Sylowin lauseet

Pro gradu
Pietari Pennanen
Matemaattisten tieteiden tutkinto-ohjelma
Oulun yliopisto
Kevät 2021

Sisällys

Johdanto

Joukkoa ja sen alkioiden välistä operaatiota kutsutaan ryhmäksi, mikäli nämä täyttävät tietyt ryhmälle asetetut ehdot. Tässä tutkielmassa tutustutaan eräisiin äärellisen ryhmäteorian tuloksiin, jotka norjalainen matemaatikko Ludvig Sylow todisti jo vuonna 1872. Nämä lauseet kantavat nykyään Sylowin nimeä ja myöskin lauseisiin liittyvät aliryhmät on nimetty Sylowin mukaan. Sylowin lauseet takaavat olemassaolon niin sanotuille Sylowin p-aliryhmille, jotka ovat inkluusion suhteen suurimpia mahdollisia ryhmän p-aliryhmiä. Lisäksi lauseet kertovat, että Sylowin p-aliryhmien lukumäärä on aina kongruentti luvun 1 kanssa alkuluvun p suhteen, ja että kaikki Sylowin p-aliryhmät ovat toistensa konjugaatteja. Lauseet ovat osa äärellisen ryhmäteorian keskeisimpiä tuloksia ja tarjoavat muun muassa osittaisen käänteistuloksen Lagrangen lauseelle.

Tutkielman Luku 1 käsittelee peruskäsitteitä ja -tuloksia, jotka eivät itsessään liity ryhmien teoriaan. Nämä ovat lähinnä joukko-oppiin ja lukuteoriaan liittyviä käsitteitä ja tuloksia, joita tarvitaan myöhemmissä luvuissa.

Luvussa 2 esitetään ryhmän määritelmä ja rakennetaan ryhmäteorian pohja Sylowin lauseiden osoittamiselle. Keskeisiä ryhmäteorian käsitteitä ovat ryhmän lisäksi esimerkiksi aliryhmä, tekijäryhmä ja homomorfismi.

Luvussa 3 perehdytään ryhmän toimintaan joukossa, joka on keskeinen työkalu Sylowin lauseiden todistamisessa. Lisäksi luvussa todistetaan Cauchyn lause ja joitakin p-ryhmiin liittyviä tuloksia.

Luvussa 4 todistetaan Sylowin lauseet ja avataan hieman Sylowin lauseiden todistamisen historiallista taustaa. Lisäksi esitetään useampia vaihtoehtoisia todistuksia Sylowin lauseille.

Tutkielman päälähteenä on käytetty teosta [5]. Sylowin lauseiden vaihtoehtoisten todistusten lähteenä on käytetty muita lähdeteoksia. Lähteiden todistuksia on täydennetty oman pohdinnan kautta. Tulokset, joille ei ole annettu todistusta, oletetaan tunnetuiksi lähtötiedoiksi.

1 Perusteita

Tässä luvussa käsitellään hieman joukko-oppia ja lukuteoriaa, joita tarvitaan myöhemmissä luvuissa ryhmäteorian tulosten osoittamisessa. Nämä eivät ole tutkielman varsinaista ydinasiaa, ja suurin osa tuloksista oletetaankin ennestään tunnetuiksi.

1.1 Kuvaukset ja relaatiot

Määritelmä 1.1. Olkoot X ja Y joukkoja. *Kuvaus* $f\colon X \to Y$ on sääntö, joka liittää jokaiseen joukon X alkioon x yksikäsitteisen joukon Y alkion y. Kun kuvaus f liittää alkioon x alkion y, niin merkitään $f(x) = y$.

Määritelmä 1.2. Olkoon $f\colon X \to Y$ kuvaus. Tällöin joukon $A \subseteq X$ *kuvaksi* sanotaan joukkoa

$$f(A) = \{f(a) \mid a \in A\}$$

ja joukon $B \subseteq Y$ *alkukuvaksi* joukkoa

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

Määritelmä 1.3. Kuvaus $f\colon X \to Y$ on

(1) *Surjektio*, jos jokaisella alkiolla $y \in Y$ on olemassa alkio $x \in X$ siten, että $y = f(x)$.

(2) *Injektio*, jos ehdosta $f(x_1) = f(x_2)$ seuraa $x_1 = x_2$.

(3) *Bijektio*, jos kuvaus f on sekä surjektio että injektio.

Määritelmä 1.4. Kuvausten $f\colon X \to Y$ ja $g\colon Y \to Z$ *yhdistetty kuvaus* on kuvaus

$$g \circ f\colon X \to Z, \quad x \mapsto g(f(x)).$$

Määritelmä 1.5. Kuvaus $f^{-1}\colon Y \to X$ on kuvauksen $f\colon X \to Y$ *käänteiskuvaus*, mikäli $(f^{-1} \circ f)(x) = x$ kaikilla $x \in X$ ja $(f \circ f^{-1})(y) = y$ kaikilla $y \in Y$.

Lause 1.6. *Kuvauksella $f\colon X \to Y$ on olemassa käänteiskuvaus f^{-1} jos ja vain jos f on bijektio.*

Lause 1.7. *Olkoot X ja Y joukkoja ja $f\colon X \to Y$ kuvaus. Tällöin*

1. *Jos $T \subseteq S \subseteq X$, niin $f(T) \subseteq f(S)$. Vastaavasti jos $U \subseteq V \subseteq Y$, niin $f^{-1}(U) \subseteq f^{-1}(V)$.*

2. *Jos f on surjektio ja $U \subseteq Y$, niin $f(f^{-1}(U)) = U$.*

3. *Jos $S \subseteq X$, niin $S \subseteq f^{-1}(f(S))$.*

Todistus.
1. Jos $y \in f(T)$, niin $y = f(t)$ jollakin $t \in T$. Nyt $t \in S$, joten $y = f(t) \in f(S)$ eli $f(T) \subseteq f(S)$. Vastaavasti jos $x \in f^{-1}(U)$, niin $f(x) \in U \subseteq V$. Nyt siis $f(x) \in V$, joten $x \in f^{-1}(V)$ eli $f^{-1}(U) \subseteq f^{-1}(V)$.

2. Jos $u \in U$ ja f on surjektio, niin on olemassa $x \in X$ siten, että $f(x) = u$. Näin ollen $x \in f^{-1}(U)$ ja edelleen $u = f(x) \in f(f^{-1}(U))$. Olkoon sitten $y \in f(f^{-1}(U))$ eli $y = f(x)$ jollain $x \in f^{-1}(U)$. Tällöin $y = f(x) \in U$. Näin ollen $f(f^{-1}(U)) = U$.

3. Olkoon $s \in S$, jolloin $f(s) \in f(S)$. Tällöin $s \in f^{-1}(f(S))$.

□

Seuraavia ekvivalenssirelaatioon liittyviä käsitteitä ja tuloksia on käsitelty lähteessä [7].

Määritelmä 1.8. Relaatio $\frown$ joukossa X on *ekvivalenssirelaatio*, mikäli relaatio on

(1) *Refleksiivinen*: $x \frown x$ kaikilla $x \in X$.

(2) *Symmetrinen*: Jos $x \frown y$, niin $y \frown x$ kaikilla $x, y \in X$.

(3) *Transitiivinen*: Jos $x \frown y$ ja $y \frown z$, niin $x \frown z$ kaikilla $x, y, z \in X$.

Määritelmä 1.9. Olkoon $\frown$ ekvivalenssirelaatio joukossa X. Tällöin jos $a \in X$, niin alkion a *ekvivalenssiluokka* on joukon X osajoukko

$$[a] = \{x \in X \mid x \frown a\}.$$

Lause 1.10. *Jos $\frown$ on ekvivalenssirelaatio joukossa X, niin $x \frown y$ jos ja vain jos $[x] = [y]$.*

Määritelmä 1.11. Joukon X osajoukot A_i ovat *pareittain erillisiä* jos

$$A_i \cap A_j = \emptyset,$$

aina kun $i \neq j$. Joukon X *osituksen* muodostavat ne joukon X epätyhjät pareittain erilliset osajoukot, joiden yhdiste on koko joukko X.

Lause 1.12. *Jos $\frown$ on ekvivalenssirelaatio joukossa X, niin ekvivalenssiluokat muodostavat joukon X osituksen.*

1.2 Lukuteoriaa

Lause 1.13. *Olkoot a ja b kokonaislukuja ja b nollasta poikkeava. Tällöin on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että $a = qb + r$, missä $0 \leq r < |b|$.*

Määritelmä 1.14. Jos a ja b ovat kokonaislukuja ja on olemassa sellainen kokonaisluku k, että $a = kb$, niin luku b *jakaa* luvun a ja tätä merkitään $b \mid a$. Tällöin lukua b kutsutaan luvun a *tekijäksi*. Mikäli kokonaislukua k ei ole olemassa, niin luku b *ei jaa* lukua a, jolloin merkitään $b \nmid a$.

Määritelmä 1.15. Olkoot a ja b kokonaislukuja ja m positiivinen kokonaisluku. Kokonaislukujen a ja b sanotaan olevan *kongruentteja modulo m*, jos $m \mid a - b$. Tällöin merkitään

$$a \equiv b \bmod m.$$

Lause 1.16. *Kongruenssi modulo m on ekvivalenssirelaatio. Lisäksi*

$$a \equiv b \bmod m$$

jos ja vain jos

$$ac \equiv bc \bmod mc,\ c \in \mathbb{Z}\backslash\{0\}.$$

Määritelmä 1.17. Kongruenssissa modulo m kokonaisluvun $y \in \mathbb{Z}$ ekvivalenssiluokkaa kutsutaan luvun y määräämäksi *jäännösluokaksi modulo m* ja merkitään $\{x \in \mathbb{Z} \mid x \equiv y \bmod m\} = [y] = [y]_m$. Jäännösluokkien modulo m joukolle käytetään merkintää $\mathbb{Z}_m$.

Määritelmä 1.18. Jos $p \in \mathbb{Z}$, $p \geq 2$ ja luvulla p ei ole muita tekijöitä kuin ± 1 ja $\pm p$, niin lukua p sanotaan *alkuluvuksi*.

Määritelmä 1.19. Olkoot a ja b kokonaislukuja ja ainakin toinen nollasta poikkeava. Positiivinen kokonaisluku s on lukujen a ja b *suurin yhteinen tekijä*, mikäli sille pätevät ehdot:

(1) $s \mid a$ ja $s \mid b$,

(2) Jos $c \mid a$ ja $c \mid b$, niin $c \mid s$.

Tällöin merkitään $s = \mathrm{syt}(a, b)$.

Lause 1.20. *Jos a ja b ovat kokonaislukuja ja ainakin toinen näistä on nollasta poikkeava, niin tällöin lukujen suurin yhteinen tekijä on yksikäsitteisesti olemassa. Lisäksi on olemassa kokonaisluvut x ja y siten, että*

$$ax + by = \mathrm{syt}(a, b).$$

Lause 1.21. *Jos alkuluku p jakaa kokonaisluvun b, niin* $\mathrm{syt}(p, b) = p$. *Muulloin* $\mathrm{syt}(p, b) = 1$.

Lause 1.22 (Eukleideen lemma)**.** *Jos alkuluku p jakaa tulon ab, niin tällöin p jakaa ainakin toisen tekijöistä a ja b.*

Lause 1.23 (Aritmetiikan peruslause)**.** *Jokainen lukua yksi suurempi kokonaisluku n voidaan esittää yksikäsitteisesti muodossa*

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},$$

missä $p_1 < p_2 < \cdots < p_k$ ovat alkulukuja ja $n_1, n_2, \ldots, n_k \in \mathbb{Z}_+$. Tätä esitystä kutsutaan luvun n alkulukuhajotelmaksi.

Määritelmä 1.24. Olkoon n positiivinen kokonaisluku. Tällöin lukua

$$n! = n \cdot (n-1) \cdots 2 \cdot 1$$

kutsutaan luvun n *kertomaksi*. Lisäksi määritellään $0! = 1$.

Lause 1.25. *Olkoot $n \geq k \geq 0$ kokonaislukuja. Jos joukossa on n alkiota, niin joukon alkioista voidaan muodostaa*

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

kappaletta erilaisia osajoukkoja, joissa on k kappaletta alkioita. Lukua $\binom{n}{k}$ kutsutaan binomikertoimeksi.

Lemma 1.26. *Jos p^r on suurin alkuluvun p potenssi, joka jakaa luvun m, niin tällöin $p^r | \binom{p^n m}{p^n}$, mutta $p^{r+1} \nmid \binom{p^n m}{p^n}$, kun $n \geq 0$.*

Todistus. Olkoon p^r suurin alkuluvun p potenssi, joka jakaa luvun m. Binomikerroin $\binom{p^n m}{p^n}$ voidaan kirjoittaa auki muodossa

$$\frac{(p^n m)!}{(p^n)!(p^n m - p^n)!} = \frac{p^n m (p^n m - 1) \cdots (p^n m - i) \cdots (p^n m - p^n + 1)}{p^n (p^n - 1) \cdots (p^n - i) \cdots (p^n - p^n + 1)}. \quad (1)$$

Olkoon p^k alkuluvun p potenssi, joka jakaa osoittajassa olevan termin $p^n m - i,\ i \geq 1$ eli $p^k \mid p^n m - i$ jollain $k \geq 0$. Koska

$$p^n m - i = (m-1)p^n + (p^n - i),$$

niin $p^k \mid (m-1)p^n + (p^n - i)$.

Nyt ei voi olla, että $k \geq n$, sillä tällöin

$$p^n m - i = qp^k = qp^{k-n} \cdot p^n,$$

ja siten $p^n \mid p^n m - i$. Näin ollen

$$p^n \mid (p^n m - i) - (m-1)p^n = p^n - i,$$

mikä on mahdotonta, sillä $p^n > p^n - i$.

Täytyy siis olla $k < n$, joten $p^k \mid (m-1)p^n$. Nyt koska

$$p^k \mid (m-1)p^n + (p^n - i),$$

niin $p^k \mid p^n - i$.
Toisaalta, jos p^k jakaa nimittäjässä olevan termin $p^n - i$ eli $p^k \mid p^n - i$, niin

$$p^k \mid (m-1)p^n + p^n - i = p^n m - i.$$

Näin ollen osoittajassa olevassa termissä $p^n m - i$ on tekijänä jokin alkuluvun p potenssi jos ja vain jos tämä sama potenssi on tekijänä nimittäjässä olevassa termissä $p^n - i$.
Tarkastellaan nyt binomikertoimen esitystä (1):

$$\binom{p^n m}{p^n} = \frac{p^n m(p^n m - 1) \cdots (p^n m - i) \cdots (p^n m - p^n + 1)}{p^n (p^n - 1) \cdots (p^n - i) \cdots (p^n - p^n + 1)}.$$

Potenssi p^n supistuu osoittajasta ja nimittäjästä. Edeltävän nojalla osoittajassa olevassa termissä $p^n m - i$ ja nimittäjässä olevassa termissä $p^n - i$ on tekijänä aina sama alkuluvun p potenssi. Näin ollen esityksessä (1) kaikki alkuluvun p potenssit, jotka jakavat termit $p^n m - i$ ja $p^n - i$, kumoavat toisensa. Täten ainoa binomikertoimen jakava alkuluvun p potenssi on se, joka jakaa luvun m eli p^r. Näin ollen $p^r \mid \binom{p^n m}{p^n}$, mutta $p^{r+1} \nmid \binom{p^n m}{p^n}$.

□

2 Ryhmäteoriaa

Ryhmä on algebrallinen rakenne, joka koostuu joukosta ja sen alkioiden välisestä binäärisestä ja assosiatiivisesta operaatiosta. Binäärisyys tarkoittaa, että alkioiden välinen operaatio kuuluu aina edelleen joukkoon ja assosiatiivisuus tarkoittaa, että lopputulos ei riipu siitä, miten sulkeet on aseteltu alkioiden välisessä operaatiossa. Ryhmässä on aina olemassa neutraalialkio e, jonka operaatio joukon alkioiden kanssa säilyttää alkiot muuttumattomina. Lisäksi ryhmässä jokaiselle alkiolle a löytyy käänteisalkio a^{-1}, jonka operaatio alkion a kanssa tuottaa neutraalialkion e.

Tässä luvussa esitetään keskeisimmät ryhmäteorian käsitteet ja tulokset, joita tarvitaan Sylowin lauseiden todistamisessa. Erityisesti luvun alkuosassa on paljon tuloksia, jotka otetaan tunnettuina lähtötietoina. Nämä ovat tuloksia, jotka on todistettu alunperin lähteessä [4]. Varsinaiset todistukset mukailevat teoksessa [5] esitettyjä todistuksia.

2.1 Ryhmä ja aliryhmä

Määritelmä 2.1. Olkoon G epätyhjä joukko. Kuvausta

$$*\colon G \times G \to G,\ *(x, y) = x * y = xy$$

kutsutaan *binääriseksi operaatioksi* joukossa G.

Määritelmä 2.2. Olkoon G epätyhjä joukko ja $*$ binäärinen operaatio joukossa G. Paria $(G, *)$ kutsutaan *ryhmäksi*, mikäli

(1) Operaatio $*$ on *assosiatiivinen* joukossa G eli kaikilla $x, y, z \in G$ pätee, että $x * (y * z) = (x * y) * z$.

(2) On olemassa sellainen alkio $e \in G$, että $e * x = x * e = x$ kaikilla alkioilla $x \in G$. Alkiota e kutsutaan *neutraalialkioksi*.

(3) Jokaiselle alkiolle $x \in G$ on olemassa alkio $x^{-1} \in G$ siten, että $x^{-1} * x = x * x^{-1} = e$. Alkiota x^{-1} kutsutaan alkion x *käänteisalkioksi*.

Lisäksi ryhmää kutsutaan *Abelin ryhmäksi*, jos operaatio $*$ on kommutatiivinen joukossa G eli $x * y = y * x$ kaikilla $x, y \in G$.

Lause 2.3. *Olkoon G ryhmä ja $x, a, b \in G$. Tällöin*

1. *Jos $x * a = x * b$ tai $a * x = b * x$, niin $a = b$.*
2. *Neutraalialkio e on yksikäsitteinen.*
3. *Jokaisen alkion x käänteisalkio x^{-1} on yksikäsitteinen.*
4. *Alkion x käänteisalkiolle x^{-1} pätee $(x^{-1})^{-1} = x$.*
5. *Alkioilla a ja b pätee $(ab)^{-1} = b^{-1}a^{-1}$.*

Määritelmä 2.4. Olkoon G äärellinen ryhmä. Ryhmän G alkioiden lukumäärää $|\,G\,|$ sanotaan *ryhmän G kertaluvuksi.*

Lause 2.5. *Olkoon m positiivinen kokonaisluku. Jäännösluokkien joukko $\mathbb{Z}_m$ varustettuna jäännösluokkien yhteenlaskulla*

$$[a] + [b] = [a + b], \quad [a], [b] \in \mathbb{Z}_m$$

on Abelin ryhmä. Ryhmän $(\mathbb{Z}_m, +)$ kertaluku on m.

Määritelmä 2.6. Ryhmän G alkion a *potenssit* $a^n, n \in \mathbb{Z}_+$, määritellään induktiivisesti

$$a^1 = a \quad \text{ja} \quad a^{n+1} = a * a^n.$$

Lisäksi $a^0 = e$ ja $a^{-n} = (a^{-1})^n$, kun $n \in \mathbb{Z}_+$.

Määritelmä 2.7. Olkoon a ryhmän G alkio ja $a^k = e$ jollakin $k \in \mathbb{Z}_+$. Tällöin pienintä tällaista kokonaislukua $k \in \mathbb{Z}_+$ kutsutaan alkion a *kertaluvuksi* ja merkitään ord $a = k$. Jos tällaista kokonaislukua ei ole olemassa, niin alkion a sanotaan olevan *ääretöntä kertalukua.*

Lause 2.8. *Olkoon a ryhmän G alkio. Tällöin $a^k = e$ jos ja vain jos alkion a kertaluku jakaa luvun k.*

Todistus. Käänteinen suunta on selvä. Jos $a^k = e$, niin ord $a = n \leq k$. Jos $n \nmid k$, niin $k = qn + r$, jollakin $1 \leq r < n$.
Tällöin

$$a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r.$$

Koska $1 \leq r < n$ ja ord $a = n$, niin $a^r \neq e$ ja siten

$$a^k = a^r \neq e,$$

mikä on ristiriita. Näin ollen täytyy olla, että $n \mid k$.

□

Lause 2.9. *Olkoon a ryhmän G alkio, jonka kertaluku on $n = qp$ jollakin alkuluvulla p. Tällöin alkion a^q kertaluku on p.*

Todistus. Nyt $(a^q)^p = a^{qp} = a^n = e$, joten edellisen Lauseen 2.8 perusteella alkion a^q kertaluku jakaa alkuluvun p eli ord a^q on joko 1 tai p. Jos ord $a^q = 1$, niin $a^q = e$. Nyt $q < n$, joten alkion a kertaluku ei olisi n vaan q. Tämä on ristiriita, joten täytyy olla, että alkion a^q kertaluku on p.

□

Lause 2.10. *Äärellisen ryhmän G alkioiden kertaluvut ovat äärellisiä.*

Todistus. Olkoon $a \in G$. Tarkastellaan osajoukkoa $\{e, a, a^2, \ldots, a^n, \ldots\}$. Koska G on äärellinen, niin edellisessä listassa täytyy olla toistoa. Toisin sanoen täytyy olla olemassa positiiviset kokonaisluvut $m > n$ siten, että $a^m = a^n$ eli $e = a^m a^{-n} = a^{m-n}$. Nyt siis $m - n \geq 1$ ja $a^{m-n} = e$.

□

Määritelmä 2.11. Olkoon H joukon G epätyhjä osajoukko ja $(G, *)$ ryhmä. Jos $(H, *)$ on ryhmä, niin H on ryhmän G *aliryhmä* ja merkitään $H \leq G$. Jos $H \neq G$, niin H on ryhmän G *aito aliryhmä* ja merkitään $H < G$.

Lause 2.12 (Aliryhmäkriteeri)**.** *Olkoon G ryhmä ja $H \subseteq G$ epätyhjä. Tällöin H on ryhmän G aliryhmä jos ja vain jos*

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

Määritelmä 2.13. Olkoon H ryhmän G aliryhmä ja a ryhmän G alkio. Tällöin joukkoa

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

kutsutaan alkion a määrämäksi aliryhmän H *vasemmaksi sivuluokaksi.* *Oikeat sivuluokat* määritellään vastaavasti

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

Lause 2.14. *Olkoot G ryhmä, $H \leq G$ ja $a_1H, a_2H, \ldots$ aliryhmän H vasemmat sivuluokat ryhmässä G. Tällöin*

$$G = \bigcup_i a_iH$$

ja aina joko

$$a_iH \cap a_jH = \emptyset \quad tai \quad a_iH = a_jH.$$

Lisäksi kun G on äärellinen, niin $|a_iH| = |H|$.

Lause 2.15 (Lagrangen lause)**.** *Olkoon H äärellisen ryhmän G aliryhmä. Tällöin aliryhmän H kertaluku jakaa ryhmän G kertaluvun eli $|G| = n|H|$ jollakin $n \in \mathbb{Z}_+$. Lisäksi luku n on aliryhmän H toisistaan eroavien vasempien sivuluokkien lukumäärä.*

Lause 2.16. *Olkoon H ryhmän G aliryhmä. Tällöin $aH = H$ jos ja vain jos $a \in H$.*

Todistus. Olkoon $ah \in aH$ ja $aH = H$. Tällöin $ah = h'$ jollain $h' \in H$ ja siten $a = h'h^{-1} \in H$. Jos $a \in H$, niin $a \in aH$, sillä $e \in H$. Siten $a \in aH$ ja $a \in H$ eli $aH \cap H \neq \emptyset$, joten Lauseen 2.14 nojalla $aH = H = eH$.

□

Määritelmä 2.17. Aliryhmän $H \leq G$ *indeksi* $[G : H]$ on aliryhmän H toisistaan eroavien vasempien sivuluokkien lukumäärä ryhmässä G. Jos G on äärellinen, niin indeksi on Lagrangen lauseen luku n.

Lause 2.18. *Olkoon G ryhmä, a ryhmän G alkio ja $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$. Tällöin joukko $\langle a \rangle$ on ryhmän G aliryhmä.*

Määritelmä 2.19. Ryhmän G aliryhmää $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ kutsutaan alkion a generoimaksi ryhmän G *sykliseksi aliryhmäksi*. Jos $\langle a \rangle = G$, niin ryhmän G sanotaan olevan *syklinen*, ja että a on ryhmän G *generaattori*.

Huomautus 2.20. Jäännösluokkaryhmä $(\mathbb{Z}_m, +)$ on aina syklinen, sillä aina $\langle [1] \rangle = \mathbb{Z}_m$. Näin ollen mitä tahansa kertalukua m oleva syklinen ryhmä on aina olemassa.

Lause 2.21. *Olkoot G ryhmä ja $a \in G$. Jos on olemassa pienin sellainen positiivinen kokonaisluku n, että $a^n = e$, niin $|\langle a \rangle| = n$ ja $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.*

Lause 2.22. *Jos ryhmän kertaluku on alkuluku, niin ryhmä on syklinen*

Lause 2.23. *Syklisen ryhmän aliryhmät ovat syklisiä. Lisäksi syklinen ryhmä on aina Abelin ryhmä.*

Lause 2.24. *Olkoon G kertalukua n oleva syklinen ryhmä ja d kertaluvun n tekijä. Tällöin ryhmällä G on yksikäsitteinen kertalukua d oleva aliryhmä.*

Todistus. Olkoon $G = \langle a \rangle$ ja $n = cd$. Nyt $(a^c)^d = a^{cd} = a^n = e$. Jos $(a^c)^r = e$, niin Lauseen 2.8 nojalla $n \mid cr$ eli $cr = ns = cds$ jollakin $s \in \mathbb{Z}_+$ ja siten $r = ds \geq d$. Näin ollen alkion a^c kertaluku on d ja $\langle a^c \rangle$ on syklinen kertalukua d oleva ryhmän G aliryhmä.

Olkoon sitten $\langle x \rangle$ kertalukua d oleva aliryhmä ryhmässä G. Nyt $x = a^m$ jollain $m \in \mathbb{Z}_+$ ja $e = x^d = a^{md}$. Täten $md = nk$ jollain $k \in \mathbb{Z}_+$. Koska $n = cd$, niin $m = ck$ ja $x = a^m = (a^c)^k$. Näin ollen $\langle x \rangle \leq \langle a^c \rangle$ ja koska $|\langle x \rangle| = d = |\langle a^c \rangle|$, niin $\langle x \rangle = \langle a^c \rangle$. Täten kertalukua d oleva aliryhmä on yksikäsitteinen.

□

Lause 2.25. *Äärellisen ryhmän G alkion a kertaluku jakaa ryhmän kertaluvun.*

Todistus. Olkoon n alkion a kertaluku. Tällöin Lauseen 2.21 mukaan $n = |\langle a \rangle|$. Nyt Lauseen 2.18 nojalla $\langle a \rangle \leq G$, joten Lagrangen lauseen nojalla n jakaa ryhmän G kertaluvun.

□

2.2 Normaali aliryhmä ja tekijäryhmä

Määritelmä 2.26. Ryhmän G aliryhmä N on *normaali aliryhmä*, mikäli

$$aN = Na, \quad \text{kaikilla } a \in G.$$

Jos N on ryhmän G normaali aliryhmä, niin merkitään $N \trianglelefteq G$.

Huomautus 2.27. Jos G on Abelin ryhmä ja $N \leq G$, niin N on normaali aliryhmä, sillä $a * n = n * a$ kaikilla $n \in N$ ja $a \in G$.

Lause 2.28. *Ryhmän G aliryhmä N on normaali jos ja vain jos*

$$aNa^{-1} \subseteq N, \quad \text{kaikilla } a \in G.$$

Määritelmä 2.29. Olkoon G ryhmä ja a ryhmän G alkio. Tällöin *alkion a konjugaatiksi* kutsutaan sellaista ryhmän G alkiota, joka on muotoa

$$gag^{-1}, \text{ missä } g \in G.$$

Jos $a, b \in G$ ja $b = gag^{-1}$ jollain $g \in G$, niin alkiot a ja b ovat *toistensa konjugaatteja.*

Määritelmä 2.30. Olkoon G ryhmä, H ryhmän G aliryhmä ja $a \in G$. Tällöin joukkoa

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

kutsutaan *aliryhmän H konjugaatiksi.*

Lause 2.31. *Aliryhmän $H \leq G$ konjugaatti aHa^{-1} on aina ryhmän G aliryhmä.*

Todistus. Selvästi $aHa^{-1} \subseteq G$ on epätyhjä. Olkoot nyt $k, l \in aHa^{-1}$. Tällöin $k = ah_1a^{-1}$ ja $l = ah_2a^{-1}$ joillakin $h_1, h_2 \in H$. Nyt $l^{-1} = (ah_2a^{-1})^{-1} = (a^{-1})^{-1}h_2^{-1}a^{-1} = ah_2^{-1}a^{-1}$. Tällöin

$$kl^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1} = (ah_1a^{-1})(ah_2^{-1}a^{-1}) = a\underbrace{h_1h_2^{-1}}_{\in H}a^{-1},$$

joten $kl^{-1} = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$. Täten $aHa^{-1} \leq G$.

□

Määritelmä 2.32. Olkoon G ryhmä ja $H \leq G$. Tällöin aliryhmän H *normalisoija* (*normalizer*) on

$$N_G(H) = \{a \in G \mid aHa^{-1} = H\}.$$

Lause 2.33. *Aliryhmän $H \leq G$ normalisoija $N_G(H)$ on aina ryhmän G aliryhmä. Lisäksi aina $H \trianglelefteq N_G(H)$.*

Todistus. Nyt $N_G(H) \subseteq G$ on epätyhjä, sillä $e \in N_G(H)$, koska $eHe^{-1} = eHe = H$. Olkoot $a, b \in N_G(H)$ eli $aHa^{-1} = H$ ja $bHb^{-1} = H$. Täten myös $b^{-1}Hb = H$ ja siten

$$(ab^{-1})H(ab^{-1})^{-1} = (ab^{-1})H(ba^{-1}) = a(b^{-1}Hb)a^{-1} = aHa^{-1} = H.$$

Näin ollen $ab^{-1} \in N_G(H)$ ja siten $N_G(H) \leq G$.
Lisäksi $H \trianglelefteq N_G(H)$, sillä kaikilla $a \in N_G(H)$ pätee $aHa^{-1} = H \subseteq H$.

□

Määritelmä 2.34. Ryhmän G *keskus* $Z(G)$ määritellään

$$Z(G) = \{z \in G \mid zg = gz \text{ kaikilla } g \in G\}.$$

Huomautus 2.35. Keskus $Z(G)$ sisältää ryhmän G alkiot, jotka kommutoivat kaikkien muiden ryhmän alkioiden kanssa. Ryhmä G on Abelin ryhmä täsmälleen silloin, kun $Z(G) = G$.

Lause 2.36. *Ryhmän G keskus $Z(G)$ on ryhmän G normaali aliryhmä.*

Todistus. Nyt $e \in Z(G)$, koska $eg = g = ge$ kaikilla $g \in G$. Näin ollen keskus $Z(G) \subseteq G$ on epätyhjä. Olkoot $w, z \in Z(G)$ ja $g \in G$. Tällöin

$$wz^{-1}g = wz^{-1}gzz^{-1} = wz^{-1}zgz^{-1} = wgz^{-1} = gwz^{-1},$$

joten $wz^{-1} \in Z(G)$ ja täten $Z(G) \leq G$. Keskus $Z(G)$ on normaali aliryhmä, sillä $gz = zg$ kaikilla $g \in G$ ja $z \in Z(G)$, joten aina $gZ(G) = Z(G)g$.

□

Huomautus 2.37. Edellisen lauseen perusteella keskus $Z(G)$ on ryhmä ja koska kaikki keskuksen alkiot kommutoivat keskenään, niin keskus $Z(G)$ on aina Abelin ryhmä.

Lause 2.38. *Ryhmän G alkio x kuuluu keskukseen $Z(G)$ jos ja vain jos alkiolla x on ainoastaan yksi konjugaatti. Tämä konjugaatti on alkio x itse.*

Todistus. Jos $x \in Z(G)$, niin konjugaatti $gxg^{-1} = gg^{-1}x = x$ kaikilla $g \in G$, joten alkiolla x on ainoastaan yksi konjugaatti; alkio x itse. Kaikki alkiot ovat aina itsensä konjugaatteja, sillä $x = exe^{-1}$. Näin ollen jos alkiolla x on ainoastaan yksi konjugaatti, niin tämän täytyy olla alkio x. Tällöin $gx = gx(g^{-1}g) = (gxg^{-1})g = xg$ kaikilla $g \in G$ eli $x \in Z(G)$.

□

Määritelmä 2.39. Olkoon $(G, *)$ ryhmä ja $a, b \in G$. Määritellään aliryhmän $(N, *) \leq (G, *)$ vasempien sivuluokkien aN ja bN välinen operaatio:

$$aN * bN = \{x * y \mid x \in aN \text{ ja } y \in bN\}.$$

Lause 2.40. *Olkoon $(N, *) \trianglelefteq (G, *)$ ja $G/N = \{aN \mid a \in G\}$.*
Tällöin

1. $(aN) * (bN) = (a * b)N$, *missä* $a, b \in G$.
2. $(G/N, *)$ *on ryhmä.*

Huomautus 2.41. Ryhmässä G/N neutraalialkio on $eN = N$ ja alkion aN käänteisalkio on $a^{-1}N$.

Määritelmä 2.42. Olkoon G/N joukko kaikista ryhmän $(G, *)$ normaalin aliryhmän N vasemmista sivuluokista eli $G/N = \{aN \mid a \in G\}$. Tällöin ryhmää $(G/N, *)$ kutsutaan ryhmän G *tekijäryhmäksi* normaalin aliryhmän N suhteen.

Huomautus 2.43. Kun G on äärellinen ryhmä, niin tekijäryhmän G/N kertaluku $|G/N|$ on indeksi $[G : N] = \frac{|G|}{|N|}$.

2.3 Homomorfismi

Määritelmä 2.44. Olkoot $(G, *)$ ja $(H, \cdot)$ ryhmiä. Tällöin kuvausta $f \colon G \to H$ kutsutaan *homomorfismiksi*, jos

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

kaikilla alkioilla $a, b \in G$. Jos f on lisäksi bijektio, niin kuvausta f kutsutaan *isomorfismiksi*. Tällöin sanotaan, että ryhmät G ja H ovat *isomorfiset* ja merkitään $G \cong H$.

Lause 2.45. *Olkoot G ja H ryhmiä ja $f \colon G \to H$ homomorfismi. Tällöin*

1. $f(e_G) = e_H$, *missä e_G ja e_H ovat neutraalialkiot ryhmissä G ja H.*
2. $f(x^{-1}) = f(x)^{-1}$ *kaikilla $x \in G$.*
3. $f(x^n) = f(x)^n$ *kaikilla $x \in G$ ja $n \in \mathbb{Z}$.*

Määritelmä 2.46. Homomorfismin $f \colon G \to H$ *ytimeksi* kutsutaan joukkoa

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

Joukkoa

$$\mathrm{Im}(f) = \{h \in H \mid h = f(x),\ x \in G\}$$

kutsutaan homomorfismin f *kuvaksi*.

Lause 2.47. *Olkoon $f\colon G \to H$ homomorfismi. Tällöin*

1. *$Ker(f) \trianglelefteq G$ ja $Im(f) \leq H$.*
2. *Homomorfismi f on injektio jos ja vain jos $Ker(f) = \{e_G\}$.*

Lause 2.48. *Olkoon $f\colon G \to H$ homomorfismi. Tällöin*

1. *Jos $S \leq G$, niin $f(S) \leq H$.*
2. *Jos $T \leq H$, niin $f^{-1}(T) \leq G$.*

Lause 2.49. *Olkoon $f\colon G \to H$ homomorfismi ja x ryhmän G alkio, jonka kertaluku on k. Tällöin kuva-alkion $f(x) \in H$ kertaluku jakaa alkion x kertaluvun k.*

Todistus. Olkoon alkio x kertalukua k ja $f\colon G \to H$ homomorfismi.
Nyt

$$f(x)^k = f(x^k) = f(e_G) = e_H,$$

joten Lauseen 2.8 perusteella ord $f(x) \mid k$. □

Lause 2.50. *Olkoon $f\colon G \to H$ isomorfismi. Jos alkion $a \in G$ kertaluku on ääretön, niin alkion $f(a) \in H$ kertaluku on ääretön. Jos alkion a kertaluku on äärellinen n, niin alkion $f(a) \in H$ kertaluku on äärellinen n.*

Todistus. Olkoon $f\colon G \to H$ isomorfismi. Koska f on isomorfismi, niin f on bijektio ja on olemassa käänteiskuvaus $f^{-1}\colon H \to G$.

Olkoon alkion a kertaluku ääretön. Jos alkion $f(a) \in H$ kertaluku olisi äärellinen, niin $f(a)^n = e_H$ jollain $n \geq 1$. Nyt

$$f(a^n) = f(a)^n = e_H \overset{f \text{ isomorf.}}{\Rightarrow} a^n = f^{-1}(e_H) = e_G.$$

Tämä on ristiriita, sillä oletuksen mukaan alkion a kertaluku oli ääretön. Täten myös alkion $f(a) \in H$ kertaluvun täytyy olla ääretön.
Olkoon sitten alkion a kertaluku äärellinen $n \in \mathbb{Z}_+$. Tällöin $f(a)^n = f(a^n) = f(e_G) = e_H$. Jos olisi olemassa $1 \leq k < n$ siten, että $f(a)^k = e_H$, niin

$$f(a^k) = f(a)^k = e_H \overset{f \text{ isomorf.}}{\Rightarrow} a^k = f^{-1}(e_H) = e_G.$$

Tämä on ristiriita, sillä alkion a kertaluku oli n. Näin ollen alkion $f(a) \in H$ kertaluku on n.

□

Määritelmä 2.51. Olkoon G ryhmä ja g ryhmän G alkio. Määritellään kuvaus $\gamma_g \colon G \to G$ seuraavasti:

$$\gamma_g(a) = gag^{-1}$$

kaikilla $a \in G$. Näin määriteltyä kuvausta γ_g kutsutaan *konjugaatioksi*.

Lause 2.52. *Konjugaatio $\gamma_g \colon G \to G$ on isomorfismi. Lisäksi alkioilla, jotka ovat toistensa konjugaatteja, on sama kertaluku.*

Todistus. Olkoot $a, b \in G$. Tällöin

$$\gamma_g(ab) = g(ab)g^{-1} = g(ag^{-1}gb)g^{-1} = (gag^{-1})(gbg^{-1}) = \gamma_g(a)\gamma_g(b),$$

joten konjugaatio on homomorfismi. Jos $\gamma_g(a) = e$, niin $gag^{-1} = e$ eli $a = e$, joten $\mathrm{Ker}(\gamma_g) = \{e\}$. Siten γ_g on injektio Lauseen 2.47 kohdan 2 nojalla.

Nyt $\gamma_{g^{-1}}(a) \in G$ ja

$$\gamma_g(\gamma_{g^{-1}}(a)) = g(g^{-1}ag)g^{-1} = a$$

kaikilla $a \in G$, joten γ_g on myös surjektio.

Jos alkiot a ja b ovat toistensa konjugaatteja eli $b = gag^{-1}$ jollain $g \in G$, niin $b = gag^{-1} = \gamma_g(a)$. Koska konjugaatio on isomorfismi, niin Lauseen 2.50 nojalla alkioilla a ja b on sama kertaluku.

□

Lause 2.53. *Olkoon $N \trianglelefteq G$. Tällöin kuvaus $\pi \colon G \to G/N,\ \pi(a) = aN$ on surjektiivinen homomorfismi, jonka ydin on N.*

Määritelmä 2.54. Olkoon G ryhmä ja $N \trianglelefteq G$. Kuvausta

$$\pi \colon G \to G/N,\ \pi(a) = aN \ \text{ kaikilla } a \in G$$

kutsutaan *luonnolliseksi homomorfismiksi*.

Lause 2.55 (Homomorfismien peruslause)**.** *Olkoon $f : G \to H$ homomorfismi. Tällöin*

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

Lause 2.56 (3. isomorfialause)**.** *Olkoot H ja N ryhmän G normaaleja aliryhmiä ja $N \leq H$. Tällöin $H/N \trianglelefteq G/N$ ja*

$$(G/N)/(H/N) \cong G/H.$$

Todistus. Määritellään kuvaus $f\colon G/N \to G/H$ siten, että $f(aN) = aH$. Kuvaus f on hyvin määritelty, sillä jos $a' \in G$ ja $a'N = aN$, niin $a^{-1}a'N = N$ eli $a^{-1}a' \in N \leq H$. Tällöin siis $a^{-1}a' \in H$, joten $a^{-1}a'H = H$ eli $a'H = aH$. Näin ollen $f(a'N) = a'H = aH = f(aN)$.

Kuvaus f on selvästi surjektio ja

$$f(aN * bN) = f((a * b)N) = (a * b)H = aH * bH = f(aN) * f(bN),$$

joten f on homomorfismi. Nyt $aH = H$ jos ja vain jos $a \in H$, joten $\mathrm{Ker}(f) = H/N$ eli $H/N \trianglelefteq G/N$. Koska f on surjektio, niin $\mathrm{Im}(f) = G/H$. Homomorfismien peruslauseen 2.55 nojalla nyt

$$(G/N)/(H/N) \cong G/H.$$

□

Huomautus 2.57. Homomorfismien peruslause tunnetaan myös nimellä 1. isomorfialause, ja lisäksi on olemassa tulos, joka tunnetaan nimellä 2. isomorfialause. Tästä johtuen Lause 2.56 on nimetty edeltävällä tavalla.

Lause 2.58 (Korrespondenssilause)**.** *Olkoot G ryhmä, $N \trianglelefteq G$ ja $\pi\colon G \to G/N$ luonnollinen homomorfismi. Tällöin*

$$\Phi\colon Sub(G; N) \to Sub(G/N),\ S \mapsto \pi(S) = S/N$$

on bijektio ryhmän G kaikkien aliryhmän N sisältävien aliryhmien S joukon $Sub(G; N)$ ja tekijäryhmän G/N kaikkien aliryhmien joukon $Sub(G/N)$ välillä.

Lisäksi, kun $S, T \in Sub(G; N)$ ja merkitään $S/N = S^*$ ja $T/N = T^*$, niin

$$T \leq S \leq G \;\Leftrightarrow\; T^* \leq S^*$$

ja

$$T \trianglelefteq S \;\Leftrightarrow\; T^* \trianglelefteq S^*, \text{ jolloin } S/T \cong S^*/T^*.$$

Todistus. Koska $N \trianglelefteq G$ ja $N \leq S$, niin $N \trianglelefteq S$. Kuvaus Φ kuvaa siis nyt normaalin aliryhmän N sisältävän aliryhmän S tekijäryhmäksi S/N. On helppo nähdä, että $S/N \leq G/N$: Jos $sN, tN \in S/N$, niin myös $(sN)(tN)^{-1} = (sN)(t^{-1}N) = st^{-1}N \in S/N$ kaikilla $s, t \in S$, sillä S on ryhmän G aliryhmä.

Osoitetaan, että Φ on injektio. Osoitetaan ensin, että $\pi^{-1}(\pi(S)) = S$. Lauseen 1.7 mukaan $S \subseteq \pi^{-1}(\pi(S))$. Olkoon sitten $a \in \pi^{-1}(\pi(S))$ eli $\pi(a) = \pi(s)$ jollain $s \in S$. Tällöin

$$\pi(as^{-1}) = \pi(a)\pi(s^{-1}) = \pi(s)\pi(s^{-1}) = \pi(ss^{-1}) = \pi(e) = N,$$

joten $as^{-1} \in \mathrm{Ker}(\pi) = N$ eli $as^{-1} = n$ jollain $n \in N$. Kuitenkin $N \leq S$, joten $a = ns \in S$ eli $\pi^{-1}(\pi(S)) \subseteq S$. Näin ollen $\pi^{-1}(\pi(S)) = S$. Nyt jos $\pi(S) = \pi(S')$, niin $\pi^{-1}(\pi(S)) = \pi^{-1}(\pi(S'))$, jolloin edellisen perusteella $S = S'$. Näin ollen Φ on injektio.

Osoitetaan sitten, että Φ on surjektio. Olkoon nyt $U \leq G/N$. Lauseen 2.48 perusteella $\pi^{-1}(U)$ on ryhmän G aliryhmä ja se sisältää myös aliryhmän N, sillä neutraalialkiona $N \in U$, joten $N = \mathrm{Ker}(\pi) = \pi^{-1}(\{N\}) \subseteq \pi^{-1}(U)$. Lauseen 1.7 mukaan nyt $\pi(\pi^{-1}(U)) = U$, joten Φ on surjektio. Kuvaus Φ on siis bijektio.

Merkitään nyt $T/N = T^*$ ja vastaavasti $S/N = S^*$. Jos $T \leq S \leq G$, niin Lauseen 1.7 kohdan 1. nojalla $T^* = \pi(T) \subseteq \pi(S) = S^*$. Näin ollen $T^* \leq S^*$. Jos taas $T^* \leq S^*$ ja $t \in T$, niin $tN \in T^* \leq S^*$. Siten $tN = sN$ jollakin $s \in S$ ja $t = sn$ jollakin $n \in N \leq S$ ja näin ollen $t \in S$. Siispä $T \leq S$ ja näin ollen

$$T \leq S \leq G \;\Leftrightarrow\; T^* \leq S^*.$$

Jos $T \trianglelefteq S$, niin 3. isomorfialauseen 2.56 nojalla $T^* \trianglelefteq S^*$ ja $S^*/T^* \cong S/T$. Tulee vielä osoittaa, että jos $T^* \trianglelefteq S^*$, niin $T \trianglelefteq S$. Olkoot $s \in S$ ja $t \in T$.

Nyt

$$\pi(sts^{-1}) = \pi(s)\pi(t)\pi(s)^{-1} \in \pi(s)T^*\pi(s)^{-1} = T^*,$$

missä viimeinen yhtäsuuruus seuraa oletuksesta $T^* \trianglelefteq S^*$. Nyt siis $sts^{-1} \in \pi^{-1}(T^*)$ ja koska Φ on bijektio, niin $\pi^{-1}(T^*) = T$ ja täten siis $sts^{-1} \in T$ eli $T \trianglelefteq S$.

□

Lemma 2.59. *Jos alkuluku p jakaa äärellisen Abelin ryhmän G kertaluvun, niin ryhmässä G on kertalukua p oleva alkio.*

Todistus. Todistetaan väite induktiolla kertaluvun $|G|$ suhteen. Tapaus $|G| = p$ on selvä, sillä Lauseen 2.25 nojalla ryhmän alkion kertaluku jakaa ryhmän kertaluvun, jolloin jokaisen neutraalialkiosta poikkeavan alkion kertaluvun täytyy olla p. Oletetaan sitten, että väite pätee kaikilla kertaluvuilla, jotka ovat pienempiä kuin jokin $n \in \mathbb{Z}_+$. Olkoon nyt $|G| = n$.

Tarkastellaan nyt alkiota $a \in G$, jonka kertaluku on jokin $k > 1$. Jos $p \mid k$ eli $k = qp$, niin tällöin Lauseen 2.9 perusteella alkion a^q kertaluku on p ja väite on osoitettu. Jos $p \nmid k$, niin tarkastellaan syklistä aliryhmää $H = \langle a \rangle$. Nyt G on Abelin ryhmä, joten $H \trianglelefteq G$ ja siten tekijäryhmä G/H on olemassa. Nyt $|G/H| = n/k < n = |G|$ ja toisaalta siis $n = k|G/H|$. Koska p jakaa kertaluvun $|G| = n$ ja p ei jaa lukua k, niin sen on Eukleideen lemman 1.22 nojalla jaettava kertaluku $|G/H|$. Täten siis $|G/H| < |G|$ ja p jakaa kertaluvun $|G/H|$, joten induktio-oletuksen nojalla tekijäryhmässä G/H on alkio bH, jonka kertaluku on p. Alkio bH saadaan alkiosta $b \in G$ luonnollisella homomorfismilla eli $bH = \pi(b)$. Täten Lauseen 2.49 perusteella $p \mid \operatorname{ord} b$ ja kuten edellä, löydetään kertalukua p oleva alkio.

□

3 Ryhmän toiminta joukossa

Ryhmän G toiminta joukossa X on eräänlainen ryhmän G ja joukon X alkioiden välinen operaatio, joka tuottaa joukon X alkion. Tässä luvussa esitellään olennaisimmat ryhmän toimintaan liittyvät käsitteet ja todistetaan näihin liittyviä tuloksia. Luvun loppupuolella esitetään todistus Cauchyn lauseelle ja lisäksi todistetaan p-ryhmiin liittyviä tuloksia. Luvussa esitetyt todistukset mukailevat lähteessä [5] esitettyjä todistuksia.

3.1 Toiminta, rata ja vakauttaja

Määritelmä 3.1. Olkoon X joukko ja G ryhmä. Tällöin ryhmä G *toimii joukossa* X, mikäli on olemassa kuvaus $f\colon G \times X \to X$, jolle pätee

(1) $f(gh, x) = f(g, f(h, x))$ kaikilla $g, h \in G$ ja $x \in X$.

(2) $f(e, x) = x$ kaikilla $x \in X$, kun e on ryhmän G neutraalialkio.

Jos ryhmä G toimii joukossa X, niin joukkoa X sanotaan *G-joukoksi*. Kuvausta f kutsutaan *vasemmanpuoleiseksi ryhmän toiminnaksi*.

Huomautus 3.2. Merkitään jatkossa yksinkertaisemmin $f(g, x) = gx$.

Lause 3.3. *Ryhmä G toimii itsellään konjugaatiolla.*

Todistus. Tulee osoittaa, että konjugaatio $\gamma_g\colon G \to G, \gamma_g(x) = gxg^{-1}$ toteuttaa Määritelmän 3.1 ehdot. Nyt

$$\begin{aligned}\gamma_{gh}(x) &= (gh)x(gh)^{-1} \\ &= (gh)x(h^{-1}g^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= g(\gamma_h(x))g^{-1} \\ &= \gamma_g(\gamma_h(x)),\end{aligned}$$

joten konjugaatio täyttää ensimmäisen ehdon. Konjugaatio täyttää myös toisen ehdon, sillä $\gamma_e(x) = exe^{-1} = x$ kaikilla $x \in G$.

□

Lause 3.4. *Ryhmä G toimii konjugaatiolla joukossa $\mathrm{Sub}(G)$, joka koostuu kaikista ryhmän G aliryhmistä.*

Todistus. Olkoon $H \in \mathrm{Sub}(G)$ ja $a \in G$. Nyt aliryhmä H kuvautuu konjugaatiksi aHa^{-1}, joka on Lauseen 2.31 nojalla myös ryhmän G aliryhmä. Määritelmän 3.1 ehtojen toteutumisen osoittaminen on täysin vastaava kuin edellisen lauseen todistuksessa.

□

Määritelmä 3.5. Jos ryhmä G toimii joukossa X ja $x \in X$, niin alkion x *rata* (*orbit*) on joukon X osajoukko

$$\mathcal{O}(x) = \{y \in X \mid y = gx \text{ jollain } g \in G\}$$

ja alkion x *vakauttaja* (*stabilizer*) on joukko

$$G_x = \{g \in G \mid gx = x\}.$$

Määritelmä 3.6. Kun ryhmä G toimii itsellään konjugaatiolla, niin alkion x rataa $x^G = \{y \in G \mid y = gxg^{-1} \text{ jollain } g \in G\}$ kutsutaan *konjugointiluokaksi*. Konjugointiluokka x^G koostuu siis kaikista alkion x konjugaateista. Tällöin alkion x vakauttajaa $C_G(x) = \{g \in G \mid gxg^{-1} = x\}$ kutsutaan alkion x *keskittäjäksi* (*centralizer*).

Huomautus 3.7. Kun ryhmä G toimii joukossa $\mathrm{Sub}(G)$ konjugaatiolla, niin aliryhmän H rata koostuu sen kaikista konjugaateista ja vakauttaja on jo aiemmin määritelty aliryhmän H normalisoija $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. Aliryhmän H normalisoija $N_G(H)$ osoitettiin ryhmän G aliryhmäksi alaluvussa 2.2. Seuraava lause näyttää, että joukon X alkion x vakauttaja on yleisemminkin aina ryhmän G aliryhmä.

Lause 3.8. *Jos ryhmä G toimii joukossa X, niin alkion $x \in X$ vakauttaja G_x on ryhmän G aliryhmä.*

Todistus. Nyt $G_x \neq \emptyset$, sillä $e \in G_x$. Olkoot $g, h \in G_x$. Tällöin

$$(hg^{-1})x = h(g^{-1}x) = h(g^{-1}(gx)) = h((g^{-1}g)x) = hx = x,$$

joten $hg^{-1} \in G_x$ eli $G_x \leq G$. □

Seuraus 3.9. *Alkion $x \in G$ keskittäjä $C_G(x)$ on ryhmän G aliryhmä.*

Todistus. Seuraa suoraan edellisestä lauseesta, sillä keskittäjä on vakauttaja. □

Lause 3.10. *Toimikoon ryhmä G joukossa X. Määritellään joukossa X relaatio $x \sim y$, jos on olemassa $g \in G$ siten, että $y = gx$. Tällöin relaatio $\sim$ on ekvivalenssirelaatio, jonka ekvivalenssiluokat ovat alkioiden $x \in X$ radat.*

Todistus. Osoitetaan, että relaatio $\sim$ toteuttaa Määritelmän 1.8 ehdot.

1. Relaatio $\sim$ on refleksiivinen, sillä $x = ex$ kaikilla $x \in X$.
2. Jos $x, y \in X$ ja $x \sim y$, niin $y = gx$ jollain $g \in G$. Tällöin

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

joten $y \sim x$ eli relaatio on symmetrinen.

3. Jos $x, y, z \in X$, $x \sim y$ ja $y \sim z$, niin $y = g_1x$ ja $z = g_2y$ joillain $g_1, g_2 \in G$. Nyt

$$z = g_2y = g_2(g_1x) = (g_2g_1)x,$$

joten $x \sim z$ eli relaatio on transitiivinen.

Näin ollen relaatio $\sim$ on ekvivalenssirelaatio. Jos $a \in [x]$, niin $x \sim a$ eli $a = gx$ jollain $g \in G$ eli $a \in \mathcal{O}(x)$. Jos $a \in \mathcal{O}(x)$, niin $a = g'x$ jollain $g' \in G$ eli $x \sim a$, joten $a \in [x]$. Näin ollen ekvivalenssiluokat ovat alkioiden $x \in X$ radat.

□

Lause 3.11. *Jos ryhmä G toimii joukossa X, niin joukon alkioiden x radat muodostavat osituksen joukolle X. Jos X on äärellinen, niin*

$$|X| = \sum_i |\mathcal{O}(x_i)|,$$

missä on valittu aina yksi alkio x_i kultakin radalta.

Todistus. Lauseessa 3.10 osoitettiin, että relaatio $x \sim y$, mikäli $y = gx$ jollain $g \in G$, on ekvivalenssirelaatio, jonka ekvivalenssiluokat ovat radat $\mathcal{O}(x)$.

Lauseen 1.12 nojalla ekvivalenssiluokat muodostavat aina osituksen, joten radat muodostavat osituksen joukolle X. Edellisen perusteella joukko X saadaan yhdisteenä radoista, jotka ovat pareittain erilliset. Täten, jos joukko X on äärellinen, niin laskettaessa summaa $\sum_i |\mathcal{O}(x_i)|$ yhtäkään joukon X alkiota ei lasketa kahdesti. Näin ollen $|X| = \sum_i |\mathcal{O}(x_i)|$.

□

Lause 3.12 (Rata-vakauttajalause)**.** *Jos äärellinen ryhmä G toimii joukossa X ja $x \in X$, niin tällöin alkion x radan kertaluku on alkion x vakauttajan indeksi eli*

$$|\mathcal{O}(x)| = [G : G_x].$$

Todistus. Merkitään vakauttajan G_x vasempien sivuluokkien joukkoa G/G_x. Nyt siis $|G/G_x| = [G : G_x]$. Määritellään kuvaus $\varphi\colon G/G_x \to \mathcal{O}(x)$ siten, että $\varphi(gG_x) = gx$. Kuvaus φ on hyvin määritelty: jos $gG_x = hG_x$, niin $h = gf$ jollain $f \in G_x$, sillä $e \in G_x$, joten $h \in hG_x = gG_x$. Nyt siis $hx = (gf)x = g(fx) = gx$ eli $\varphi(hG_x) = \varphi(gG_x)$, joten φ on hyvin määritelty.

Kuvaus φ on injektio, sillä jos $gx = \varphi(gG_x) = \varphi(hG_x) = hx$, niin

$$(h^{-1}g)x = h^{-1}(gx) = h^{-1}(hx) = (h^{-1}h)x = x$$

eli $h^{-1}g \in G_x$ ja näin ollen $h^{-1}gG_x = G_x$ eli $gG_x = hG_x$. Kuvaus φ on myös surjektio, sillä jos $a \in \mathcal{O}(x)$, niin $a = gx$ jollain $g \in G$ ja siten $a = \varphi(gG_x)$. Kuvaus φ on siis bijektio, joten $|\mathcal{O}(x)| = |G/G_x| = [G : G_x]$.

□

Seuraus 3.13. *Äärellisen ryhmän G alkion x konjugaattien lukumäärä on alkion x keskittäjän indeksi eli*

$$\left|x^G\right| = [G : C_G(x)].$$

Lisäksi äärellisen ryhmän G aliryhmän H konjugaattien lukumäärä on sen normalisoijan indeksi $[G : N_G(H)]$.

Todistus. Väitteet seuraavat suoraan Rata-vakauttajalauseesta 3.12.
Alkion tapauksessa $\mathcal{O}(x) = x^G$ ja $G_x = C_G(x)$, joten $\left|x^G\right| = [G : C_G(x)]$.

Aliryhmän tapauksessa rata $\mathcal{O}(H)$ koostuu kaikista aliryhmän H konjugaateista ja vakauttaja $G_H = N_G(H)$. □

Lause 3.14. *Ryhmän G kertaluku voidaan esittää muodossa*

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

missä on valittu yksi alkio x_i kustakin konjugointiluokasta, jossa on enemmän kuin yksi alkio.

Todistus. Tuloksien 3.11, 3.12 ja 3.13 perusteella ryhmän G kertaluku voidaan esittää summana $|G| = \sum_k [G : C_G(x_k)]$, missä on valittu yksi alkio x_k kustakin konjugointiluokasta. Summa voidaan edelleen kirjoittaa muodossa

$$\sum_k [G : C_G(x_k)] = \sum_j [G : C_G(x_j)] + \sum_i [G : C_G(x_i)],$$

missä on valittu yksi alkio x_j kustakin vain yhden alkion sisältävästä konjugointiluokasta ja yksi alkio x_i kustakin useamman kuin yhden alkion sisältävästä konjugointiluokasta. Lauseen 2.38 perusteella kaikilla ryhmän keskukseen $Z(G)$ kuuluvilla alkioilla x pätee $[G : C_G(x)] = 1$. Täten $\sum_j [G : C_G(x_j)] = |Z(G)|$ ja näin ollen edellinen summa saa muodon

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

missä on valittu yksi alkio x_i kustakin konjugointiluokasta, jossa on enemmän kuin yksi alkio.

□

Määritelmä 3.15. Äärellisen ryhmän G kertaluvun esitystä muodossa

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

missä on valittu yksi alkio x_i kustakin useamman kuin yhden alkion sisältävästä konjugointiluokasta, kutsutaan ryhmän G *luokkayhtälöksi*.

3.2 Cauchyn lause ja p-ryhmä

Lause 3.16 (Cauchyn lause)**.** *Jos äärellisen ryhmän G kertaluku on jaollinen alkuluvulla p, niin tällöin ryhmässä G on kertalukua p oleva alkio.*

Todistus. Perusaskel $|G| = p$ on selvä, sillä Lauseen 2.25 nojalla ryhmän alkion kertaluku jakaa aina ryhmän kertaluvun. Neutraalialkio on ainoa alkio, jonka kertaluku on 1, joten jokaisen neutraalialkiosta poikkeavan alkion kertaluku on p.

Tehdään nyt induktio-oletus, että väite pätee kaikille sellaisille kertaluvuille n, joille $n < |G|$ ja $p \mid n$ ja osoitetaan, että väite pätee myös kertaluvulla $|G|$. Lemma 2.59 osoittaa väitteen kaikille äärellisille Abelin ryhmille, joten riittää osoittaa, että väite pätee kaikille äärellisille ryhmille, jotka eivät ole Abelin ryhmiä.

Voidaan siis nyt olettaa, että G ei ole Abelin ryhmä. Tällöin on olemassa ainakin yksi alkio x, joka ei kuulu keskukseen $Z(G)$. Näin ollen Lauseen 2.38 perusteella konjugointiluokassa x^G on enemmän kuin yksi alkio eli $|x^G| = [G : C_G(x)] \neq 1$. Nyt G on äärellinen ryhmä, joten

$$[G : C_G(x)] = \frac{|G|}{|C_G(x)|} \neq 1,$$

eli $|C_G(x)| \neq |G|$. Täten $|C_G(x)| < |G|$.

Jos p jakaa kertaluvun $|C_G(x)|$ jollain alkiolla $x \notin Z(G)$, niin induktio-oletuksen nojalla keskittäjässä $C_G(x) < G$ on alkio, jonka kertaluku on p, ja väite on osoitettu.

Oletetaan sitten, että p ei jaa kertalukua $|C_G(x)|$ millään $x \notin Z(G)$. Nyt $|G| = [G : C_G(x)] \cdot |C_G(x)|$. Täten jos p jakaa ryhmän kertaluvun $|G|$ ja ei jaa keskittäjän kertalukua $|C_G(x)|$, niin Eukleideen lemman 1.22 nojalla alkuluku p jakaa indeksin $[G : C_G(x)]$ kaikilla $x \notin Z(G)$. Koska alkuluku p jakaa oletuksen mukaan kertaluvun $|G|$ ja edellisen perusteella kaikki indeksit $[G : C_G(x)]$ alkioilla $x \notin Z(G)$, niin ryhmän G luokkayhtälöstä nähdään, että alkuluvun p on jaettava myös keskuksen kertaluku $|Z(G)|$. Keskus $Z(G)$ on Abelin ryhmä, joten Lemman 2.59 nojalla keskuksessa $Z(G)$ on alkio, jonka kertaluku on p. Näin ollen ryhmässä G on kertalukua p oleva alkio.

□

Huomautus 3.17. Jos alkuluku p jakaa äärellisen ryhmän G kertaluvun, niin Cauchyn lauseen nojalla ryhmällä G on myös kertalukua p oleva aliryhmä; kertalukua p olevan alkion generoima syklinen ryhmä.

Määritelmä 3.18. Olkoon p alkuluku ja G ryhmä. Jos ryhmän G alkioiden kertaluvut ovat luvun p ei-negatiivisia potensseja, niin ryhmää G kutsutaan *p-ryhmäksi*. Vastaavasti jos aliryhmän $S \leq G$ alkioiden kertaluvut ovat alkuluvun p ei-negatiivisia potensseja, niin aliryhmää S kutsutaan *p-aliryhmäksi*.

Huomautus 3.19. Triviaali aliryhmä $\{e\} \leq G$ on p-aliryhmä, sillä neutraalialkion e kertaluku on $1 = p^0$. Näin ollen jokaisella ryhmällä G on aina olemassa p-aliryhmä.

Lause 3.20. *Äärellinen ryhmä on p-ryhmä jos ja vain jos ryhmän kertaluku on alkuluvun p potenssi.*

Todistus. Olkoon G p-ryhmä ja sen alkion a kertaluku p^j jollain $j \geq 0$. Lauseen 2.25 nojalla alkion a kertaluku jakaa ryhmän G kertaluvun eli $|G| = np^j$ jollain $n \in \mathbb{Z}_+$. Jos luku n ei ole alkuluvun p potenssi, niin luvun n alkulukuhajotelmassa on jokin alkuluvun $q \neq p$ potenssi. Tällöin alkuluku q jakaa ryhmän kertaluvun $|G|$, jolloin Cauchyn lauseen 3.16 nojalla ryhmässä G on alkio, jonka kertaluku on q. Tämä on ristiriita, sillä p-ryhmän G jokaisen alkion kertaluku on jokin alkuluvun p potenssi. Näin ollen luvun n täytyy olla alkuluvun p potenssi, jolloin myös ryhmän G kertaluku on alkuluvun p potenssi.

Jos äärellisen ryhmän G kertaluku on alkuluvun p potenssi, niin Lauseen 2.25 nojalla jokaisen alkion $a \in G$ kertaluku on väistämättä alkuluvun p potenssi. Näin ollen G on p-ryhmä.

□

Lause 3.21. *Olkoon p alkuluku ja $G \neq \{e\}$ p-ryhmä. Tällöin $Z(G) \neq \{e\}$.*

Todistus. Ryhmän G kertaluku on nyt siis p^n jollain $n > 0$. Kuten Cauchyn lauseen todistuksessa nähtiin, niin kaikilla alkioilla $x \notin Z(G)$ keskittäjä $C_G(x)$ on ryhmän G aito aliryhmä eli $|C_G(x)| \neq |G|$. Nyt $|G| = [G : C_G(x)]|C_G(x)|$ eli indeksi $[G : C_G(x)]$ jakaa ryhmän G kertaluvun. Indeksi $[G : C_G(x)]$ on siten jokin alkuluvun p aito potenssi eli alkuluku p jakaa indeksin kaikilla $x \notin Z(G)$. Ryhmän G luokkayhtälö on

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)], \quad x_i \notin Z(G).$$

Alkuluku p jakaa ryhmän G kertaluvun ja kaikki luokkayhtälössä esiintyvät indeksit, joten alkuluvun p on jaettava myös keskuksen $Z(G)$ kertaluku. Näin ollen keskuksessa on vähintään p alkiota eli $Z(G) \neq \{e\}$.

□

Lause 3.22. *Olkoon p alkuluku ja G p-ryhmä, jonka kertaluku on $|G| = p^n$ jollain $n \geq 0$. Tällöin ryhmällä G on kaikilla $k \leq n$ normaali aliryhmä, jonka kertaluku on p^k .*

Todistus. Väite pätee, jos $n = 0$, sillä tällöin $G = \{e\}$. Kun $k = 0$ ja $n > 0$ mielivaltainen, niin kysytty aliryhmä on $\{e\}$, joten väite pätee myös tällöin.

Voidaan siis olettaa, että $n \geq k \geq 1$. Todistetaan väite induktiolla eksponentin $n \geq 1$ suhteen. Perusaskel $n = 1$ on tosi, sillä nyt $k = 1$, jolloin $|G| = p^1 = p$. Ainoa mahdollinen aliryhmä on tällöin ryhmä G itse. Ryhmä on aina itsensä normaali aliryhmä, sillä $aG = G = Ga$ kaikilla $a \in G$.

Oletetaan nyt, että väite pätee kaikille ryhmille, joiden kertaluvut ovat alkuluvun p potensseja, mutta ovat pienempiä kuin p^n. Osoitetaan, että väite pätee, kun ryhmän kertaluku on p^n. Olkoon nyt siis $|G| = p^n$

Lauseen 3.21 perusteella $Z(G) \neq \{e\}$. Olkoon $Z \leq Z(G)$ aliryhmä, jonka kertaluku on p. Tällainen aliryhmä Z on aina olemassa Cauchyn lauseen nojalla. Keskus $Z(G)$ on Lauseen 2.36 nojalla aina ryhmän G normaali aliryhmä. Näin ollen myös aliryhmä Z on ryhmän G normaali aliryhmä ja siten tekijäryhmä G/Z on olemassa.

Jos nyt $1 \leq k \leq n$, niin myös

$$1 \leq p^{k-1} \leq p^{n-1} = \frac{p^n}{p} = |G/Z|.$$

Induktio-oletuksen perusteella tekijäryhmällä G/Z on normaali aliryhmä N^*, jonka kertaluku on p^{k-1}. Nyt Korrespondenssilauseen 2.58 nojalla ryhmällä G on aliryhmä N, joka sisältää normaalin aliryhmän Z, siten, että $N^* = N/Z$. Nyt

$$p^{k-1} = |N^*| = |N/Z| = \frac{|N|}{|Z|} = \frac{|N|}{p},$$

joten $|N| = p^k$. Lisäksi Korrespondenssilauseen perusteella $N \trianglelefteq G$, sillä $N^* \trianglelefteq G/Z$.

□

4 Sylowin lauseet

Ludvig Sylow esitti ja todisti vuonna 1872 artikkelissaan *Théorémes sur les groupes de substitutions* tulokset, jotka tunnetaan nykyään Sylowin lauseina. Joskus puhutaan myös pelkästään Sylowin lauseesta, jolloin tulosten sisältö on sisällytetty yhdeksi lauseeksi. Tätä nimitystä on käytetty esimerkiksi lähdeteoksessa [2]. Lauseet koskevat äärellisen ryhmän maksimaalisia p-aliryhmiä, joita kutsutaan Sylowin p-aliryhmiksi. Maksimaalisuudella tarkoitetaan, että Sylowin p-aliryhmä on suurin mahdollinen p-aliryhmä inkluusion ($\subseteq$) suhteen. Sylowin p-aliryhmä ei siis voi olla minkään p-aliryhmän aito aliryhmä.

Lauseiden pääsisältö on seuraava:

- Jokaisella äärellisellä ryhmällä on olemassa Sylowin p-aliryhmä.
- Sylowin p-aliryhmät ovat toistensa konjugaatteja.
- Sylowin p-aliryhmien lukumäärä on $1 + lp,\ l \in \mathbb{Z}_+$.
- Jos p^n on suurin alkuluvun p potenssi, joka jakaa äärellisen ryhmän kertaluvun, niin tällöin Sylowin p-aliryhmän kertaluku on p^n.

Tulokset ovat hyvin erityislaatuisia siksi, että ne antavat tietoa äärellisen ryhmän aliryhmistä pelkän ryhmän kertaluvun perusteella. Lagrangen lause kertoo itsessään aliryhmien olemassaolon kannalta vain, millaista kertalukua olevia aliryhmiä ei voi olla olemassa. Sylowin lauseet kertovat kuitenkin suoraan maksimaalisten p-aliryhmien olemassaolosta, niiden lukumäärästä ja yhteydestä toisiinsa. Seuraavat todistukset Sylowin lauseille mukailevat lähdeteoksessa [5] esitettyjä todistuksia.

4.1 Lauseiden todistaminen

Määritelmä 4.1. Olkoon p alkuluku ja G äärellinen ryhmä. Tällöin ryhmän G maksimaalista p-aliryhmää P sanotaan *Sylowin p-aliryhmäksi*. Maksimaalisuus tarkoittaa, että jos Q on ryhmän G p-aliryhmä ja $P \leq Q$, niin $Q = P$.

Lause 4.2 (Sylow)**.** *Äärellisellä ryhmällä G on aina olemassa Sylowin p-aliryhmä.*

Todistus. Olkoon S ryhmän G p-aliryhmä. Todettakoon, että p-aliryhmä S on aina olemassa, sillä $\{e\} \leq G$ on p-aliryhmä. Jos ei ole olemassa p-aliryhmää P, jolla $S < P$, niin tällöin S on maksimaalinen eli S on Sylowin p-aliryhmä. Muulloin on olemassa p-aliryhmä P_1, jolla $S < P_1$. Jos P_1 on maksimaalinen, niin tällöin P_1 on Sylowin p-aliryhmä. Jos P_1 ei ole maksimaalinen, niin on olemassa p-aliryhmä P_2, jolla $P_1 < P_2$. Tätä prosessia jatkamalla päädytään aina lopulta maksimaaliseen p-aliryhmään, sillä G on äärellinen ja $|P_i| \leq |G|$ kaikilla i. Suurimman kertaluvun omaavan p-aliryhmän P_i on näin ollen oltava Sylowin p-aliryhmä.

□

Lemma 4.3. *Olkoon P äärellisen ryhmän G Sylowin p-aliryhmä.*
Tällöin

1. *Jokainen aliryhmän P konjugaatti on Sylowin p-aliryhmä.*
2. *$|N_G(P)/P|$ on jaoton luvulla p.*
3. *Jos alkion $a \in G$ kertaluku on jokin alkuluvun p potenssi ja $aPa^{-1} = P$, niin $a \in P$.*

Todistus. 1. Olkoon $a \in G$. Nyt jokaisen alkion $b \in P$ kertaluku on jokin alkuluvun p potenssi, sillä P on p-aliryhmä. Lauseen 2.52 mukaan myös jokaisen konjugaatin $aba^{-1} \in aPa^{-1}$ kertaluku on alkuluvun p potenssi. Näin ollen aPa^{-1} on p-aliryhmä. Jos aPa^{-1} ei ole maksimaalinen p-aliryhmä, niin on olemassa sellainen p-aliryhmä Q, jolla $aPa^{-1} < Q$. Täten siis myös $P < a^{-1}Qa$, mikä on mahdotonta, sillä P oli maksimaalinen p-aliryhmä. Näin ollen aPa^{-1} on maksimaalinen p-aliryhmä ja siten Sylowin p-aliryhmä.

2. Lause 2.33 osoittaa, että $P \trianglelefteq N_G(P)$, joten tekijäryhmä $N_G(P)/P$ on olemassa. Jos p jakaa kertaluvun $|N_G(P)/P|$, niin Cauchyn lauseen 3.16 nojalla tekijäryhmässä $N_G(P)/P$ on alkio aP, jonka kertaluku on p. Näin ollen tekijäryhmä $N_G(P)/P$ sisältää kertalukua p olevan syklisen aliryhmän

$S^* = \langle aP \rangle$. Nyt Korrespondenssilauseen 2.58 mukaan on olemassa aliryhmä S, jolla $P \leq S \leq N_G(P)$ ja $S/P \cong S^*$. Nyt siis $|S^*| = p = |S/P|$. Olkoon nyt p-aliryhmän P kertaluku p^k. Koska G on äärellinen, niin $|S| = |S/P|\,|P| = p \cdot p^k = p^{k+1}$. Näin ollen $S \leq N_G(P)$ on p-aliryhmä, jonka kertaluku on suurempi kuin Sylowin p-aliryhmän P kertaluku eli $P < S$. Tämä on ristiriidassa aliryhmän P maksimaalisuuden kanssa, joten täytyy olla, että luku p ei jaa kertalukua $|N_G(P)/P|$.

3. Määritelmän 2.32 mukaan $a \in N_G(P)$. Oletetaan, että alkio a ei kuuluisi aliryhmään P. Tällöin Lauseen 2.16 nojalla $aP \neq P$. Nyt $aP = \pi(a)$, joten Lauseen 2.49 nojalla ord $aP \mid$ ord a, joka on alkuluvun p potenssi. Alkion aP kertaluku ei voi olla 1, sillä $aP \neq P$, joten kertaluvun on oltava alkuluvun p aito potenssi. Alkio aP on siis tekijäryhmän $N_G(P)/P$ alkio, jonka kertaluku on alkuluvun p potenssi. Lauseen 2.25 perusteella äärellisen ryhmän alkion kertaluku jakaa aina ryhmän kertaluvun, joten alkion aP kertaluku jakaa tekijäryhmän $N_G(P)/P$ kertaluvun. Koska luvun p potenssi jakaa kertaluvun $|N_G(P)/P|$, niin myös p jakaa tämän, mikä on mahdotonta edellisen kohdan nojalla. Täytyy siis olla $a \in P$.

□

Lemma 4.4. *Olkoon P Sylowin p-aliryhmä ryhmässä G ja X joukko kaikista Sylowin p-aliryhmän P toisistaan eroavista konjugaateista. Tällöin mikä tahansa ryhmän G aliryhmä Q toimii joukossa X konjugaatiolla.*

Todistus. Olkoon Q mikä tahansa ryhmän G aliryhmä. Määritelmän 3.1 kohdat (1) ja (2) osoittaa täysin vastaava tarkastelu kuin Lauseessa 3.3, joten riittää osoittaa, että konjugaatiolla kuvattaessa kuva-alkiot ovat joukon X alkioita. Sylowin p-aliryhmän P konjugaattien joukon X alkiot ovat muotoa $gPg^{-1},\ g \in G$. Kun $a \in Q$, niin konjugaatti gPg^{-1} kuvautuu konjugaatiolla alkioksi

$$\gamma_a(gPg^{-1}) = a(gPg^{-1})a^{-1} = (ag)P(g^{-1}a^{-1}) = (ag)P(ag)^{-1},$$

joka kuuluu edelleen joukkoon X, sillä $ag \in G$. Näin ollen aliryhmä Q toimii joukossa X. □

Lause 4.5 (Sylow). *Olkoon G äärellinen ryhmä, jonka kertaluvun alkulukuhajotelma on $p_1^{n_1} \cdots p_t^{n_t}$ ja P ryhmän G Sylowin p-aliryhmä jollekin alkuluvulle $p = p_j$. Tällöin*

1. *Jokainen Sylowin p-aliryhmä on aliryhmän P konjugaatti.*
2. *Jos Sylowin p_j-aliryhmien lukumäärä on r_j, niin $r_j \equiv 1 \bmod p_j$ ja r_j jakaa luvun $|G|/p_j^{n_j}$.*

Todistus. Olkoon $X = \{P_1, \ldots, P_{|X|}\}$ joukko kaikista Sylowin p-aliryhmän P toisistaan eroavista konjugaateista, missä on merkitty $P = P_1$. Olkoon Q mikä tahansa Sylowin p-aliryhmä ryhmässä G. Tällöin Q toimii joukossa X konjugaatiolla Lemman 4.4 nojalla. Nyt jokaisen alkion $P_i \in X$ radan kertaluku jakaa aliryhmän Q kertaluvun Rata-vakauttajalauseen 3.12 perusteella: $|\mathcal{O}(P_i)| = [Q : Q_{P_i}]$ eli $|Q| = |\mathcal{O}(P_i)|\,|Q_{P_i}|$, missä Q_{P_i} on konjugaatin P_i vakauttaja. Koska Q on p-aliryhmä, niin jokaisen radan kertaluku täytyy olla jokin alkuluvun p potenssi.

Jos on olemassa alkio $P_i \in X$, jolle $aP_ia^{-1} = P_i$ kaikilla $a \in Q$, niin alkion P_i radan kertaluku on 1. Lemman 4.3 perusteella nyt $a \in P_i$ kaikilla $a \in Q$ ja siten $Q \leq P_i$. Koska Q on Sylowin p-aliryhmä, niin täytyy olla $Q = P_i$. Alkion P_i rata on tällöin myös ainoa rata, jonka kertaluku on 1. Jos kertalukua 1 olevia ratoja olisi enemmän kuin yksi, niin olisi ainakin kaksi toisistaan poikkeavaa konjugaattia, jotka molemmat ovat Sylowin p-aliryhmä Q, mikä on tietysti mahdotonta. Toisaalta, jos on olemassa rata, jonka kertaluku on 1, niin joukossa X on alkio P_i, jolle $aP_ia^{-1} = P_i$ kaikilla $a \in Q$. Tällöin vastaavasti nähdään, että $Q = P_i$.

Erityisesti $P = P_1$ on Sylowin p-aliryhmä, joten P toimii joukossa X. Nyt $aPa^{-1} = aP = P$ kaikilla $a \in P$. Täten edellisen kappaleen perusteella radan $\mathcal{O}(P)$ kertaluku on 1 ja muita kertalukua 1 olevia ratoja ei ole. Näin ollen muiden ratojen kertaluvut ovat alkuluvun p aitoja potensseja. Merkitään ratoja $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$, missä $\mathcal{O}_1 = \mathcal{O}(P)$. Nyt Lauseen 3.11 perusteella

$$|X| = |\mathcal{O}_1| + |\mathcal{O}_2| + \ldots + |\mathcal{O}_k| = 1 + p \cdot l$$

jollakin $l \in \mathbb{Z}_+$, sillä $|\mathcal{O}_1| = 1$ ja muiden ratojen kertaluvuissa on tekijänä alkuluku p. Täten

$$|X| \equiv 1 \bmod p.$$

Oletetaan sitten, että olisi olemassa Sylowin p-aliryhmä Q, joka ei ole Sylowin p-aliryhmän P konjugaatti eli $Q \neq P_i$ kaikilla i. Aliryhmä Q toimii nyt joukossa X, ja yhdenkään radan kertaluku ei ole 1. Jos jonkin radan kertaluku olisi 1, niin kuten edellä nähtiin $Q = P_i$ jollakin i, mikä on ristiriita, sillä $Q \notin X$. Näin ollen jokaisen radan kertaluku on jokin alkuluvun p aito potenssi, mikä tarkoittaa, että kertaluvun $|X|$ tekijänä on alkuluku p. Tämä tarkoittaa, että $|X| \equiv 0 \bmod p$, mikä on ristiriita, sillä joukon X kertaluvulle täytyy päteä edelleen kongruenssi $|X| \equiv 1 \bmod p$. Täten tällaista aliryhmää Q ei voi olla olemassa, ja kaikki Sylowin p-aliryhmät ovat aliryhmän P konjugaatteja. Näin ollen $|X| = r_j$ ja siten

$$r_j \equiv 1 \bmod p.$$

Kaikki Sylowin p-aliryhmät ovat siis toistensa konjugaatteja, joten $r_j = [G : N_G(P)]$ Seurauksen 3.13 nojalla. Täten r_j jakaa ryhmän G kertaluvun eli $|G| = qr_j$ jollain $q \in \mathbb{Z}_+$. Merkitään nyt $|G|/p_j^{n_j} = m$. Koska $r_j \equiv 1 \bmod p_j$, niin syt $(r_j, p_j) = 1$, sillä p_j on alkuluku. Tällöin myös syt $\left(r_j, p_j^{n_j}\right) = 1$, joten $1 = sp_j^{n_j} + tr_j$ joillain $s, t \in \mathbb{Z}$ ja tästä saadaan

$$m = smp_j^{n_j} + mtr_j = s|G| + mtr_j = sqr_j + mtr_j = (sq + mt)r_j$$

eli

$$r_j \mid m$$

eli

$$r_j \mid |G|/p_j^{n_j}.$$

□

Seuraus 4.6. *Äärellisen ryhmän G Sylowin p-aliryhmä P on yksikäsitteinen jos ja vain jos $P \trianglelefteq G$.*

Todistus. Olkoon P Sylowin p-aliryhmä. Lemman 4.3 nojalla jokainen aliryhmän P konjugaatti on Sylowin p-aliryhmä. Jos P on yksikäsitteinen Sylowin p-aliryhmä, niin täytyy olla, että $aPa^{-1} = P$ kaikilla $a \in G$. Näin ollen P on normaali aliryhmä.

Jos Q on Sylowin p-aliryhmä, niin Lauseen 4.5 nojalla $Q = aPa^{-1}$ jollakin $a \in G$. Jos P on normaali aliryhmä, niin $aPa^{-1} \subseteq P$ eli $Q \leq P$. Koska Q on Sylowin p-aliryhmä ja P on p-aliryhmä, niin $Q = P$.

□

Lause 4.7 (Sylow)**.** *Jos äärellisen ryhmän G kertaluku on $p^n m$, missä p on alkuluku ja p ei jaa lukua m, niin Sylowin p-aliryhmän P kertaluku on p^n.*

Todistus. Sylowin p-aliryhmän P indeksi on $[G : P] = |G|/|P|$. Nyt $|G| = p^n m$, missä $p \nmid m$ ja $|P| = p^k$ jollakin $k \in \mathbb{Z}_+$. Näin ollen $[G : P] = p^n m/p^k = p^{n-k} m$. Jos alkuluku p jakaisi indeksin $[G : P]$, niin sen täytyisi Eukleideen lemman 1.22 nojalla jakaa p^{n-k}. Jos saadaan osoitettua, että p ei jaa indeksiä $[G : P]$, niin tällöin $p^{n-k} = p^0 = 1$ eli $n = k$ eli $|P| = p^n$.

Indeksi $[G : P]$ voidaan esittää muodossa

$$[G : P] = \frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|} \cdot \frac{|N_G(P)|}{|P|} = [G : N_G(P)][N_G(P) : P].$$

Indeksi $[G : N_G(P)]$ on Seurauksen 3.13 nojalla aliryhmän P konjugaattien lukumäärä ja toisaalta jokainen Sylowin p-aliryhmä on jokin näistä konjugaateista. Siten $[G : N_G(P)]$ on Sylowin p-aliryhmien lukumäärä ja Lauseen 4.5 nojalla $[G : N_G(P)] \equiv 1 \bmod p$ eli $p \nmid [G : N_G(P)]$. Lisäksi indeksi $[N_G(P) : P] = |N_G(P)/P|$ on Lemman 4.3 nojalla jaoton alkuluvulla p. Näin ollen molemmat indeksit $[G : N_G(P)]$ ja $[N_G(P) : P]$ ovat jaottomia alkuluvulla p ja siten Eukleideen lemman nojalla p ei jaa indeksiä $[G : P]$. Edeltävän perusteella täytyy siis olla, että $|P| = p^n$.

□

Lagrangen lauseen käänteinen suunta ei ole yleisesti totta. Sylowin lauseiden seurauksena saadaan kuitenkin tulos, joka on osittainen käänteistulos Lagrangen lauseelle:

Seuraus 4.8. *Olkoon G äärellinen ryhmä. Jos p on alkuluku ja p^k jakaa ryhmän G kertaluvun, niin ryhmällä G on olemassa kertalukua p^k oleva aliryhmä.*

Todistus. Jos $|G| = p^n m$, missä p ei jaa lukua m, niin Lauseen 4.7 nojalla ryhmällä G on Sylowin p-aliryhmä, jonka kertaluku on p^n. Nyt jos $p^k \mid |G|$, niin $p^k \mid |P|$, jolloin Lauseen 3.22 nojalla Sylowin p-aliryhmällä P on aliryhmä, jonka kertaluku on p^k.

□

4.2 Vaihtoehtoisia lähestymistapoja

Sylowin aikana ryhmäteoriassa ei käsitelty niinkään nykyisen määritelmän mukaista abstraktia ryhmää vaan tarkastelun kohteena olivat permutaatiot. Sylowin alkuperäisen todistuksen ([6]) ideoita on avattu artikkelissa [1] moderneja käsitteitä käyttäen. Tarkastellaan seuraavaksi lyhyesti Sylowin alkuperäisen todistuksen ideaa Sylowin p-aliryhmien olemassaololle.

Olkoon p^n suurin alkuluvun p potenssi, joka jakaa ryhmän G kertaluvun $|G|$, $P \leq G$ maksimaalista kertalukua oleva p-aliryhmä ja N aliryhmän P normalisoija. Sylow näyttää ensin, että $[N : P]$ ei ole jaollinen alkuluvulla p. Sitten Sylow näyttää, että aliryhmä P sisältää kaikki normalisoijan N alkiot, joiden kertaluvut ovat alkuluvun p potensseja: Jos ϕ on normalisoijan alkio, joka ei ole aliryhmässä P, niin alkiot $\vartheta\phi^i$, missä $\vartheta \in P$ ja $i \in \mathbb{Z}$ muodostavat normalisoijassa aliryhmän, joka sisältää aidosti aliryhmän P. Tämän aliryhmän kertaluku on $|P|m$, missä m on pienin sellainen $j \in \mathbb{Z}_+$, että $\phi^j \in P$. Nyt m jakaa kertaluvun $|\phi|$. Koska P on maksimaalinen p-aliryhmä, niin alkion ϕ kertaluku ei voi olla alkuluvun p potenssi. Sylow näyttää sitten vielä, että alkuluku p ei jaa indeksiä $[G : N]$. Kun tämä

tiedetään, niin nähdään, että $|P| = p^n$ ja näin ollen Sylowin p-aliryhmiä on olemassa.

Sylowin todistuksen idea on olennaisesti samankaltainen kuin Lausessa 4.7. Erona tässä on kuitenkin se, että Sylowin p-aliryhmän määritelmä ei ole täysin sama kuin Määritelmä 4.1, jossa Sylowin p-aliryhmä määriteltiin vain maksimaalisena p-aliryhmänä. Sylow osoittaa, että on olemassa aliryhmä, jonka kertaluku on p^n, kun tämä on suurin ryhmän G kertaluvun jakava alkuluvun p potenssi. Sylowin p-aliryhmä voitaisiinkin määritellä myös toisella tavalla:

Määritelmä 4.9. Olkoon G äärellinen ryhmä, jonka kertaluku on $p^n m$, missä $p \nmid m$. Sylowin p-aliryhmäksi kutsutaan sellaista ryhmän G aliryhmää, jonka kertaluku p^n.

Tämä on yhtäpitävä Määritelmän 4.1 kanssa: Jos tällainen Sylowin p-aliryhmä on olemassa, niin se on varmasti myös maksimaalinen, sillä p-aliryhmän kertaluku ei voi olla suurempi kuin p^n Lagrangen lauseen perusteella. Toisaalta edellä nähtiin, että lähtien Määritelmästä 4.1 saadaan lopulta osoitettua Lause 4.7.

Sylowin alkuperäinen todistus nojaa Cauchyn lauseeseen. Cauchyn lauseen alkuperäinen todistus oli aika monimutkainen, ja siksipä myöhemmin etsittiinkin Sylowin lauseille todistusta, joka ei olisi riippuvainen Cauchyn lauseesta. Esimerkiksi Frobenius onnistui vuonna 1887 todistamaan Sylowin p-aliryhmien olemassaolon ilman Cauchyn lausetta.([1])

Paljon myöhemmin vuonna 1959 saksalainen matemaatikko H. Wielandt esitti todistuksen, jossa ei myöskään kosketa Cauchyn lauseseen. Tarkastellaan seuraavaksi tätä Wielandtin todistusta. Todistus on peräisin teoksesta [2]. Tulos on sama kuin Seuraus 4.8, mutta nyt todistuksessa ei käytetä Sylowin lausetta, vaan Sylowin lause on erityistapaus tuloksesta.

Lause 4.10. *Jos p on alkuluku ja p^n jakaa ryhmän G kertaluvun, niin tällöin ryhmällä G on olemassa aliryhmä kertalukua p^n.*

Todistus. Olkoon G ryhmä, jonka kertaluku on jaollinen luvulla p^n. Tällöin ryhmän G kertaluku on $p^n m$ jollakin $m \in \mathbb{Z}_+$. Olkoon sitten $\mathscr{M}$ joukko kaikista ryhmän G osajoukoista, joissa on p^n alkiota. Tällöin joukossa $\mathscr{M}$ on $\binom{p^n m}{p^n}$ alkiota.

Määritellään kuvaus $T_g(M) = gM$, missä $g \in G$ ja $M \in \mathscr{M}$. Kun $M \subseteq G$ ja $g, h \in G$, niin $(gh)M = g(hM)$ ja $eM = M$. Näin ollen ryhmä G toimii joukossa $\mathscr{M}$. [1]

Olkoon p^r suurin alkuluvun p potenssi, joka jakaa luvun m. Jos nyt p^{r+1} jakaisi kaikkien ratojen kertaluvut, niin silloin se jakaisi myös joukon $\mathscr{M}$ kertaluvun, mikä on Lemman 1.26 perusteella mahdotonta. Näin ollen on olemassa ainakin yksi sellainen rata, jonka kertaluku ei ole luvun p^{r+1} monikerta.

Olkoon $\{M_1, \ldots, M_k\}$ tällainen rata, missä nyt siis $p^{r+1} \nmid k$. Tällöin jos $g \in G$, niin jokaisella $i = 1, \ldots, k \quad gM_i = M_j$ jollakin $j = 1, \ldots, k$. Olkoon $H = \{g \in G \mid gM_1 = M_1\}$. H on nyt ryhmän G aliryhmä, sillä se on alkion M_1 vakauttaja ja Rata-vakauttajalauseen 3.12 perusteella $|G| = k|H|$.

Nyt $p^{n+r} \mid p^n m = |G|$, sillä $p^n \mid p^n$ ja $p^r \mid m$. Toisaalta $|G| = k|H|$, joten $p^{n+r} \mid k|H|$. Koska $p^{r+1} \nmid k$, niin Eukleideen lemman 1.22 nojalla $p^n \mid |H|$. Näin ollen

$$p^n \mid |H| \;\Rightarrow\; |H| \geq p^n.$$

Kuitenkin jos $m_1 \in M_1$, niin kaikilla $h \in H$ pätee $hm_1 \in M_1$, joten osajoukossa M_1 on ainakin aliryhmän H kertaluvun verran alkiota eli $|M_1| \geq |H|$. Nyt M_1 on ryhmän G osajoukko, jossa on p^n alkiota eli $|M_1| = p^n$. Täten

$$p^n \leq |H| \leq |M_1| = p^n$$

eli $|H| = p^n$. Aliryhmä H on siis ryhmän G aliryhmä, jonka kertaluku on p^n. □

[1] Lähdeteoksen [2] todistuksessa ei käytetä ryhmän toimintaa vaan määritellään ekvivalenssirelaatio joukon $\mathscr{M}$ alkioiden välille: $M_1 \sim M_2$ jos on olemassa $g \in G$ siten, että $M_1 = gM_2$. Toiminnan käyttämisessä on nyt etuna, että voidaan hyödyntää suoraan ryhmän toimintaan liittyviä tuloksia.

Koska Wielandtin todistus ei käytä Cauchyn lausetta, niin Cauchyn lause saadaan nyt seurauksena Lauseesta 4.10: jos alkuluku p jakaa ryhmän G kertaluvun, niin on olemassa aliryhmä kertalukua p ja tässä aliryhmässä jokaisen neutraalialkiosta poikkeavan alkion kertaluku on p.

Lähde [2] esittää myös todistuksen Sylowin p-aliryhmän olemassaololle käyttäen induktiota. Todistuksessa on paljon samoja elementtejä kuin lähteestä [5] peräisin olevassa Lauseen 3.22 todistuksessa.

Lause 4.11. *Äärellisellä ryhmällä G on aina olemassa Sylowin p-aliryhmä jokaisella alkuluvulla p, joka jakaa ryhmän kertaluvun.*

Todistus. Jos ryhmän kertaluku on 2, niin ainoastaan alkuluku 2 jakaa ryhmän kertaluvun. Kertalukua 2 oleva aliryhmä on varmasti olemassa, sillä tämä on ryhmä G itse.

Oletetaan sitten, että väite pätee kaikille ryhmille, joiden kertaluvut ovat pienempiä kuin $|G|$. Osoitetaan, että väite pätee myös kertaluvulla $|G|$.

Olkoon nyt $p^m \mid |G|$ ja $p^{m+1} \nmid |G|$, missä $m \geq 1$. Jos p^m jakaa minkä tahansa aidon aliryhmän $H < G$ kertaluvun, niin induktio-oletuksen nojalla aliryhmällä H on aliryhmä T, jonka kertaluku on p^m. Nyt $T \leq H$ ja $H < G$, joten $T < G$. T on siis Sylowin p-aliryhmä.

Oletetaan sitten, että $p^m \nmid |H|$ millään $H < G$. Alkion $a \in G$ keskittäjä $C_G(a) = \{x \in G \mid xax^{-1} = a\}$ on ryhmän G aliryhmä. Lisäksi jos alkio a ei kuulu keskukseen $Z(G)$, niin $C_G(a) \neq G$. Tarkastellaan nyt luokkayhtälöä

$$|G| = |Z(G)| + \sum_i [G : C_G(a_i)], \quad a_i \notin Z(G).$$

Koska $p^m \nmid |H|$ millään $H < G$, niin $p^m \nmid |C_G(a)|$ millään $a \notin Z(G)$. Kuitenkin $p^m \mid |G|$, joten $p \mid [G : C_G(a)] = \frac{|G|}{|C_G(a)|}$ kaikilla $a \notin Z(G)$. Näin ollen p jakaa summan $\sum_i [G : C_G(a_i)]$ ja ryhmän kertaluvun $|G|$, joten luokkayhtälön perusteella sen täytyy jakaa myös $|Z(G)|$. Näin ollen Cauchyn lauseen 3.16 nojalla keskuksessa $Z(G)$ on alkio $b \neq e$, jonka kertaluku on p. Alkion b generoima syklinen ryhmä $B = \langle b \rangle$ on nyt kertalukua p ja se on ryhmän G aliryhmä. Lisäksi, koska $b \in Z(G)$, niin B normaali, joten tekijäryhmä G/B

on olemassa. Tekijäryhmän G/B kertaluku on nyt $\frac{|G|}{|B|} = \frac{|G|}{p}$ eli pienempi kuin ryhmän G kertaluku. Lisäksi $p^{m-1} \mid |G/B|$, mutta $p^m \nmid |G/B|$. Näin ollen induktio-oletuksen perusteella tekijäryhmällä G/B on aliryhmä P^*, jonka kertaluku on p^{m-1}. Korrespondenssilauseen 2.58 perusteella ryhmällä G on sellainen aliryhmä P, että $P^* = P/B$. Nyt

$$p^{m-1} = |P^*| = \frac{|P|}{p},$$

joten $|P| = p^m$, ja näin ollen P on Sylowin p-aliryhmä.

□

Lähde [2] esittää lisäksi kolmannen tavan todistaa Sylowin p-aliryhmän olemassaolo ja käyttää tätä lähestymistapaa myös muiden Sylowin lauseiden todistamisessa. Kolmannessa tavassa käytetään apuna permutaatioita ja symmetristä ryhmää S_n, joka koostuu kaikista permutaatioista n:n alkion joukossa ja operaatio on kuvausten yhdistämisoperaatio. Tässä tutkielmassa ei ole käsitelty näitä sen tarkemmin, joten tarkastellaan tämä kolmas tapa vain idean tasolla menemättä yksityiskohtiin.

Kolmas tapa lähtee liikkeelle osoittamalla induktiolla, että symmetrisellä ryhmällä S_{p^k} on aina Sylowin p-aliryhmä. Tämän jälkeen osoitetaan aputulos: jos ryhmä G on ryhmän M aliryhmä ja ryhmällä M on Sylowin p-aliryhmä, niin tällöin myös ryhmällä G on olemassa Sylowin p-aliryhmä. Cayleyn lauseen mukaan jokainen äärellinen ryhmä on isomorfinen jonkin symmetrisen ryhmän S_n aliryhmän kanssa. Täten ryhmä G on isomorfinen jonkin ryhmän S_n aliryhmän kanssa. Kun valitaan tarpeeksi suuri k siten, että $n < p^k$, niin ryhmä S_n on isomorfinen jonkin ryhmän S_{p^k} aliryhmän kanssa. Näin ollen ryhmä G on isomorfinen erään ryhmän S_{p^k} aliryhmän kanssa. Koska ryhmällä S_{p^k} on aina Sylowin p-aliryhmä, niin on myös sen aliryhmillä, joista yksi on isomorfinen ryhmän G kanssa. Näin ollen myös ryhmällä G on aina Sylowin p-aliryhmä.

Edellä on esitetty erilaisia todistuksia Sylowin p-aliryhmien olemassaololle. Tarkastellaan seuraavaksi vaihtoehtoisia todistuksia muille Sylowin lauseille. Teoksessa [2] käytetään edellä esitettyä kolmatta todistustapaa muiden

lauseiden todistamiseen. Koska tämä tapa käsiteltiin vain idean tasolla, niin ei ole järkevää lähestyä muita lauseita tällä tavalla. Tarkastellaan sen sijaan lähdeteoksen [3] todistuksia Sylowin lauseille.

Lähteessä [3] Sylowin lauseita ei todisteta tavanomaisessa järjestyksessä, vaan ensin oletetaan, että Sylowin p-aliryhmiä on olemassa ja näytetään, että ne ovat toistensa konjugaatteja. Sitten osoitetaan, että Sylowin p-aliryhmien lukumäärälle N_p pätee $N_p \equiv 1 \bmod p$. Tästä seuraa, että $N_p \neq 0$, joten Sylowin p-aliryhmiä on olemassa.

Lause 4.12. *Olkoon G ryhmä ja $|G| = p^n m$, missä $p \nmid m$. Jos P ja P_1 ovat Sylowin p-aliryhmiä ryhmässä G, niin on olemassa $a \in G$ siten, että $P_1 = aPa^{-1}$.*

Todistus. Olkoon P Sylowin p-aliryhmä ja P_1 jokin toinen Sylowin p-aliryhmä ryhmässä G. Aliryhmä P_1 toimii aliryhmän P vasempien sivuluokkien joukossa G/P vasemmalla translaatiolla: $(x, gP) \mapsto x(gP) = (xg)P$ kaikilla $x \in P_1$. Rata-vakauttajalauseen 3.12 nojalla jokaisen radan $\mathcal{O}(gP)$ kertaluku jakaa ryhmän P_1 kertaluvun $|P_1| = p^n$. Näin ollen

$$m = \frac{p^n m}{p^n} = \frac{|G|}{|P|} = p^{k_1} + p^{k_2} + \ldots,$$

missä $p^{k_1}, p^{k_2}, \ldots$ ovat ratojen kertaluvut. Koska $p \nmid m$, niin on ainakin yksi rata, jonka kertaluku on $p^{k_i} = 1$. Täten jollakin $a \in G$ pätee $x(aP) = aP$ eli $x(aPa^{-1}) = aPa^{-1}$ kaikilla $x \in P_1$. Koska konjugaatti aPa^{-1} on aliryhmä, niin täytyy olla, että $x \in aPa^{-1}$ ja siten $P_1 \subseteq aPa^{-1}$.

Koska P_1 on Sylowin p-aliryhmä, niin $|P_1| = |P| = p^n$. Koska $|aPa^{-1}| = |P| = |P_1|$ ja $P_1 \subseteq aPa^{-1}$, niin $P_1 = aPa^{-1}$.

□

Lause 4.13. *Jos P on Sylowin p-aliryhmä ryhmässä G, niin Sylowin p-aliryhmien lukumäärä on $N_p = [G : N_G(P)]$ ja aina pätee $N_p \equiv 1 \bmod p$.*

Todistus. Olkoon ryhmän G kertaluku $|G| = p^n m$, missä $p \nmid m$ ja P Sylowin p-aliryhmä ryhmässä G. Edellisen lauseen nojalla jokainen Sylowin p-aliryhmä on konjugaatti aPa^{-1}, joten $N_p = [G : N_G(P)]$.

Osoitetaan sitten hieman yleisempi tulos, josta toinen väite seuraa. Olkoon $|G| = p^s t, s \leq n$ ja $N_p(s)$ kertalukua p^s olevien aliryhmien lukumäärä ryhmässä G. Vasen translaatio on nyt ryhmän G toiminta joukossa $\Omega = \{M \subseteq G \mid |M| = p^s\}$[2]:

$$(x, yM) \mapsto x(yM) = (xy)M \in \Omega$$

kaikilla $x, y \in G$ ja

$$(e, M) \mapsto eM = M.$$

Nyt

$$|\Omega| = \sum_i |\Omega_i|, \quad |\Omega_i| = [G : G_i],$$

missä on valittu aina yksi alkio M_i radalta Ω_i ja G_i on vakauttaja $G_i = \{g \in G \mid gM_i = M_i\}$. Koska $G_i M_i = M_i$, niin $M_i = \bigcup_{j=1}^{\nu_i} G_i g_{ij}$ on yhdiste tietystä määrästä vakauttajan G_i oikeita sivuluokkia. Tällöin $p^s = |M_i| = \nu_i |G_i|$, joten $|G_i| = p^{s_i} \leq p^s$.

Jos $|G_i| < p^s$, niin

$$|\Omega_i| = [G : G_i] = \frac{|G|}{|G_i|} = p^{s-s_i} \cdot t \equiv 0 \bmod pt.$$

Jos $|G_i| = p^s$, niin $|\Omega_i| = [G : G_i] = \dfrac{|G|}{|G_i|} = t$. Toisaalta jos $|\Omega_i| = t$, niin $|G_i| = p^s$. Tällöin saadaan siis, että

$$\binom{|G|}{p^s} = |\Omega| \equiv \sum_{|\Omega_i|=t} |\Omega_i| \bmod pt.$$

Edeltävän nojalla

$$|\Omega_i| = t \;\Rightarrow\; |G_i| = p^s \;\Rightarrow\; M_i = G_i a_i \qquad (\nu_i = 1)$$

jollain $a_i \in G$. Siten $a_i^{-1} M_i = a_i^{-1} G_i a_i = P_i$ on kertalukua p^s oleva aliryhmä. Olkoon $a \in G$ ja $g = a a_i$. Tällöin $aM_i = (g a_i^{-1}) M_i = gP_i$, joten radan Ω_i alkiot ovat aliryhmän P_i vasempia sivuluokkia gP_i.

[2]Tämä on sama joukko kuin Wielandtin todistuksen joukko $\mathscr{M}$. Myös Wielandtin todistuksessa käytetty toiminta oli vasen translaatio.

Jos $H \leq G$ on kertalukua p^s oleva aliryhmä, niin aliryhmän H vakauttajan G_H kertaluku on p^s, sillä $gH = H$ jos ja vain jos $g \in H$. Näin ollen jokainen kertalukua p^s oleva aliryhmä $H \leq G$ johtaa rataan $\Omega' = \{gH \mid g \in G\}$, jonka kertaluku on $|\Omega'| = \dfrac{|G|}{|G_H|} = t$. Eri aliryhmät H_i johtavat eri ratoihin Ω'_i, sillä jos $H_i = gH_j$, niin $e = gh_j$ eli $g \in H_j$ ja siten $H_i = H_j$. Näin ollen kertalukua p^s olevien aliryhmien H_i ja kertalukua t olevien ratojen Ω_i välillä on yksi-yhteen -vastaavuus. Täten kertalukua t olevia ratoja on $N_p(s)$ kappaletta ja aiempi kongruenssi voidaan nyt kirjoittaa muotoon

$$\binom{|G|}{p^s} = |\Omega| \equiv \sum_{|\Omega_i|=t} |\Omega_i| = tN_p(s) \bmod pt.$$

Olkoon nyt G' kertalukua $p^s t$ oleva syklinen ryhmä. Tällainen ryhmä on aina olemassa Huomautuksen 2.20 perusteella. Lauseen 2.24 mukaan ryhmässä G' täytyy päteä $N_p(s) = 1$ eli

$$\binom{|G'|}{p^s} \equiv t \cdot 1 = t \bmod pt.$$

Nyt $|G'| = |G|$, joten

$$t \equiv \binom{|G'|}{p^s} = \binom{|G|}{p^s} \equiv tN_p(s) \bmod pt.$$

Näin ollen ryhmässä G pätee, että

$$N_p(s)t \equiv t \bmod pt$$

eli

$$N_p(s) \equiv 1 \bmod p.$$

Kun $s = n$, niin saadaan $N_p \equiv 1 \bmod p$.

□

Lähdeluettelo

[1] Gow, R.: *Sylow's Proof of Sylow's Theorem.* Bulletin of the Irish Mathematical Society 33, (55-63), 1994.

[2] Herstein, I. N.: *Topics in Algebra.* 2. ed. New York: Wiley, 1975.

[3] Kostrikin, A. I.: *Introduction to Algebra.* New York, NY: Springer, 1982.

[4] Niemenmaa, M., Myllylä, K. ja Törmä, T.: *802354A Algebran perusteet Luentorunko Kevät 2020.* Oulun yliopisto, 2020.

[5] Rotman, J.: *Advanced Modern Algebra.* Upper Saddle River, NJ: Prentice Hall, 2003.

[6] Sylow, L.: *Théorémes sur les groupes de substitutions.* Mathematische Annalen 5, (584-594), 1872.

[7] Törmä, T.: *800339A Lukualueet Luentomoniste 2017.* Oulun yliopisto, 2017.