Eräitä ratkeavuustarkasteluja

Pro gradu-tutkielma
Milla Jantunen
2124227
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2014

Sisältö

Johdanto

Tässä tutkielmassa on käsitelty ratkeavia ryhmiä, ja tarkasteltu ryhmän ratkeavuutta sen kertaluvun suhteen. Tärkeänä aputuloksena ratkeavuustarkasteluissa on käytetty Sylowin lauseita. Lopuksi on osoitettu ratkeaviksi kaikki sellaiset ryhmät, joiden kertaluku on jokin luku yhdestä sataan, poislukien luku kuusikymmentä.

Luvussa yksi on määritelty ryhmäteorian peruskäsitteitä, kuten ryhmä, aliryhmä, syklinen ryhmä, normaali aliryhmä, tekijäryhmä sekä kompleksi. Lisäksi on esitelty joitakin jatkon kannalta olennaisia tuloksia, kuten esimerkiksi Lagrangen lause ja Homomorfismien peruslause.

Toisessa luvussa on määritelty konjugaatti, konjugointiluokat, kaksoissivuluokat sekä permutaatioryhmän rata. Lisäksi on esitelty lisää tärkeitä aputuloksia, joita ovat muun muassa Luokkayhtälö ja Cauchyn lause.

Kolmannessa luvussa on käsitelty Sylowin lauseita, jotka ovat tärkeitä työkaluja Sylowin p-aliryhmien tutkimiseen. Ennen sitä on määritelty Sylowin p-aliryhmä, sekä sen ominaisuudet.

Neljännessä luvussa on määritelty kommutaattori, kommutaattorialiryhmä sekä ratkeava ryhmä. Luvussa on lisäksi esitelty muutamia ratkeavuuskriteerejä ja erityisesti on tarkasteltu ryhmän ratkeavuutta sen kertaluvun suhteen.

Lopuksi on annettu esimerkkejä ratkeavuustarkasteluista kun ryhmän kertaluku tunnetaan. Tässä luvussa on osoitettu ratkeavuus niille ryhmille, joiden kertaluku on korkeintaan sata, muttei kuitenkaan kuusikymmentä.

1 Ryhmät ja aliryhmät

Tässä luvussa määritellään useita ryhmäteorian peruskäsitteitä joita ovat muun muassa ryhmä, aliryhmä, syklinen ryhmä, normaali aliryhmä, tekijäryhmä sekä kompleksi. Lisäksi esitellään joitakin tutkielmassa myöhemminkin tarvittavia tuloksia, kuten esimerkiksi Lagrangen lause, Homomorfismien peruslause ja Vastaavuuslause.

1.1 Ryhmä

Määritelmä 1.1.1. Olkoon S epätyhjä joukko. Kuvaus $* : S \times S \to S, (a, b) \mapsto a * b$ on joukon S binäärinen operaatio. Lisäksi binäärinen operaatio $(*)$ on *kommutatiivinen* joukossa S, jos $a * b = b * a$ aina, kun $a \in S$ ja $b \in S$ ja *assosiatiivinen* joukossa S, jos $a * (b * c) = (a * b) * c$ aina, kun $a, b, c \in S$.

Määritelmä 1.1.2. Olkoon $G \neq \emptyset$. Joukko G varustettuna binäärisellä operaatiolla $(*)$ on *ryhmä* $(G, *)$, mikäli seuraavat kolme ehtoa toteutuvat:

1. $(*)$ on assosiatiivinen eli

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

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

2. Joukossa G on sellainen alkio e, että

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

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

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

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

Alkiota a^{-1} kutsutaan *alkion a käänteisalkioksi.*

Jos lisäksi $(G, *)$ toteuttaa ehdon

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

niin kyseessä on *Abelin ryhmä* eli kommutatiivinen ryhmä

Määritelmä 1.1.3. Ryhmä G on äärellinen, jos siinä on äärellinen määrä alkioita. Alkioiden lukumäärää sanotaan *kertaluvuksi* ja merkitään $|G|$.

1.2 Aliryhmä

Määritelmä 1.2.1. Olkoon $(G, *)$ ryhmä ja $H \subseteq G, H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sitä sanotaan *ryhmän* $(G, *)$ *aliryhmäksi* ja merkitään $H \leq G$.

Lause 1.2.2. *Olkoon G ryhmä ja $H \subseteq G, H \neq \emptyset$. Nyt $H \leq G$ jos ja vain jos seuraava ehto toteutuu:*

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

Todistus. ([2], s. 17) □

Määritelmä 1.2.3. Olkoon $H \leq G$ ja $a \in G$. Joukkoa $aH = \{ah \mid h \in H\}$ sanotaan *alkion a määräämäksi aliryhmän H vasemmaksi sivuluokaksi.* Vastaavasti joukkoa $Ha = \{ha \mid h \in H\}$ sanotaan alkion a määräämäksi aliryhmän H oikeaksi sivuluokaksi.

Määritelmä 1.2.4. Aliryhmän H indeksi ryhmässä G, merkitään $[G : H]$, on ryhmän H sivuluokkien lukumäärä ryhmässä G.

Lause 1.2.5 (Lagrangen lause)**.** *Olkoon G äärellinen ryhmä, $H \leq G$ ja t aliryhmän H vasempien sivuluokkien lukumäärä ryhmässä G. Tällöin*

$$|G| = t|H|,$$

ts. äärellisen ryhmän aliryhmän kertaluku jakaa ryhmän kertaluvun.

Todistus. ([5], s. 156) □

Seuraus 1.2.6. *Jos H on äärellisen rymän G aliryhmä niin*

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

Todistus. ([5], s. 156) Lagrangen lauseen nojalla $|G| = t|H|$, missä t on vasempien sivuluokkien lukumäärä. Tällöin $t = [G : H]$, eli $|G| = [G : H]|H|$, mikä todistaa lauseen. □

1.3 Syklinen ryhmä

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

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

Siis H on lauseen 1.2.2 nojalla ryhmän G aliryhmä.

Määritelmä 1.3.1. Yllä määriteltyä ryhmää H sanotaan *alkion a generoimaksi sykliseksi ryhmäksi* ja sitä merkitään $H = \langle a \rangle$. Alkio a on *generoija.*

Alkion a *kertaluku* on pienin sellainen positiivinen kokonaisluku n, jolla $a^n = e$. Alkion kertaluvusta käytetään merkintää $|a|$

Lause 1.3.2. *Jos ryhmän kertaluku on alkukuku, niin ryhmä on syklinen.*

Todistus. ([2], s. 19) □

Huom. Syklinen ryhmä on aina Abelin ryhmä.

1.4 Normaali aliryhmä ja tekijäryhmä

Määritelmä 1.4.1. Olkoon $N \leq G$. Aliryhmää N sanotaan *normaaliksi* mikäli $aN = Na$ aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.

Lause 1.4.2. *Ryhmän G aliryhmä N on normaali jos ja vain jos*

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

Todistus. ([2], s. 20) Oletetaan ensin, että $N \trianglelefteq G$ eli $aN = Na$ aina, kun $a \in G$. Jos $y \in aNa^{-1} = \{ana^{-1} \mid n \in N\}$, niin alkio y voidaan kirjoittaa muodossa $y = aka^{-1}$,missä $k \in N$. Nyt $ak \in aN$. Koska $aN = Na$, niin tällöin $ak = k'a$, missä $k' \in N$. Siis $y = aka^{-1} = k'aa^{-1} = k'e = k'$. Näin ollen $aNa^{-1} \subseteq N$.

Oletetaan nyt, että $aNa^{-1} \subseteq N$ aina, kun $a \in G$. Olkoon $y \in aN$, jolloin $y = an$, missä $n \in N$. Tällöin $y = an = ane = ana^{-1}a = (ana^{-1})a \in Na$ eli $aN \subseteq Na$.

Olkoon sitten $t \in Na$, jolloin $t = ma$, missä $m \in N$. Tällöin $t = ma = ema = aa^{-1}ma = a(a^{-1}ma) = a(a^{-1}m(a^{-1})^{-1}) \in aN$ eli $Na \subseteq aN$. Täten $Na = aN$ eli $N \trianglelefteq G$. □

Lemma 1.4.3. *Olkoon G ryhmä, $H \leq G$ ja $[G : H] = 2$. Tällöin $H \trianglelefteq G$.*

Todistus. Nyt $[G : H] = 2$ on aliryhmän H sivuluokkien lukumäärä ryhmässä G. Jos $a \in H$, niin $aH = H = Ha$. Jos taas $a \notin H$, niin $aH \neq H$ eli $aH = \{g \in G \mid g \notin H\}$. Samoin kun $a \notin H$, niin $Ha \neq H$, joten $Ha = \{k \in G \mid k \notin H\} = aH$. Näin ollen $aH = Ha$ aina, kun $a \in G$ ja siten $H \trianglelefteq G$. □

Määritelmä 1.4.4. Jos ryhmällä G on vain triviaalit normaalit aliryhmät $\{e\}$ ja G, niin G on *yksinkertainen ryhmä.*

Olkoon $N \trianglelefteq G$. Sivuluokkien joukossa $\{aN \mid a \in G\}$ voidaan määritellä tulo $(\cdot)$ seuraavasti:

$$aN \cdot bN = abN.$$

Lause 1.4.5. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin $(\{aN \mid a \in G\}, \cdot)$ on ryhmä.*

Todistus. ([2], s. 21) Nyt $aN \cdot bN = abN$ eli $(\cdot)$ on binäärinen operaatio joukossa $\{aN \mid a \in G\}$. Binäärinen operaatio $(\cdot)$ on assosiatiivinen, sillä $(aN \cdot bN) \cdot cN = abN \cdot cN = (ab)cN = a(bc)N = aN \cdot bcN = aN \cdot (bN \cdot cN)$.

Neutraalialkio on sivuluokka eN, sillä $eN \cdot aN = eaN = aN = aeN = aN \cdot eN$. Alkion aN käänteisalkio taas on sivuluokka $a^{-1}N$, sillä $a^{-1}N \cdot aN = a^{-1}aN = eN = N$ ja $aN \cdot a^{-1}N = aa^{-1}N = eN = N$. Siten $(\{aN \mid a \in G\}, \cdot)$ on ryhmä. □

Määritelmä 1.4.6. Edellä esiteltyä paria $(\{aN \mid a \in G\}, \cdot)$ kutsutaan *ryhmän G tekijäryhmäksi normaalin aliryhmän N suhteen.* Kyseisestä ryhmästä käytetään merkintää G/N ja

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

mikäli ryhmä G on äärellinen.

1.5 Kompleksi

Olkoon $A \leq G$ ja $B \leq G$. Kompleksi AB on joukko $\{ab \mid a \in A, b \in B\}$. Yleensä kompleksi AB ei ole aliryhmä.

Lemma 1.5.1. *Olkoot A ja B ryhmän G äärellisiä aliryhmiä. Tällöin*

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

Todistus. ([1], s. 6) Kompleksissa AB tulo ab voidaan kirjoittaa $|A| \cdot |B|$ tavalla, mutta osa tuloista on keskenään identtisiä. Tarkastellaan karteesista tuloa $A \times B$ ja määritellään joukossa $A \times B$ relaatio $(\sim) : (a_1, b_1) \sim (a_2, b_2) \Leftrightarrow (a_1 b_1) = (a_2 b_2)$. Nyt $(\sim)$ on ekvivalenssirelaatio ja $|AB|$ =ekvivalenssiluokkien lukumäärä. Osoitetaan, että jokaisessa ekvivalenssiluokassa on $|A \cap B|$ alkiota. Olkoon $a \in A, b \in B$ ja olkoon E se ekvivalenssiluokka, johon pari (a, b) kuuluu. Osoitetaan, että $E = \{(ax^{-1}, xb) \mid x \in A \cap B\}$. Nyt $ax^{-1} \in A$ ja $xb \in B$, sekä $(ax^{-1})(xb) = ab$. Siis $\{(ax^{-1}, xb) \mid x \in A \cap B\} \subseteq E$. Jos taas $(c, d) \in E$, niin $cd = ab$. Tällöin $c^{-1}a = db^{-1} \in A \cap B$. Merkitään $x = c^{-1}a = db^{-1} \in A \cap B$. Tällöin $c = ax^{-1}$ ja $d = xb$. Siis $E \subseteq \{(ax^{-1}, xb) \mid x \in A \cap B\}$. Täten $E = \{(ax^{-1}, xb) \mid x \in A \cap B\}$ ja $|E| = |A \cap B|$. Siis

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

□

Esimerkki 1.5.2. Olkoon $|G| = 165 = 3 \cdot 5 \cdot 11$, $N \leq G, |N| = 15$ sekä $H \leq G, |H| = 55$. Mitä voidaan sanoa kompleksista NH?

Tarkastellaan aliryhmien leikkausta: $N \cap H \leq N \Rightarrow |N \cap H|$ jakaa kertaluvun $|N| = 15$ ja $N \cap H \leq H \Rightarrow |N \cap H|$ jakaa kertaluvun $|H| = 55$. Tällöin $|N \cap H|$ jakaa luvun $\text{syt}(15, 55) = 5$, joten $|N \cap H| = 1$ tai 5. Jos $|N \cap H| = 1$, niin $|NH| = \frac{15 \cdot 55}{1} > 165 = |G|$, mikä aiheuttaa ristiriidan. Siten $|N \cap H| = 5$, $|NH| = \frac{15 \cdot 55}{5} = 165 = |G|$ ja $NH = G$.

1.6 Homomorfismi

Määritelmä 1.6.1. Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä. Kuvausta $f : G \to H$ sanotaan *ryhmähomomorfismiksi* ryhmältä G ryhmälle H, mikäli

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

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

Esimerkki 1.6.2. Nyt $G = (\mathbb{R}^+, \cdot)$ ja $H = (\mathbb{R}, +)$ ovat ryhmiä, sekä $f : G \to H, f(x) = \ln x$. Onko kuvaus f ryhmähomomorfismi?

Olkoon $x, y \in G$. Nyt $f(x \cdot y) = \ln(x \cdot y) = \ln x + \ln y = f(x) + f(y)$. Siten kuvaus f on ryhmähomomorfismi.

Määritellään seuraavaksi kaksi olennaista käsitettä homomorfismeihin liittyen. Olkoon $f : G \to H$ homomorfismi. Joukkoa $Im(f) = f(G) = \{f(x) \mid x \in G\}$ sanotaan homomorfismin f *kuvaksi* ja joukkoa $Ker(f) = \{x \in G \mid f(x) = e_H\}$ sanotaan homomorfismin f *ytimeksi*. Lisäksi $Im(f) \leq H$ ja $Ker(f) \trianglelefteq G$ (myöhemmin tulevan vastaavuuslauseen nojalla).

Määritelmä 1.6.3. Ryhmät $(G, \cdot)$ ja $(H, *)$ ovat *isomorfiset* eli rakenneyhtäläiset, mikäli on olemassa bijektio $f : G \to H$, joka toteuttaa ehdon $f(a \cdot b) = f(a) * f(b)$ aina, kun $a, b \in G$. Tällöin merkitään $G \cong H$ ja sanotaan, että f on *ryhmäisomorfismi*.

Lause 1.6.4 (Homomorfismien peruslause)**.** *Olkoon $f : G \to H$ homomorfismi. Tällöin*

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

Todistus. ([2], s. 23) Merkitään $Ker(f) = K$ ja määritellään kuvaus $F : G/K \to Im(f)$ siten, että $F(aK) = f(a)$ aina, kun $a \in G$.

1. Olkoon $a'K = aK$, jolloin $a' \in aK$ ja $a' = ak$, jollakin $k \in K$. Nyt $F(a'K) = f(a') = f(ak) = f(a) * f(k) = f(a) * e_H = f(a) = F(aK)$, joten kuvaus F on hyvin määritelty.

2. Kuvaus F on surjektio sen määrittelystä johtuen. Olkon nyt $F(aK) = F(bK)$, jolloin $f(a) = f(b)$. Tällöin $f(b)^{-1} * f(a) = e_H \Rightarrow f(b^{-1}) * f(a) = e_H \Rightarrow f(b^{-1}a) = e_H$. Näin ollen $b^{-1}a \in K = eK \Rightarrow b^{-1}aK = eK \Rightarrow b^{-1}K \cdot aK = eK$, joten $bK \cdot (b^{-1}KaK) = bKeK \Rightarrow eKaK = bKeK \Rightarrow aK = bK$. Siis kuvaus F on myös injektio ja siten bijektio. Olkoon sitten $aK, bK \in G/K$. Nyt $F(aK \cdot bK) = F(abK) = f(ab) = f(a) * f(b) = F(aK) * F(bK)$, joten kuvaus $F : G/Ker(f) \to Im(f)$ on homomorfismi ja siten isomorfismi.

Näin ollen $G/Ker(f) \cong Im(f)$. □

Lause 1.6.5 (Vastaavuuslause)**.** *Olkoon $f : G \to H$ homomorfismi, jonka ydin on K. Nyt*

1. *Jos $D \leq G$, niin $f(D) \leq H$, ja jos $T \leq H$, niin $f^{-1}(T) \leq G$.*

2. *Jos $N \trianglelefteq G$ ja f on surjektio, niin $f(N) \trianglelefteq H$. Jos $M \trianglelefteq H$, niin $f^{-1}(M) \trianglelefteq G$.*

3. *Olkoon $T \leq H$ ja $D = \{a \in G \mid f(a) \in T\}$. Tällöin $D \leq G$, $K \trianglelefteq D$ ja $D/K \cong T$.*

Todistus. ([4], s. 86 & [2], s. 22-23)

1. Olkoon $D \leq G$. Selvästi $f(D) \subseteq H$ ja $f(D) \neq \emptyset$, sillä $e_G \in D$, jolloin $f(e_G) = e_H$. Olkoon nyt $c, d \in f(D)$. Tällöin on olemassa sellaiset $a, b \in D$, että $c = f(a)$ ja $d = f(b)$. Koska $D \leq G$, niin $ab^{-1} \in D$ eli $f(ab^{-1}) \in f(D)$. Näin ollen $f(a) * f(b^{-1}) \in f(D)$ eli $f(a) * f(b)^{-1} \in f(D)$ ja siten $c * d^{-1} \in f(D)$. Siis lauseen 1.2.2 nojalla $f(D) \leq H$.

Olkoon sitten $T \leq H$. Selvästi $f^{-1}(T) \subseteq G$ ja $f^{-1}(T) \neq \emptyset$, sillä $e_H = f(e_G) \in T \Rightarrow e_G \in f^{-1}(T)$. Olkoon nyt $a, b \in f^{-1}(T)$, jolloin $f(a), f(b) \in T$. Koska $T \leq H$, niin $f(a) * f(b)^{-1} \in T$, jolloin $f(a) * f(b^{-1}) \in T$ eli $f(ab^{-1}) \in T$ ja siten $ab^{-1} \in f^{-1}(T)$. Näin ollen $f^{-1}(T) \leq G$.

2. Oletetaan, että $N \trianglelefteq G$ ja f on surjektio. Tällöin kohdan 1. perusteella $f(N) \leq H$. Olkoon $z \in f(N)$ ja $d \in H$. Nyt on olemassa sellainen alkio $x \in N$, että $f(x) = z$ ja lisäksi surjektiivisuudesta johtuen on olemassa sellainen alkio $a \in G$, että $f(a) = d$. Koska $N \trianglelefteq G$, niin $axa^{-1} \in N$. Siten $f(axa^{-1}) \in f(N)$, jolloin $f(a) * f(x) * f(a^{-1}) \in f(N) \Rightarrow f(a) * f(x) * f(a)^{-1} \in f(N) \Rightarrow d * z * d^{-1} \in f(N)$. Näin ollen lauseen 1.4.2 nojalla $f(N) \trianglelefteq H$.

   Olkoon sitten $M \trianglelefteq H$, jolloin kohdan 1. perusteella $f^{-1}(M) \leq G$. Olkoon $x \in f^{-1}(M)$ ja $a \in G$. Nyt $f(x) \in M$ ja $f(a) \in H$. Koska M on ryhmän H normaali aliryhmä, niin $f(a) * f(x) * f(a)^{-1} \in M$, jolloin $f(a) * f(x) * f(a^{-1}) \in M \Rightarrow f(axa^{-1}) \in M \Rightarrow axa^{-1} \in f^{-1}(M)$. Näin ollen $f^{-1}(M) \trianglelefteq G$.

3. Nyt $T \leq H$ ja $D = f^{-1}(T)$, jolloin kohdan 1. nojalla $D \leq G$. Nyt $f(K) = e_H \subset T$, jolloin $K \subset D$. Lisäksi $K \trianglelefteq G$, jolloin $K \trianglelefteq D$. Kuvaus f rajattuna aliryhmään D määrittelee homomorfismin ryhmältä D ryhmälle T, jonka ydin on K. Tällöin Homomorfismien peruslauseen nojalla $D/K \cong T$.

□

Huom. Jos K on mikä tahansa ryhmän G normaali aliryhmä, ja f on luonnollinen homomorfismi ryhmältä G ryhmälle G/K, niin tällöin vastaavuus $D/K \cong T$ pätee kaikilla $T \leq G/K$ ja sellaisilla $D \leq G$ jotka sisältävät ryhmän K. Lisäksi kyseinen vastaavuus säilyttää normaaliuden siten, että $T \trianglelefteq G/K$ jos ja vain jos $D \trianglelefteq G$.

Lause 1.6.6. *Olkoon $U \leq G$ ja $N \trianglelefteq G$. Tällöin $UN/N \cong U/U \cap N$.*

Todistus. ([1], s. 6) Jos $x \in U \cap N$ ja $u \in U$, niin $uxu^{-1} \in U \cap N$. Siis $U \cap N \trianglelefteq U$ ja tekijäryhmä $U/U \cap N$ on olemassa. Nyt $N \trianglelefteq G$, joten jos $un \in UN$ ja $x \in N$, niin $xunx^{-1} = uxnx^{-1} \in UN$ eli $UN \trianglelefteq N$ ja tekijäryhmä UN/N on olemassa. Tarkastellaan kuvausta $f : UN/N \to U/U \cap N$, $f(uN) = u(U \cap N)$. Helposti voidaan todeta, että f on hyvin määritelty. Nyt f on surjektiivinen kuvaus ja myös homomorfismi. Edelleen

$$\begin{aligned} Ker(f) &= \{uN \mid f(uN) = U \cap N\} \\ &= \{uN \mid u(U \cap N) = U \cap N\} \\ &= \{uN \mid u \in U \cap N\} \\ &= \{N\}, \end{aligned}$$

joka on ryhmän UN/N ykkösalkio. Homomorfismien peruslauseen nojalla $UN/N \cong U/U \cap N$. □

2 Konjugointi

Toisessa luvussa määriteltäviä käsitteitä ovat konjugaatti, konjugointiluokat, kaksoissivuluokat sekä permutaatioryhmän rata. Lisäksi luvussa esitellään jatkon kannalta olennaisia tuloksia liittyen määriteltäviin käsitteisiin. Näitä tuloksia ovat muun muassa Luokkayhtälö ja Cauchyn lause.

2.1 Konjugaatti

Määritelmä 2.1.1. Olkoot a ja g ryhmän G alkioita. Alkio $g^a = a^{-1}ga$ on alkion g *konjugaatti* ryhmässä G.

Esimerkki 2.1.2. Ryhmässä S_5 alkio (2 3 5) on alkion (1 3 5) konjugaatti, sillä $(1\ 2)^{-1}(1\ 3\ 5)(1\ 2) = (2\ 3\ 5)$.

Lemma 2.1.3. *Konjugaatille on voimassa*

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

2) $(gh)^a = g^a h^a$ *ja*

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

Todistus. ([1], s. 7) Seuraa suoraan määritelmästä. □

2.2 Konjugointiluokka

Olkoon $\emptyset \neq M \subset G$. Joukko $M^g = \{m^g \mid m \in M\}$ on joukon M konjugaatti ryhmässä G. Jos $H \leq G$, niin $H^g \leq G$. Perustelu: nyt $f_g : x \to x^g$ on

automorfismi $G \to G$ (bijektiivinen homomorfismi ryhmältä G ryhmälle G), joten Vastaavuuslauseen nojalla $f_g(H) = H^g \leq G$. Sanotaan, että aliryhmät H ja H^g konjugoivat ryhmässä G.

Määritellään ryhmässä G relaatio $(\sim)$, jolle $x \sim y$ jos ja vain jos on olemassa sellainen $a \in G$, että $x^a = y$. Nyt $(\sim)$ on ekvivalenssirelaatio, joka jakaa ryhmän G pistevieraisiin ekvivalenssiluokkiin, joiden unionina saadaan G. Vastaavia ekvivalenssiluokkia sanotaan *konjugointiluokiksi*. Jos K on konjugointiluokka ja $g \in K$, niin $K = \{g^x \mid x \in G\}$.

Määritelmä 2.2.1. Olkoon $\emptyset \neq M \subset G$. Tällöin joukko

$$N_G(M) = \{g \in G \mid M^g = M\}$$

on joukon M *normalisoija* ryhmässä G.

Lemma 2.2.2. *Nyt $N_G(M) \leq G$.*

Todistus. ([1], s. 7) Nyt $N_G(M) = \{g \in G \mid M^g = M\} = \{g \in G \mid g^{-1}Mg = M\} = \{g \in G \mid Mg = gM\} \subseteq G$. Koska $M^1 = M$ ja $1 \in G$, niin $1 \in N_G(M) \Rightarrow N_G(M) \neq \emptyset$. Olkoon nyt $n_1 \in N_G(M)$ ja $n_2 \in N_G(M)$. Koska $n_1 \in N_G(M)$, niin $Mn_1 = n_1M \Rightarrow n_1^{-1}M = Mn_1^{-1}$, jolloin $n_1^{-1} \in N_G(M)$. Nyt $M^{n_1^{-1}n_2} = (n_1^{-1}n_2)^{-1}Mn_1^{-1}n_2 = n_2^{-1}((n_1^{-1})^{-1}Mn_1^{-1})n_2 = n_2^{-1}Mn_2 = M$. Siten $n_1^{-1}n_2 \in N_G(M)$ ja lauseen 1.2.2 nojalla $N_G(M) \leq G$. □

Määritelmä 2.2.3. Olkoon $\emptyset \neq M \subset G$. Joukko

$$C_G(M) = \{g \in G \mid gm = mg \text{ } kaikilla \text{ } m \in M\}$$

on joukon M *sentralisoija* ryhmässä G.

Nyt $C_G(M) \leq N_G(M)$. Itse asiassa sentralisoija on lisäksi normalisoijan normaali aliryhmä (todistus sivuutetaan). Erityisesti, jos joukko M koostuu vain yhdestä alkiosta x, merkitään

$$N_G(\{x\}) = C_G(\{x\}) = C_G(x) = \{g \in G \mid gx = xg\}.$$

Määritelmä 2.2.4. Aliryhmä

$$Z(G) = C_G(G) = \{g \in G \mid xg = gx \text{ } kaikilla \text{ } x \in G\}$$

on ryhmän G *keskus.*

Lause 2.2.5. *Alkion $a \in G$ määräämässä konjugointiluokassa on*

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

alkiota.

Todistus. ([3], s. 9) Alkion a konjugaatit ryhmässä G ovat alkioita $x^{-1}ax, x \in G$. Milloin päädytään samaan alkioon? Nyt

$$\begin{aligned} & x_1^{-1}ax_1 = x_2^{-1}ax_2 \\ \Leftrightarrow\ & (x_2x_1^{-1})a = a(x_2x_1^{-1}) \\ \Leftrightarrow\ & x_2x_1^{-1} \in C_G(a) \\ \Leftrightarrow\ & x_2 \in C_G(a)x_1. \end{aligned}$$

Siis jokaista alkion a konjugaattia ryhmässä G vastaa tarkalleen yksi aliryhmän $C_G(a)$ oikeanpuoleinen sivuluokka. Täten

$$|\{x^{-1}ax \mid x \in G\}| = [G : C_G(a)].$$

□

Lause 2.2.6. *Olkoon G äärellinen ryhmä ja $\emptyset \neq M \subseteq G$. Tällöin joukon M koljugaattien lukumäärä ryhmässä G on $[G : N_G(M)] = \frac{|G|}{|N_G(M)|}$.*

Todistus. ([1], s. 8) Osoitetaan, että $f : tN_G(M) \to M^{t^{-1}}$ on bijektiivinen kuvaus $\{gN_G(M) \mid g \in G\} \to \{M^y \mid y \in G\}$.

1. Nyt jos $tN_G(M) = sN_G(M)$, niin $t \in sN_G(M)$, jolloin $t = sn, n \in N_G(M) \Rightarrow t^{-1} = n^{-1}s^{-1}$. Tällöin $M^{t^{-1}} = M^{n^{-1}s^{-1}} = (M^{n^{-1}})^{s^{-1}} = M^{s^{-1}}$. Siten f on kuvaus.

2. Nyt $M^g = f(g^{-1}N_G(M))$, joten f on surjektio.

3. Lisäksi jos $f(tN_G(M)) = f(sN_G(M))$, niin $M^{t^{-1}} = M^{s^{-1}}$, jolloin $(M^{t^{-1}})^s = (M^{s^{-1}})^s \Rightarrow M^{t^{-1}s} = M$. Näin ollen $t^{-1}s \in N_G(M) \Rightarrow t^{-1}sN_G(M) = N_G(M)$, jolloin $sN_G(M) = tN_G(M)$. Näin ollen f on injektio.

□

Lause 2.2.7 (Luokkayhtälö)**.** *Jos G on äärellinen ryhmä, niin*

$$|G| = \sum_a [G : C_G(a)] = \sum_a \frac{|G|}{|C_G(a)|},$$

missä summa käy läpi yhden alkion a jokaisesta konjugointiluokasta.

Todistus. ([4], s. 102-103) Kuten aiemmin todettiin konjugointiluokat ovat keskenään pistevieraita ekvivalenssiluokkia. Näin ollen tulos seuraa suoraan lauseesta 2.2.5. □

Seuraavassa todistuksessa nähdään esimerkki siitä, miten Luokkayhtälöä voidaan käyttää hyväksi.

Lause 2.2.8. *Olkoon G ryhmä ja $|G| = p^n$, missä p on alkuluku. Tällöin ryhmän G keskus $Z(G)$ ei ole triviaali, eli on olemassa sellainen alkio $a \in G, a \neq e$, että $ax = xa$, kaikilla $x \in G$.*

Todistus. ([4], s. 103) Olkoon $z = |Z(G)|$, jolloin z on sellaisten ryhmän G alkioiden lukumäärä, joiden konjugointiluokassa on vain yksi alkio. Koska $e \in Z(G)$, niin $z \geq 1$. Minkä tahansa alkion $b \in G \setminus Z(G)$ konjugointiluokka koostuu useammasta kuin yhdestä alkiosta ja $|C_G(b)| < |G|$. Lisäksi Lagrangen lauseen nojalla $|C_G(b)|$ jakaa kertaluvun $|G|$, joten $|C_G(b)| = p^m$, missä $1 \leq m < n$.

Nyt luokkayhtälö voidaan jakaa kahteen osaan, niihin alkioihin jotka sisältyvät keskukseen sekä niihin jotka eivät sisälly keskukseen. Siten saadaan

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

Selvästi p jakaa vasemman puolen sekä oikealta puolelta termin $\sum_{m<n} p^{n-m}$. Näin ollen luvun p täytyy jakaa myös termi z. Koska $z \geq 1$, niin täytyy olla $z \geq p$. Tällöin $|Z(G)| > 1$, joten täytyy olla jokin alkio $a \neq e, a \in Z(G)$, mikä todistaa lauseen. □

Esimerkki 2.2.9. Osoita, että ryhmä G on Abelin ryhmä, jos $|G| = p^2$, missä p on alkuluku.

Ratkaisu: Nyt lauseen 2.2.8 mukaan $Z(G) > \{1\}$, joten $|Z(G)| = p$ tai $|Z(G)| = p^2$. Jos $|Z(G)| = p^2$, niin $Z(G) = G$, jolloin G on Abelin ryhmä.

Jos $|Z(G)| = p$, niin $|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$, joten $G/Z(G)$ on syklinen ryhmä. Nyt $G/Z(G) = \{gZ(G) \mid g \in G\} = \langle aZ(G)\rangle$. Olkoon $g_1, g_2 \in G$. Tällöin $g_1 Z = a^m Z'$ ja $g_2 Z = a^n Z'$, joillakin $m, n \in \mathbb{Z}$. Valitaan $1 \in Z$. Tällöin $g_1 = g_1 \cdot 1 = a^m z_1$ ja $g_2 = g_2 \cdot 1 = a^m z_2$, joillakin $z_1, z_2 \in Z$. Nyt

$$\begin{aligned} g_1 g_2 &= a^m z_1 a^n z_2 = z_2 a^m a^n z_1 = z_2 a^{m+n} z_1 \\ &= z_2 a^{n+m} z_1 = z_2 a^n a^m z_1 = a^n z_2 a^m z_1 = g_2 g_1. \end{aligned}$$

Näin ollen $g_1 g_2 = g_2 g_1$ aina, kun $g_1, g_2 \in G$, joten G on Abelin ryhmä.

2.3 Kaksoissivuluokka

Määritelmä 2.3.1. Olkoot $A \leq G$ ja $B \leq G$. Ryhmän G *kaksoissivuluokka* aliryhmien A ja B suhteen on joukko $AgB = \{agb \mid a \in A, b \in B\}$.

Lause 2.3.2. *Jos $AgB \cap AhB \neq \emptyset$, niin $AgB = AhB$. Jos G on äärellinen ryhmä, niin $G = \bigcup_{i=1}^{r} Ag_iB$, missä $Ag_jB \cap Ag_kB = \emptyset$, mikäli $j \neq k$. Lisäksi*

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

Todistus. ([1], s. 8) Jos $AgB \cap AhB \neq \emptyset$, niin $a_1 g b_1 = a_2 h b_2$, missä $a_1, a_2 \in A$ ja $b_1, b_2 \in B$. Siten $g = a_1^{-1} a_2 h b_2 b_1^{-1}$, eli $AgB = A a_1^{-1} a_2 h b_2 b_1^{-1} B = AhB$. Siis $G = \bigcup Ag_iB$ (keskenään pistevieraat kaksoissivuluokat). Jos G on äärellinen, niin $G = \bigcup_{i=1}^{r} Ag_iB$. Täten lemman 1.5.1 nojalla

$$|G| = \sum_{i=1}^{r} |Ag_iB| = \sum_{i=1}^{r} |g_i^{-1} Ag_iB| = \sum_{i=1}^{r} |A^{g_i} B|$$

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

□

Lemma 2.3.3. *Olkoon $|G| = p^n$, missä p on alkuluku. Jos $U < G$, niin $U < N_G(U)$.*

Todistus. ([1], s. 17-18) Koska $U < G$, niin $\frac{|G|}{|U|} = p^m$, missä $1 \leq m \leq n$. Nyt

$$G = \bigcup_{i=1}^{s} U x_i U,$$

on ryhmän G esitys aliryhmän U kaksoissivuluokkien avulla (voidaan olettaa, että $x_1 = 1$. Lauseen 2.3.2 nojalla

$$p^n = |G| = \sum_{i=1}^{s} \frac{|U||U|}{|U^{x_i} \cap U|} = |U| + \sum_{i=2}^{s} \frac{|U||U|}{|U^{x_i} \cap U|}.$$

$$\Rightarrow \frac{|G|}{|U|} = p^m = 1 + \sum_{i=2}^{s} \frac{|U|}{|U^{x_i} \cap U|}.$$

Tällöin on olemassa sellainen $j \in \{2, \cdots, s\}$, että $\frac{|U|}{|U^{x_j} \cap U|} = 1$, jolloin $U = U^{x_j} \cap U \Rightarrow U^{x_j} = U$ eli $x_j \in N_G(U)$. Koska $Ux_1U \neq Ux_jU$, niin $x_j \notin U$. Siten $U < N_G(U)$. □

2.4 Permutaatioryhmän rata

Olkoon $X = \{1, 2 \cdots, n\}$. Ryhmän $S_X = S_n$ aliryhmää G sanotaan *astetta n olevaksi permutaatioryhmäksi.* Määritellään joukossa X relaatio $(\sim)$ siten, että $k \sim l$, jos ja vain jos on olemassa sellainen alkio $g \in G$, jolla $g(k) = l$. Selvästi $(\sim)$ on ekvivalenssirelaatio joukossa X. Tällöin X jakautuu pistevieraisiin ekvivalenssiluokkiin $T_1, \cdots, T_r$:

$$X = \bigcup_{i=1}^{r} T_i \quad ja \quad |X| = \sum_{i=1}^{r} |T_i|.$$

Ekvivalenssiluokkia $T_1, \cdots, T_r$ sanotaan permutaatioryhmän G *radoiksi* joukossa X.

Huom. Jos T on ryhmän G rata ja $k \in T$, niin $T = \{g(k) \mid g \in G\}$.

Määritelmä 2.4.1. Alkion $k \in X$ *stabiloija* ryhmässä G on

$$G_k = \{g \in G \mid g(k) = k\} \leq G.$$

Lause 2.4.2. *Olkoon G permutaatioryhmä, T sen rata ja $k \in T$. Tällöin $|T| = [G : G_k]$.*

Todistus. ([3], s. 10-11) Olkoon $G = \bigcup_{i=1}^{r} g_i G_k$.

1. Jos $x \in g_i G_k$, niin $x = g_i g$, missä $g \in G_k$. Tällöin $x(k) = g_i g(k) = g_i(k)$.
2. Jos $h(k) = g_i(k)$, niin $g_i^{-1} h(k) = k$, joten $g_i^{-1} h \in G_k$. Siis $h \in g_i G_k$. Täten joukossa $\{g(k) \mid g \in G\} = T$ on sama määrä alkioita kuin joukossa $\{g_i G_k \mid i = 1, \cdots, r\}$, toisin sanoen $|T| = [G : G_k]$.

□

Seuraus 2.4.3. *Olkoon G äärellinen permutaatioryhmä ja T jokin sen rata. Tällöin radan T kertaluku jakaa ryhmän G kertaluvun.*

Todistus. ([5], s. 199) Lauseesta 2.4.2 ja Lagrangen lauseesta seuraa, että $|T| = [G : G_k] = \frac{|G|}{|G_k|} \Rightarrow |G| = |T||G_k|$. □

Määritelmä 2.4.4. Olkoon G ryhmä. Homomorfismi $f : G \to S_n$ on ryhmän G astetta n oleva permutaatioesitys.

Lause 2.4.5. *Olkoon $N < G, [G : N] = n$ ja $G = \bigcup_{i=1}^{n} g_i N$. Kuvaus*

$$f : G \to S_n, f(g) = \begin{pmatrix} g_i N \\ g g_i N \end{pmatrix}$$

on homomorfismi. Lisäksi

$$Ker(f) = \bigcap_{g \in G} N^g.$$

Todistus. ([1], s. 9) Jos $x_1, x_2 \in G$, niin

$$f(x_1 x_2) = \begin{pmatrix} g_1 N & \cdots & g_n N \\ (x_1 x_2) g_1 N & \cdots & (x_1 x_2) g_n N \end{pmatrix} = \begin{pmatrix} g_1 N & \cdots & g_n N \\ x_1(x_2 g_1 N) & \cdots & x_1(x_2 g_n N) \end{pmatrix}$$

$= f(x_1) \circ f(x_2)$ eli f on homomorfismi. Lisäksi

$$\begin{aligned}
Ker(f) &= \{x \in G \mid f(x) = (1) \in S_n\} \\
&= \{x \in G \mid xg_1N = g_1N, \cdots, xg_nN = g_nN\} \\
&= \{x \in G \mid xg_iN = g_iN, \forall i \in \{1, \cdots, n\}\} \\
&= \{x \in G \mid g_i^{-1}xg_iN = N, \forall i \in \{1, \cdots, n\}\} \\
&= \{x \in G \mid g_i^{-1}xg_i \in N, \forall i \in \{1, \cdots, n\}\} \\
&= \{x \in G \mid x \in g_iNg_i^{-1}, \forall i \in \{1, \cdots, n\}\} \\
&= \{x \in G \mid x \in N^{g_i^{-1}} \forall i \in \{1, \cdots, n\}\} \\
&= \bigcap_{i=1}^{n} N^{g_i^{-1}} = \bigcap_{g \in G} N^{g^{-1}} = \bigcap_{g \in G} N^g.
\end{aligned}$$

□

Lemma 2.4.6. *Olkoon f joukon S permutaatio kertalukua p, missä p on alkuluku. Tällöin minkä tahansa joukon S alkion rata permutaation f suhteen sisältää joko yhden tai p alkiota.*

Todistus. ([4], s. 88-89) Olkoon $s \in S$. Jos $f(s) = s$, niin alkion s rata sisältää ainoastaan alkion s. Oletetaan sitten, että $f(s) \neq s$ ja tarkastellaan alkioita $s, f(s), f^2(s), \cdots, f^{p-1}(s)$. Väitetään, että nämä p alkiota ovat kaikki eri alkioita ja muodostavat alkion s radan joukossa S. Jos tämä ei pidä paikkaansa, niin $f^i(s) = f^j(s)$, joillakin $o \leq i < j \leq p-1$, mistä seuraa, että $f^{j-i}(s) = s$. Olkoon $m = j - i$, jolloin $0 < m \leq p-1$ ja $f^m(s) = s$. Kuitenkin $f^p(s) = s$ ja koska p ei jaa lukua m täytyy olla $ap + bm = 1$ joillakin vakioilla a ja b. Siten $f^1(s) = f^{ap+bm}(s) = f^{ap}(f^{bm}(s)) = f^{ap}(s) = s$, koska $f^m(s) = f^p(s) = s$. Syntyy ristiriita, sillä alussa oletettiin, että $f(s) \neq s$. Näin ollen alkion s rata sisältää tarkastellut p alkiota $s, f(s), f^2(s), \cdots, f^{p-1}(s)$. □

Lause 2.4.7 (Cauchyn lause)**.** *Jos ryhmän G kertaluku on jaollinen alkuluvulla p, niin ryhmä G sisältää alkion, jonka kertaluku on p.*

Todistus. ([4], s. 89) Jos $p = 2$, niin todistus on triviaali, joten oletetaan, että $p \neq 2$. Olkoon joukko $S = \{(a_1, a_2, \cdots, a_{p-1}, a_p) \mid a_1, a_2, \cdots, a_p \in$

$G, a_1a_2\cdots a_{p-1}a_p = e\}$. Väitetään nyt, että joukko S sisältää n^{p-1} alkiota, missä $n = |G|$. Näin voidaan väittää, sillä alkiot $a_1, \cdots, a_{p-1}$ voidaan valita ryhmästä G sattumanvaraisesti, ja asettamalla $a_p = (a_1a_2\cdots a_{p-1})^{-1}$ alkio $(a_1, a_2, \cdots, a_{p-1}, a_p)$ toteuttaa ehdon

$$a_1a_2\cdots a_{p-1}a_p = a_1a_2\cdots a_{p-1}(a_1a_2\cdots a_{p-1})^{-1} = e$$

ja kuuluu siten joukkoon S. Näin ollen joukossa S on n^{p-1} alkiota.

Koska G on ryhmä, niin jos $a_1a_2\cdots a_{p-1}a_p = e$, niin myös $a_pa_1a_2\cdots a_{p-1} = e$. Niinpä kun kuvaus $f : S \to S$ määritellään siten, että $f(a_1, \cdots, a_p) = (a_p, a_1, a_2, \cdots, a_{p-1})$ niin f on joukon S permutaatio. Huomataan myös, että $f \neq i$ (identiteettikuvaus joukossa S), ja että $f^p = i$, joten $|f| = p$.

Jos alkion $s \in S$ rata sisältää yhden alkion, niin $f(s) = s$. Toisaalta, jos $f(s) \neq s$, niin lemman 2.4.6 perusteella alkion s rata sisältää p alkiota. Nyt voidaan väittää, että $f(s) \neq s$ jos ja vain jos $s = (a_1, a_2, \cdots, a_p)$, missä $a_i \neq a_j$ jollakin $i \neq j$. Siispä $f(s) = s$ jos ja vain jos $s = (a, a, \cdots, a)$ jollakin $a \in G$.

Olkoon m niiden alkioiden $s \in S$ lukumäärä, joille $f(s) = s$. Koska alkiolle $s = (e, e, \cdots, e)$ pätee $f(s) = s$, tiedetään, että $m \geq 1$. Toisaalta jos $f(s) \neq s$, niin alkion s rata sisältää p alkiota, ja nämä radat ovat keskenään pistevieraita. Jos on olemassa k sellaista rataa, missä $f(s) \neq s$, niin $n^{p-1} = m + kp$, sillä tällöin on laskettu jokainen joukon S alkio.

Kuitenkin oletuksen nojalla $p \mid n$ ja selvästi $p \mid kp$, mistä seuraa, että $p \mid m$, jolloin $m > 1$, sillä $m \neq 0$. Siten on olemassa $s \in S$, jolle $s = (a, a, \cdots, a) \neq (e, e, \cdots, e)$ ja joukon S määritelmästä johtuen tällöin $a^p = e$. Koska $a \neq e$, niin a on haluttu kertalukua p oleva alkio. □

3 Sylowin lauseet

Kolmannessa luvussa määritellään p-ryhmä, p-aliryhmä, p-alkio sekä Sylowin p-aliryhmä. Erityisesti tarkastellaan Sylowin p-aliryhmää, sekä sen ominaisuuksia. Lisäksi osoitetaan ryhmälle eräitä tärkeitä tuloksia Sylowin p-aliryhmiin liittyen. Näitä tuloksia kutsutaan Sylowin lauseiksi.

Määritelmä 3.0.1. Jos G on ryhmä ja $|G| = p^n$, missä p on alkuluku ja $n \in \mathbb{N}$, niin sanotaan, että G on p-ryhmä. Jos F on ryhmän G aliryhmä ja $|F| = p^l$, missä $l \leq n$, niin F on ryhmän G *p-aliryhmä*. Jos $x \in G$ ja $|x| = p^t$, niin x on *p-alkio*.

Määritelmä 3.0.2. Olkoon $|G| = p^a n$, missä p on alkuluku, $a \in \mathbb{N}$ ja p ei ole luvun n tekijä. Jos on olemassa sellainen ryhmän G aliryhmä P, että $|P| = p^a$, niin P on ryhmän G *Sylowin p-aliryhmä*. Merkitään S_p-aliryhmä.

Lemma 3.0.3. *Olkoon P ryhmän G S_p-aliryhmä.*

1. *Kaikki ryhmän P konjugaatit ovat myös ryhmän G S_p-aliryhmiä.*
2. *Luku p ei ole kertaluvun $|N_G(P)/P|$ tekijä.*
3. *Jos alkion $g \in G$ kertaluku on jokin luvun p potenssi ja $g^{-1}Pg = P$, niin $g \in P$.*

Todistus. ([5], s. 492)

1. Nyt konjugaateille pätee, että $|P^g| = |g^{-1}Pg| = |P|$, joten ryhmän P konjugaatit ovat myös S_p-aliryhmiä.

2. Jos p jakaa kertaluvun $|N_G(P)/P|$, niin Cauchyn lauseen mukaan $N_G(P)/P$ sisältää alkion gP, jonka kertaluku on p. Siten $N_G(P)/P$ sisältää syklisen aliryhmän $S^* = \langle gP \rangle$, jonka kertaluku on p. Vastaavuuslauseen huomautuksen nojalla on olemassa aliryhmä S, jolle $P \leq S \leq N_G(P)$ siten, että $S/P \cong S^*$. Tällöin $|S/P| = |S^*| = p$, jolloin $|S| > |P|$. Kuitenkin S on ryhmän $N_G(P)$ p-aliryhmä, jolloin syntyy ristiriita sillä P on maksimaalinen aliryhmä. Näin ollen p ei jaa $|N_G(P)|$.

3. Normalisoijan määritelmän mukaan $g \in N_G(P)$. Jos $g \notin P$, niin sivuluokka gP on ryhmän $N_G(P)/P$ alkio, jonka kertaluku on jokin luvun p potenssi. Kohdan 2. valossa syntyy ristiriita Lagrangen lauseen kanssa, joten $g \in P$.

□

Lause 3.0.4 (Sylowin 1. lause)**.** *Olkoon G kertalukua $p^a n$ oleva ryhmä, missä p on alkuluku ja p ei ole luvun n tekijä. Tällöin ryhmällä G on Sylowin p-aliryhmä.*

Todistus. ([4], s. 105) Jos $a = 0$ todistus on triviaali. Voidaan siten olettaa, että $a \geq 1$. Edetään induktiolla kertaluvun $|G|$ suhteen olettaen lause todeksi kaikille ryhmille H, joille $|H| < |G|$.

Oletetaan, että lause ei päde ryhmälle G. Tällöin induktio-oletuksen nojalla p^a ei voi jakaa kertalukua $|H|$, jos H on ryhmän G aito aliryhmä. Erityisesti jos $b \notin Z(G)$, niin $C_G(b) \neq G$, joten $|C_G(b)|$ ei ole jaollinen luvulla p^a. Siten p jakaa indeksin $[G : C_G(b)] = \frac{|G|}{|C_G(b)|}$, kun $b \notin Z(G)$.

Kirjoitetaan ryhmälle G Luokkayhtälö samoin kuin lauseessa 2.2.8. Jos $z = |Z(G)|$, niin $z \geq 1$ ja

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

Nyt p jakaa indeksin $[G : C_G(b)]$, kun $b \notin Z(G)$, joten $p \mid \sum_{b \notin Z(G)} [G : C_G(b)]$. Koska p jakaa myös vasemman puolen $p^a n$, saadaan että $p \mid z$. Tällöin Cauc-

hyn lauseen mukaan on olemassa alkio $b \in Z(G)$, jonka kertaluku on p. Jos B on alkion b generoima ryhmä, niin $|B| = p$ ja $B \triangleleft G$, koska $b \in Z(G)$.

Tarkastellaan ryhmää $T = G/B$, jolle $|T| = |G|/|B| = p^a n/p = p^{a-1}n$. Koska $|T| < |G|$, niin induktio-oletuksen nojalla ryhmällä T on aliryhmä M kertalukua p^{a-1}. Nyt Vastaavuuslauseen huomautuksen nojalla on olemassa ryhmän G aliryhmä P siten, että $B \subset P$ ja $|P/B| = |M|$. Siten $|P| = |M||B| = p^{a-1}p = p^a$ ja P on kysytty ryhmän G kertalukua p^a oleva aliryhmä. Tällöin syntyy ristiriita sen oletuksen kanssa, että ryhmällä G ei ole tällaista aliryhmää. Tämä täydentää induktion ja todistaa lauseen. □

Lause 3.0.5 (Sylowin 2. ja 3. lause)**.** *Olkoon G kertalukua $p^a n$ oleva ryhmä, missä p on alkuluku ja p ei ole luvun n tekijä, ja olkoon P ryhmän G Sylowin p-aliryhmä.*

1. *Kaikki S_p-aliryhmät konjugoivat ryhmän P kanssa.*
2. *Jos N on S_p-aliryhmien lukumäärä, niin $N \equiv 1$ (mod p) ja N jakaa luvun $\frac{|G|}{p^a}$. Edelleen $N = [G : N_G(P)]$.*

Todistus. ([5], s. 492-493) Olkoon $X = \{P_1 \cdots P_N\}$ ryhmän P konjugaattien joukko, missä ryhmää P merkitään P_1. Jos Q on mikä tahansa ryhmän G S_p-aliryhmä, niin Q toimii joukossa X konjugoimalla. Jos $a \in Q$, niin

$$(P_i)^a = (g_i^{-1} P g_i)^a = a^{-1}(g_i^{-1} P g_i)a = (g_i a)^{-1} P (g_i a) \in X.$$

Nyt seurauslauseen 2.4.3 mukaan kunkin radan alkioiden lukumäärä jakaa kertaluvun $|Q|$, eli jokaisen radan koko on jokin luvun p potenssi, koska Q on p-aliryhmä. Jos on olemassa rata jonka koko on 1, niin tällöin on olemassa jokin P_i, jolle $a^{-1}P_i a = P_i$ aina, kun $a \in Q$. Lemman 3.0.3 kohdan 3. mukaan siten on olemassa $a \in P_i$ aina, kun $a \in Q$, joten $Q \leq P_i$. Kuitenkin Q on S_p-aliryhmä, joten se on ryhmän G maksimaalinen p-aliryhmä, jolloin $Q = P_i$. Kun asetetaan $Q = P_1$ nähdään, että jokaisen radan koko on jokin luvun p aito potenssi, paitsi sen radan joka sisältää vain ryhmän P_1. Siten $|X| \equiv 1 \pmod{p}$.

Oletetaan nyt, että on olemassa jokin S_p-aliryhmä Q, joka ei konjugoi ryhmän P kanssa, eli $Q \neq P_i$ kaikilla indeksin i arvoilla. Annetaan taas ryhmän Q konjugoida joukkoa X, ja kysytään taas onko olemassa sellaista rataa P_j, jonka koko on 1. Kuten aiemmassa kappaleessa tämä johtaa siihen, että $Q = P_j$ aiheuttaen ristiriidan sen oletuksen kanssa, että $Q \notin X$. Siten ei ole olemassa rataa jonka koko on 1, vaan jokaisen radan koko on jokin luvun p aito potenssi. Siitä seuraa, että $|X|$ on luvun p monikerta, eli $|X| \equiv 0 \pmod{p}$, mikä aiheuttaa ristiriidan kongruentin $|X| \equiv 1 \pmod{p}$ kanssa. Tästä johtuen ei voi olla olemassa oletuksen mukaista ryhmää Q, ja siten kaikki S_p-aliryhmät ovat ryhmän P konjugaatteja.

Näin ollen joukko X sisältää kaikki ryhmän G Sylowin p-aliryhmät, eli $|X| = N \equiv 1 \pmod{p}$. Lopuksi koska kaikki S_p-aliryhmät ovat ryhmän P konjugaatteja, niin lauseen 2.2.6 nojalla pätee, että $N = [G : N_G(P)]$. Tällöin $|G| = N|N_G(P)|$, joten N jakaa kertaluvun $|G| = p^a n$. Kuitenkin $\text{syt}(N, p) = 1$, sillä $N \equiv 1 \pmod{p}$. Siten koska $N \mid p^a n$, niin $N \mid n$, joten N jakaa luvun $|G|/p^a$. □

Seuraus 3.0.6. *Äärellisen ryhmän G Sylowin p-aliryhmä P on yksikäsitteinen jos ja vain jos $P \trianglelefteq G$.*

Todistus. ([5], s. 493) Oletetaan, että P on ryhmän G ainoa S_p-aliryhmä. Kaikilla $a \in G$ konjugaatti $a^{-1}Pa$ on myös S_p aliryhmä, mutta yksikäsitteisyydestä johtuen $a^{-1}Pa = P$ aina, kun $a \in G$, joten $P \trianglelefteq G$.

Oletetaan sitten, että $P \trianglelefteq G$. Jos Q on mikä tahansa S_p-aliryhmä, niin $Q = a^{-1}Pa$, jollakin $a \in G$. Kuitenkin normaaliuden vuoksi $a^{-1}Pa = P$, joten $Q = P$ ja P on yksikäsitteinen. □

Esimerkki 3.0.7. Olkoon G ryhmä ja $|G| = 21 = 3 \cdot 7$. Mikä on ryhmän G S_7-aliryhmien lukumäärä?

Ratkaisu: Sylowin 7-aliryhmien lukumäärä, merkitään $N(7)$, toteuttaa ehdot:

$$N(7) \equiv 1 \ (mod\ 7), \quad N(7) \mid \frac{21}{7} = 3.$$

Ehtojen nojalla $N(7) = 1$ ja tällöin kyseinen ainoa S_7-aliryhmä on normaali.

Esimerkki 3.0.8. Olkoon $|G| = 36$. Osoita, että ryhmä G ei ole yksinkertainen.

Ratkaisu: Nyt $|G| = 36 = 2^2 \cdot 3^2$. Lisäksi $N(2^2) \equiv 1 \pmod 2$ ja $N(2^2) \mid 9$, joten $N(2^2) = 1$, 3 tai 9. Samoin $N(3^2) \equiv 1 \pmod 3$ ja $N(3^2) \mid 4$, joten $N(3^2) = 1$ tai 4.

Nyt ryhmässä G on S_3-aliryhmä P, jolle $|P| = 9$. Tällöin $[G : P] = 4$ ja lauseen 2.4.5 nojalla saadaan permutaatioesitys $f : G \to S_4$, joka on homomorfismi. Siten Homomorfismien peruslauseen nojalla $G/Ker(f) \cong f(G)$ ja lisäksi Vastaavuuslauseen mukaan $f(G) \leq S_4$. Jos G on yksinkertainen, niin ydin $Ker(f) = \{1\}$ ja $G \cong f(G) \leq S_4$ eli $|G| = 36 \mid 24 = |S_4|$. Tämä on kuitenkin ristiriita, joten ryhmä G ei voi olla yksinkertainen.

4 Ratkeavat ryhmät

Tässä luvussa määritellään kommutaattori, kommutaattorialiryhmä, ratkeava ryhmä sekä maksimaalinen aliryhmä. Erityisesti tarkastellaan ryhmän ratkeavuutta ja lisäksi näytetään millaista muotoa olevat kertaluvut johtavat aina ryhmän ratkeavuuteen.

4.1 Kommutaattori

Määritelmä 4.1.1. Olkoon G ryhmä ja $a, b \in G$. Alkiota $[a, b] = a^{-1}b^{-1}ab$ sanotaan alkioiden a ja b *kommutaattoriksi.*

Huom. $ab = ba[a, b]$

Huom. Jos $[a, b] = 1$, niin $ab = ba$.

Määritelmä 4.1.2. Aliryhmä $G' = [G, G] = \langle [a, b] \mid a, b \in G \rangle$ on ryhmän G *kommutaattorialiryhmä.*

Huom. Ryhmä G' on Abelin ryhmä jos ja vain jos $G' = 1$.
Korkeammat kommutaattorialiryhmät määritellään rekursiivisesti: $G^{(0)} = G$, $G^{(1)} = G'$, $G^{(2)} = [G', G'] = G''$ ja yleisesti $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Tietysti $G \geq G^{(1)} \geq G^{(2)} \geq \cdots$

Lemma 4.1.3. *Olkoon $U \leq G$. Nyt $G' \leq U$ jos ja vain jos $U \trianglelefteq G$ ja G/U on Abelin ryhmä.*

Todistus. ([1], s. 16) Olkoon nyt $G' \leq U$. Jos $u \in U$ ja $g \in G$, niin $u^g = g^{-1}ug = uu^{-1}g^{-1}ug = u[u, g] \in U$ ja siten $U \trianglelefteq G$. Jos $a, b \in G$, niin $[a, b] = a^{-1}b^{-1}ab \in G' \leq U$. Tällöin $a^{-1}b^{-1}abU = U$, joten G/U on Abelin ryhmä.

Olkoon $U \trianglelefteq G$ ja G/U Abelin ryhmä. Jos $a, b \in G$, niin $aUbU = bUaU$ eli $abU = baU$, jolloin $a^{-1}b^{-1}abU = U \Rightarrow a^{-1}b^{-1}ab = [a, b] \in U$. Siten $G' \leq U$. □

Lemma 4.1.4. *Olkoon $N \trianglelefteq G$. Tällöin $(G/N)^{(i)} = G^{(i)}N/N$ aina, kun $i \in \mathbb{N}$.*

Todistus. ([1], s. 17) Todistetaan lause induktiolla indeksin i suhteen. Nyt $(G/N)' = \langle [aN, bN] \mid a, b \in G \rangle = \langle [a, b]N \mid a, b \in G \rangle = G'N/N$. Siis väite pätee, kun $i = 1$.

Induktio-oletus: $(G/N)^{(k)} = G^{(k)}N/N$.

Nyt $(G/N)^{(k+1)} = [(G/N)^{(k)}]' = [G^{(k)}N/N]' = [G^{(k)}N]'N/N$
$\geq [G^{(k)}]'N/N = G^{(k+1)}N/N$.

Toisaalta $G^{(k)}N/G^{(k+1)}N = G^{(k)}[G^{(k+1)}N]/G^{(k+1)}N$, mikä on lauseen 1.6.6 mukaan $\cong G^{(k)}/G^{(k)} \cap G^{(k+1)}N$. Merkitään nyt $G^{(k)} \cap G^{(k+1)}N = L$.

Koska $[G^{(k)}]' = G^{(k+1)} \leq L$, niin lemman 4.1.3 nojalla $G^{(k)}/L$ on Abelin ryhmä. Siis $G^{(k)}N/G^{(k+1)}N$ on Abelin ryhmä, joten edelleen lemman 4.1.3 nojalla $[G^{(k)}N]' \leq G^{(k+1)}N$, ja $[G^{(k)}N]'N/N \leq G^{(k+1)}N/N$.

Näin ollen $(G/N)^{(k+1)} = G^{(k+1)}N/N$. □

4.2 Ryhmän ratkeavuus

Määritelmä 4.2.1. Ryhmä G on *ratkeava*, mikäli on olemassa jokin sellainen $k \in \mathbb{N}$, että $G^{(k)} = 1$.

Huom. Jos G on syklinen ryhmä niin se on ratkeava, koska syklinen ryhmä on aina Abelin ryhmä. Abelin ryhmät ovat ratkeavia, sillä niille pätee, että $G' = 1$.

Esimerkki 4.2.2. Osoita, että ryhmä $G = S_3$ on ratkeava.

Ratkaisu: $|G| = 6 = 3 \cdot 2$, joten ryhmän G S_3-aliryhmien lukumäärä $N(3) \equiv 1 \pmod 3$ ja $N(3) \mid 2$. Siten $N(3) = 1$ ja kyseinen S_3-aliryhmä P on normaali. Nyt $|G/P| = 2$, joten G/P on syklinen ryhmä. Lemman 4.1.3 mukaan $G' \leq P$. Koska $|P| = 3$, niin myös aliryhmä P on syklinen ja siten $P' = \{1\}$. Siis $G'' \leq P'$ eli $G'' = \{1\}$ ja G on ratkeava.

Lause 4.2.3. *Jos ryhmä G on ratkeava, niin myös ryhmän G aliryhmät ja tekijäryhmät ovat ratkeavia.*

Todistus. ([1], s. 17) Koska G on ratkeava, niin on olemassa $k \in \mathbb{N}$ siten, että $G^{(k)} = \{1\}$. Jos $H \leq G$, niin $H^{(k)} \leq G^{(k)} = \{1\}$, jolloin $H^{(k)} = \{1\}$ ja H on ratkeava.

Olkoon sitten $N \trianglelefteq G$ ja tarkastellaan tekijäryhmää G/N. Lemman 4.1.4 nojalla $(G/N)^{(k)} = G^{(k)}N/N = N/N = \{1_{G/N}\}$, joten G/N on ratkeava. □

Lause 4.2.4. *Muutamia ratkeavuuskriteerejä:*

1. *Olkoon $N \trianglelefteq G$. Jos N ja G/N ovat ratkeavia, niin myös G on ratkeava.*
2. *Olkoot $M \trianglelefteq G$ ja $N \trianglelefteq G$. Jos G/M ja G/N ovat ratkeavia, niin $G/M \cap N$ on ratkeava.*
3. *Olkoot $M \trianglelefteq G$ ja $N \trianglelefteq G$, sekä M ja N ratkeavia. Tällöin MN on ratkeava.*

Todistus. ([1], s. 17)

1. Koska N on ratkeava, niin on olemassa $k \in \mathbb{N}$ siten, että $N^{(k)} = \{1\}$. Koska G/N on ratkeava, niin on olemassa $m \in \mathbb{N}$ siten, että $(G/N)^{(m)} = \{1_{G/N}\} = \{N/N\}$. Lemman 4.1.4 nojalla $(G/N)^{(m)} = G^{(m)}N/N = \{N/N\}$, joten $G^{(m)} \leq N$. Täten $G^{(m+k)} = [G^{(m)}]^{(k)} \leq N^{(k)} = \{1\}$, jolloin $G^{(m+k)} = \{1\}$ eli G on ratkeava.

2. Koska G/M on ratkeava niin on olemassa $m \in \mathbb{N}$ siten, että $G^{(m)} \leq M$. Koska G/N on ratkeava niin on olemassa $k \in \mathbb{N}$ siten, että $G^{(k)} \leq N$. Jos $r = \max\{m, k\}$, niin $G^{(r)} \leq M \cap N$ ja $(G/M \cap N)^{(r)} = G^{(r)}M \cap N/M \cap N = M \cap N/M \cap N = \{1_{G/M\cap N}\}$. Näin ollen $G/M \cap N$ on ratkeava.

3. Nyt $M \trianglelefteq G$ ja $N \trianglelefteq G$, joten $MN \trianglelefteq G$. Lauseen 1.6.6 nojalla $MN/N \cong M/M \cap N$. Koska M on ratkeava, niin $M/M \cap N$ on ratkeava ja siten myös MN/N on ratkeava. Koska N on ratkeava niin kohdan 1. nojalla MN on ratkeava.

□

Määritelmä 4.2.5. Ryhmän G aliryhmä M on *maksimaalinen* jos $M < G$ ja ehdosta $M < B \leq G$ seuraa aina, että $B = G$.

Lemma 4.2.6. *Olkoon $|G| = p^n$, missä p on alkuluku. Jos M on ryhmän G maksimaalinen aliryhmä, niin $M \trianglelefteq G$ ja $|M| = p^{n-1}$ eli $[G : M] = p$.*

Todistus. ([1], s. 18) Lemman 2.3.3 nojalla $M < N_G(M) \leq G$. Koska M on maksimaalinen aliryhmä niin $N_G(M) = G$ ja siten $M \trianglelefteq G$. Lagrangen lauseen nojalla aliryhmän M kertaluku jakaa ryhmän G kertaluvun ja on siten jokin luvun p potenssi. Jos $|M| < p^{n-1}$, niin löytyy sellainen ryhmän G aliryhmä S, jolle $|S| = p^{n-1}$. Tällöin $M < S < G$, mikä aiheuttaa ristiriidan ryhmän M maksimaalisuuden kanssa. Siten $|M| = p^{n-1}$ ja $[G : M] = p$. □

4.3 Ratkeavat ryhmät

Lause 4.3.1. *Olkoon $|G| = p^n$, missä p on alkuluku ja $n \geq 1$. Tällöin ryhmä G on ratkeava.*

Todistus. ([1], s. 18) Todistetaan lause induktiolla eksponentin n suhteen. Jos $n = 1$, niin $|G| = p$. Tällöin G on syklinen ryhmä ja siten ratkeava.

Induktio-oletus: Jos ryhmän kertaluku on p^k, niin ryhmä on ratkeava.

Olkoon $|G| = p^{k+1}$. Olkoon K ryhmän G maksimaalinen aliryhmä. Lemman 4.2.6 nojalla $K \trianglelefteq G$ ja $[G : K] = p$. Nyt $|G/K| = p$, joten G/K on ratkeava. Koska $|K| = p^k$, niin induktio-oletuksen nojalla K on ratkeava. Tällöin lauseen 4.2.4 kohdan 1. nojalla G on ratkeava. □

Lause 4.3.2. *Olkoon $|G| = pq$, missä p ja q ovat alkulukuja ja $p \geq q$. Tällöin ryhmä G on ratkeava.*

Todistus. ([1], s. 18) Jos $p = q$, niin $|G| = p^2$, jolloin G on Abelin ryhmänä ratkeava. Voidaan jatkossa olettaa, että $p > q$. Nyt $N(p) \equiv 1 \pmod{p}$ ja $N(p) \mid q$, joten $N(p) = 1$. Näin ollen ryhmän G Sylowin p-aliryhmä P on normaali aliryhmä. Koska $|P| = p$, niin P on ratkeava ja koska $|G/P| = q$,

niin G/P on ratkeava. Täten lauseen 4.2.4 kohdan 1. nojalla G on ratkeava. □

Lause 4.3.3. *Olkoon $|G| = p^n q$, missä p ja q ovat eri alkulukuja ja $n \in \mathbb{N}$. Tällöin ryhmä G on ratkeava.*

Todistus. ([1], s. 18) Todistetaan lause induktiolla eksponentin n suhteen. Jos $n = 1$, niin $|G| = pq$ ja G on lauseen 4.3.2 nojalla ratkeava.

Induktio-oletus: Jos ryhmän G kertaluku on $p^b q$, missä $b < n$, niin G on ratkeava.

Olkoon $|G| = p^n q$. Nyt $N(p^n) \mid q$, joten $N(p^n) = 1$ tai $N(p^n) = q$. Jos $N(p^n) = 1$, niin ryhmän G S_p-aliryhmä P on normaali ryhmässä G. Tällöin P ja G/P ovat molemmat ratkeavia, joten G on ratkeava. Oletetaan siis jatkossa, että $N(p^n) = q$.

Nyt ryhmällä G on q kappaletta S_p-aliryhmiä. Olkoot sitten P_1 ja P_2 sellaiset S_p-aliryhmät, että leikkaus $D = P_1 \cap P_2$ on kertaluvultaan suurin mahdollinen. Jaetaan todistus kahteen osaan.

1° Olkoon $D = \{1\}$. Siis $P_i \cap P_j = \{1\}$ aina kun $i \neq j, 1 \leq i, j \leq q$. Merkitään $A = \{x \in G \mid |x| = p^d, d \geq 1\}$, jolloin A sisältää ryhmän G kaikki p-alkiot. Nyt $|A| = q(p^n - 1) = qp^n - q = |G| - q$. Täten ryhmässä G on vain yksi S_q-aliryhmä Q, joten $Q \trianglelefteq G$. Koska $|Q| = q$ ja $|G/Q| = p^n$, niin Q ja G/Q ovat ratkeavia ja siten myös G on ratkeava.

2° Olkoon nyt $D > \{1\}$. Nyt $D = P_1 \cap P_2 < P_1$ ja $D < P_2$. Lemman 2.3.3 nojalla $D < N_{P_1}(D) = B_1 \leq P_1$ ja $D < N_{P_2}(D) = B_2 \leq P_2$. Nyt $D \trianglelefteq B_1$ ja $D \trianglelefteq B_2$, joten $D \trianglelefteq \langle B_1, B_2 \rangle = \{x \mid x = s_1 \cdots s_n, s_i \in B_1 \cup B_2\} = L$.

Onko L p-ryhmä? Jos $|L| = p^t, t \geq 1$, niin Sylowin lauseiden nojalla on olemassa sellainen ryhmän G S_p-aliryhmä P_3, että $L \leq P_3$. Tällöin $P_1 \cap P_3 \geq P_1 \cap L \geq B_1 \geq D$, joten $P_1 = P_3$. Edelleen $P_2 \cap P_3 \geq P_2 \cap L \geq B_2 \geq D$, joten $P_2 = P_3$. Näin saadaan $P_1 = P_2$, mikä on ristiriita, joten L ei ole p-ryhmä. Voidaan siis jatkossa olettaa, että kertaluku $|L|$ on jaollinen luvulla q. Täten $|L| = p^t q, t \geq 1$. Olkoon Q eräs ryhmän L

S_q-aliryhmä. Nyt

$$|QP_1| = \frac{|Q||P_1|}{|Q \cap P_1|} = \frac{qp^n}{1} = qp^n = |G| \;\Rightarrow\; G = QP_1.$$

Merkitään $K = \langle D^g \mid g \in G \rangle$. Nyt $K \trianglelefteq G$ ja $\{1\} < D \leq K$. Jos $g \in G = QP_1$, niin $g = xy$, missä $x \in Q$ ja $y \in P_1$. Siis $D^q = D^{xy} = (D^x)^y = D^y \leq P_1$. Siten $K \leq P_1$ ja koska $K \trianglelefteq G$, niin $K < P_1$. Siis $|G/K| = p^b q$, missä $b < n$. Induktio-oletuksen nojalla G/K on ratkeava. Koska $K < P_1$, niin $|K| = p^t, t \geq 1$, joten myös K on ratkeava ja siten G on ratkeava.

□

Lause 4.3.4. *Olkoon $|G| = pqr$, missä $p > q > r$ ovat alkulukuja. Tällöin ryhmä G on ratkeava.*

Todistus. ([1], s. 18-19) Ryhmällä G on S_p-, S_q- ja S_r-alirymiä. Jos $N(p) = 1$ niin ryhmällä G on normaali S_p-aliryhmä P, joka on ratkeava. Tällöin $|G/P| = qr$, jolloin G/P on lauseen 4.3.2 nojalla ratkeava. Siten G on ratkeava. Jos $N(q) = 1$ tai $N(r) = 1$, niin ryhmän G ratkeavuus saadaan kuten edellä.

Voidaan siis jatkossa olettaa, että $N(p) > 1$, $N(q) > 1$ ja $N(r) > 1$. Nyt $N(p) \equiv 1 \pmod{p}$ ja $N(p) \mid qr$. Koska $p > q > r$, niin $N(p) = qr$. Lisäksi $N(q) \equiv 1 \pmod{q}$ ja $N(q) \mid pr$. Nyt $N(q) = p$ tai $N(q) = pr$ $(q > r)$. Joka tapauksessa $N(q) \geq p$. Edelleen $N(r) \equiv 1 \pmod{r}$ ja $N(r) \mid pq$. Nyt $N(r) = p$, $N(r) = q$ tai $N(r) = pq$, joten $N(r) \geq q$.

Kahden eri S_p-aliryhmän leikkaus on $\{1\}$, ja sama pätee myös S_q- ja S_r-aliryhmille. Tällöin ryhmässä G on:

- p-alkioita: $N(p) \cdot (p-1) = qr(p-1)$,
- q-alkioita: $N(q) \cdot (q-1) \geq p(q-1)$ ja
- r-alkioita: $N(r) \cdot (r-1) \geq q(r-1)$.

Nyt

$$\begin{aligned} |G| = pqr &\geq 1 + qr(p-1) + p(q-1) + q(r-1) \\ pqr &\geq 1 + pqr - qr + pq - p + qr - q \\ 0 &\geq 1 + pq - p - q \\ p - 1 &\geq pq - q \\ p - 1 &\geq q(p-1), \end{aligned}$$

mikä aiheuttaa ristiriidan, sillä $q \geq 2$. Siis joko $N(p)$, $N(q)$ tai $N(r) = 1$, joten G on ratkeava. □

Lause 4.3.5. *Olkoon $|G| = p^2q^2$, missä p ja q ovat alkulukuja. Tällöin ryhmä G on ratkeava.*

Todistus. ([1], harjoitus 8, t. 3) Jos $p = q$, niin $|G| = p^4$, jolloin G on ratkeava. Oletetaan siis, että $p > q$. Nyt Sylowin p-aliryhmien lukumäärä ryhmässä G täyttää ehdot $N(p^2) \equiv 1 \pmod{p}$ ja $N(p^2) \mid \frac{|G|}{p^2} = q^2$. Näin ollen $N(p^2) = 1$, $N(p^2) = q$ tai $N(p^2) = q^2$.

1. $N(p^2) = 1$. Tällöin ainoa ryhmän G S_p-aliryhmä P on normaali. Koska $|P| = p^2$, niin P on ratkeava ja koska $|G/P| = q^2$, niin G/P on ratkeava. Tällöin ryhmä G on ratkeava.

2. $N(p^2) = q$. Tällöin $q \equiv 1 \pmod{p}$ eli $p \mid q - 1$. Tämä on ristiriita, sillä $p > q$ eikä p siten voi jakaa lukua $q - 1$.

3. $N(p^2) = q^2$. Tällöin $q^2 \equiv 1 \pmod{p}$ eli $p \mid q^2 - 1$, jolloin $p \mid (q-1)(q+1)$. Nyt p ei jaa lukua $q - 1$, joten täytyy olla $p \mid q + 1$. Koska $p > q$, niin $p \geq q + 1$. Koska lisäksi $p \mid q + 1$, niin $p = q + 1$. Ainoat alkuluvut, jotka ovat yhden numeron päässä toisistaan ovat 2 ja 3, joten $|G| = 2^2 \cdot 3^2 = 36$.

   Esimerkissä 3.0.8 osoitettiin, että kertalukua 36 oleva ryhmä ei ole yksinkertainen. Tällöin on olemassa sellainen $N \trianglelefteq G$, että $\{1\} < N < G$,

jolloin $1 < |N| < |G|$. Näin ollen vaihtoehdot ryhmän N kertaluvuksi ovat:

$$|N| = p,\ q,\ p^2,\ pq,\ q^2,\ qp^2\ tai\ pq^2.$$

Koska $|G/N| = \frac{|G|}{|N|}$, niin vastaavasti vaihtoehdot ryhmän G/N kertaluvuksi ovat:

$$|G/N| = pq^2,\ qp^2,\ q^2,\ pq,\ p^2,\ q\ tai\ p.$$

Kaikki kertalukuvaihtoehdot ovat sellaista muotoa, että ryhmät N ja G/N ovat ratkeavia, joten tällöin myös ryhmä G on ratkeava.

□

5 Ratkeavuustarkasteluja

Lopuksi tarkastellaan eräiden ryhmien ratkeavuutta, kun niiden kertaluvut tunnetaan. Päätavoitteena on osoittaa ratkeaviksi kaikki sellaiset ryhmät, joiden kertaluku on jokin luku yhdestä sataan, poislukien luku kuusikymmentä.

Esimerkki 5.0.1. Olkoon G ryhmä ja $|G| = 945$. Osoita että ryhmä G on ratkeava.

Ratkaisu: Nyt $|G| = 3^3 \cdot 5 \cdot 7$, joten ryhmällä G on Sylowin 3-, 5- ja 7-aliryhmiä. Tutkitaan näiden aliryhmien lukumääriä:

$$\begin{aligned} N(3^3) \equiv 1\ (3)\ ja\ N(3^3) \mid 5 \cdot 7 \qquad &\Rightarrow N(3^3) = 1\ tai\ N(3^3) = 7, \\ N(5) \equiv 1\ (5)\ ja\ N(5) \mid 3^3 \cdot 7 \qquad &\Rightarrow N(5) = 1\ tai\ N(5) = 21, \\ N(7) \equiv 1\ (7)\ ja\ N(7) \mid 3^3 \cdot 5 \qquad &\Rightarrow N(7) = 1\ tai\ N(7) = 15. \end{aligned}$$

Jos $N(3^3) = 1$, niin on olemassa vain yksi ryhmän G Sylowin 3-aliryhmä P, joten $P \trianglelefteq G$. Koska $|P| = 3^3$, niin lauseen 4.3.1 nojalla P on ratkeava, ja koska $|G/P| = 5 \cdot 7$, niin lauseen 4.3.2 mukaan G/P on ratkeava. Näin ollen ryhmä G on ratkeava lauseen 4.2.4 nojalla.

Jos taas $N(5) = 1$, niin on olemassa vain yksi ryhmän G Sylowin 5-aliryhmä Q, joten $Q \trianglelefteq G$. Koska $|Q| = 5$, niin Q on ratkeava, ja koska $|G/Q| = 3^3 \cdot 7$, niin lauseen 4.3.3 nojalla G/Q on ratkeava. Näin ollen ryhmä G on ratkeava.

Samoin jos $N(7) = 1$, niin on olemassa vain yksi ryhmän G Sylowin 7-aliryhmä R, joten $R \trianglelefteq G$. Koska $|R| = 7$, niin R on ratkeava, ja koska $|G/R| = 3^3 \cdot 5$, niin G/R on ratkeava. Näin ollen ryhmä G on ratkeava.

Olkoon nyt $N(3^3) = 7$, $N(5) = 21$ ja $N(7) = 15$. Jos P on ryhmän G S_3-aliryhmä, niin Sylowin 3. lauseen nojalla $[G : N_G(P)] = 7$, jolloin $|N_G(P)| = 3^3 \cdot 5$. Merkitään $N = N_G(P)$ ja tutkitaan ryhmän N Sylowin aliryhmiä.

$$\begin{aligned} N(3^3) \equiv 1\ (3)\ ja\ N(3^3) \mid 5 \qquad &\Rightarrow N(3^3) = 1, \\ N(5) \equiv 1\ (5)\ ja\ N(5) \mid 3^3 \qquad &\Rightarrow N(5) = 1. \end{aligned}$$

Nyt $N(5) = 1$, joten on olemassa vain yksi ryhmän N Sylowin 5-aliryhmä Q, joten $|Q| = 5$ ja $Q \trianglelefteq N$. Nyt $|G| = 3^3 \cdot 5 \cdot 7$, joten Q on myös ryhmän G S_5-aliryhmä, mutta koska S_5-aliryhmien lukumäärä ryhmässä G on 21, niin seurauksen 3.0.6 nojalla Q ei ole ryhmän G normaali aliryhmä. Tällöin $N \leq N_G(Q) < G$, joten $|N| = 3^3 \cdot 5$ jakaa kertaluvun $|N_G(Q)|$, joka vastaavasti jakaa kertaluvun $|G| = 3^3 \cdot 5 \cdot 7$. Koska $N_G(Q) < G$, niin $|N_G(Q)| = 3^3 \cdot 5 = |N|$. Siten $N_G(Q) = N = N_G(P)$. Sylowin 3. lauseen nojalla tiedetään, että $[G : N_G(Q)] = N(5) = 21$, mutta toisaalta

$$[G : N_G(Q)] = \frac{|G|}{|N_G(Q)|} = \frac{3^3 \cdot 5 \cdot 7}{3^3 \cdot 5} = 7,$$

mikä aiheuttaa ristiriidan.

Siten joko $N(3^3) = 1$, $N(5) = 1$ tai $N(7) = 1$ (vähintään yksi niistä), jolloin ryhmä G on ratkeava.

Esimerkki 5.0.2. Olkoon G ryhmä, $|G| \leq 100$ ja $|G| \neq 60$. Tällöin ryhmä G on ratkeava.

Ratkaisu: On olemassa kertalukua 60 oleva ei-ratkeava ryhmä, minkä vuoksi ei ole mielekästä tarkastella kertalukua 60 olevan ryhmän ratkeavuutta. Kyseinen ei-ratkeava ryhmä on alternoiva ryhmä A_5, joka on yksinkertainen ryhmä. Luvussa 4. osoitettiin ratkeavaksi kaikki sellaiset ryhmät, jotka ovat kertaluvultaan muotoa p^n, pq, pqr, p^nq ja p^2q^2, missä p, q ja r ovat alkulukuja ja $n \in \mathbb{N}$. Jaetaan luvut yhdestä sataan (lukuunottamatta tietysti lukua 60, joka voidaan jättää huomiotta) alkulukutekijöihin ja lajitellaan ne sen mukaan mitä muotoa ne ovat. Luvut on lajiteltu seuraavaan taulukkoon.

p	p^n	pq	pqr	p^nq	p^2q^2
1	$4 = 2^2$	$6 = 2 \cdot 3$	$30 = 2 \cdot 3 \cdot 5$	$12 = 2^2 \cdot 3$	$36 = 2^2 \cdot 3^2$
2	$8 = 2^3$	$10 = 2 \cdot 5$	$42 = 2 \cdot 3 \cdot 7$	$18 = 3^2 \cdot 2$	$100 = 2^2 \cdot 5^2$
3	$9 = 3^2$	$14 = 2 \cdot 7$	$66 = 2 \cdot 3 \cdot 11$	$20 = 2^2 \cdot 5$	
5	$16 = 2^4$	$15 = 3 \cdot 5$	$70 = 2 \cdot 5 \cdot 7$	$24 = 2^3 \cdot 3$	
7	$25 = 5^2$	$21 = 3 \cdot 7$	$78 = 2 \cdot 3 \cdot 13$	$28 = 2^2 \cdot 7$	
11	$27 = 3^3$	$22 = 2 \cdot 11$		$40 = 2^3 \cdot 5$	
13	$32 = 2^5$	$26 = 2 \cdot 13$		$44 = 2^2 \cdot 11$	
17	$49 = 7^2$	$33 = 3 \cdot 11$		$45 = 3^2 \cdot 5$	
19	$64 = 2^6$	$34 = 2 \cdot 17$		$48 = 2^4 \cdot 3$	
23	$81 = 3^4$	$35 = 5 \cdot 7$		$50 = 5^2 \cdot 2$	
29		$38 = 2 \cdot 19$		$52 = 2^2 \cdot 13$	
31		$39 = 3 \cdot 13$		$54 = 3^3 \cdot 2$	
37		$46 = 2 \cdot 23$		$56 = 2^3 \cdot 7$	
41		$51 = 3 \cdot 17$		$63 = 3^2 \cdot 7$	
43		$55 = 5 \cdot 11$		$68 = 2^2 \cdot 17$	
47		$57 = 3 \cdot 19$		$75 = 5^2 \cdot 3$	
53		$58 = 2 \cdot 29$		$76 = 2^2 \cdot 19$	
59		$62 = 5 \cdot 13$		$80 = 2^4 \cdot 5$	
61		$69 = 3 \cdot 23$		$88 = 2^3 \cdot 11$	
67		$74 = 2 \cdot 37$		$92 = 2^2 \cdot 23$	
71		$77 = 7 \cdot 11$		$96 = 2^5 \cdot 3$	
73		$82 = 2 \cdot 41$		$98 = 7^2 \cdot 2$	
79		$85 = 5 \cdot 17$		$99 = 3^2 \cdot 11$	
83		$86 = 2 \cdot 43$			
89		$87 = 3 \cdot 29$			
97		$91 = 7 \cdot 13$			
		$93 = 3 \cdot 31$			
		$94 = 2 \cdot 47$			
		$95 = 5 \cdot 19$			

Nyt taulukosta puuttuvat luvut $72 = 2^3 \cdot 3^2$, $84 = 2^2 \cdot 3 \cdot 7$ sekä $90 = 3^2 \cdot 2 \cdot 5$, jotka eivät ole mitään aiemmin mainittua muotoa. Tarkastellaan näitä lukuja erikseen.

1. Olkoon $|G| = 72 = 2^3 \cdot 3^2$. Tutkitaan ryhmän G Sylowin 2- ja 3-aliryhmiä. Nyt

$$N(2^3) \equiv 1\ (2)\ ja\ N(2^3) \mid 3^2 \qquad \Rightarrow N(2^3) = 1,\ 3\ tai\ 9,$$
$$N(3^2) \equiv 1\ (3)\ ja\ N(3^2) \mid 2^3 \qquad \Rightarrow N(3^2) = 1\ tai\ 4.$$

   Jos $N(3^2) = 1$, niin on olemassa vain yksi ryhmän G Sylowin 3-aliryhmä P, jolloin $P \trianglelefteq G$. Koska $|P| = 3^2$, niin lauseen 4.3.1 nojalla P on ratkeava. Samoin koska $|G/P| = 2^3$, niin myös tekijäryhmä G/P on ratkeava ja siten lauseen 4.2.4 mukaan ryhmä G on ratkeava.

   Jos taas $N(3^2) = 4$ ja P on jokin ryhmän G S_3-aliryhmistä, niin Sylowin 3. lauseen mukaan $[G : N_G(P)] = 4$. Lemman 2.2.2 nojalla $N_G(P) \leq G$ ja koska $|G| = 4 \cdot |N_G(P)|$, niin $N_G(P) < G$. Tällöin lauseen 2.4.5 mukaan on olemassa homomorfismi $f : G \to S_4$, joten Homomorfismien peruslauseen nojalla $G/Ker(f) \cong f(G)$. Lisäksi $f(G) \leq S_4$, jolloin $|f(G)|$ jakaa kertaluvun $|S_4| = 4!$. Oletetaan, että ryhmä G on yksinkertainen, jolloin $Ker(f) = \{1\}$ ja $G \cong f(G) \leq S_4$. Siten $|f(G)| = |G| = 72 \mid 24 = |S_4|$, mikä on ristiriita, joten G ei ole yksinkertainen ryhmä. Tällöin on olemassa sellainen $N \trianglelefteq G$, että $\{1\} < N < G$, jolloin $1 < |N| < |G|$. Näin ollen vaihtoehdot ryhmän H kertaluvuksi ovat:

$$|N| = 2,\ 3,\ 2^2,\ 3^2,\ 2 \cdot 3,\ 2^2 \cdot 3,\ 2^3,\ 2 \cdot 3^2,\ 2^3 \cdot 3,\ tai\ 2^2 \cdot 3^2.$$

   Koska $|G/N| = \frac{|G|}{|N|}$, niin vastaavasti vaihtoehdot tekijäryhmän G/N kertaluvuksi ovat:

$$|N| = 2^2 \cdot 3^2,\ 2^3 \cdot 3,\ 2 \cdot 3^2,\ 2^3,\ 2^2 \cdot 3,\ 2 \cdot 3,\ 3^2,\ 2^2,\ 3,\ tai\ 2.$$

   Kaikki kertalukuvaihtoehdot ovat lauseiden 4.3.1, 4.3.2, 4.3.3 ja 4.3.5 nojalla sellaista muotoa, että ryhmät H ja G/H ovat ratkeavia, jolloin ryhmä G on ratkeava.

2. Olkoon $|G| = 84 = 2^2 \cdot 3 \cdot 7$. Tutkitaan ryhmän G Sylowin 2-, 3- ja 7-aliryhmiä. Nyt

$$\begin{aligned} N(2^2) \equiv 1\ (2)\ ja\ N(2^2) \mid 3 \cdot 7 \qquad &\Rightarrow N(2^2) = 1,\ 3,\ 7\ tai\ 21, \\ N(3) \equiv 1\ (3)\ ja\ N(3) \mid 2^2 \cdot 7 \qquad &\Rightarrow N(3) = 1,\ 4,\ 7\ tai\ 28, \\ N(7) \equiv 1\ (7)\ ja\ N(7) \mid 2^2 \cdot 3 \qquad &\Rightarrow N(7) = 1. \end{aligned}$$

Koska $N(7) = 1$ on olemassa täsmälleen yksi ryhmän G S_7-aliryhmä P, jolloin P on ryhmän G normaali aliryhmä. Nyt $|P| = 7$, joten P on ratkeava ja samoin $|G/P| = 2^2 \cdot 3$, joten lauseen 4.3.3 nojalla myös tekijryhmä G/P on ratkeava. Näin ollen ryhmä G on ratkeava.

3. ([6], s. 8) Olkoon $|G| = 90 = 3^2 \cdot 2 \cdot 5$. Tutkitaan ryhmän G Sylowin 2-, 3- ja 5-aliryhmiä. Nyt

$$\begin{aligned} N(2) \equiv 1\ (2)\ ja\ N(2) \mid 3^2 \cdot 5 \qquad &\Rightarrow N(2) = 1,\ 3,\ 5,\ 9,\ 15\ tai\ 45, \\ N(3^2) \equiv 1\ (3)\ ja\ N(3^2) \mid 2 \cdot 5 \qquad &\Rightarrow N(3^2) = 1\ tai\ 10, \\ N(5) \equiv 1\ (5)\ ja\ N(5) \mid 3^2 \cdot 2 \qquad &\Rightarrow N(5) = 1\ tai\ 6. \end{aligned}$$

Aivan kuten kohdissa 1. ja 2. ryhmä G on ratkeava jos $N(3^2) = 1$ tai $N(5) = 1$. Oletetaan siis, että $N(5) = 6$ ja $N(3^2) = 10$. Kahden eri S_5-aliryhmän leikkaus on $\{1\}$, joten ryhmässä G on yhteensä $6 \cdot (5-1) = 24$ 5-alkiota. Kahden eri S_3-aliryhmän leikkaus ei voi aina olla $\{1\}$, sillä tällöin ryhmässä G olisi yhteensä $10 \cdot (9-1) = 80$ 9-alkiota, jolloin 5- ja 9-alkioita olisi yhteensä $24 + 80 = 104 > 90 = |G|$.

Siten ryhmässä G on Sylowin 3-aliryhmät P ja Q, joiden leikkaus ei ole triviaali. Tällöin $1 < |P \cap Q| < 9 = |P|$, sillä $P \neq Q$. Koska $P \cap Q \leq P$, niin $|P \cap Q|$ jakaa kertaluvun $|P|$ ja siten $|P \cap Q| = 3$. Merkitään $T = P \cap Q$ ja tutkitaan ryhmää $N_G(T)$. Nyt P ja Q ovat esimerkin 2.2.9 nojalla Abelin ryhmiä ja T on ryhmien P ja Q aliryhmä, joten $P, Q \leq N_G(T)$. Tällöin $|N_G(T)| > 9 + 9 - 3 = 15$ ja koska $N_G(T) \leq G$, niin $|N_G(T)|$ jakaa kertaluvun $|G|$. Lisäksi $|P| = 9$ jakaa kertaluvun $|N_G(T)|$, joten $|N_G(T)| = 18$, 45 tai 90.

(*i*) Jos $|N_G(T)| = 90$, niin tällöin $N_G(T) = G$, joten T on normaali ryhmässä G. Nyt $|T| = 3$ eli ryhmä T on ratkeava, ja lisäksi $|G/T| = 30 = 2 \cdot 3 \cdot 5$, jollon tekijäryhmä G/T on lauseen 4.3.4 nojalla ratkeava. Näin ollen ryhmä G on ratkeava.

(*ii*) Jos $|N_G(T)| = 45$, niin $[G : N_G(T)] = 2$, jolloin lemman 1.4.3 nojalla $N_G(T) \trianglelefteq G$. Nyt $|N_G(T)| = 3^2 \cdot 5$, joten $N_G(T)$ on ratkeava. Myös tekijäryhmä $G/N_G(T)$ on ratkeava, sillä $|G/N_G(T)| = 2$, ja siten ryhmä G on ratkeava.

(*iii*) Jos $|N_G(T)| = 18$, niin $N_G(T) < G$ ja $[G : N_G(T)] = 5$. Lauseen 2.4.5 nojalla on olemassa homomorfismi $f : G \to S_5$ ja $G/Ker(f) \cong f(G) \leq S_5$. Nyt G ei voi olla yksinkertainen ryhmä, sillä tällöin $|f(G)| = |G/Ker(f)| = |G| = 3^2 \cdot 2 \cdot 5 \mid 5! = |S_5|$, mikä aiheuttaa ristiriidan. Näin on olemassa jokin $N \trianglelefteq G$, jolle $\{1\} < N < G$. Vaihtoehdot ryhmän N kertaluvuiksi ovat:

$$|N| = 2,\ 3,\ 5,\ 2 \cdot 3,\ 3^2,\ 2 \cdot 5,\ 3 \cdot 5,\ 2 \cdot 3^2,\ 2 \cdot 3 \cdot 5 \ tai\ 3^2 \cdot 5.$$

Kuten kohdassa 1. tekijäryhmän G/N kertalukuvaihtoehdot ovat täsmälleen samat kuin ryhmällä N (käänteisessä järjestyksessä). Kaikki kertalukuvaihtoehdot ovat sellaista muotoa, että ryhmät N ja G/N ovat ratkeavia, joten ryhmä G on ratkeava.

Näin ollen ryhmä G on ratkeava, kun $|G| = 90$.

Nyt kaikki ryhmät joiden kertaluku esiintyy taulukossa voidaan todeta kappaleen 4. nojalla ratkeaviksi. Lisäksi kohdissa 1.-3. osoitettiin, että myös ryhmät, joiden kertaluku jäi taulukon ulkopuolelle, ovat ratkeavia. Näin ollen on osoitettu ratkeavuus kaikille ryhmille G, joille $|G| \leq 100$ ja $|G| \neq 60$.

Lähdeluettelo

[1] Markku Niemenmaa: *Ryhmäteoria luentorunko, muistiinpanot ja harjoitukset*, Oulun yliopisto, 2009.

[2] Markku Niemenmaa, Kari Myllylä, Juha-Matti Tirilä: *Algebra I luentorunko ja muistiinpanot*, Oulun yliopisto, 2010.

[3] Markku Niemenmaa: *Algebra II luentorunko ja muistiinpanot*, Oulun yliopisto, 2008.

[4] I.N. Herstein: *Abstract Algebra*, New Jersey, 1996.

[5] Joseph J. Rotman: *A First Course in Abstract Algebra With Applications*, New Jersey, 2006.

[6] Thanos Gentimis: *Solvable Groups - A Numerical Approach*, haettu 25.2.2014 osoitteesta http://plaza.ufl.edu/thanos/Text%20Files/solvable.pdf