x^n)^m = x^{mn}$

Todistus. [3, Lause 3.8.]. □

Lemma 2.3. *Äärellisen ryhmän laskutoimitustaulussa jokainen alkioista esiintyy vain yhden kerran jokaisella rivillä ja jokaisessa sarakkeessa.*

Todistus. [3, Lemma 3.10.]. □

2.2 Aliryhmä

Määritelmä 2.4. Oletetaan, että G on ryhmä ja H sen epätyhjä osajoukko. H on ryhmän G *aliryhmä*, mikäli seuraavat ehdot pätevät.

(H1): $g \cdot h \in H$ kaikilla $g, h \in H$.

(H2): Neutraalialkio $e \in H$.

(H3): jos $g \in H$, niin $g^{-1} \in H$.

Ryhmän G aliryhmää H merkitään $H \leq G$ tai $H < G$, jos $H \neq G$.

Lause 2.4. *Oletetaan, että* $H_1 \leq G$ *ja* $H_2 \leq G$. *Tällöin* $H_1 \cap H_2 \leq G$.

Todistus. [3, Lause 3.17.]. □

Lause 2.5. *Oletetaan, että* $(G, \cdot)$ *ja* $(H, \cdot)$ *ovat ryhmiä. Jos* H *on joukon* G *osajoukko, se on ryhmän* G *aliryhmä.*

Todistus. [3, Lause 3.18.]. □

Lause 2.6. *Oletetaan, että* H *on ryhmän* G *osajoukko. Tällöin* H *on ryhmän* G *aliryhmä, jos ja vain jos:*

a) H *on epätyhjä.*

b) $g \cdot h^{-1} \in H$ *kaikilla* $g, h \in H$.

Todistus. [3, Lause 3.19.]. □

2.3 Permutaatioryhmät

Määritelmä 2.5. Joukon G *permutaatio* τ on bijektio $\tau : G \to G$.

Määritelmä 2.6. *Symmetrinen ryhmä* S_n on joukon $A = \{1, 2, ..., n\}$ kaikkien permutaatioiden muodostoma ryhmä. Laskutoimituksena on kuvaustulo $\circ$.

Ei ole vaikea nähdä, että S_n on ryhmä. Tämä seuraa suoraan bijektiivisten kuvausten ominaisuuksista, identiteetin bijektiivisyydestä ja kuvaustulon ominaisuuksista. Joskus symmetristä ryhmää merkitään $\mathrm{Sym}(X)$, missä X on joku mielivaltainen joukko.

Lause 2.7. *Symmetrisen ryhmän* S_n *kertaluku on* $n!$.

Todistus. [3, Lause 4.3.]. □

Määritelmä 2.7. Olkoon τ joukon $A = \{1, 2, ..., n\}$ permutaatio, joka kuvaa toisistaan poikkeavat alkiot $a_1, a_2, ..., a_k$ seuraavasti:

$$a_1 \to a_2 \to a_3 \to \cdots \to a_k \to a_1.$$

Muut alkiot τ kuvaa itselleen. Tälläista permutaatiota kutsutaan nimellä *sykli*.

Määritelmä 2.8.

Merkitsemme syklien tuloa usein $\tau \circ \sigma = \tau\sigma$. Kutsumme tätä permutaation *rataesitykseksi*. Jätämme merkitsemättä yhden mittaiset syklit niiden rataesityksessä. Esimerkiksi $(abc)(de)(f)(g) = (abc)(de)$.

Lemma 2.8. *Oletetaan että* $\tau_1 = (b_1...b_k)$ *ja* $\tau_2 = (c_1...c_m)$ *ovat kaksi sykliä joukossa* $A = \{1, 2, ..., n\}$ *ja* σ *on joukon* A *permutaatio, jolla on rataesitys* $(b_1...b_k)(c_1...c_m)$. *Tällöin pätee*

$$\sigma = \tau_1 \circ \tau_2.$$

Todistus. [3, Lemma 4.7.]. □

Lause 2.9. *Jokainen äärellisen joukon permutaatio voidaan kirjoittaa erillisten syklien tulona.*

Todistus. [3, Lause 4.8.]. □

Lause 2.10. *Erilliset syklit ovat vaihdannaisia.*

Todistus. [1, Theorem 5.2]. □

2.4 Ryhmien isomorfia

Määritelmä 2.9. Olkoot $(G, \star)$ ja $(H, \circ)$ ryhmiä. Jos $f : G \to H$ on jokin kuvaus, f on *ryhmäisomorfismi*, jos:

(I1): Kuvaus f on bijektio.

(I2): Kaikilla ryhmän G alkioilla g ja h pätee

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

Ryhmien välistä isomorfisuutta merkitaan $G \cong H$. Ryhmäteorian näkökulmasta keskenään isomorfiset ryhmät ovat sama ryhmä.

Lause 2.11. *Jos $f : G \to H$ on ryhmäisomorfismi, niin seuraavat väitteet pätevät:*

1. $f(e_G) = e_H$.
2. $f(g^{-1}) = f(g)^{-1}$.
3. $f(g^k) = f(g)^k$ *kaikilla* $k \in \mathbb{Z}$.
4. f^{-1} *on isomorfismi.*

Todistus. [3, Lause 5.8, Lemma 5.9., Lause 5.10.]. □

Lause 2.12. *Olkoot $f : G \to H$ ja $g : H \to K$ ryhmäisomorfismeja. Tällöin yhdistetty kuvaus $f \circ g$ on ryhmäisomorfismi.*

Todistus. **(I1):** Seuraa bijektion ominaisuuksista.

(I2): $(f \circ g)(x \cdot y) = f(g(x) \star g(y)) = f(g(x)) * f(g(y)) = (f \circ g)(x) * (f \circ g)(y)$

□

Korollaari 2.12.1. *Olkoot G, H ja K ryhmiä. Seuraavat säännöt pätevät:*

a) $G \cong G$.

b) jos $G \cong H$ *niin* $H \cong G$.

c) jos $G \cong H$ *ja* $H \cong K$, *niin* $G \cong K$.

Ryhmän sisäinen isomorfismi on *automorfismi*. Esimerkiksi $\mathrm{id} : G \to G$ toteuttaa tämän ehdon.

Lause 2.13 (Cayleyn Lause). *Jokainen ryhmä on isomorfinen jonkun symmetrisen ryhmän aliryhmän kanssa.*

Todistus. [1, Theorem 6.1]. □

2.5 Virittäminen

Määritelmä 2.10. Olkoon G ryhmä ja g sen alkio. Pienintä aliryhmää, joka sisältää alkion g, kutsutaan *alkion g virittämäksi aliryhmäksi* ja merkitään symbolilla $\langle g \rangle$. Alkiota g kutsutaan aliryhmän $\langle g \rangle$ virittäjäksi.

Lause 2.14. *Ryhmän G alkion g virittämä aliryhmä voidaan kirjoittaa muodossa*

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

.

Todistus. [3, Lause 6.2.]. □

Lemma 2.15. *Olkoon G ryhmä ja $g \in G$. Oletetaan, että positiiviselle kokonaisluvulle pätee $g^n = e$. Tällöin*

$$\langle g \rangle = \{e, g,^2 , ..., g^{n-1}\}.$$

Todistus. [3, Lemma 6.6.]. □

Määritelmä 2.11. Olkoon G ryhmä. Alkion $g \in G$ *kertaluku* $\mathrm{ord}(g)$ on sen virittämän aliryhmän $\langle g \rangle$ kertaluku.

Lause 2.16. *Olkoon G ryhmä ja g jokin alkio. Alkion g kertaluku on pienin positiivinen kokonaisluku n, jolla pätee $g^n = e$. Jos tällaista ei löydy, niin kertaluku on ääretön.*

Todistus. [3, Lause 6.9.]. □

Lause 2.17. *Jos alkion g kertaluku on ääretön, niin sen virittämä aliryhmä on*

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

missä $g^k \neq g^m$, kun $k \neq m$.

Todistus. [3, Lause 6.11.]. □

Määritelmä 2.12. Olkoon G ryhmä ja olkoon $S \subset G$. Joukon S virittämä aliryhmä $\langle S \rangle$ on pienin ryhmän G aliryhmä, joka sisältää joukon S.

Lause 2.18. *Olkoon G ryhmä ja S sen osajoukko. Tällöin*

$$\langle S \rangle = \{s_1^{k_1} s_2^{k_2} ... s_n^{k_n} : n \geq 0, k_i \in \mathbb{Z} \text{ ja } s_i \in S \text{ kaikilla } i \leq n\}.$$

Todistus. [3, Lause 6.16.]. □

2.6 Lukuteoriaa

Määritelmä 2.13. Kokonaisluku n on *jaollinen* kokonaisluvulla m, jos jollakin kokonaisluvulla a pätee $n = am$. Tällöin merkitään $m \mid n$.

Lause 2.19 (**Jakoyhtälö**)**.** *Olkoot a ja b kokonaislukuja. Oletetaan, että $b \neq 0$. Tällöin on olemassa yksikäsitteiset $q, r \in \mathbb{Z}$, joille pätee*

$$a = qb + r \text{ ja } 0 \leq r < |b|.$$

Todistus. [3, Lause 7.2.]. □

Määritelmä 2.14. Olkoot a ja b kokonaislukuja joista ainakin toinen on nollasta poikkeava. Suurinta lukua, joka jakaa luvut a ja b kutsutaan niiden *suurimmaksi yhteiseksi tekijäksi* ja merkitään $\text{syt}(a, b)$.

Jos $\text{syt}(a, b) = 1$, niin a ja b ovat *keskenään jaottomat*. Myös aina pätee $\text{syt}(a, b) = \text{syt}(b, a)$ ja $\text{syt}(a, 0) = a$.

Lause 2.20 (**Bezout'n lemma**)**.** *Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta poikkeava. Tällöin on olemassa kokonaisluvut x ja y, joille pätee*

$$syt(a, b) = xa + yb.$$

Todistus. [3, Lause 7.4.]. □

Korollaari 2.20.1. *Oletetaan, että a,b ja c ovat kokonaislukuja, joista joko a tai b on nollasta poikkeava. Yhtälöllä $ax + by = c$ on kokonaislukuratkaisu, jos ja vain jos $syt(a, b) \mid c$.*

Todistus. [3, Korollaari 7.5.]. □

Lemma 2.21 (**Eukleideen lemma**)**.** *Oletetaan, että $a, b, c \in \mathbb{Z} \setminus \{0\}$ ja että a ja b ovat keskenään jaottomat. Jos $a \mid bc$, niin $a \mid c$.*

Todistus. [3, Korollaari 7.6.]. □

Määritelmä 2.15. Olkoot a ja b nollasta poikkeavia kokonaislukuja. Pienintä positiivista lukua, jonka sekä a että b jakavat, kutsutaan niiden *pienimmäksi yhteiseksi monikerraksi* ja merkitään $\text{pym}(a, b)$.

Lause 2.22. *Nollasta poikkeaville kokonaisluvuille a ja b pätee*

$$syt(a, b) \cdot pym(a, b) = ab.$$

Todistus. [3, Lause 7.8.]. □

Määritelmä 2.16. Kokonaisluku $p > 1$ on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja p.

Lause 2.23. *Olkoon $a, b \in \mathbb{Z}$, ja olkoon p alkuluku. Jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

Todistus. [3, Lause 7.10.]. □

Korollaari 2.23.1. *Olkoot $a_1, a_2, ..., a_n \in \mathbb{Z}$, ja olkoon p alkuluku. Jos p jakaa tulon $a_1 a_2 \cdots a_n$, niin p jakaa jonkin luvuista a_i*

Todistus. [3, Korollaari 7.11.]. □

Lause 2.24 (**Aritmetiikan peruslause**)**.** *Jokainen positiivinen kokonaisluku voidaan esittää alkulukujen tulona. Esitys on tekijöiden järjestystä lukuunottamatta yksikäsitteinen.*

Todistus. [3, Korollaari 7.12.]. □

Lause 2.25. *Alkulukuja on äärettömän monta.*

Todistus. [3, Korollaari 7.13.]. □

Lemma 2.26. *Luvuilla a ja b on positiivisella kokonaisluvulla n jaettaessa sama jakojäännös, jos ja vain jos $n \mid (a - b)$.*

Todistus. [3, Lemma 7.14.]. □

Määritelmä 2.17. Oletetaan, että $a, b \in \mathbb{Z}$ ja n on positiivinen kokonaisluku. Jos $a - b$ on jaollinen luvulla n, sanotaan, että a ja b ovat *kongruentit modulo n*, ja merkitään $a \equiv b \pmod{n}$.

Lemma 2.27. *Olkoot $a, b, c \in \mathbb{Z}$, ja olkoon n positiivinen kokonaisluku. Tällöin seuraavat väitteet pätevät:*

a) $a \equiv a \pmod{n}$.

b) Jos $a \equiv b \pmod{n}$, *niin* $b \equiv a \pmod{n}$.

c) Jos $a \equiv b \pmod{n}$ *ja* $b \equiv c \pmod{n}$, *niin* $a \equiv c \pmod{n}$.

Todistus. a) Selvästi $n \mid a - a$.

b) Jos $a \equiv b \pmod{n}$, niin $a - b = kn$ jollakin $k \in \mathbb{Z}$. Täten $b - a = -kn$, josta saadaan $b \equiv a \pmod{n}$.

c) Jos $a - b = k_1 n$ ja $b - c = k_2 n$ joillakin $k_1, k_2 \in \mathbb{Z}$, niin saadaan $(a - b) + (b - c) = (k_1 + k_2)n$. Täten $(a - c) = (k_1 + k_2)n$ eli $a \equiv c \pmod{n}$.

□

Määritelmä 2.18. Olkoon n positiivinen kokonaisluku. Kokonaisluvun a *jäännösluokka modulo n* on joukko

$$[a]_n = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}.$$

Jäännösluokkien joukkoa merkitään $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, ..., [n-1]_n\}$.

Lause 2.28. *Olkoot $a, b, c, d \in \mathbb{Z}$, ja olkoon n positiivinen kokonaisluku. Tällöin seuraavat väitteet pätevät:*

a) Jos $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$, niin $a + c \equiv b + d \pmod{n}$ ja $ac \equiv bd \pmod{n}$.

b) Jos $ca \equiv cb \pmod{n}$ ja $syt(c, n) = 1$, niin $a \equiv b \pmod{n}$.

c) Jos $a \equiv b \ (mod\ kn)$ jollakin $k \in \mathbb{Z}$, niin $a \equiv b \pmod{n}$.

Todistus. [3, lause 7.18.]. □

Lause 2.29. *Olkoot a, c ja n kokonaislukuja, ja olkoon n lisäksi positiivinen. Kongruenssiyhtälöllä $ax \equiv c \pmod{n}$ on kokonaislukuratkaisu, jos ja jos vain $syt(a, n) \mid c$.*

Todistus. [3, Lause 7.20.]. □

2.7 Sykliset ryhmät

Palaamme tässä pikaisesti kohtaan 2.5.

Määritelmä 2.19. Yhden alkion virittämää ryhmää $G = \langle g \rangle$ kutsutaan *sykliseksi ryhmäksi.*

Lause 2.30. *Sykliset ryhmät ovat vaihdannaisia.*

Todistus. [3, Lause 8.1.]. □

Palaamalla Lemmaan 2.15. saadaan äärellisille syklisille ryhmille esitysmuoto

$$\langle g \rangle = \{e, g, ^2, ..., g^{n-1}\}.$$

Lause 2.31. *Jäännösluokkien joukossa $\mathbb{Z}_n$ voidaan määritellä yhteenlasku*

$$[a]_n + [b]_n = [a + b]_n.$$

Todistus. [3, Lause 8.3.]. □

Lause 2.32. *Ryhmä $(\mathbb{Z}_n, +)$ on syklinen ja sen kertaluku on n.*

Todistus. [3, Lause 8.4.]. □

Usein ryhmäteoriassa paria $(\mathbb{Z}_n, +)$ merkitään $\mathbb{Z}_n$.

Lause 2.33. *Jokainen syklinen ryhmä, jonka kertaluku on ääretön, on isomorfinen ryhmän $(\mathbb{Z}, +)$ kanssa.*

Todistus. [3, Lause 8.6.]. □

Lemma 2.34. *Oletetaan, että G on ryhmä ja $g \in G$. Jos $g^m = e$, alkion g kertaluku jakaa luvun m.*

Todistus. [3, Lemma 8.7.]. □

Lause 2.35. *Jokainen syklinen ryhmä, jonka kertaluku on n, on isomorfinen ryhmän Z_n kanssa.*

Todistus. [3, Lause 8.8.]. □

Korollaari 2.35.1. *Jos kahdella syklisellä ryhmällä on sama kertaluku, ryhmät ovat isomorfiset.*

Lause 2.36. *Syklisen ryhmän kaikki aliryhmät ovat syklisiä.*

Todistus. [3, Lause 8.10.]. □

Lause 2.37. *Jos syklinen ryhmä G on ääretön, sen aliryhmät ovat täsmälleen muotoa $\langle g^k \rangle$, missä $k \in \mathbb{Z}$.*

Todistus. [3, Lause 8.11.]. □

Korollaari 2.37.1. *Ryhmän $(\mathbb{Z}, +)$ aliryhmät ovat muotoa $k\mathbb{Z}$, missä $k \in \mathbb{N}$.*

Lemma 2.38. *Olkooon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku on $n \in \mathbb{N}$. Kaikilla $m \in \mathbb{Z}$ pätee $\langle g^m \rangle = \langle g^d \rangle$, missä $d = syt(n, m)$.*

Todistus. [3, Lemma 8.13.]. □

Lause 2.39. *Olkoon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku $n \in \mathbb{N}$. Alkion g^m kertaluku on $\frac{n}{syt(n,m)}$ kaikilla $m \in \mathbb{Z}$.*

Todistus. [3, Lause 8.14.]. □

Korollaari 2.39.1. *Äärellisen syklisen ryhmän aliryhmien kertaluvut jakavat koko ryhmän kertaluvun.*

Todistus. [3, Korollaari 8.16.] □

Korollaari 2.39.2. *Olkoon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku on $n \in \mathbb{N}$. Ryhmän muut virittäjät ovat muotoa $\langle g^m \rangle$, missä $syt(m, n) = 1$.*

Todistus. [3, Korollaari 8.17.] □

Lause 2.40. *Olkoon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku on $n \in \mathbb{N}$. Sen aliryhmät ovat ryhmät $\langle g^d \rangle$, missä d on luvun n positiivinen tekijä. Eri tekijöitä vastaavat aliryhmät poikkeavat toisistaan.*

Todistus. [3, Lause 8.18.]. □

2.8 Sivuluokat ja Lagrangen lause

Lagrangen lause on yksi tärkeimmistä ryhmäteorian tuloksista. Saammekin jo todella alkeellisella ryhmäteorialla paljon tietoa äärellisen ryhmän mahdollisista aliryhmistä. Se nimittäin kertoo minkä kertaluvun aliryhmiä äärellisellä ryhmällä ei voi olla.

Määritelmä 2.20. Olkoon G ryhmä ja H sen aliryhmä. Kaikille $g \in G$ joukkoa $\{gh : h \in H\}$ kutsutaan aliryhmän H *vasemmaksi sivuluokaksi* ja sitä merkitään gH. Joukkoa Hg kutsutaan aliryhmän H *oikeaksi sivuluokaksi.*

Seuraavaksi listaamme joitakin sivuluokkien ominaisuuksia.

Lemma 2.41. *Olkoon H ryhmän G aliryhmä ja olkoot $a, b \in G$. Tällöin pätee*

1. $a \in aH$.
2. $aH = H$, *jos ja vain jos* $a \in H$.
3. $(ab)H = a(bH)$ *ja* $H(ab) = (Ha)b$.
4. $aH = bH$, *jos ja vain jos* $a \in bH$.
5. $aH = bH$ *tai* $aH \cap bH = \emptyset$.
6. $aH = bH$, *jos ja vain jos* $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$, *jos ja vain jos* $H = aHa^{-1}$.
9. aH *on ryhmän G aliryhmä, jos ja vain jos* $a \in H$.

Todistus. [1, Lemma s. 146]. □

Lause 2.42 (**Lagrangen lause**)**.** *Jos G on äärellinen ryhmä ja H sen aliryhmä, niin kertaluku $|H|$ jakaa kertaluvun $|G|$. Lisäksi, aliryhmän H oikeiden (vasempien) sivuluokkien määrä on $|G|/|H|$.*

Todistus. [1, Theorem 7.1.]. □

Korollaari 2.42.1. *Jos G on äärellinen ryhmä ja H sen aliryhmä, niin $[G : H] = |G|/|H|$, missä $[G : H]$ on vasempien sivuluokkien määrä.*

Tämä seuraa suoraan Lagrangen lauseesta.

Korollaari 2.42.2. *Äärellisen ryhmän alkioiden kertaluku jakaa koko ryhmän kertaluvun.*

Todistus. [1, Corollary 2. s. 148]. □

Korollaari 2.42.3. *Jos ryhmän kertaluku on alkuluku, niin se on syklinen.*

Todistus. [1, Corollary 3. s. 148]. □

Korollaari 2.42.4. *Olkoon G äärellinen ryhmä ja olkoon $a \in G$. Tällöin $a^{|G|} = e$.*

Todistus. [1, Corollary 4. s. 149]. □

Korollaari 2.42.5 (**Fermat'n pieni lause**). *Jokaiselle kokonaisluvulle a ja alkuluvulle p pätee*

$$a^p \equiv a \pmod{p}$$

Todistus. [1, Corollary 5. s.149]. □

Lagrangen lauseen todistus oli olemassa kauan ennen ryhmäteorian syntyä. Se kertoo millaisia aliryhmiä jollakin äärellisillä ryhmillä ei voi olla olemassa. Kuitenkaan Lagrangeen lause ei ole tosi käänteisesti. Esimerkiksi $|A_4| = 12$, missä A_n on *alternoiva ryhmä* [1, Definition s.110]. Sillä ei kuitenkaan ole kertaluvun 6 aliryhmää. Sylowin lauseet antavat meille myöhemmin kuitenkin varman tavan löytää yhden tyyppisiä äärellisen ryhmän aliryhmiä.

Lause 2.43. *Olkoot K ja H jonkun ryhmän aliryhmiä. Määrittelemme joukon $HK := \{hk : h \in H, k \in K\}$. Täten $|HK| = |H||K|/|H \cap K|$.*

Todistus. [1, Theorem 7.2.]. □

2.9 Homomorfismi, normaali aliryhmä ja tekijäryhmä

Määritelmä 2.21. Olkoot $(G, \star)$ ja $(H, *)$ ryhmiä. Kuvaus $f : G \to H$ on *ryhmähomomorfismi*, jos seuraava ehto pätee:

$$f(g \star h) = f(g) * f(h).$$

Homomorfismien suuri merkitys on siinä, että kuvaus säilyttää rakenteen algebralliset ominaisuudet. Jos kuvaus on homeomorfismi ja bijektio, niin se on isomorfismi. Tässä tutkielmassa tarkoitamme homomorfismilla aina ryhmähomomorfismia.

Lause 2.44. *Oletetaan, että $f : G \to H$ on homomorfismi ja $g \in G$. Tällöin seuraavat väitteet pätevät:*

1. $f(e_G) = e_H$.
2. $f(g^{-1}) = f(g)^{-1}$.
3. $f(g^k) = f(g)^k$.

Todistus. [3, Lause 18.5.] □

Lause 2.45. *Olkoon $f : G \to G'$ homomorfismi. Oletetaan, että $H \leq G$ ja $H' \leq G'$. Tällöin seuraavat väitteet pätevät:*

1. *$fH \leq G'$.*
2. *$f^{-1}H' \leq G$.*
3. *Kertaluku $|f(H)|$ jakaa kertaluvun $|H|$.*

Todistus. [1, Theorem 10.2] □

Lause 2.46. *Jos $f : G \to H$ ja $g : H \to K$ ovat homomorfismeja, myös kuvaus $g \circ f : G \to K$ on homomorfismi.*

Todistus. [3, Lause 18.8.] □

Määritelmä 2.22. Homomorfismin $f : G \to H$ *ydin* $\ker f$ koostuu niistä alkioista, jotka kuvautuvat neutraalialkiolle:

$$\ker f = \{g \in G : f(g) = e_H\}.$$

Täten $\ker f = f^{-1}\{e_H\}$.

Lause 2.47. *Olkoon $f : G \to H$ homomorfismi. Kuvaus f on injektiivinen, jos ja vain jos* $\ker(f) = \{e_G\}$.

Todistus. [3, Lause 18.13.] □

Kuvaus f on myös selvästi surjektio, jos ja vain jos $\mathrm{im} f = H$.

Oletamme ekvivalenssirelaatioihin ja ekvivalenssiluokkiin liittyvien perustuloksien olevan tuttuja lukijalle.

Määritelmä 2.23. Olkoon R joukon A ekvivalenssirelaatio. Ekvivalenssiluokkien joukko A/R on joukon A *ositus*.

Määritelmä 2.24. Olkoon X joukko, jossa on määritelty laskutoimitus $*$ sekä ekvivalenssirelaatio R. Oletetaan lisäksi, että kaikille $x, x', y, y' \in X$ pätee: jos xRx' ja yRy', niin $x * yRx' * y'$. Tällöin sanotaan laskutoimituksen $*$ olevan *yhteensopiva* relaation R kanssa.

Lause 2.48. *Olkoon $*$ laskutoimitus joukossa X, ja olkoon R laskutoimituksen $*$ kanssa yhteensopiva ekvivalenssirelaatio. Tällöin on olemassa joukon X/R laskutoimitus $*'$, jolle pätee*

$$[x] *' [y] = [x * y]$$

kaikilla $x, y \in X$.

Todistus. [2, Lause 1.3.] □

Määritelmä 2.25. Olkoon X joukko, jossa on määritelty ekvivalenssirelaatio R sekä kuvaus $f : X \to Y$. Oletetaan lisäksi, että kaikille $x, x' \in X$ pätee: jos xRx', niin $f(x) = f(x')$. Tällöin sanotaan, että kuvaus f on yhteensopiva ekvivalenssirelaation R kanssa.

Lause 2.49 (**Homomorfismin hajottaminen**). *Olkoon $f : X \to Y$ homomorfismi ja olkoon joukossa X määritelty laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Jos f on yhteensopiva ekvivalenssirelaation R kanssa, niin on olemassa yksikäsitteinen homomorfismi $f^* : X/R \to Y$, jolle pätee*

$$f = f^* \circ \pi,$$

missä π on kanoninen surjektio $X \to X/R$.

Toisin sanoen alla oleva kaavio *kommutoi*.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\pi}\downarrow & \nearrow_{f^*} & \\ X/R & & \end{array}$$

Todistus. [2, Lause 1.7.] □

Nyt pystymme määrittelemään tekijäryhmän määrittelemällä ensin normaalin aliryhmän.

Määritelmä 2.26. Aliryhmää $H \leq G$ kutsutaan *normaaliksi*, jos sen vasemmat ja oikeat sivuluokat ovat samat, eli $gH = Hg$ kaikilla $g \in G$. Ryhmän G normaalia aliryhmää H merkitään $H \trianglelefteq G$.

Lause 2.50 (**Aliryhmän normaalisuuskriteeri**). *Olkoon G ryhmä ja N sen aliryhmä. Aliryhmä N on normaali, jos ja vain jos*

$$gng^{-1} \in N \text{ kaikilla } n \in N \text{ ja } g \in G.$$

Myös $gNg^{-1} \subset N$ on yhtäpitävä ehto normaalisuuskriteerin kanssa.

Todistus. [3, Lause 15.13.] □

Lause 2.51. *Oletetaan, että H on ryhmän G normaali aliryhmä. Tällöin ekvivalenssirelaatio xRx', jos ja vain jos $x \in x'H$ on yhteensopiva laskutoimituksen kanssa.*

Todistus. [2, Lause 1.12.] □

Määritelmä 2.27. Olkoon G ryhmä ja N sen normaali aliryhmä. Ryhmää G/N kutsutaan ryhmän G *tekijäryhmäksi* aliryhmän N suhteen, kun laskutoimituksena on

$$gN \cdot hN = ghN.$$

Todistus siihen, että tekijäryhmä on todellakin ryhmä kyseisellä laskutoimituksella löytyy [3, Lause 15.7.].

Lause 2.52. *Oletetaan, että R on ryhmässä G määritelty, laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Tällöin neutraalialkion luokka $N = [e]$ on ryhmän G normaali aliryhmä ja kaikilla $g, g' \in G$ pätee gRg', jos ja vain jos $g' \in gN$.*

Todistus. [2, Lause 1.13.] □

Lause 2.53. *Homomorfismin ydin on normaali aliryhmä.*

Todistus. [3, Lause 18.14.] □

Lause 2.54. *Olkoon $f : G \to H$ homomorfismi, ja olkoon $N \trianglelefteq G$. Tällöin on olemassa yksikäsitteinen homomorfismi $f^* : G/N \to H$, jolle pätee $f^*([g]) = f(g)$ kaikilla $g \in G$, jos ja jos vain $N \subset \ker f$.*

Todistus. [2, Lause 1.14.] □

Korollaari 2.54.1 (**Homomorfialause**)**.** *Olkoon $f : G \to H$ homomorfismi. Tällöin ryhmät $G/\ker f$ ja $\mathrm{im} f$ ovat isomorfiset.*

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ \downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow{\ \cong\ } & \mathrm{im} f \end{array}$$

Todistus. [2, Korollaari 1.15.] □

Lause 2.55. *Olkoon N ryhmän G normaali aliryhmä. Tällöin jokainen tekijäryhmän G/N aliryhmä voidaan esittää muodossa H/N, missä $N \leq H \leq G$.*

Todistus. Tarkastellaan kanonista kuvausta $\pi : G \to G/N$. Kuvaus π on homomorfismi, kuten määritelmästä 2.27 huomaa. Olkoon $A \leq G/N$ mikä tahansa aliryhmä. Merkitään $H = \pi^{-1}A$ ja osoitetaan, että se on kelvollinen aliryhmä. Lauseen 2.45 perusteella $H \leq G$. Myös lauseen 2.45 perusteella $N \leq H$, koska $\pi(N)$ on ryhmän G/N triviaali aliryhmä. Viimeiseksi osoitamme, että $A = H/N$. Koska kanoninen kuvaus tekijäryhmään on surjektio, niin

$$H/N = (\pi^{-1}A)/N = \pi\pi^{-1}A = A.$$

□

3 Ryhmän toiminta

Tässä kappaleessa siirrymme käsittelemään ryhmän toimintaa. Tarkoituksena on esitellä ryhmän toiminnan perusteet, tarvittavia toimintoja, hyödyllisiä lauseita ja muutamia yleisiä esimerkkejä. Toiminnat ovat tehokas työkalu saada informaatiota ryhmän rakenteesta. Varsinkin jos joukko, missä ryhmä toimii omaa jotain muutakin matemaattista rakennetta on sillä paljon sovellutuksia. Ryhmän toimintaa voi ajatella eräänlaisena yleistyksenä permutaation käsitteestä. Kappaleen rakenne seuraa pääosin Jokke Häsän *Algebra II* luentomuistiinpanojen kappaletta 2.

3.1 Ryhmän toiminta yleisesti

Seuraavassa määritelmässä merkintätapa X^X tarkoittaa kuvausten muodostamaa joukkoa $\{f \mid f : X \to X\}$.

Määritelmä 3.1. Olkoon G ryhmä ja X joukko. Kuvausta $\varphi : G \to X^X$, missä $g \mapsto f_g$ kaikilla $g \in G$ kutsutaan ryhmän *vasemmanpuoleiseksi (oikeanpuoleiseksi) toiminnaksi* joukossa X, jos seuraavat ehdot toteutuvat:

1. $f_e = \mathrm{id}_X$
2. $f_{gh} = f_g \circ f_h$.

Ehto 2. korvataan oikeanpuoleisessa tapauksessa ehdolla $f_{gh} = f_h \circ f_g$.

Vasemmanpuoleista toimintaa merkitään usein $f_g(x) = gx$. Täten $ex = x$ ja $(gh)x = g(hx)$. Vastaavasti merkintätapa $f_g(x) = xg$ on käytössä oikeanpuoleiselle toiminnalle. Yleensä kontekstista on selvää milloin merkintä liittyy toimintaan. Kuitenkin alan kirjallisuudessa ei tunnu olevan yleistä standardia tämän notaation suhteen.

Lause 3.1. *Olkoon φ ryhmän G toiminta. Tällöin jokainen $\varphi(g) = f_g$ on kääntyvä.*

Todistus. Nähdään, että $f_g \circ f_{g^{-1}} = f_e = f_{g^{-1}} \circ f_g$. □

Tämä tarkoittaa, että jokainen ryhmän G jäsen vastaa jotakin bijektiota $X \to X$. Kuvaus φ on myös homomorfismi, koska $\varphi(gh) = f_{gh} = f_g \circ f_h = \varphi(g) \circ \varphi(h)$. Voimme myös huomata, että φ on injektio, josta seuraa Lause 2.13 (Cayleyn lause). Tämän todistuksessa käytimmekin jo ryhmän toimintaa määrittelemättä sitä. Jotkut teokset, kuten Serge Langin *Algebra* [4, s. 25] määrittelee ryhmän toiminnan suoraan kuvauksena symmetriseen ryhmään.

Esimerkkinä voimme ottaa ryhmän G toiminnan, jossa $f_g : h \mapsto ghg^{-1}$ joukossa G. Tätä toimintaa kutsutaan *konjugoinniksi*. Vaikkapa matriisin diagonalisoimisessa ominaisarvojen avulla päästään muotoon $A = PDP^{-1}$, missä D on diagonaalimatriisi. Konjugointi on esimerkki ryhmän sisäisestä toiminnasta. Tämä nähdään käymällä

läpi määritelmän 3.1 ehdot. Ensiksi $f_e : h \mapsto ehe^{-1} = h$, eli $f_e = id_G$. Toiseen ehtoon huomataan, että

$$f_{gh}(x) = ghxh^{-1}g^{-1} = gf_h(x)g^{-1} = f_g(f_h(x)) = f_g \circ f_h(x).$$

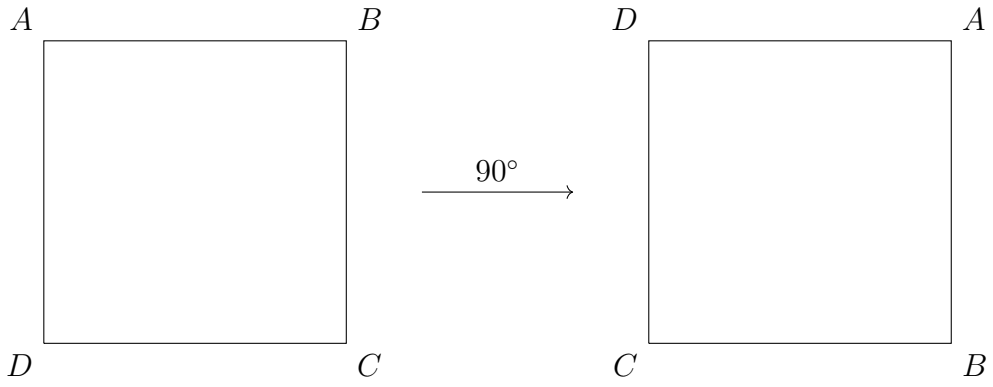
Tämä on erityisen mielenkiintoinen toiminta, koska jokainen $f_g : G \to G$ on isomorfismi. Tämä nähdään helposti, sillä jokainen f_g on kääntyvä ja

$$f_g(hx) = ghxg^{-1} = ghg^{-1}gxg^{-1} = f_g(h)f_g(x).$$

Konjugointi on kuvaus ryhmältä sen *automorfismiryhmään* $\varphi : G \to \mathrm{Aut}(G)$ [4, s. 8]. Kuvauksen φ ydintä $\ker \varphi = \{g \in G \mid gxg^{-1} = x \text{ kaikilla } x \in G\}$ kutsutaan *keskukseksi* ja merkitään $Z(G)$. Ei ole myöskään vaikeaa nähdä, että keskus on Abelin ryhmä kertomalla määritelmän yhtälöä oikealta alkiolla g. Täten kaikilla $g, x \in G$ pätee $gx = xg$. Toisaalta, jos G on Abelin ryhmä, niin myös selkeästi $Z(G) = G$.

Toinen yleinen esimerkki on ryhmän *esitys*. Se on homomorfismi $\rho : G \to \mathrm{GL}(n, V)$, missä G on ryhmä, V jokin vektoriavaruus yli skalaarikunnan K ja $\mathrm{GL}(n, V)$ kaikkien kääntyvien $n \times n$ matriisien ryhmä varustettuna matriisitulolla [4, s. 8]. Esitysteoria on matematiikan osa-ala, joka tutkii algebrallisten rakenteiden esityksiä yli vektoriavaruuksien.

Olkoon G *diedriryhmä* D_4 [1, s. 34] ja $X = \{A, B, C, D\}$, missä joukon X alkiot esittävät neliön kärkipisteitä.



Tässä ryhmän toiminta vaihtaa kärkipisteiden paikkoja ikään kuin neliön symmetria sitä kääntäessä tai peilatessa.

Määritelmä 3.2. Olkoot X, Y joukkoja ja G ryhmä, joka toimii niissä. Tällaisia joukkoja kutsutaan *G-joukoiksi* ja kuvaus $f : X \to Y$ on *G-morfismi*, jos

$$gf(x) = f(gx) \text{ kaikilla } x \in X, g \in G.$$

Seuraavaksi esittelemme kaksi tärkeää ryhmän toimintaan liittyvää käsitettä, jotka ovat rata ja vakauttaja. Oletetaan, että ryhmä G toimii joukossa X. Tällöin joukon X osajoukkoa Y kutsutaan *vakaaksi*, jos $gy \in Y$ kaikilla $g \in G, y \in Y$.

Määritelmä 3.3. Olkoon G ryhmä ja X $G-$joukko. Alkion $x \in X$ *rata* on joukko

$$\mathrm{Orb}_G(x) = \{gx \mid g \in G\}.$$

Kutsumme usein ryhmän G alkion rataa *G-radaksi*, jos toimintoja on useampi.

Lause 3.2. *Ryhmän G radat muodostavat ekvivalenssirelaation joukossa X:*

$$xRy \text{ jos on olemassa } g \in G \text{ siten, että } x = gy.$$

Todistus. Refleksiivisyys pätee, koska $x = ex$. Symmetrisyys saadaan, koska $x = gy$ on yhtäpitävää $y = g^{-1}x$ kanssa. Transitiivisuuteen valitaan $x, y, z \in X$, joille xRy ja yRz. Täten on olemassa $g, g' \in G$ siten, että $x = gy$ ja $y = g'z$. Täten $x = gg'z$ ja tällöin xRz. □

Radat siis muodostavat osituksen joukolle X.

Määritelmä 3.4. Olkoon Y joukko, $X \subset Y$ ja G ryhmä joka toimii joukossa Y. Jos $x \in X$ niin joukkoa

$$\mathrm{Stab}_G(X) = \{g \in G \mid gx \in X \text{ kaikilla } x \in X\}$$

kutsutaan joukon X *vakauttajaksi*. Jos X on yksiö niin kutsumme sitä *kiinnittäjäksi* ja merkitsemme sitä $\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$.

Kiinnittäjä on ryhmän G aliryhmä, koska kaikille $g, h \in \mathrm{Stab}_G(x)$ pätee $(gh)x = g(hx) = gx = x$, $e \in \mathrm{Stab}_G(x)$ triviaalisti ja $g^{-1}x = g^{-1}gx = ex = x$. Joskus kiinnittäjästä käytetään myös termiä *isotropiaryhmä*, kuten esimerkiksi [4, s. 27]. Kuitenkaan kiinnittäjä ei ole välttämättä normaali aliryhmä. Voidaan ottaa esimeriksi ryhmän $G = S_3$ konjugointi ja valitaan $x = (12)$. Tällöin $\mathrm{Stab}_G(x) = \{e, (12)\}$. Tämä ei ole normaali aliryhmä, sillä valitsemalla $(132) \in S_3$ nähdään että

$$(132)\{e, (12)\} = \{e, (23)\} \neq \{e, (13)\} = \{e, (12)\}(132).$$

Lause 3.3 (**Rata-vakauttajalause**)**.** *Olkoon X jokin $G-$joukko ja $x \in X$. Tällöin on olemassa bijektio $f : G/Stab_G(x) \to Orb_G(x)$, jolle $gStab_G(x) \mapsto gx$.*

Todistus. Aluksi näytämme, että f on hyvin määritelty. Valitaan $g, g' \in g\mathrm{Stab}_G(x)$. Täten on olemassa jokin $h \in \mathrm{Stab}_G(x)$, että $g = g'h$. Koska h kiinnittää alkion x, niin $gx = g'hx = g'x$. Osoitamme seuraavaksi vielä, että kuvaus f on bijektio. Tiedetään, että f on surjektio radalle $\mathrm{Orb}_G(x)$. Tulee siis osoittaa, että f on injektio. Oletetaan, että $gx = hx$ joillakin $g, h \in G$. Tällöin

$$h^{-1}gx = h^{-1}hx = x.$$

Siis $h^{-1}g$ kiinnittää alkion x. Siis lemman 2.41.6 perusteella h ja g kuuluvat samaan sivuluokkaan. □

Määritelmä 3.5. Ryhmän G toimintaa joukossa X kutsutaan *transitiiviseksi*, jos kaikille $x, y \in X$ on olemassa $g \in G$ siten, että $x = gy$. Kutsumme myös $G-$joukkoa X *homogeeniseksi*.

Tästä seuraa suoraan, että jokainen rata on homogeeninen. Täten saadaan myös, että ryhmä G toimii transitiivisesti, jos ja vain jos $\mathrm{Orb}_G(x) = X$ kaikille $x \in X$.

Lause 3.4. *Oletetaan, että ryhmä G toimii transitiivisesti joukossa X. Tällöin*

$$|X| = [G : Stab_G(x)],$$

missä $Stab_G(x)$ kiinnittää jonkin alkion $x \in X$.

Todistus. Koska $\mathrm{Orb}_G(x) = X$, niin rata-vakauttajalauseen mukaan on olemassa bijektio $f : G/\mathrm{Stab}_G(x) \to X$. □

Korollaari 3.4.1. *Ryhmä G toimii joukossa X ja T on kaikkien $G-$ratojen edustajisto (joukko T sisältää jokaisesta $G-$radasta täsmälleen yhden edustavan alkion). Tällöin pätee*

$$|X| = \sum_{x \in T} [G : Stab_G(x)].$$

Todistus. Koska $G-$radat muodostavat joukon X osituksen, niin $X = \bigsqcup_{x \in T} \mathrm{Orb}_G(x)$. Täten lauseesta 3.4 ja ratojen transitiivisuudesta saadaan

$$|X| = \left| \bigsqcup_{x \in T} \mathrm{Orb}_G(x) \right| = \sum_{x \in T} |\mathrm{Orb}_G(x)| = \sum_{x \in T} [G : \mathrm{Stab}_G(x)].$$

□

3.2 Konjugointi

Palaamme vielä takaisin kappaleen alussa mainittuun konjugointiin. Siinä tuli esille alkioiden konjugointi ghg^{-1}. Voimme myös määritellä *aliryhmien konjugoinnin* gHg^{-1}, missä H on ryhmän G aliryhmä. Ryhmän G aliryhmät A ja B ovat siis konjugaatit keskenään, jos $A = gBg^{-1}$ jollakin $g \in G$.

Jos ryhmä G toimii konjugoimalla sisäisesti, niin sen ratoja kutsutaan *konjugaattiluokiksi*. Merkitsemme alkion x konjugaattiluokkaa $\mathrm{Cl}(x) = \{gxg^{-1} \mid g \in G\}$. Tämä tarkoittaa sitä, että $x, y \in \mathrm{Cl}(x)$, jos ja vain jos $y = gxg^{-1}$, jollakin $g \in G$. Neutraalialkion muodostama konjugaattiluokka on alkio itse. Tämä nähdään, koska $geg^{-1} = gg^{-1} = e$ kaikilla $g \in G$. Seuraavaksi näemmekin, että normaaleilla aliryhmillä on suora linkki konjugaattiluokkiin.

Lause 3.5. *Normaali aliryhmä on yhdiste konjugaattiluokista.*

Todistus. Olkoon H ryhmän G normaali aliryhmä. Täten lauseen 2.50 perusteella jokainen $\mathrm{Cl}(h) \subset H$ eli $\bigcup_{h \in H} \mathrm{Cl}(h) \subset H$. Seuraavaksi olkoon $h \in H$ mielivaltainen alkio. Tällöin $h = ehe^{-1} \in \mathrm{Cl}(h) \subset \bigcup_{h \in H} \mathrm{Cl}(h)$. Siis $\bigcup_{h \in H} \mathrm{Cl}(h) = H$. □

Jos ryhmä G toimii konjugoimalla itseään, niin sen kiinnittäjää kutsutaan *keskittäjäksi*. Merkitsemme alkion $x \in G$ keskittäjää $C_G(x) = \{g \in G \mid gxg^{-1} = x\}$. Itseasiassa kaikkien kiinnittäjien leikkaus on ryhmän keskus $Z(G) = \bigcap_{x \in G} C_G(x)$. Ryhmän keskuksen muodostavat juuri ne alkiot, jotka pysyvät paikallaan konjugoinnissa.

Lause 3.6. *Olkoon G ryhmä ja olkoon $Z(G)$ sen keskus. Jos $G/Z(G)$ on syklinen, niin G on Abelin ryhmä.*

Todistus. Kuten kappaleen 3 alussa konjugointiin liittyvässä esimerkissä todettiin, että G on Abelin ryhmä, jos ja vain jos $Z(G) = G$. Nyt jos $G/Z(G)$ on syklinen on olemassa jokin $x \in G$ siten, että $G/Z(G) = \langle xZ(G) \rangle$. Valitaan myös jokin $g \in G$ ja tällöin $gZ(G) = (xZ(G))^k = x^k Z(G)$, jollakin kokonaisluvulla k. Siis $g = x^k z$ jollain $z \in Z(G)$. Koska z ja x^k kuuluvat kiinnittäjään $C_G(x)$, niin myös $g \in C_G(x)$. Koska alkion g valinta oli mielivaltainen niin $gZ(G) = Z(G)$ kaikilla $g \in G$ eli ryhmä $G/Z(G)$ on triviaali eli $Z(G) = G$. □

Jos ryhmä G toimii konjugoimalla sen aliryhmien joukossa, niin kutsumme aliryhmien ratoja *(aliryhmien) konjugaattiluokiksi*, aliryhmien kiinnittäjiä taas *normalisoijiksi*. Merkitsemme normalisoijaa $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

Lause 3.7. *Olkoon G ryhmä ja $x \in G$. Konjugaattiluokan koko on*

$$|Cl(x)| = [G : C_G(x)]$$

Todistus. Todistus seuraa lauseesta 3.4. □

Lause 3.8 (**Luokkayhtälö**)**.** *Olkoon G ryhmä ja T kaikkien ryhmän G konjugaattiluokkien edustajisto. Tällöin*

$$|G| = \sum_{x \in T} [G : C_G(x)]$$

Todistus. Todistus seuraa korollaarista 3.4.1 ja lauseesta 3.7. □

4 Sylowin lauseet

Kuten jo aikaisemmin mainitsimme Sylowin lauseet ovat osittainen käänteinen versio Lagrangen lauseesta. Aliryhmien löytäminen on yleisesti todella vaikeaa. Kuitenkin Sylowin lauseet luovat meille tehokkaan tavan löytää tietynlaisia aliryhmiä. Myöhemmin kappaleessa myös selviää erilaisia sovellutuksia ryhmäteoriassa. Sylowin lauseiden numeroinnille ei ole standardia luokittelua alan kirjallisuudessa. Myös lauseiden sisältö saattaa vaihdella hieman teosten välillä.

Ymmärtääksemme Sylowin lauseiden sisällön tulee meidän määritellä hieman terminologiaa. Lisäksi todistamme muutaman tuloksen auttamaan lauseiden todistuksissa ja niitä soveltavissa esimerkeissä. Kappale seuraa pääosin Joseph A. Gallianin *Contemporary Abstract Algebra* teosta ja Jokke Häsän *Algebra II* kurssimuistiinpanoja.

Määritelmä 4.1. Olkoon p alkuluku. Tällöin äärellistä ryhmää sanotaan *p-ryhmäksi*, jos sen kertaluku on p^n jollain $n \in \mathbb{N}$, $n \geq 1$.

Lause 4.1. *Olkoon G jokin $p-$ryhmä. Tällöin sen keskus on epätriviaali eli $|Z(G)| > 1$.*

Todistus. Huomataan aluksi, että $\mathrm{Cl}(a) = \{a\}$, jos ja vain jos $a \in Z(G)$. Täten voimme kirjoittaa lauseen 3.8 muodossa

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

Koska $|G : C_G(a)| = |G|/|C_G(a)|$ täten konjugaattiluokkien, missä $a \in T \setminus Z(G)$ kertaluku on jokin alkuluvun p positiivinen potenssi. Täten saamme yhtälön

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

Selvästi siis vasen puoli on jaollinen luvulla p eli myös $|Z(G)|$ on jaollinen luvulla p. Ryhmän G keskus on siis epätriviaali.

□

Korollaari 4.1.1. *Olkoon G ryhmä jonka kertaluku on p^2. Tällöin G on Abelin ryhmä.*

Todistus. Lagrangen lauseesta ja lauseesta 4.1 nähdään, että $|Z(G)|$ on joko p tai p^2. Jos $|Z(G)| = p^2$, niin $G = Z(G)$, joten G on Abelin ryhmä. Jos taas $|Z(G)| = p$, niin $|G/Z(G)| = p$ ja lauseen 3.6 perusteella G on Abelin ryhmä. □

Lause 4.2. *Olkoon G äärellinen Abelin ryhmä, jossa alkuluku p jakaa ryhmän G kertaluvun. Tällöin ryhmällä G on kertaluvun p alkio.*

Todistus. Oletetaan, että väite pätee kaikille Abelin ryhmille, joiden kertaluku on pienempi, kuin $|G|$. Jos $|G| = p$, niin se on syklinen, joten sillä on kertaluvun p alkio. Jos $|G| > p$ niin valitaan niin $x \in G$ jonka kertaluku on qm, missä q on alkuluku, m positiivinen kokonaisluku. Lauseen 2.39 perusteella $|x^m| = q$. Täten on siis olemassa jokin alkio, jonka kertaluku on alkuluku. Nyt jos $q = p$, niin todistus on valmis. Oletetaan siis, että $q \neq p$. Tiedetään, että kaikki Abelin ryhmän aliryhmät ovat normaaleja. Täten voidaan konstruoida tekijäryhmä $G^* = G/\langle a \rangle$, missä alkion a kertaluku on q. Koska $|G^*| = |G|/q$, niin voimme käyttää induktio-oletusta ryhmään G^*. Ryhmällä G^* on alkio $y\langle a \rangle$, jonka kertaluku on p. Nähdään, että $(y\langle a \rangle)^p = y^p\langle a \rangle = \langle a \rangle$ ja tällöin $y^p \in \langle a \rangle$. Jos $y^p = e$, niin väite pätee. Jos $y^p \neq e$ alkion y^p kertaluku on q, koska y^p on kertaluvun q syklisen ryhmän $\langle a \rangle$ epätriviaali alkio. Täten lauseen 2.39 perusteella alkion $(y^p)^q$ kertaluku on $q/\text{syt}(q, q) = 1$ siis $y^{pq} = e$. Tällöin alkion y^q kertaluku on p.

□

Määritelmä 4.2. Oletetaan, että ryhmän kertaluku on $p^n m$, missä p on alkuluku, $n \in \mathbb{N} \setminus \{0\}$ ja m ei ole jaollinen luvulla p. Sellaista aliryhmää, jonka kertaluku on p^n kutsutaan *Sylowin p-aliryhmäksi.*

Toisaalta jos p ei jaa ryhmän kertalukua, niin ainoa Sylowin p-aliryhmä on triviaali ryhmä. Sylowin $p-$aliryhmä on siis ryhmän maksimaalinen p-ryhmä. Merkitsemme ryhmän G Sylowin $p-$aliryhmien kokoelmaa $\text{Syl}_p(G)$. Seuraavaksi osoitamme Sylowin $p-$aliryhmien olemassaolon.

Lause 4.3 (**Sylowin ensimmäinen lause.**). *Olkoon G äärellinen ryhmä ja p alkuluku, missä p^k jakaa ryhmän G kertaluvun jollain $k \in \mathbb{N}$. Tällöin ryhmällä G on kertaluvun p^k aliryhmä.*

Todistus. Käytämme todistukseen induktiota ryhmän kertaluvun suhteen. Jos $|G| = 1$, niin väite pätee selkeästi. Oletetaan, että väite pätee kaikille ryhmille joiden kertaluku on pienempi, kuin $|G|$. Jos ryhmällä G on olemassa aito aliryhmä, jonka kertaluku on jaollinen luvulla p^k, niin väite pätee vedoten induktio-oletukseen. Jos tällaistä ei ole niin voidaan päätellä, että p^k ei jaa ryhmän G minkään aidon aliryhmän kertalukua. Katsotaan seuraavaksi lauseen 4.1 versiota luokkayhtälöstä

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

Tiedetään, että $|G| = |G : C_G(a)||C_G(a)|$ kaikilla $a \notin Z(G)$. Täten, koska p^k jakaa ryhmän G kertaluvun ja p^k ei jaa kiinnittäjän $C_G(a)$ kertalukua, niin p jakaa indeksin $[G : C_G(a)]$. Luokkayhtälöstä seuraa täten, että p jakaa keskuksen $Z(G)$ kertaluvun. Lauseen 4.2 perusteella $Z(G)$ sisältää kertaluvun p alkion x. Koska $x \in Z(G)$, niin $\langle x \rangle$ on ryhmän G normaali aliryhmä. Voimme siis katsoa tekijäryhmää $G^* = G/\langle x \rangle$ ja huomata, että p^{k-1} jakaa ryhmän G^* kertaluvun, sillä $|G^*| = |G|/p$. Induktio-oletuksen myötä, ryhmällä G^* on kertaluvun p^{k-1} aliryhmä. Lauseen 2.55 perusteella voimme siis esittää tämän aliryhmän muodossa $H/\langle x \rangle$. Nyt meillä on yhtälö $|H/\langle x \rangle| = p^{k-1}$ joka johtaa siihen, että $|H| = p^k$, missä H on ryhmän G aliryhmä. □

Intuitiivisesti Sylowin ensimmäinen lause sanoo, että voimme ottaa esimerkiksi äärellisen ryhmän G ja sen kertaluvun alkulukuhajotelman. Tästä saamme pääteltyä millaisia $p-$aliryhmiä ryhmällä on. Esimerkiksi jos $|G| = 2^2 \cdot 3^2 \cdot 5$, niin on olemassa kertalukujen $2, 4, 3, 9$ ja 5 $p-$aliryhmiä. Näistä Sylowin $p-$aliryhmät ovat kertalukua $4, 9$ ja 5. Kuitenkaan Sylowin ensimmäinen lause ei takaa esimerkiksi kertaluvun 6 aliryhmän olemassa-oloa, vaikka Lagrangen lause kertoisi sen mahdollisesta olemassaolosta. Tulos siis takaa ainakin yhden Sylow $p-$aliryhmän olemassaolon, mutta ei vielä kerro niiden lukumäärästä. Sylowin ensimmäinen lause on yleistys kuuluisasta Cauchyn lauseesta. Käytimme todistuksessa myös lausetta 4.2, joka on Cauchyn lause Abelin ryhmille.

Korollaari 4.3.1 (**Cauchyn lause**). *Olkoon G äärellinen ryhmä ja olkoon p alkuluku, joka jakaa ryhmän G kertaluvun. Tällöin ryhmällä G on kertaluvun p alkio.*

Ennen Sylowin toista lausetta todistemma hyödyllisen lemman. Siinä tulee ilmi yleistys keskuksen käsitteestä.

Lemma 4.4. *Olkoon H äärellinen äärellinen $p-$ryhmä ja olkoon X äärellinen $H-$joukko. Määritellään joukko $\Omega = \{x \in X \mid hx = x \text{ kaikilla } h \in H\}$. Tällöin $|X| \equiv |\Omega| \mod p$.*

Todistus. Joukko X voidaan kirjoittaa muodossa

$$X = \Omega \cup \bigcup_{h \in T \setminus \Omega} \mathrm{Orb}_H(h),$$

missä T on kaikkien ratojen edustajisto. Koska radat muodostavat osituksen, niin

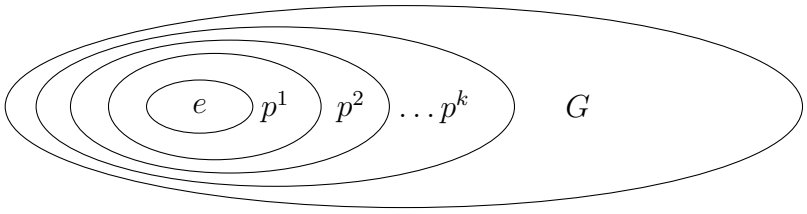
$$|X| = \sum_{h \in T} |H|/|\mathrm{Stab}_H(h)| = |\Omega| + \sum_{h \in T \setminus \Omega} |H|/|\mathrm{Stab}_H(h)| = |\Omega| + \sum_{h \in T \setminus \Omega} p^{\alpha_h}.$$

Tässä alkiot p^{α_h} ovat alkion p potensseja ja $\alpha_h > 0$. Koska $\sum_{h \in T \setminus \Omega} p^{\alpha_h}$ on jaollinen luvulla p, niin $|X| \equiv |\Omega| \mod p$.

□

Lause 4.5 (**Sylowin toinen lause**). *Sylowin p-aliryhmät ovat konjugaatteja keskenään. Lisäksi jokainen p-aliryhmä sisältyy Sylowin p-aliryhmään.*

Todistus. Olkoon $P \in \mathrm{Syl}_p(G)$, Q jokin $p-$aliryhmä ja $|G| = p^k m$. Katsomme ryhmän Q kertolaskutoimintaa ryhmän P sivuluokkien joukossa. Lagrangen lauseesta seuraa, että $[G : P] = m$. Soveltamalla lemmaa 4.4 aliryhmän P sivuluokkien joukkoon. saadaan $m \equiv |\Omega| \mod p$. Kuitenkaan luku m ei ole jaollinen luvulla p ja siten ei myöskään $|\Omega|$. Tämä johtaa siihen, että $|\Omega| \neq 0$. Siis ratojen joukossa on ainakin jokin yksiö $\{gP\}$ eli $QgP = gP$. Sivuluokkien ominaisuuksista seuraa, että $qg \in gP$ kaikilla $q \in Q$. Siis kertomalla puolittain käänteisalkiolla saadaan $g^{-1}qg \in P$. Voimme tällöin päätellä, että $g^{-1}Qg \subset P$. Toisaalta jos Q on Sylowin $p-$aliryhmä, niin $|P| = |Q|$. Tällöin $g^{-1}Qg = P$, koska konjugointi on automorfismi eli siis bijektio. Lopuksi palattaessa tilanteeseen $qg \in gP$ voidaan päätellä, että $q \in gPg^{-1}$ kaikilla $q \in Q$. Toisin sanoen $Q \leq gPg^{-1}$, missä gPg^{-1} on Sylowin $p-$aliryhmä. □



Kuva 4.1: Havainnollistava kuva Sylowin p-aliryhmistä, missä symboli p^k esittää ryhmän G Sylowin $p-$aliryhmää ja symbolit p^n, kun $n < k$ siihen sisältyviä $p-$aliryhmiä

Korollaari 4.5.1. *Ryhmän G Sylowin $p-$aliryhmä on normaali, jos ja vain jos se on ryhmän G ainoa Sylowin $p-$aliryhmä.*

Todistus. Olkoon P ryhmän G yksikäsitteinen Sylowin $p-$aliryhmä. Koska konjugointi on automorfismi, niin $|gPg^{-1}| = |P|$ kaikilla $g \in G$. Siis gPg^{-1} on Sylowin $p-$aliryhmä. Koska P on yksikäsitteinen niin $gPg^{-1} = P$ kaikilla $g \in G$, joka täyttää normaalisuuskriteerin 2.50. Käänteisesti oletetaan, että $P \trianglelefteq G$. Koska normaalit aliryhmät ovat invariantteja konjugoinnissa, niin tällöin $gPg^{-1} \subset P$ kaikilla $g \in G$. Kuitenkin lauseen 4.5 todistuksen tavoin konjugoinnin automorfismista seuraa, että $gPg^{-1} = P$. Myös lauseen 4.5 perusteella kaikki Sylowin $p-$aliryhmät ovat konjugaatteja keskenään, mutta kaikille $g \in G$ pätee $gPg^{-1} = P$, joten P on näistä ainoa. □

Tämä korollaari on itseasiassa erittäin hyödyllinen normaalien aliryhmien olemassaolon takaamisessa. Esimerkiksi kuten myöhemmin näemme, niin normaalin aliryhmän olemassaolo antaa paljon kriittistä informaatiota ryhmän rakenteesta.

Lause 4.6 (**Sylowin kolmas lause**)**.** *Olkoon ryhmän G kertaluku $p^k m$, missä p on alkuluku, $k \geq 1, m \in \mathbb{N}$ ja p ei jaa lukua m. Tällöin Sylowin $p-$aliryhmien määrä $n_p = \left|Syl_p(G)\right| \equiv 1 \mod p$ ja n_p jakaa luvun m.*

Todistus. Olkoon P taas jokin ryhmän G Sylowin $p-$aliryhmä. Tutkimme nyt aliryhmän P toimintaa konjugoimalla joukossa $\mathrm{Syl}_p(G)$. Selvästi alkion P rata on yksiö, koska $gPg^{-1} = P$ kaikilla $g \in P$. Seuraavaksi osoitamme, että tämä on itseasiassa ainoa rata, jonka suuruus on yksi. Toisin sanoen lemmassa 4.4 esille tulleen joukon Ω kardinaliteetti on yksi. Oletetaan, että $Q \neq P$ on jokin Sylowin p-aliryhmä, joka muodostaa kokoa yksi olevan radan. Koska $gQg^{-1} = Q$ kaikilla $g \in P$, niin $P \in N_G(Q)$. Tiedetään, että normalisoija on ryhmän G aliryhmä eli se jakaa ryhmän G kertaluvun $p^k m$. Tällöin myös aliryhmän P ja Q kertaluku p^k jakaa normalisoijan kertaluvun. Siis aliryhmien P ja Q täytyy olla normalisoijan Sylow $p-$aliryhmiä. Siis Sylowin toisen lauseen mukaan jollakin $g \in N_G(Q)$ pätee $gQg^{-1} = P$. Kuitenkin kaikilla $g \in N_G(Q)$ pätee, että $gQg^{-1} = Q$. Tällöin $Q = P$ ja lemmasta 4.4 seuraa $n_p \equiv 1 \mod p$, sillä $|\Omega| = 1$.

Osoitamme vielä, että n_p jakaa luvun m. Katsotaan nyt ryhmän G toimintaa konjugoimalla joukossa $\mathrm{Syl}_p(G)$. Sylowin toisen lauseen perusteella kaikki Sylowin $p-$aliryhmät ovat konjugaatteja. Toisin sanoen ne kuuluvat siis samaan rataan.

Tämä rata on joukko $\mathrm{Syl}_p(G)$ eli toiminta on transitiivista. Voimme siis lauseen 3.4 perusteella ilmaista luvun n_p muodossa

$$n_p = [G : N_G(Q)],$$

jollakin $Q \in \mathrm{Syl}_p(G)$. Tästä seuraa, että n_p jakaa ryhmän G kertaluvun $p^k m$. Tiedetään myös, että $n_p \equiv 1 \mod p$. Tästä seuraa, että n_p ja p ovat keskenään jaottomia. Siis Eukleideen lemman perusteella n_p jakaa luvun m. □

4.1 Sylowin lauseiden sovelluksia

Yksi keskeinen asema Sylowin lauseilla on äärellisten yksinkertaisten ryhmien luokittelussa. Se oli proseduuri, joka sisälsi noin 10000 sivua ryhmäteorian julkaisuja ja saatin viimein valmiiksi vuonna 2004 [1, s. 432]. Äärellisten yksinkertaisten ryhmien luokittelu jakaa kaikki äärelliset ryhmät kertaluvun p syklisiin ryhmiin, yli viidennen asteen alternoiviin ryhmiin, Lie tyyppisiin ryhmiin tai 27 sporadiseen ryhmään. Sylowin lauseet ovat tehokas tapa luokitella joitakin äärellisiä ryhmiä niiden kertaluvun perusteella, varsinkin pienen kertaluvun tilanteessa. Kuitenkin yleiselle äärelliselle ryhmällä Sylowin lauseet ovat vain tapauskohtaisesti tehokkaita.

Määritelmä 4.3. Ryhmä on *yksinkertainen*, jos sen ainoat normaalit aliryhmät ovat ryhmä itse ja triviaali ryhmä.

Esimerkki. Kertaluvun 30 ryhmä ei ole yksinkertainen. Olkoon G ryhmä, jolle $|G| = 30 = 2 \cdot 3 \cdot 5$. Täten Sylowin kolmannen lauseen mukaan $n_5 \equiv 1 \mod 5$ ja $n_5 \mid 6$. Täten

$$n_5 = 1 \text{ tai } n_5 = 6.$$

Myös $n_3 \equiv 1 \mod 3$ ja $n_3 \mid 10$. Täten

$$n_3 = 1 \text{ tai } n_3 = 10$$

Jos $n_5 = 6$ niin kahden eri kertaluvun 5 aliryhmän leikkaus on vain neutraalialkio, sillä epätriviaalit alkiot virittävät ryhmän itse. Tämä johtuu siitä, että aliryhmän kertaluku 5 on alkuluku. Täten kaikkien kuuden kertaluvun 5 aliryhmien yhdisteen alkioiden lukumäärä on ainakin 24. Jos myös oletamme saman tapauksessa $n_3 = 10$, saamme ainakin 20 alkiota niiden yhdisteeseen. Samoin myös kaikkien kertaluvun 3 ja 5 aliryhmien leikkaus on vain neutraalialkio, koska niiden epätriviaalit alkiot virittävät oman aliryhmänsä. Kuitenkin $24 + 20 = 44$ joka on enemmän kuin ryhmän G kertaluku eli siis ristiriita. Täten siis ryhmällä G on ainakin yksi epätriviaali normaali aliryhmä. Voimme tällöin päätellä, että ryhmä G ei ole yksinkertainen.

Samalla tekniikalla voimme myös esimerkiksi osoittaa, että mikä tahansa kertaluvun p^2q ryhmä, missä p ja q ovat alkulukuja ja $p \neq q$ ei ole yksinkertainen. Yleisesti Sylowin lauseet ovat tehokkaita osoittamaan ryhmien (epä)yksinkertaisuuden, joiden kertaluvussa on vähän tekijöitä.

Lause 4.7 (**Sylowin testi epäyksinkertaisuudelle**). *Olkoon n positiivinen kokonaisluku, joka ei ole alkuluku. Lisäksi olkoon p alkuluku, joka jakaa luvun n. Jos* 1 *on luvun n ainoa tekijä, jolle $n \equiv 1 \mod p$, niin kertaluvun n yksinkertaista ryhmää ei ole olemassa.*

Todistus. Olkoon G ryhmä, jonka kertaluku on n. Ensiksi oletamme, että G on $p-$ryhmä. Toisin sanoen $n = p^k$ jollakin positiivisella kokonaisluvulla k. Tällöin ryhmällä G on epätriviaali keskus lauseen 4.1 perusteella, joka on epätriviaali normaali aliryhmä. Jos $Z(G)$ on aito aliryhmä, niin väite pätee ja jos $Z(G) = G$, niin G on Abelin ryhmä eli epäyksinkertainen. Jos G ei ole $p-$ryhmä, niin jokainen Sylowin $p-$aliryhmä sisältyy aidosti ryhmään G. Sylowin kolmannen lauseen perusteella $n_p \equiv 1 \mod p$ ja $n_p \mid n$. Kuitenkin $n_p = 1$ on ainoa mahdollinen tapaus, joten korollaarin 4.5.1 perusteella on Sylowin $p-$aliryhmä normaali. Siis kertaluvun n ryhmä ei voi olla yksinkertainen. □

Supertietokoneiden testit ovat osoittanut, että kyseinen testi löytää noin $\sim 90\%$ kaikista epäyksinkertaisista ryhmistä, joiden kertaluvut eivät ole alkulukuja suurilla lukuväleillä [1, s. 433]. Esimerkiksi tarkastelemalla välillä $1 - 200$ kaikkia ei alkuluvullisten kertalukujen ryhmiä, voimme testin mukaan seuloa pois useita kertalukuja. Tällöin ainoat mahdolliset kandidaatit yksinkertaisille ryhmille kertaluvun perusteella ovat $12, 24, 30, 36, 48, 56, 60, 72, 80, 90, 96, 105, 108, 112, 120, 132, 144, 150, 160, 168, 180$ ja 192.

Seuraavaksi tutkimme toista äärellisille ryhmille keskeistä asiaa, nimittäin ryhmän ratkeavuutta.

Määritelmä 4.4. Ryhmä G on *ratkeava*, jos sillä on *normaalijono* aliryhmiä

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

joille tekijäryhmät G_{k+1}/G_k ovat Abelin ryhmiä kaikilla $k \in \{0, 1, 2, \ldots, n-1\}$.

Seuraavan lauseen todistus on taas eräs esimerkki Sylowin lauseiden käytöstä.

Lause 4.8. *Olkoot, p ja q erillisiä alkulukuja, joille $p > q$. Jos ryhmän G kertaluku on pq, niin G on ratkeava.*

Todistus. Koska $|G| = pq$, niin Sylowin ensimmäisen lauseen perusteella on olemassa kertaluvun q ja kertaluvun p Sylowin $p-$aliryhmät. Tällöin $n_p \mid q$ ja $n_p \equiv 1 \mod p$. On mahdollista vain, että $n_p = 1$, sillä q on alkuluku. Jos $n_p = q$, niin $q - 1$ olisi jaollinen luvlla p. Tämä on selvästi ristiriitaista suhteessa oletukseen $p > q$. Tällöin korollaarin 4.5.1 perusteella siis meillä on olemassa ryhmälle G normaali Sylowin $p-$aliryhmä P. Ei ole vaikea nähdä, että saamme tästä normaalijonon

$$\{e\} \trianglelefteq P \trianglelefteq G.$$

Myös jokainen normaalijonon tekijäryhmä G_{k+1}/G_k on syklinen, eli siis myös vaihdannainen, koska $|G/P| = p$, ja $|P/\{e\}| = p$. Siis kertaluvun pq ryhmä on ratkeava. □

On myös monia muita tapauksia, missä Sylowin lauseet voivat olla hyödyllinen tapa tutkia ratkeavuutta. Ryhmän ratkeavuus on itseasiassa yhtäpitävää polynomien ratkeavuuden kanssa. Jos määritelmä 4.4 pätee ryhmälle $G = \mathrm{Gal}(f)$, jossa G on polynomin f *Galois'n ryhmä*, niin polynomi on juurtamalla ratkeava, jos ja vain jos sen Galois'n ryhmä on ratkeava. Polynomin Galois'n ryhmän määrittelemiseksi tarvitsisimme hieman kuntalaajennoksien teoriaa. Tätä alaa kutsutaan *Galois'n teoriaksi*. Siinä kuntalaajennoksien automorfismeja tutkimalla saadaan yhteys ryhmäteoriaan. Tämän yhteyden luo Galois'n teorian peruslause, joka pätee normaaleille ja separoituville kuntalaajennoksille. Kuuluisa esimerkki on Abelin Ruffinin lause, jossa todistetaan viidennen tai korkeamman asteen polynomin yleisen ratkaisukaavan mahdottomuus. Tämä voidaan todistaa etsimällä viidennen asteen polynomi, joka ei ole ratkeava. Usein esimerkkinä toimii jokin polynomi, jonka Galois'n ryhmä on ratkeamaton ryhmä S_5. Aiheesta lisää teoksissa [2], [1] ja [4].

Lähteet

[1] Joseph A. Gallian, *Contemporary abstract algebra*, 8th ed., Brooks/Cole Cengage Learning, Boston, MA, 2013 (eng).

[2] J Häsä, *Algebra 2*, Helsinki, 2010 (fin).

[3] J Rämö ja J Häsä, *Johdatus abstraktiin algebraan*, 2. uud. p., Gaudeamus, Helsinki, 2013 (fin).

[4] Serge Lang, *Algebra*, Revised third edition., Graduate texts in mathematics ; 211, Springer, New York (N.Y.), 2002 (eng).