Frobeniuksen lauseesta ja sen yleistyksistä

Pro Gradu-tutkielma
Mikko Korhonen
Matemaattisten tieteiden laitos
Oulun yliopisto
2013

Sisältö

1 Johdanto

Tässä tutkielmassa perehdytään yhtälön $X^n = c$ ratkaisuihin liittyviin kysymyksiin äärellisessä ryhmässä. Emme kiinnitä juurikaan huomiota ratkaisujen olemassaoloon tai niiden etsimiseen, vaan olemme lähinnä kiinnostuneita ratkaisujen lukumäärästä[1]. Tarkka lukumäärä tietysti riippuu ryhmästä, mutta yleisessä tapauksessa voidaan osoittaa, että missä tahansa äärellisessä ryhmässä ratkaisujen lukumäärä on tietyn luvun monikerta.

Lähtökohtana on yhtälö $X^n = 1$. Luvussa 3 todistamme Frobeniuksen lauseen, jonka mukaan yhtälön $X^n = 1$ ratkaisujen lukumäärä ryhmässä G on luvun $(n, |G|)$ monikerta. Näin ollen jos n jakaa ryhmän G kertaluvun, niin ratkaisujen lukumäärä on luvun n monikerta. Luvussa 4 tarkastelemme Frobeniuksen lauseen yleistyksiä. Pääpaino on yhtälössä $X^n = c$, missä c on jokin ryhmän G alkio. Tällöin voidaan osoittaa, että ratkaisujen lukumäärä on luvun $(n, |C_G(c)|)$ monikerta. Tarkastelemme myös ratkaisujen lukumäärää kaksoissivuluokissa HyH, missä y on jokin ryhmän alkio ja H on aliryhmä. Lisäksi esitämme ilman todistuksia muun muassa Philip Hallin [13] sanayhtälöihin liittyvät tulokset.

Yhtälöön $X^n = 1$ liittyy Frobeniuksen otaksuma, johon perehdymme luvussa 5. Frobeniuksen otaksuman mukaan jos yhtälön $X^n = 1$ ratkaisujen lukumäärä ryhmässä G on tarkalleen $(n, |G|)$, niin ratkaisujen joukko muodostaa normaalin aliryhmän. Käymme läpi useita otaksuman erikoistapauksia ja todistamme Frobeniuksen otaksuman ratkeaville ryhmille. Lisäksi osoitamme, että Frobeniuksen otaksuma pätee mille tahansa ryhmälle kun n on neliövapaa. Luvun 4 tuloksien sovelluksena todistamme Richard Zemlinin [23] tuloksen, jonka mukaan jos Frobeniuksen otaksuma ei pidä paikkansa, niin pienintä mahdollista kertalukua oleva vastaesimerkki otaksumalle on yksinkertainen ryhmä. Näin ollen Frobeniuksen otaksuman todistamisessa voidaan turvautua äärellisten yksinkertaisten ryhmien luokitteluun. Otaksuman todistus valmistui 90-luvun alkupuolella kun jokainen yksinkertaisten ryhmien perhe oli tarkastettu. Alternoiville ryhmille otaksuman todisti James Rust [24]. Suurimman työn tekivät Nobuo Iiyori ja Hiroyoshi Yamaki [31], jotka kävivät läpi loput yksinkertaiset ryhmät artikkeleissa, jotka ilmestyivät vuosina 1983-1993.

Luvussa 6 tutkimme yhtälön $X^n = 1$ ratkaisujen generoiman aliryhmän $B_n(G) = \langle x \in G : x^n = 1 \rangle$ ominaisuuksia. Osoitamme Zemlinin [23] tuloksen, jonka mukaan $|B_n(G)| \leq 2^{a-1}$, missä a on yhtälön $X^n = 1$ ratkaisujen lukumäärä ryhmässä G. Luvussa 7 käymme läpi useita Frobeniuksen lauseen

[1] Ratkaisujen etsiminen ja niiden olemassaolon tutkiminen on *diskreetin logaritmin ongelma*, joka on tärkeä käsite kryptografiassa.

sovelluksia. Osoitamme esimerkiksi, että ryhmä on ratkeava jos sen jokainen Sylowin p-aliryhmä on syklinen. Erityisesti tästä seuraa Frobeniuksen tulos, jonka mukaan ryhmä on ratkeava jos sen kertaluku on neliövapaa. Lisäksi tutkimme yhtälön $X^n = 1$ ratkaisujen lukumäärän vaikutusta ryhmän G rakenteeseen. Tähän liittyen todistamme, että G on ratkeava jos kaikilla kokonaisluvuilla n yhtälöllä $X^n = 1$ on korkeintaan $6n$ ratkaisua.

Joitakin tutkielmassa käytettyjä lähteitä on hieman vaikea löytää. Esimerkiksi Frobeniuksen otaksumaan liittyvän Zemlinin tuloksen todistus löytyy kokonaisuudessaan ainoastaan muutamasta vanhasta väitöskirjasta (esim. Zemlin [23] tai McKean [25]), joiden saatavuus on todella huono. Vaihtoehtoisesti todistuksen voi koota hajanaisista lähteistä (esim. Arad [26, Lemma 4], Hall [13, 1.3, III], Murai [22, Theorem 1.1]), mutta kaikkia todistukseen tarvittavia osia ei löydy tiedejulkaisuista. Frobeniuksen alkuperäiset tutkimukset (1893-1907) löytyvät julkaisusta *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften*, jonka numeroita löytyy esimerkiksi Internet Archivesta osoitteessa `www.archive.org`.

Luvussa 2 käymme läpi tutkielmassa tarvittavat ryhmäteorian tulokset. Esitiedoiksi lukijalle riittää alkuun ryhmäteorian perustiedot, joista tarkemmin luvun 2 alussa. Luvuissa 3 ja 4 ei käytännössä tarvita Cauchyn lausetta monimutkaisempaa teoriaa. Myöhemmissä luvuissa tarvitaan muun muassa Sylowin lauseita sekä ryhmien ratkeavuuteen liittyviä tuloksia. Lisäksi Schur-Zassenhausin lause on muutaman kerran tarpeellinen Frobeniuksen otaksuman käsittelyssä.

2 Määritelmiä ja perustuloksia

Tämän luvun tarkoituksena on käydä läpi tutkielmassa tarvittavia tuloksia ja käsitteitä. Tarkoituksena ei ole käydä läpi tarkasti kaikkia asioita, vaan enemmänkin koota yhteen tarvittavat tulokset. Tarkastelemme tutkielmassa ainoastaan äärellisiä ryhmiä, joten jatkossa *ryhmä* tarkoittaa äärellistä ryhmää. Ryhmäteorian alkeet ja peruskäsitteet oletetaan tunnetuiksi. Otamme lisäksi käyttöön seuraavat merkinnät, määritelmät ja tulokset ilman tarkempaa käsittelyä, kts. tarvittaessa esimerkiksi [4].

Kahden joukon A ja B erotuksesta käytetään merkintää $A-B = \{x \in A : x \notin B\}$. Joukkojen $\{A_i\}_{i\in I}$ yhdiste $\cup_{i\in I} A_i$ on *erillinen yhdiste*, jos $A_i \cap A_j = \emptyset$ kun $i \neq j$.

Olkoon G ryhmä. Ryhmän G neutraalialkiosta käytetään merkintää 1 tai 1_G. Alkion $x \in G$ kertaluvusta käytetään merkintää $|x|$. Jos H on ryhmän G aliryhmä, niin merkitään $H \leq G$ ja jos lisäksi $H \neq G$, niin merkitään $H < G$. Jos $H < G$, niin H on *aito aliryhmä*. Jos H on ryhmän G normaali aliryhmä, niin merkitään $H \trianglelefteq G$ ja jos lisäksi $H \neq G$ niin merkitään $H \triangleleft G$. Ryhmä G on *yksinkertainen*, jos sen ainoat normaalit aliryhmät ovat $\{1\}$ ja G.

Jos H ja K ovat ryhmän G aliryhmiä, niin aliryhmien H ja K *tulo* on joukko $HK = \{hk : h \in H, k \in K\}$, jonka kertaluku $|HK| = \frac{|H||K|}{|H\cap K|}$. Tässä HK on aliryhmä jos ja vain jos $HK = KH$, joten HK on aliryhmä erityisesti kun $H \trianglelefteq G$ tai $K \trianglelefteq G$.

Ryhmien G ja H *suora tulo* on karteesinen tulo $G \times H = \{(g, h) : g \in G, h \in H\}$ varustettuna operaatiolla $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_1, h_1 h_2)$. Kahden ryhmän suora tulo on aina ryhmä. Vastaavasti määritellään useamman ryhmän suora tulo, ja käytetään merkintää $G^n = G \times G \times \ldots \times G$, missä G esiintyy tulossa n kertaa.

Ryhmän G *keskus* on aliryhmä $Z(G) = \{z \in G : zg = gz$ kaikilla $g \in G\}$.

Alkion $x \in G$ *konjugaatti* on mikä tahansa alkio gxg^{-1}, missä $g \in G$. Alkion $x \in G$ *sentralisoija* on aliryhmä $C_G(x) = \{g \in G : gx = xg\}$, ja tällöin alkion x konjugaattien lukumäärä on $[G : C_G(x)]$.

Vastaavasti aliryhmän H konjugaatti on mikä tahansa aliryhmä gHg^{-1}, missä $g \in G$. Aliryhmän $H \leq G$ *normalisoija* on aliryhmä $N_G(H) = \{g \in G : gHg^{-1} = H\}$. Aliryhmän H eri konjugaattien lukumäärä on $[G : N_G(H)]$. Tässä $H \trianglelefteq N_G(H)$ ja $N_G(H)$ on ryhmän G suurin aliryhmä, jossa H on normaali aliryhmä.

Kuvaus $\phi : G \to G$ on *automorfismi*, jos ϕ on isomorfismi eli bijektio ja homomorfismi. Ryhmän G automorfismien joukko $\mathrm{Aut}(G)$ muodostaa ryhmän kuvausten yhdistämisen suhteen. Aliryhmä $H \leq G$ on *karakteristinen aliryhmä*, jos $\phi(H) = H$ kaikilla $\phi \in \mathrm{Aut}(G)$ ja tällöin merkitään

$H \operatorname{char} G$. Esimerkiksi ryhmän keskus $Z(G)$ on aina karakteristinen aliryhmä. Jos $H \operatorname{char} G$, niin H on normaali aliryhmä, sillä kaikilla $g \in G$ kuvaus $x \mapsto gxg^{-1}$ on automorfismi.

Joukon $X = \{1, 2, \ldots, n\}$ permutaatioiden muodostama ryhmä on astetta n oleva symmetrinen ryhmä, josta käytetään merkintää $\mathrm{Sym}(n)$. Parillisten joukon X permutaatioiden muodostama ryhmä on astetta n oleva alternoiva ryhmä, josta käytetään merkintää $\mathrm{Alt}(n)$. Mikä tahansa permutaatio voidaan esittää erillisten syklien tulona, ja permutaation kertaluku ja konjugointiluokka ryhmässä $\mathrm{Sym}(n)$ määräytyy syklirakenteen perusteella.

Jäännösluokkien modulo n muodostamasta yhteenlaskuryhmästä käytetään merkintää $\mathbb{Z}_n$. Ryhmä $\mathbb{Z}_n$ on aina kertalukua n oleva syklinen ryhmä.

2.1 Lukuteoriaa

Kokonaislukujen r ja s suurimmasta yhteisestä tekijästä käytetään merkintää (r, s). Tällöin lukujen r ja s pienin yhteinen jaettava on $\frac{ab}{(a,b)}$. Jos r jakaa luvun s, niin merkitään $r \mid s$. Jos r ei jaa lukua s, niin merkitään $r \nmid s$. Kokonaislukujen r ja s lineaarikombinaatiolla tarkoitetaan jotakin lukua muotoa $\lambda r + \mu s$, missä λ ja μ ovat kokonaislukuja. Suurin yhteinen tekijä (r, s) voidaan aina esittää lukujen r ja s lineaarikombinaationa. Jos $n \geq 1$ on kokonaisluku, niin $\varphi(n)$ on niiden kokonaislukujen $1 \leq k \leq n$ lukumäärä, joilla $(n, k) = 1$. Funktiota φ kutsutaan *Eulerin phi-funktioksi*. Jos p^a on alkuluvun potenssi, niin $\varphi(p^a) = p^{a-1}(p-1)$. Lisäksi $\varphi(mn) = \varphi(m)\varphi(n)$ kun $(m, n) = 1$.

Lemma 2.1. *Kaikilla positiivisilla kokonaisluvuilla a, b ja g pätee $g(a, b) = (ga, gb)$.*

Todistus. Nyt (a, b) on lukujen a ja b lineaarikombinaatio, joten $g(a, b)$ on lukujen ga ja gb lineaarikombinaatio. Näin ollen $(ga, gb) \mid g(a, b)$.

Koska $(a, b) \mid a$ ja $(a, b) \mid b$, niin $g(a, b) \mid ga$ ja $g(a, b) \mid gb$. Tämän perusteella $g(a, b) \mid (ga, gb)$, joten $g(a, b) = (ga, gb)$. □

Lemma 2.2. *Jos $(n_1, n_2) = 1$, niin $(n_1, g)(n_2, g) = (n_1 n_2, g)$.*

Todistus. Koska $(n_1, g) \mid n_1$ ja $(n_2, g) \mid n_2$, niin $((n_1, g), (n_2, g)) = 1$. Lisäksi $(n_1, g) \mid (n_1 n_2, g)$ ja $(n_2, g) \mid (n_1 n_2, g)$, joten $(n_1, g)(n_2, g) \mid (n_1 n_2, g)$. Nyt (n_1, g) on lukujen n_1 ja g lineaarikombinaatio, ja vastaavasti (n_2, g) on lukujen n_2 ja g lineaarikombinaatio. Tällöin $(n_1, g)(n_2, g)$ on lukujen $n_1 n_2$ ja g lineaarikombinaatio. Näin ollen $(n_1 n_2, g) \mid (n_1, g)(n_2, g)$. □

2.2 Sykliset ryhmät

Seuraavassa joitakin syklisiin ryhmiin ja alkioiden kertalukuihin liittyviä yksinkertaisia tuloksia. Jatkossa erityisen tärkeä tulos on lemma 2.9, jota tarvitaan Frobeniuksen lauseen todistuksessa luvussa 3.

Lemma 2.3. *Olkoon x kertalukua n oleva alkio ja $d \mid n$. Tällöin alkion x^d kertaluku on n/d.*

Todistus. Nyt $(x^d)^{n/d} = x^n = 1$, joten $|x^d| \mid \frac{n}{d}$. Jos $(x^d)^k = 1$, niin $n \mid dk$. Nyt $d \mid n$, joten $\frac{n}{d} \mid k$. Erityisesti siis $\frac{n}{d} \mid |x^d|$, ja näin ollen $|x^d| = \frac{n}{d}$. □

Lemma 2.4. *Olkoon x kertalukua n oleva alkio ja k kokonaisluku. Tällöin $\langle x^k \rangle = \langle x^{(n,k)} \rangle$.*

Todistus. Koska $(n,k) \mid k$, niin $x^k \in \langle x^{(n,k)} \rangle$. Näin ollen $\langle x^k \rangle \leq \langle x^{(n,k)} \rangle$. Nyt $(n,k) = \lambda n + \mu k$ missä λ ja μ ovat kokonaislukuja. Siispä $x^{(n,k)} = (x^k)^\mu$ koska $x^n = 1$. Näin ollen $x^{(n,k)} \in \langle x^k \rangle$ ja $\langle x^{(n,k)} \rangle \leq \langle x^k \rangle$. □

Lemma 2.5. *Olkoon k kokonaisluku ja x kertalukua n oleva alkio. Tällöin*

$$|x^k| = \frac{n}{(n,k)}.$$

Todistus. Lemmoista 2.3 ja 2.4 seuraa $|x^k| = |x^{(n,k)}| = \frac{n}{(n,k)}$. □

Lemma 2.6. *Olkoon x kertalukua n oleva alkio. Tällöin $\langle x \rangle = \langle x^k \rangle$ jos ja vain jos $(n,k) = 1$. Näin ollen ryhmällä $\langle x \rangle$ on tarkalleen $\varphi(n)$ generoivaa alkiota.*

Todistus. Koska $\langle x \rangle = \langle x^k \rangle$ jos ja vain jos $|x| = |x^k|$, niin väite seuraa lemmasta 2.5. □

Lemma 2.7. *Olkoon $G = \langle x \rangle$ kertalukua n oleva syklinen ryhmä. Jos $d \mid n$ on positiivinen kokonaisluku, niin ryhmällä G on yksikäsitteinen kertalukua d oleva aliryhmä.*

Todistus. Nyt lemman 2.3 nojalla $|x^{n/d}| = d$, joten $\langle x^{n/d} \rangle$ on kertalukua d oleva aliryhmä. Jos $H \leq G$ on kertalukua d oleva aliryhmä, niin H on syklinen. Näin ollen $H = \langle x^k \rangle$. Jos $t = (n,k)$, niin lemman 2.4 nojalla $H = \langle x^t \rangle$, ja edelleen $d = |H| = |x^t| = n/t$. Näin ollen $t = n/d$ ja $H = \langle x^{n/d} \rangle$. □

Lemma 2.8. *Olkoot x ja y ryhmän G alkioita joille pätee $x^n = y^n$ ja $x^m = y^m$, missä $(m,n) = 1$. Tällöin $x = y$. Erityisesti siis ehdosta $x^m = 1$ ja $x^n = 1$ seuraa $x = 1$ kun $(m,n) = 1$.*

Todistus. Koska $(m,n)=1$, niin $\lambda m+\mu n=1$ joillekin kokonaisluvuille λ ja μ. Näin ollen $x=x^{\lambda m+\mu n}=(x^m)^\lambda(x^n)^\mu=(y^m)^\lambda(x^n)^\mu=y^{\lambda m+\mu n}=y$. □

Lemma 2.9. *Olkoon $|x|=mn$, missä $(m,n)=1$. Tällöin on olemassa sellaiset alkiot y ja z, että $x=yz=zy$ sekä $|y|=m$ ja $|z|=n$. Lisäksi alkiot y ja z ovat yksikäsitteisiä.*

Todistus. Koska $(m,n)=1$, niin löytyy sellaiset kokonaisluvut λ ja μ, että $\lambda n+\mu m=1$. Merkitään $\alpha=\lambda n$ ja $\beta=\mu m$. Nyt $x^{\alpha m}=1$ ja jos $x^{\alpha t}=1$, niin $mn\mid \alpha t$. Tämän perusteella $m\mid t$, koska $(\alpha,m)=1$. Näin ollen alkiolla x^α on kertaluku m, ja vastaavalla päättelyllä voidaan osoittaa että alkiolla x^β on kertaluku n. Lisäksi $x=x^\alpha x^\beta$, joten alkioiden y ja z olemassaolo on todistettu.

Todistetaan seuraavaksi yksikäsitteisyys. Nyt jos y ja z ovat kuten lauseen oletuksissa, niin $xy=(zy)y=y(zy)=yx$, ja vastaavasti $xz=zx$. Näin ollen x^α ja y kommutoivat keskenään ja samoin x^β ja z kommutoivat keskenään. Koska $x=x^\alpha x^\beta$, niin $y^{-1}x^\alpha=zx^{-\beta}$. Korottamalla molemmat puolet potenssiin n saadaan $(y^{-1}x^\alpha)^n=z^nx^{-\beta n}=1$. Toisaalta $(y^{-1}x^\alpha)^m=y^{-m}x^{\alpha m}=1$. Koska $(m,n)=1$, niin saadaan $y^{-1}x^\alpha=1$ ja $y=x^\alpha$. Näin ollen myös $z=x^\beta$. □

2.3 Joitakin ryhmiin liittyviä tuloksia

Lemma 2.10. *Olkoon G ryhmä ja S ryhmän G epätyhjä osajoukko. Olkoon H ryhmän G aliryhmä. Tällöin konjugaattien hSh^{-1}, missä $h\in H$, lukumäärä on $[H:N_H(S)]=[H:N_G(S)\cap H]$. Erityisesti konjugaatteja gSg^{-1}, missä $g\in G$, on tarkalleen $[G:N_G(S)]$ kappaletta.*

Todistus. Olkoot $h,h_0\in H$. Väite seuraa siitä, että $hSh^{-1}=h_0Sh_0^{-1}$ jos ja vain jos $hN_H(S)=h_0N_H(S)$. Tällöin kuvaus $hSh^{-1}\mapsto hN_H(S)$ on hyvin määritelty bijektio konjugaattien hSh^{-1} joukosta sivuluokkien $hN_H(S)$ joukkoon. □

Jos $S\subseteq G$ on ryhmän G epätyhjä osajoukko, niin joukon S generoimasta aliryhmästä käytetään merkintää $\langle S\rangle$. Tässä $\langle S\rangle$ on siis suppein ryhmän G aliryhmä, joka sisältää joukon S. Jos $S=\{x_1,x_2,\ldots\}$, niin usein merkitään myös $\langle S\rangle=\langle x_1,x_2,\ldots\rangle$.

Lemma 2.11. *Olkoon G ryhmä ja $S\subseteq G$ epätyhjä osajoukko. Tällöin*

$$\langle S\rangle=\{s_1s_2\ldots s_t : s_i\in S \text{ kaikilla } i\}.$$

Todistus. Koska $\langle S \rangle$ sisältää joukon S ja on suljettu ryhmäoperaation suhteen, sen täytyy sisältää kaikki tulot $s_1 s_2 \dots s_t$. Riittää siis osoittaa, että yhtälön oikealla puolella oleva joukko on aliryhmä. Olkoot $s_1 s_2 \dots s_t$ ja $s'_1 s'_2 \dots s'_{t'}$ tuloja tästä joukosta. Tällöin $s_1 s_2 \dots s_t s'_1 s'_2 \dots s'_{t'}$ sisältyy selvästi joukkoon. □

Huomaa, että tässä ryhmän G äärellisyyttä käytetään olennaisesti hyväksi. Yleisessä tapauksessa tuloissa pitää sallia alkioiden s_i lisäksi niiden käänteisalkiot s_i^{-1}.

Lemma 2.12. *Olkoon G ryhmä ja $(|G|, n) = 1$. Tällöin kuvaus $g \mapsto g^n$ on bijektio $G \to G$.*

Todistus. Nyt $\lambda|G| + \mu n = 1$ kokonaisluvuilla λ ja μ, joten $g = g^{\lambda|G|+\mu n} = g^{\mu n}$ koska $g^{|G|} = 1$. Näin ollen kuvaus on surjektio. Jos $g^n = h^n$, niin $g^{\mu n} = h^{\mu n}$ eli $g = g^{\mu n} = h^{\mu n} = h$. Määritelty kuvaus on siis myös injektio. □

Lemma 2.13. *Olkoon $H < G$ ja $[G : H] = n$. Tällöin on olemassa homomorfismi $\phi : G \to \mathrm{Sym}(n)$, jolle $\mathrm{Ker}(\phi) = \cap_{g \in G} g H g^{-1}$.*

Todistus. Olkoon C aliryhmän H vasempien sivuluokkien joukko ryhmässä G. Tällöin joukon C permutaatioiden muodostama ryhmä $\mathrm{Sym}(C)$ on isomorfinen ryhmän $\mathrm{Sym}(n)$ kanssa, joten riittää osoittaa, että on olemassa homomorfismi $\phi : G \to \mathrm{Sym}(C)$, jolle $\mathrm{Ker}(\phi) = \cap_{x \in G} x H x^{-1}$.

Määritellään kuvaus $f_g : C \to C$ ehdolla $xH \mapsto gxH$. Tällöin $xH = yH$ jos ja vain jos $gxH = gyH$, joten f_g on hyvin määritelty injektio. Kuvaus f_g on myös surjektio, sillä $xH = g(g^{-1}xH)$. Näin ollen $f_g \in \mathrm{Sym}(C)$. Lisäksi $f_g f_h = f_{gh}$, joten kuvaus $\phi : G \to \mathrm{Sym}(C)$, missä $\phi(g) = f_g$, on homomorfismi. Nyt f_g on identiteettikuvaus jos ja vain jos $gxH = xH$ kaikilla $x \in G$, eli jos ja vain jos $x^{-1}gx \in H$ kaikilla $x \in G$. Tämä pätee jos ja vain jos $g \in xHx^{-1}$ kaikilla $x \in G$, joten $\mathrm{Ker}(\phi) = \cap_{x \in G} x H x^{-1}$. □

Jos G on yksinkertainen ryhmä ja $H < G$ sekä $[G : H] = n$, niin lemman 2.13 kuvaukselle ϕ pätee $\mathrm{Ker}(\phi) = \{1\}$. Tällöin ϕ on upotuskuvaus, eli G on isomorfinen ryhmän $\mathrm{Sym}(n)$ jonkin aliryhmän kanssa.

Olkoon p alkuluku ja G ryhmä, jonka kertaluku on jaollinen luvulla p. Olkoon p^n suurin alkuluvun p potenssi joka jakaa ryhmän G kertaluvun. Jos $P \leq G$ ja $|P| = p^n$, niin sanotaan, että P on ryhmän G *Sylowin p-aliryhmä*. Emme todista Sylowin lauseita tässä tutkielmassa, tarvittaessa todistukset löytyvät esimerkiksi lähteestä [4, Theorem 4.12, 4.17, s.73-81] tai [5, Theorem 5.9, s. 91].

Lause 2.14. *Olkoon G ryhmä ja p alkuluku. Oletetaan lisäksi, että $p^k \mid |G|$. Tällöin*

(i) Ryhmällä G on kertalukua p^k oleva aliryhmä,

(ii) Ryhmän G Sylowin p-aliryhmät ovat toistensa konjugaatteja,

(iii) Ryhmän G kertalukua p^k olevien aliryhmien lukumäärä on $\equiv 1 \mod p$.

Jos ryhmän kertaluku on alkuluku, niin ryhmä on syklinen. Näin ollen kohdasta (i) seuraa tapauksessa $k = 1$ Cauchyn lause: jos p on alkuluku ja $p \mid |G|$, niin ryhmällä G on kertalukua p oleva alkio. Lisäksi kohdan (ii) nojalla ryhmällä G on tarkalleen yksi Sylowin p-aliryhmä jos ja vain jos ryhmällä G on ainakin yksi normaali Sylowin p-aliryhmä. Seuraavat tulokset ovat usein hyödyllisiä Sylowin lauseita soveltaessa. Jatkossa *p-ryhmä* tarkoittaa ryhmää, jonka kertaluku on muotoa p^k.

Lemma 2.15. *Olkoon G ryhmä. Tällöin*

(i) Jos $H \leq G$ on p-ryhmä, niin $H \leq P$, missä P on jonkin ryhmän G Sylowin p-aliryhmä.

(ii) Jos $H \leq G$ on p-ryhmä ja P on ryhmän G jokin Sylowin p-aliryhmä, niin $H \leq N_G(P)$ jos ja vain jos $H \leq P$.

(iii) Jos P_1 ja P_2 ovat ryhmän G Sylowin p-aliryhmiä, niin konjugaattien xP_2x^{-1}, missä $x \in P_1$, lukumäärä on $[P_1 : P_1 \cap P_2]$.

Todistus. (i) on usein osa Sylowin lauseiden todistusta, katso esimerkiksi [5, Theorem 5.9, s. 91].

(ii) Jos $H \leq P$, niin $H \leq N_G(P)$ koska $P \leq N_G(P)$. Olkoon $H \leq N_G(P)$. Nyt P on ryhmän $N_G(P)$ normaali aliryhmä, joten P on ryhmän $N_G(P)$ ainoa Sylowin p-aliryhmä, ja täten kohdan (i) nojalla $H \leq P$.

(iii) Lemman 2.10 nojalla riittää osoittaa, että $N_{P_1}(P_2) = P_1 \cap N_G(P_2) = P_1 \cap P_2$. Koska $P_2 \leq N_G(P_2)$, niin $P_1 \cap P_2 \leq P_1 \cap N_G(P_2)$. Koska $P_1 \cap N_G(P_2)$ on p-ryhmä ja sisältyy aliryhmään $N_G(P_2)$, niin kohdan (ii) nojalla $P_1 \cap N_G(P_2) \leq P_2$. Koska $P_1 \cap N_G(P_2)$ sisältyy myös aliryhmään P_1, niin $P_1 \cap N_G(P_2) \leq P_1 \cap P_2$.

□

Seuraavan lauseen todistus löytyy esimerkiksi lähteestä [4, Theorem 5.33, s.115]

Lause 2.16 (Normalisoijaehto)**.** *Olkoon G kertalukua p^n oleva ryhmä, missä p on alkuluku. Tällöin jos $H < G$, niin $H < N_G(H)$. Näin ollen jos $[G : H] = p$, niin $G = N_G(H)$ ja H on normaali ryhmässä G.*

Määritelmä 2.17. Olkoot H ja K ryhmän G aliryhmiä. Olkoon lisäksi x jokin ryhmän G alkio. Tällöin aliryhmien H ja K sekä alkion x määräämä *kaksoissivuluokka* on joukko

$$HxK = \{hxk : h \in H, k \in K\}.$$

Kuten vasempien ja oikeiden sivuluokkien tapauksessa, eri kaksoissivuluokat ovat keskenään pistevieraita ja peittävät koko ryhmän G. Tämä nähdään esimerkiksi seuraavalla tavalla. Määritellään relaatio $\sim$ ryhmässä G asettamalla $x \sim y$ jos ja vain jos $x \in HyK$. Tällöin $\sim$ on ekvivalenssirelaatio jonka ekvivalenssiluokat ovat tarkalleen kaikki kaksoissivuluokat HxK, joten väite pätee. Kaksoissivuluokan HxK kertaluku on

$$|HxK| = |(x^{-1}Hx)K| = \frac{|x^{-1}Hx||K|}{|x^{-1}Hx \cap K|} = \frac{|H||K|}{|x^{-1}Hx \cap K|}.$$

Näin ollen eri kaksoissivuluokissa voi olla eri määrä alkioita, sillä yleensä ei päde $|x^{-1}Hx \cap K| = |y^{-1}Hy \cap K|$.

Seuraava lause on tärkeä, mutta sen todistus on pitkä ja vaatii paljon teoriaa. Sivuutamme todistuksen tässä tutkielmassa, todistus löytyy esimerkiksi lähteistä [4, s.190, Theorem 7.41] ja [5, s.251, Theorem 10.30].

Lause 2.18. *(Schur-Zassenhausin lause) Olkoon G ryhmä ja $N \trianglelefteq G$ sellainen, että $(|N|, [G : N]) = 1$. Tällöin ryhmällä G on kertalukua $[G : N]$ oleva aliryhmä.*

2.4 Ratkeavista ryhmistä

Olkoot a ja b ryhmän G alkioita. Tällöin alkioiden a ja b *kommutaattori* on alkio $a^{-1}b^{-1}ab$, josta käytetään merkintää $[a, b]$. Määritellään, että ryhmän G *kommutaattorialiryhmä* on kommutaattorien $[a, b]$ generoima aliryhmä, merkitään $G' = [G, G] = \langle [a, b] : a, b \in G \rangle$. Induktiivisesti määritellään $G^{(0)} = G$ ja $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ kaikilla $i \geq 1$.

Lemma 2.19. *Aliryhmä $G^{(k)}$ on karakteristinen aliryhmä kaikilla $k \geq 1$.*

Todistus. Olkoon $f : G \to L$ homomorfismi. Osoitetaan seuraavaksi, että $f(G^{(k)}) = f(G)^{(k)}$. Nyt $f([a, b]) = [f(a), f(b)]$, joten $f([G, G]) = [f(G), f(G)]$. Näin ollen $f(G^{(1)}) = f(G)^{(1)}$. Jos $f(G^{(k)}) = f(G)^{(k)}$, niin tällöin

$$f(G^{(k+1)}) = f([G^{(k)}, G^{(k)}]) = [f(G^{(k)}), f(G^{(k)})] = [f(G)^{(k)}, f(G)^{(k)}]$$

eli $f(G^{(k+1)}) = f(G)^{(k+1)}$. Näin ollen jos $f : G \to G$ on automorfismi, niin $f(G^{(k)}) = f(G)^{(k)} = G^{(k)}$ koska f on surjektio. Siispä $G^{(k)} \operatorname{char} G$ kaikilla $k \geq 1$. □

Määritelmä 2.20. Jos $G^{(k)} = \{1\}$ jollakin $k \in \mathbb{N}$, niin ryhmä G on *ratkeava*.

Ratkeavia ryhmiä ovat esimerkiksi kaikki Abelin ryhmät, sillä $G' = \{1\}$ jos ja vain jos G on Abelin ryhmä. Symmetrinen ryhmä $\mathrm{Sym}(n)$ ei ole ratkeava kun $n \geq 5$, mutta $\mathrm{Sym}(3)$ ja $\mathrm{Sym}(4)$ ovat ratkeavia. Lemman 2.19 nojalla jos G on ei-kommutatiivinen yksinkertainen ryhmä, niin $G' = G$ ja G ei ole ratkeava. Jos G on ratkeava ja yksinkertainen, niin $G \cong \mathbb{Z}_p$, missä p on jokin alkuluku.

Lemma 2.21. *Ratkeavan ryhmän aliryhmät ja tekijäryhmät ovat ratkeavia.*

Todistus. Induktiolla nähdään, että $H^{(k)} \leq G^{(k)}$ kaikilla k. Näin ollen jos $G^{(k)} = \{1\}$, niin myös $H^{(k)} = \{1\}$ ja H on ratkeava.

Lemman 2.19 todistuksen perusteella jos $f : G \to G/N$ on luonnollinen homomorfismi $g \mapsto gN$, niin $f(G^{(k)}) = f(G)^{(k)}$. Toisin sanoen $G^{(k)}N/N = (G/N)^{(k)}$. Jos $G^{(k)} = \{1\}$, niin

$$(G/N)^{(k)} = G^{(k)}N/N = N/N = \{1_{G/N}\}$$

ja G/N on ratkeava. □

Lemma 2.22. *Jos N on ryhmän G normaali aliryhmä ja N sekä G/N ovat ratkeavia, niin myös G on ratkeava.*

Todistus. Jos N ja G/N ovat ratkeavia, niin $G^{(k)}N/N = (G/N)^{(k)} = \{1_{G/N}\}$ jollain k. Näin ollen $G^{(k)} \leq N$. Koska $N^{(l)} = \{1\}$ jollain l, niin $G^{(k+l)} = (G^{(k)})^{(l)} \leq N^{(l)}$. Siispä $G^{(k+l)} = \{1\}$. □

Määritelmä 2.23. Olkoon G ryhmä. Sanotaan, että ryhmän G normaali aliryhmä N on *minimaalinen normaali aliryhmä*, jos $N \neq 1$ ja ehdosta $H \leq N$, $H \triangleleft G$ seuraa $H = 1$ tai $H = N$.

Lemma 2.24. *Jos $H \operatorname{char} N \trianglelefteq G$, niin tällöin $H \trianglelefteq G$.*

Todistus. Olkoon $g \in G$. Koska N on normaali aliryhmä, niin $gNg^{-1} = N$ ja siten kuvaus $x \mapsto gxg^{-1}$ on ryhmän N automorfismi. Näin ollen se kuvaa aliryhmän H itselleen, eli toisin sanoen $gHg^{-1} = H$. □

Lemma 2.25. *Olkoon G ratkeava ryhmä. Jos N on ryhmän G minimaalinen normaali aliryhmä, niin $|N| = p^k$ on alkuluvun potenssi ja N on Abelin ryhmä. Lisäksi $x^p = 1$ kaikilla $x \in N$.*

Todistus. Nyt $N' \operatorname{char} N \trianglelefteq G$, joten lemman 2.24 nojalla $N' \trianglelefteq G$. Koska N on minimaalinen normaali aliryhmä, niin $N' = \{1\}$ tai $N' = N$. Ryhmän G ratkeavuuden nojalla N on ratkeava, joten $N' = \{1\}$. Näin ollen N on Abelin

ryhmä. Olkoon p luvun $|N|$ alkulukutekijä. Jos P on ryhmän N Sylowin p-aliryhmä, niin $P \trianglelefteq N$ koska N on Abelin ryhmä ja näin ollen $P \operatorname{char} N$. Kuten edellä, aliryhmän N minimaalisuuden nojalla $P = N$ ja $|N| = p^k$. Koska N on Abelin ryhmä, niin joukko $T = \{x \in N : x^p = 1\}$ on ryhmän N aliryhmä. Lisäksi T on karakteristinen aliryhmä, joten edelleen aliryhmän N minimaalisuuden nojalla $T = N$. Tässä $T \neq \{1\}$ koska Cauchyn lauseen nojalla ryhmässä N on kertalukua p oleva alkio. □

Lause 2.26 (P. Hall, 1928)**.** *Olkoon G ratkeava ryhmä jonka kertaluku $|G| = ab$, missä $(a, b) = 1$. Tällöin ryhmällä G on kertalukua a oleva aliryhmä.*

Todistus. Induktiolla ryhmän G kertaluvun $|G|$ suhteen. Tapaus $|G| = 1$ on triviaali, joten oletetaan, että väite pätee kaikille ratkeaville ryhmille joiden kertaluku on $< |G|$. Olkoon $N \trianglelefteq G$ minimaalinen normaali aliryhmä. Tälläinen aliryhmä on aina olemassa, sillä voidaan esimerkiksi valita normaali aliryhmä $N \neq 1$ jonka kertaluku on pienin mahdollinen. Lemman 2.25 nojalla $|N| = p^k$, missä p on alkuluku ja $k \geq 1$.

Jos $p \mid a$, niin tällöin $p^k \mid a$ ehdon $(a, b) = 1$ nojalla. Nyt $|G/N| = \frac{a}{p^k} b < ab$, joten voidaan soveltaa induktio-oletusta ryhmään G/N. Näin ollen ryhmällä G/N on kertalukua $\frac{a}{p^k}$ oleva aliryhmä H/N, jolloin H on kertalukua a oleva aliryhmä.

Jos $p \nmid a$, niin tällöin $p^k \mid b$. Kuten edellä, G/N on kertalukua $a\frac{b}{p^k}$ oleva ryhmä, jolla induktio-oletuksen nojalla on kertalukua a oleva aliryhmä H/N. Tällöin aliryhmän H kertaluku on ap^k. Jos $ap^k < ab$, niin aliryhmä H sisältää kertalukua a olevan aliryhmän. Voidaan siis olettaa, että $b = p^k$. Tällöin N on kertalukua b oleva normaali aliryhmä ja näin ollen $(|N|, [G : N]) = 1$. Schur-Zassenhausin lauseen nojalla (2.18) ryhmällä G on kertalukua $[G : N] = a$ oleva aliryhmä. □

3 Frobeniuksen lause

Todistamme tässä luvussa Frobeniuksen lauseen, jonka mukaan jos n on positiivinen kokonaisluku, niin yhtälön $X^n = 1$ ratkaisujen lukumäärä ryhmässä G on luvun $(n, |G|)$ monikerta. Lause saa nimensä Georg Frobeniukselta, joka todisti sen vuonna 1895. Frobenius löysi tulokselleen useita sovelluksia, joista tunnetuin on luultavasti eräs Sylowin lauseen yleistys (kts. luku 7). 1900-luvun alkupuolella lausetta pidettiin tärkeänä[2], mutta nykyään Frobeniuksen lause ei kuitenkaan ole kovin tunnettu tulos. Frobeniuksen lause esiintyy vanhoissa ryhmäteorian oppikirjoissa (esim. [2, Theorem VII, s. 110-112] [3, §32, s. 77-81]), mutta käytännössä mikään uudempi algebran oppikirja ei käsittele Frobeniuksen lausetta. Nykyiset oppikirjat todistavat Frobeniuksen lauseen seuraukset työkaluilla, jotka toimivat yleisemmin ja sopivat paremmin muuhun ryhmäteoriaan. Esimerkiksi lauseesta seuraavat ryhmien ratkeavuuteen liittyvät tulokset voidaan usein todistaa myös siirtohomomorfismiin (engl. transfer homomorphism) liittyvän teorian avulla. Lisäksi lauseen todistus vaatii aina melko pitkän käsittelyn tai vaihtoehtoisesti paljon muuta teoriaa. Finkelsteinin [6, s. 188] mielestä syynä kiinnostuksen vähenemiseen on myös se, että Frobeniuksen lause sijoittuu puhtaan ryhmäteorian sijaan jonnekin kombinatoriikan, lukuteorian ja ryhmäteorian välimaastoon. Frobeniuksen työn merkitystä ei voi kuitenkaan vähätellä, sillä Frobeniuksen lause on motivoinut paljon erilaisia ongelmia ja on tärkeä lähtökohta yleisempiä yhtälöitä tutkittaessa.

Abelin ryhmille Frobeniuksen lause nähdään suhteellisen helposti seuraavalla tavalla. Jos alkuluvun potenssi p^k jakaa luvun $(n, |G|)$, niin Sylowin lauseen nojalla ryhmästä G löytyy kertalukua p^k oleva aliryhmä. Koska ehdosta $x^{p^k} = 1$ seuraa $x^n = 1$, niin tämä aliryhmä sisältyy ratkaisujen joukkoon. Jos G on Abelin ryhmä, niin ratkaisujen joukko muodostaa aliryhmän ja tällöin Lagrangen lauseen nojalla ratkaisujen lukumäärä on siis luvun p^k monikerta. Koska tämä pätee millä tahansa alkuluvun potenssilla joka jakaa luvun $(n, |G|)$, niin ratkaisujen lukumäärä on luvun $(n, |G|)$ monikerta. Entä jos G ei ole Abelin ryhmä? Tällöin ratkaisujen joukko ei yleensä muodosta aliryhmää, joten vastaavanlainen argumentti ei enää toimi. Ei myöskään vaikuta millään tapaa ilmeiseltä, että ratkaisujen joukko jakautuisi $(n, |G|)$ yhtä suureen osaan[3].

Heti ensisilmäykseltä tulos vaikuttaa siis hieman erikoiselta ja yllättäväl-

[2]Frobenius kirjoitti kaksi artikkelia lauseensa yleistyksistä otsikolla *Über einen Fundamentalsatz der Gruppentheorie* [11]. G. A. Miller [3, §32, s.77] kuvaili vuonna 1905 Frobeniuksen lausetta "erittäin keskeiseksi lauseeksi".

[3]Jos n on alkuluvun potenssi, niin tämä onnistuu kappaleessa 4.2 esiteltävän ekvivalenssirelaation avulla.

tä. Frobeniuksen lause pätee kyllä mille tahansa ryhmälle, mutta sen todistaminen on aina hieman monimutkaista. Marshall Hall [1, 9.1, s. 136] toteaa, että Frobeniuksen lause on "luonteeltaan täysin erilainen kuin suurin osa muista ryhmäteorian tuloksista". Frobeniuksen tulos ei liity aliryhmiin, homomorfismeihin tai muihin ryhmäteoreettisiin rakenteisiin, vaan tarkastelun kohteena on ryhmän osajoukko, jolla ei yleensä ole ryhmärakennetta lainkaan. Tässä on varmasti yksi syy sille, miksi Frobeniuksen lauseen todistaminen ei ole helppoa.

Olkoon G ryhmä, S ryhmän G osajoukko ja n kokonaisluku. Merkitään

$$A_n(S) = \{x \in S : x^n = 1\}$$
$$a_n(S) = |A_n(S)|$$

Tässä siis $A_n(G)$ on yhtälön $X^n = 1$ ratkaisujen joukko ja $a_n(G)$ on ratkaisujen lukumäärä ryhmässä G.

Lemma 3.1. *Olkoon H ryhmän G aliryhmä ja $g \in G$. Tällöin $A_n(gHg^{-1}) = gA_n(H)g^{-1}$, joten $a_n(gHg^{-1}) = a_n(H)$.*

Todistus. Väite seuraa siitä, että $(ghg^{-1})^n = gh^ng^{-1}$ kaikilla kokonaisluvuilla n. □

Seuraava lemma on tärkeä Frobeniuksen lauseen todistuksen kannalta. Sen nojalla yhtälön $X^n = 1$ ratkaisujen lukumäärä ei muutu kun siirrytään tietynlaiseen tekijäryhmään. Tämä on tietysti hyödyllistä induktiotodistuksessa, jos induktio-oletusta voidaan soveltaa tekijäryhmään.

Lemma 3.2. *Olkoon $N \leq Z(G)$ ja $(|N|, s) = 1$. Tällöin*

$$a_s(G) = a_s(G/N).$$

Todistus. Olkoon $aN \in A_s(G/N)$. Tällöin $a^s \in N$, joten $(a^{|N|})^s = 1$, eli $a^{|N|} \in A_s(G)$. Nyt jos $aN = bN$, niin $a = bn$, missä $n \in N$. Koska $N \leq Z(G)$, niin $a^{|N|} = b^{|N|}n^{|N|} = b^{|N|}$. Näin ollen voidaan määritellä kuvaus $f : A_s(G/N) \to A_s(G)$, missä $aN \mapsto a^{|N|}$. Olkoon $aN, bN \in A_s(G/N)$ ja $a^{|N|} = b^{|N|}$. Tällöin $(aN)^{|N|} = (bN)^{|N|}$ ja $(aN)^s = (bN)^s = N$, joten oletuksen $(|N|, s) = 1$ nojalla $aN = bN$. Kuvaus f on siis injektio. Koska $(|N|, s) = 1$, niin $x|N| + ys$ joillekin kokonaisluvuille x ja y. Näin ollen jos $a^s = 1$, niin $a = a^{x|N|+ys} = (a^x)^{|N|}$. Lisäksi $(a^xN)^s = (a^sN)^x = N$, joten $a = f(a^xN)$. Kuvaus f on siis bijektio ja väite on todistettu. □

Lemma 3.3. *Ryhmässä G kertalukua n olevien alkioiden lukumäärä on luvun $\varphi(n)$ monikerta.*

Todistus. Jokaisella kertalukua n olevalla syklisellä ryhmällä on tarkalleen $\varphi(n)$ generoivaa alkiota. Näin ollen jos k on kertalukua n olevien syklisten ryhmien lukumäärä ryhmässä G, niin ryhmässä G on tarkalleen $k \cdot \varphi(n)$ kertalukua n olevaa alkiota. □

Frobeniuksen lauseen todistuksessa käytämme ensin induktiota ryhmän G kertaluvun $|G|$ suhteen. Tämän jälkeen todistamme lauseen kaikille luvun $|G|$ tekijöille n käymällä tekijät läpi suuruusjärjestyksessä suurimmasta pienimpään. Lähtökohtana on siis tapaus $n = |G|$, jolle lause on helppo osoittaa. Todistustekniikkaa voi kuvailla induktioksi alaspäin (luvusta $|G|$ lukuun 1) luvun n suhteen. Tämän voi ajatella myös tavalliseksi induktioksi luvun $|G|/n$ suhteen, jossa aloitetaan tapauksesta $|G|/n = 1$. Seuraava lemma on hyödyllinen, sillä sen avulla päästään käsiksi suuremmista tekijöistä pienempiin. Jatkossa tullaan huomaamaan, että sama idea toimii monessa Frobeniuksen lauseeseen liittyvässä tuloksessa (kts. lemma 5.9 ja sen seuraukset, lause 7.1).

Lemma 3.4. *Olkoon G ryhmä, p alkuluku ja $n = p^\lambda r$, missä $p \nmid r$. Oletetaan lisäksi, että np jakaa ryhmän G kertaluvun $|G|$. Olkoon $T = A_{np}(G) - A_n(G)$. Tällöin $\varphi(p^{\lambda+1}) = p^\lambda(p-1)$ jakaa luvun $|T|$.*

Todistus. Nyt jos $x \in T$, niin $x^{np} = 1$ ja $x^n \neq 1$. Näin ollen $|x| \mid np$ ja $|x| \nmid n$, joten $p^{\lambda+1} \mid |x|$. Siispä $|x| = p^{\lambda+1}d$, missä $d \mid r$. Lisäksi jokainen alkio, jonka kertaluku on tätä muotoa kuuluu joukkoon T. Näin ollen joukko T saadaan erillisenä yhdisteenä

$$T = \bigcup_{d|r} \{x \in G : |x| = p^{\lambda+1}d\}.$$

Nyt lemman 3.3 nojalla jokaisen yhdistessä esiintyvän joukon kertaluku on jaollinen luvulla $\varphi(p^{\lambda+1}d) = \varphi(p^{\lambda+1})\varphi(d)$, sillä $(p, d) = 1$. Siispä yhdisteessä esiintyvien joukkojen kertaluvut ovat jaollisia luvulla $\varphi(p^{\lambda+1})$. Koska yhdiste on erillinen, niin $\varphi(p^{\lambda+1})$ jakaa luvun $|T|$. □

Lemma 3.5. *Olkoon G ryhmä ja n kokonaisluku. Tällöin $A_n(G) = A_{(n,|G|)}(G)$.*

Todistus. Väite seuraa siitä, että $x^n = 1$ jos ja vain jos $x^{(n,|G|)} = 1$. Jos $x^n = 1$, niin $|x|$ jakaa luvun n. Koska alkion kertaluku jakaa ryhmän kertaluvun, niin $|x|$ jakaa luvun $(n, |G|)$ ja näin ollen $x^{(n,|G|)} = 1$. Jos taas $x^{(n,|G|)} = 1$, niin $x^n = 1$ koska $(n, |G|)$ on luvun n tekijä. □

Huomaa, että lemman 3.5 nojalla yhtälön $X^n = 1$ ratkaisujen tarkastelu palautuu tapaukseen, jossa n on luvun $|G|$ tekijä.

Näiden aputulosten jälkeen voidaan siirtyä itse todistukseen. Todistuksen idea on sama kuin Frobeniuksen alkuperäisessä todistuksessa [10], josta omia versioitaan ovat esittäneet muun muassa Burnside [2, Theorem VII, s. 110-112] ja Miller [3, §32, s. 77-81]. Frobeniuksen lause voidaan todistaa myös esitysteorian avulla. Erilaisen todistuksen on esittänyt Brauer [8], jonka todistus perustuu tiettyjen ekvivalenssirelaatioiden käyttöön. Perehdymme Brauerin todistukseen kappaleessa 4.2 ja todistamme sen avulla Frobeniuksen lauseen yleistyksen.

Lause 3.6 (G. Frobenius, 1895)**.** *Olkoon G äärellinen ryhmä ja n positiivinen kokonaisluku. Tällöin ryhmässä G yhtälön $X^n = 1$ ratkaisujen lukumäärä on luvun $(n, |G|)$ monikerta.*

Todistus. Lemman 3.5 nojalla voidaan olettaa, että n jakaa luvun $|G|$. Nyt täytyy siis osoittaa, että n jakaa luvun $a_n(G)$. Todistetaan väite induktiolla ryhmän G kertaluvun ja luvun n suhteen. Tapaukset $|G| = 1$ ja $n = |G|$ ovat triviaaleja. Oletetaan, että väite on todistettu kaikille ryhmille joiden kertaluku on pienempi kuin $|G|$ ja kaikille luvun $|G|$ tekijöille jotka ovat suurempia kuin n.

Olkoon p jokin luvun $|G|/n$ alkulukutekijä. Induktion nojalla np jakaa luvun $a_{np}(G)$, joten n jakaa luvun $a_{np}(G)$. Olkoon $T = A_{np}(G) - A_n(G)$. Nyt $|T| = a_{np}(G) - a_n(G)$, joten riittää osoittaa, että n jakaa luvun $|T|$. Tällöin n jakaa myös luvun $a_n(G) = a_{np}(G) - |T|$.

Olkoon p^λ suurin alkuluvun p potenssi joka jakaa luvun n. Siis $n = p^\lambda r$, missä $p \nmid r$. Lemman 3.4 nojalla $|T|$ on jaollinen luvulla $\varphi(p^{\lambda+1}) = p^\lambda(p-1)$ ja siten jaollinen luvulla p^λ.

Nyt $(p^\lambda, r) = 1$, joten riittää osoittaa, että r jakaa luvun $|T|$. Lemman 3.4 todistuksessa osoitettiin, että joukko T on muotoa

$$T = \bigcup_{d|r} \{x \in G : |x| = p^{\lambda+1}d\}.$$

Näin ollen jokaisella joukon T alkiolla x on yksikäsitteinen esitys muotoa $x = yz = zy$, missä $|y| = p^{\lambda+1}$ ja $|z| \mid r$ (lemma 2.9). Siispä joukon T kertaluku on yhdisteen

$$\bigcup_{|y|=p^{\lambda+1}} \{z \in C_G(y) : |z| \mid r\}$$

kertaluku. Olkoon D edustajien joukko niille konjugointiluokille, joissa alkioiden kertaluku on $p^{\lambda+1}$. Koska $C_G(gyg^{-1}) = gC_G(y)g^{-1}$ kaikilla $g \in G$, niin lemman 3.1 nojalla saadaan yllä olevan yhdisteen kertaluvuksi

$$\sum_{y \in D} [G : C_G(y)] a_r(C_G(y)).$$

Näin ollen riittää osoittaa, että jokainen summan termi on jaollinen luvulla r. Olkoon $y \in D$ ja aliryhmän $C_G(y)$ kertaluku $p^{\lambda+1}s$. Nyt

$$a_r(C_G(y)) = a_{(r,s)}(C_G(y))$$

koska $p \nmid r$. Koska $\langle y \rangle$ kuuluu ryhmän $C_G(y)$ keskukseen ja $(|\langle y \rangle|, (r,s)) = 1$, niin lemman 3.2 nojalla

$$a_{(r,s)}(C_G(y)) = a_{(r,s)}(C_G(y)/\langle y \rangle).$$

Nyt ryhmän $C_G(y)/\langle y \rangle$ kertaluku on pienempi kuin $|G|$, joten induktio-oletuksen nojalla (r,s) jakaa luvun $a_r(C_G(y))$. Koska $|G|$ on jaollinen luvuilla r ja s, se on jaollinen niiden pienimmällä yhteisellä jaettavalla $\frac{rs}{(r,s)}$. Näin ollen $[G : C_G(y)]a_r(C_G(y))$ on jaollinen luvulla r.

□

Koska neutraalialkio toteuttaa aina yhtälön $X^n = 1$, niin ratkaisuja on ainakin $(n, |G|)$ kappaletta. Huomaa, että Cauchyn lausetta ei tarvita todistuksessa missään vaiheessa. Näin ollen seurauksena saadaan

Seuraus 3.7 (Cauchyn lause)**.** *Olkoon G ryhmä ja alkuluku p luvun $|G|$ tekijä. Tällöin ryhmässä G on kertalukua p oleva alkio.*

Todistus. Frobeniuksen lauseen nojalla $a_p(G)$ on luvun p monikerta. Koska neutraalialkio toteuttaa aina yhtälön $X^p = 1$, niin $a_p(G) \geq p$. Näin ollen löytyy alkio $x \neq 1$ ryhmästä G jolle $x^p = 1$. □

4 Frobeniuksen lauseen yleistyksiä

Tarkastelemme tässä luvussa joitakin Frobeniuksen lauseen yleistyksiä. Yksi tapa yleistää Frobeniuksen lausetta on tarkastella yhtälön $X^n = 1$ sijaan yleisempiä yhtälöitä. Tutkimme kappaleessa 4.1 yhtälöä $X^n = c$ ja lisäksi kappaleessa 4.3 esitämme Philip Hallin sanayhtälöihin liittyvät tulokset (ilman todistuksia). Toisaalta voidaan myös tutkia sitä, miten paljon ratkaisuja sijoittuu tiettyyn ryhmän osajoukkoon. Kappaleessa 4.2 tutkimme ratkaisujen lukumäärää kaksoissivuluokissa.

Kappaleissa 4.1 ja 4.2 esitettävien yleistyksien todistuksissa ei käytetä Frobeniuksen lausetta ja todistukset eivät riipu toisistaan, joten näin saadaan kaksi uutta todistusta Frobeniuksen lauseelle.

4.1 Yhtälö $X^n = c$

Olkoon G jokin ryhmä ja c jokin ryhmän G alkio. Luonnollinen tapa yleistää Frobeniuksen lausetta on tutkia yhtälön $X^n = c$ ratkaisuja ryhmässä G. Tälle yhtälölle saadaan vastaavanlainen tulos kuin Frobeniuksen lausessa: ratkaisujen lukumäärä on luvun $(n, |C_G(c)|)$ monikerta. Otamme käyttöön seuraavat merkinnät.

$$A_n(G, c) = \{x \in G : x^n = c\}$$
$$a_n(G, c) = |A_n(G, c)|$$

Tässä $A_n(G, c)$ on siis yhtälön $X^n = c$ ratkaisujen joukko ryhmässä G ja $a_n(G, c)$ on ratkaisujen lukumäärä ryhmässä G.

Lemma 4.1. *Olkoot g ja c ryhmän G alkioita ja n positiivinen kokonaisluku. Tällöin $A_n(G, gcg^{-1}) = gA_n(G, c)g^{-1}$, joten $a_n(G, gcg^{-1}) = a_n(G, c)$.*

Todistus. Kuten aiemmin, väite seuraa siitä, että $(gxg^{-1})^n = gx^ng^{-1}$. □

Lemma 4.2. *Olkoon p alkuluku ja $x^{p^u} = c$, missä $p \mid |c|$. Tällöin $|x| = p^u|c|$.*

Todistus. Nyt lemman 2.5 nojalla $|x^{p^u}| = \frac{|x|}{(|x|, p^u)}$, joten $|x| = (|x|, p^u)|c|$. Näin ollen riittää osoittaa, että $p^u \mid |x|$. Olkoon p^k suurin alkuluvun p potenssi joka jakaa luvun $|x|$. Jos $k < u$, niin tällöin $|x| = p^k|c|$. Koska $p \mid |c|$, niin $p^{k+1} \mid |x|$, mikä on ristiriita. Näin ollen $k \geq u$ mistä $p^u \mid |x|$ seuraa. □

Tässä esitettävä Frobeniuksen lauseen yleistyksen todistus ei riipu aiemmin esitetystä Frobeniuksen lauseen todistuksesta, mutta tällä kertaa Cauchyn lause on tarpeellinen. Frobeniuksen lause on erikoistapaus $c = 1$. Todistus perustuu Marshall Hallin esitykseen [1, Theorem 9.1.1., s.136-137].

Lause 4.3 (Frobenius, 1903)**.** *Olkoon G ryhmä, $c \in G$ ja n positiivinen kokonaisluku. Tällöin yhtälön $X^n = c$ ratkaisujen lukumäärä on luvun $(n, |C_G(c)|)$ monikerta.*

Todistus. Induktiolla kertaluvun $|G|$ ja luvun n suhteen. Tapaukset $|G| = 1$ ja $n = 1$ ovat helppoja, joten oletetaan että väite pätee kaikille ryhmille joiden kertaluku on $< |G|$ ja kaikille positiivisille kokonaisluvuille jotka ovat $< n$.

Nyt jos $x^n = c$, niin $xc = xx^n = x^n x = cx$, eli $x \in C_G(c)$. Näin ollen kaikki yhtälön $X^n = c$ ratkaisut ovat aliryhmän $C_G(c)$ alkioita. Jos $|C_G(c)| < |G|$, niin induktio-oletuksen nojalla $a_n(G, c)$ on luvun $(n, |C_{C_G(c)}(c)|) = (n, |C_G(c)|)$ monikerta. Jatkossa voidaan siis olettaa $|C_G(c)| = |G|$, eli toisin sanoen $c \in Z(G)$. Seuraavaksi pitää osoittaa, että $a_n(G, c)$ on luvun $(n, |G|)$ monikerta.

Tarkastellaan tapausta $n = n_1 n_2$, missä $(n_1, n_2) = 1$, $n_1 < n$ ja $n_2 < n$. Nyt $x^n = c$ jos ja vain jos $x^{n_1} \in A_{n_2}(G, c)$. Näin ollen $A_n(G, c)$ on erillinen yhdiste

$$A_n(G, c) = \bigcup_{y \in A_{n_2}(G,c)} A_{n_1}(G, y)$$

Koska $c \in Z(G)$, niin $A_{n_2}(G, c)$ on suljettu konjugoinnin suhteen. Siispä $A_{n_2}(G, c)$ joidenkin ryhmän G konjugointiluokkien yhdiste. Olkoon D näiden konjugointiluokkien edustajien joukko. Tällöin lemman 4.1 nojalla

$$a_n(G, c) = \sum_{y \in D} [G : C_G(y)] a_{n_1}(G, y).$$

Induktio-oletuksen ja lemman 2.1 nojalla jokainen summan termi on luvun $[G : C_G(y)](n_1, |C_G(y)|) = (n_1[G : C_G(y)], |G|)$ monikerta. Erityisesti jokainen summan termi on luvun $(n_1, |G|)$ monikerta, joten $a_n(G, c)$ on luvun $(n_1, |G|)$ monikerta. Täysin vastaavalla päättelyllä nähdään, että $a_n(G, c)$ on myös luvun $(n_2, |G|)$ monikerta. Koska $(n_1, n_2) = 1$, niin $a_n(G, c)$ on luvun $(n_1, |G|)(n_2, |G|) = (n_1 n_2, |G|) = (n, |G|)$ monikerta (lemma 2.2).

Näin ollen jatkossa voidaan olettaa, että n ei ole muotoa $n_1 n_2$, missä $(n_1, n_2) = 1$, $n_1 < n$ ja $n_2 < n$. Tämä tarkoittaa sitä, että $n = p^u$ on alkuluvun potenssi.

Jos $p \mid |c|$, niin lemman 4.2 nojalla jokaisella ratkaisulla $x^{p^u} = c$ on kertaluku $|x| = p^u |c|$. Lisäksi alkion x generoimassa syklisessä ryhmässä ratkaisujen määrä on tarkalleen p^u. Tämä nähdään esimerkiksi seuraavasti. Määritellään $f : \langle x \rangle \to \langle x \rangle$ ehdolla $f(x^i) = (x^i)^{p^u}$. Tällöin f on homomorfismi koska $\langle x \rangle$ on Abelin ryhmä. Lisäksi $|\operatorname{Ker}(f)| = p^u$, koska ryhmällä $\langle x \rangle$ on yksikäsitteinen kertalukua p^u oleva aliryhmä. Koska f on homomorfismi ja $f(x) = c$,

niin $f^{-1}(c) = x\,\mathrm{Ker}(f)$. Näin ollen $|f^{-1}(c)| = |\mathrm{Ker}(f)| = p^u$. Koska jokainen ratkaisu generoi kertalukua $p^u|c|$ olevan syklisen aliryhmän joka sisältää tarkalleen p^u ratkaisua, niin ratkaisujen lukumäärä on luvun p^u monikerta.

Voidaan siis olettaa, että $p \nmid |c|$. Olkoon $T = \{x \in Z(G) : p \nmid |x|\}$. Jos $x, y \in T$, niin $(xy)^{|x||y|} = x^{|x||y|}y^{|x||y|} = 1$ jolloin $|xy|$ jakaa luvun $|x||y|$. Tästä seuraa $p \nmid |xy|$, sillä p on alkuluku ja $p \nmid |x|$ sekä $p \nmid |y|$. Näin ollen T on ryhmän G aliryhmä. Lisäksi Cauchyn lauseen nojalla $p \nmid |T|$, sillä muutoin ryhmässä T olisi kertalukua p oleva alkio.

Olkoon $c_1, c_2 \in T$. Koska $(|T|, n) = 1$, niin lemman 2.12 nojalla on olemassa yksikäsitteinen alkio $y \in T$, jolle $c_2^{-1}c_1 = y^n$, eli $c_1 = c_2y^n$. Nyt jos $x^n = c_1$, niin $(xy^{-1})^n = x^ny^{-n} = c_1y^{-n} = c_2$. Tämän perusteella voidaan määritellä kuvaus $f : A_n(G, c_1) \to A_n(G, c_2)$ ehdolla $x \mapsto xy^{-1}$. Kuvaus f on selvästi injektio. Jos $z^n = c_2$, niin $(zy)^n = z^ny^n = c_2y^n = c_1$, joten $f(zy) = z$. Näin ollen f on bijektio ja $a_n(G, c_1) = a_n(G, c_2)$. Koska $c \in T$, niin saadaan

$$|G| = \sum_{y \notin T} a_n(G, y) + \sum_{y \in T} a_n(G, y) = \sum_{y \notin T} a_n(G, y) + |T|a_n(G, c).$$

Koska $Z(G)$ on normaali aliryhmä, niin $Z(G)$ on konjugointiluokkien yhdiste. Näin ollen myös erotus $G - Z(G)$ on konjugointiluokkien yhdiste. Olkoon D joukossa $G - Z(G)$ esiintyvien konjugointiluokkien edustajien joukko. Kuten aiemmin, lemman 4.1 nojalla summa saadaan muotoon

$$\begin{aligned} |G| &= \sum_{y \in Z(G), y \notin T} a_n(G, y) + \sum_{y \notin Z(G)} a_n(G, y) + |T|a_n(G, c) \\ &= \sum_{y \in Z(G), y \notin T} a_n(G, y) + \sum_{y \in D} [G : C_G(y)]a_n(G, y) + |T|a_n(G, c) \end{aligned}$$

Aiempien kohtien perusteella $(n, |G|)$ jakaa kaikki kahdessa summassa esiintyvät termit, joten $(n, |G|)$ jakaa luvun $|T|a_n(G, c)$. Koska $p \nmid |T|$, niin $(n, |G|)$ jakaa luvun $a_n(G, c)$. □

Huomaa, että jos $c \in Z(G)$, niin yhtälön $X^n = c$ ratkaisujen lukumäärä on luvun $(n, |G|)$ monikerta. Eli ryhmän keskuksen alkioiden tapauksessa saadaan yhtä hyvä tulos kuin alkuperäisen yhtälön $X^n = 1$ tapauksessa. Seurauksena saadaan taas yksi Frobeniuksen lauseen yleistys.

Seuraus 4.4 (Frobenius, 1903)**.** *Olkoon G ryhmä, C jokin ryhmän G konjugointiluokka ja n positiivinen kokonaisluku. Tällöin niiden alkioiden lukumäärä, joilla $x^n \in C$ on luvun $(|C|n, |G|)$ monikerta.*

Todistus. Olkoon $c \in C$, jolloin $|C| = [G : C_G(c)]$. Lemman 4.1 nojalla alkioita joille $x^n \in C$ on tarkalleen $|C|a_n(G, c)$ kappaletta. Lauseen 4.3 nojalla tämä lukumäärä on luvun $|C|(n, |C_G(c)|) = (n|C|, |G|)$ monikerta. □

Tässä Frobeniuksen lause on tapaus $C = \{1\}$.

4.2 Yhtälön $X^n = c$ ratkaisut kaksoissivuluokissa

Olkoon G ryhmä, c sekä y ryhmän G alkioita ja n positiivinen kokonaisluku. Sen lisäksi että voidaan tarkastella yleisempää yhtälöä $X^n = c$, Frobeniuksen lausetta voidaan edelleen yleistää tarkastelemalla ratkaisujen lukumäärää tietyssä ryhmän G osajoukossa. Tarkastelemme seuraavaksi yhtälön $X^n = c$ ratkaisujen lukumäärää kaksoissivuluokassa HyH, missä H on jokin ryhmän G aliryhmä. Tarkastelu perustuu Brauerin todistukseen [8] lauseelle 4.4, joka taas perustuu tiettyjen ekvivalenssirelaatioiden käyttöön. Todistuksessaan Brauer osoittaa, että ratkaisujen joukko on samankokoisten ekvivalenssiluokkien yhdiste, jolloin ratkaisujen lukumäärä on tietyn luvun monikerta. Perimmäinen idea on siis hyvin intuitiivinen ja sama kuin esimerkiksi Lagrangen lauseen todistuksessa. Lisäksi erona aiempiin esitettyihin todistuksiin on se, että tällä kertaa sama todistus toimii kaikissa tapauksissa, eikä induktiolle ole lainkaan tarvetta. Sama todistus toimii myös äärettömille ryhmille, jotka sisältävät sopivan kokoisia äärellisiä aliryhmiä.

McKean huomaa väitöskirjassaan [25], että Brauerin todistus toimii yleisemmin myös kaksoissivuluokkien tapauksessa[4]. Näitä ideoita käyttämällä todistamme tässä kappaleessa vielä hieman yleisemmän tuloksen. Sen avulla saadaan todistettua, että jos $c \in C_G(H)$, niin yhtälön $X^n = c$ ratkaisujen lukumäärä kaksoissivuluokassa HyH on luvun $(n, |H|)$ monikerta. Tämän tuloksen on todistanut ensimmäisenä Philip Hall [13] vuonna 1935.

Olkoot x ja y ryhmän G alkioita. Sanotaan, että x ja y ovat *toistensa konjugaatteja aliryhmän H suhteen* jos $x = hyh^{-1}$ jollakin $h \in H$, ja merkitään tällöin $x \sim_H y$. Relaatio $\sim_H$ on ekvivalenssirelaatio, ja alkion x määräämä $\sim_H$-ekvivalenssiluokka on $\{hxh^{-1} : h \in H\}$. Kutsutaan tätä alkion x määrämäksi *H-konjugointiluokaksi*. Huomaa, että G-konjugointiluokat ovat tarkalleen ryhmän G konjugointiluokat. Lisäksi ehdosta $x \sim_H y$ seuraa $x \sim_G y$, joten jokainen ryhmän G konjugointiluokka on H-konjugointiluokkien yhdiste.

Seuraava yksinkertainen tulos on hyödyllinen jatkossa. Olkoot x ja y ovat toistensa konjugaatteja. Nyt siis $x = gyg^{-1}$, joten korottamalla molemmat puolet potenssiin n saadaan $x^n = gy^ng^{-1}$. Näin ollen x^n ja y^n ovat toistensa

[4] Brauerin ekvivalenssirelaatioita on hyödyntänyt myös Mckeanin väitöskirjan ohjaaja Isaacs artikkelissa [16].

konjugaatteja saman alkion g avulla. Erityisesti siis jos $d \mid n$ ja $x^d = gy^d g^{-1}$, niin korottamalla potenssiin n/d saadaan $x^n = gy^n g^{-1}$.

Lemma 4.5 (Brauer)**.** *Olkoon G ryhmä ja $H \trianglelefteq G$. Jos $xH = yH$, niin $x^{|H|}$ ja $y^{|H|}$ ovat toistensa konjugaatteja aliryhmän H suhteen.*

Todistus. Nyt $xH = yH$, joten $x^n H = y^n H = Hy^n$ ja näin ollen $x^n H y^{-n} = H$ kaikilla kokonaisluvuilla n. Näin ollen voidaan määritellä ryhmässä H ekvivalenssirelaatio $\sim$ asettamalla $h \sim h'$ jos ja vain jos $h' = x^n h y^{-n}$ jollakin kokonaisluvulla n. Selvästi $\sim$ on ekvivalenssirelaatio, ja alkion $h \in H$ määräämä ekvivalenssiluokka on muotoa

$$S_h = \{x^n h y^{-n} : n \in \mathbb{Z}\}.$$

Nyt $x^n h y^{-n} = x^m h y^{-m}$ jos ja vain jos $h^{-1} x^{n-m} h = y^{n-m}$. Näin ollen jos N on pienin positiivinen kokonaisluku jolle $h^{-1} x^N h = y^N$, niin $n \equiv m \bmod N$. Täten joukossa S_h on tarkalleen N alkiota.

Olkoot m pienin mahdollinen joukon S_h kertaluku ja $S_{h_1}, S_{h_2}, \ldots, S_{h_r}$ ne ekvivalenssiluokat joilla $|S_{h_i}| = m$. Koska ekvivalenssiluokat ovat erillisiä, näiden joukkojen yhdisteessä U on yhteensä rm alkiota. Nyt kaikilla joukon S_{h_i} alkioilla h pätee $h^{-1} x^m h = y^m$. Lisäksi jos $h \in H$ on sellainen, että $h^{-1} x^m h = y^m$, niin luvun m minimaalisuuden nojalla $|S_h| = m$. Siispä

$$U = \{h \in H : h^{-1} x^m h = y^m\}.$$

Näin ollen U on sentralisoijan $C_H(x^m)$ tietty sivuluokka, joten joukossa U alkioiden lukumäärä $rm = |C_H(x^m)|$ on luvun $|H|$ tekijä. Erityisesti siis m on luvun $|H|$ tekijä. Näin ollen jos $h \in U$, niin $h^{-1} x^m h = y^m$ ja tällöin $h^{-1} x^{|H|} h = y^{|H|}$. □

Olkoon G ryhmä, $H \leq G$ ja $x \in G$. Määritellään aliryhmä $F_x \leq H$ asettamalla

$$F_x = \bigcap_{w \in \langle x \rangle} wHw^{-1} = \bigcap_{j \in \mathbb{Z}} x^j H x^{-j}$$

Ei ole vaikeaa osoittaa, että $x \in N_G(F_x)$.

Seuraava huomio on hyödyllinen aliryhmän F_x käsittelyssä. Olkoon $J \leq H$ ja $x \in N_G(J)$. Tällöin $J \leq F_x$, sillä $J = x^j J x^{-j} \leq x^j H x^{-j}$ kaikilla $j \in \mathbb{Z}$.

Määritellään relaatio $\equiv_H$ asettamalla $x \equiv_H y$ jos ja vain jos $xF_x = yF_x$. Jos $xF_x = yF_x$, niin $y \in xF_x \leq N_G(F_x)$ joten edellisen perusteella $F_x \leq F_y$. Tämän avulla saadaan $x \in yF_x \leq yF_y \leq N_G(F_y)$, joten $F_y \leq F_x$. Näin ollen $F_x = F_y$ jos $x \equiv_H y$.

Nyt voidaan osoittaa, että $\equiv_H$ on ekvivalenssirelaatio. Selvästi $x \equiv_H x$. Olkoon $x \equiv_H y$ eli $xF_x = yF_x$. Edellisen perusteella $yF_y = yF_x = xF_x = xF_y$, eli $y \equiv_H x$. Vastaavasti jos $x \equiv_H y \equiv_H z$, niin $xF_x = yF_x = yF_y = zF_y = zF_x$, eli $x \equiv_H z$.

Huomaa, että $\equiv_H$-ekvivalenssiluokat ovat muotoa xF_x. Lisäksi nähdään, että $hF_xh^{-1} = F_{hxh^{-1}}$. Tämän perusteella $h(xF_x)h^{-1} = hxh^{-1}hF_xh^{-1} = hxh^{-1}F_{hxh^{-1}}$. Siispä $\equiv_H$-ekvivalenssiluokkien konjugaatit ovat myös $\equiv_H$- ekvivalenssiluokkia.

Lemma 4.6. *Olkoon $H \leq G$ ja $x \equiv_H y$. Tällöin $x^{|H|}$ ja $y^{|H|}$ ovat toistensa konjugaatteja aliryhmän H suhteen. Lisäksi jos $h \in H$, niin $hxh^{-1} \equiv_H hyh^{-1}$.*

Todistus. Koska $x \in N_G(F_x)$, niin $F_x \trianglelefteq \langle x, F_x \rangle$. Oletuksen nojalla $xF_x = yF_x$, joten lemman 4.5 nojalla $x^{|F_x|}$ ja $y^{|F_x|}$ ovat toistensa konjugaatteja aliryhmän F_x suhteen. Nyt $|F_x|$ on luvun $|H|$ tekijä, joten $x^{|H|}$ ja $y^{|H|}$ ovat myös toistensa konjugaatteja aliryhmän F_x ja siten aliryhmän H suhteen.

Olkoon $h \in H$. Tällöin $hxh^{-1}F_{hxh^{-1}} = h(xF_x)h^{-1}$, joten koska $xF_x = yF_y$, niin $hxh^{-1}F_{hxh^{-1}} = h(yF_y)h^{-1} = hyh^{-1}F_{hyh^{-1}}$. Näin ollen $hxh^{-1} \equiv_H hyh^{-1}$. □

Määritellään seuraavaksi relaatio $\approx_H$ asettamalla $x \approx_H y$ jos ja vain jos $x \equiv_H hyh^{-1}$ jollain $h \in H$. Osoitetaan, että $\approx_H$ on ekvivalenssirelaatio. Nyt $x \approx_H x$ koska $x \equiv_H x$. Olkoon $x \approx_H y$, eli $x \equiv_H hyh^{-1}$, missä $h \in H$. Tällöin lemman 4.6 nojalla $h^{-1}xh \equiv_H y$, eli $y \equiv_H h^{-1}xh$ ja $y \approx_H x$. Vastaavasti jos $x \approx_H y \approx_H z$, niin $x \equiv_H hyh^{-1}$ ja $y \equiv_H h_0zh_0^{-1}$ jollakin $h, h_0 \in H$. Jälleen lemman 4.6 nojalla $hyh^{-1} \equiv_H (hh_0)z(hh_0)^{-1}$, joten $x \equiv_H (hh_0)z(hh_0)^{-1}$ ja $x \approx_H z$.

Käytetään seuraavassa alkion x määräämästä $\approx_H$-ekvivalenssiluokasta merkintää $\approx_H [x]$.

Lemma 4.7. *Olkoon $H \leq G$ ja $x \in G$. Tällöin*

(i) $|\approx_H [x]| = |H|$

(ii) Jos $x \approx_H y$, niin $x^{|H|}$ ja $y^{|H|}$ ovat toistensa konjugaatteja aliryhmän H suhteen.

Todistus. (i) Alkion x määräämä $\approx_H$-ekvivalenssiluokka on muotoa

$$\approx_H [x] = \bigcup_{h \in H} h(xF_x)h^{-1} = \bigcup_{h \in H} (hxh^{-1})(F_{hxh^{-1}}).$$

Nyt jokainen joukon xF_x konjugaatti on $\equiv_H$-ekvivalenssiluokka, joten yllä oleva yhdiste on erillinen. Lemman 2.10 nojalla osajoukolla xF_x on H-konjugaatteja tarkalleen $[H : S]$ kappaletta, missä $S = N_H(xF_x)$. Koska $|hxF_xh^{-1}| = |F_x|$, niin $|\approx_H [x]| = |F_x|[H : S]$. Väitteen todistamiseksi riittää siis osoittaa, että $S = F_x$. Jos $t \in F_x$, niin tällöin

$$t(xF_x)t^{-1} = txF_x = tF_xx = F_xx = xF_x$$

sillä $x \in N_G(F_x)$. Näin ollen $t \in S$ ja $F_x \leq S$. Olkoon $s \in S$. Tällöin $sxF_xs^{-1} = xF_x$, joten $x^{-1}sx \in F_xs \subseteq S$. Tämän perusteella $x \in N_G(S)$, ja tällöin $S \leq H$ nojalla $S \leq F_x$.

(ii) Nyt $x \equiv_H hyh^{-1}$, missä $h \in H$. Lemman 4.6 nojalla $x^{|H|}$ ja $(hyh^{-1})^{|H|} = hy^{|H|}h^{-1}$ ovat toistensa konjugaatteja aliryhmän H suhteen, eli $x^{|H|} = h_0hy^{|H|}h^{-1}(h_0)^{-1} = (h_0h)y^{|H|}(h_0h)^{-1}$ missä $h_0 \in H$. Näin ollen $x^{|H|}$ ja $y^{|H|}$ ovat toistensa konjugaatteja aliryhmän H suhteen.

□

Olkoot S ja K ryhmän G epätyhjiä osajoukkoja ja olkoon n positiivinen kokonaisluku. Merkitään

$$A_n(S, K) = \{x \in S : x^n \in K\}$$
$$a_n(S, K) = |A_n(S, K)|$$

Lause 4.8. *Olkoon $H \leq G$ aliryhmä, $y \in G$ ja C jokin H-konjugointiluokka. Tällöin $a_n(HyH, C)$ on luvun $(n, |H|)$ monikerta.*

Todistus. Merkitään $d = (n, |H|)$. Olkoon p luvun d alkulukutekijä ja p^r suurin alkuluvun p potenssi joka jakaa luvun d. Nyt riittää osoittaa, että p^r jakaa luvun $a_n(HyH, C)$. Olkoon $U \leq H$ kertalukua p^r oleva aliryhmä.

Olkoon $x \in G$ sellainen, että $x^n \in C$. Tällöin jos $x \approx_U y$, niin lemman 4.7 (ii) nojalla $x^{|U|}$ ja $y^{|U|}$ kuuluvat samaan U-konjugointiluokkaan ja siten samaan H-konjugointiluokkaan. Koska $|U| \mid n$, niin x^n ja y^n kuuluvat samaan H-konjugointiluokkaan. Näin ollen $y^n \in C$. Tämän perusteella $A_n(G, C)$ koostuu kokonaisista $\approx_U$-ekvivalenssiluokista.

Nyt jos $x \approx_U y$, niin $x \equiv_U uyu^{-1}$ jollakin $u \in U$. Tällöin $xF_x = uyu^{-1}F_x$, joten $uyu^{-1} \in xF_x \subseteq xU \subseteq UxU$. Näin ollen $y \in UxU$, eli $UxU = UyU$. Näin ollen jokainen kaksoissivuluokka UxU on $\approx_U$-ekvivalenssiluokkien yhdiste. Koska $U \leq H$, niin jokainen kaksoissivuluokka HyH on tiettyjen kaksoissivuluokkien UxU yhdiste. Täten HyH on myös $\approx_U$-ekvivalenssiluokkien

yhdiste. Edellisen perusteella jokainen näistä ekvivalenssiluokista sisältää joko pelkästään joukon $A_n(G,C)$ alkioita tai ei lainkaan joukon $A_n(G,C)$ alkioita. Lisäksi lemman 4.7 (i) nojalla jokainen näistä ekvivalenssiluokista sisältää tarkalleen p^r alkiota, joten $a_n(HyH,C)$ on luvun p^r monikerta. □

Lause pätee myös äärettömille ryhmille tietyillä lisäoletuksilla [8, Section 5]. Olkoon p alkuluku ja $p^r \mid n$. Jos G on ääretön ryhmä, $a_n(HyH,C)$ on äärellinen ja H sisältää kertalukua p^r olevan aliryhmän U, niin $a_n(HyH,C)$ on luvun p^r monikerta. Tämä nähdään täysin samalla todistuksella kuin edellä, sillä ekvivalenssirelaation $\approx_U$ ominaisuuksien todistamiseen ei tarvita ryhmän G äärellisyyttä.

Koska jokainen ryhmän G konjugointiluokka on H-konjugointiluokkien erillinen yhdiste, lause pätee myös kun oletetaan, että C on mikä tahansa ryhmän G konjugointiluokka. Jos $c \in C_G(H)$, niin tällöin alkion c määräämä H-konjugointiluokka on $C = \{c\}$. Tällöin $x^n \in C$ jos ja vain jos $x^n = c$, joten seurauksena saadaan seuraava tulos.

Seuraus 4.9 (Hall, 1935)**.** *Olkoon $H \leq G$ aliryhmä, $y \in G$, $c \in C_G(H)$ ja n positiivinen kokonaisluku. Tällöin yhtälön $X^n = c$ ratkaisujen lukumäärä kaksoissivuluokassa HyH on luvun $(n, |H|)$ monikerta.*

Tässä erityisesti jos $y \in N_G(H)$, niin $HyH = yy^{-1}HyH = yHH = yH$ ja ratkaisujen määrä sivuluokassa yH on luvun $(n, |H|)$ monikerta. Näin ollen jos H on normaali aliryhmä, niin vastaava tulos pätee mille tahansa sivuluokalle yH. Lisäksi kun $C = \{1\}$ ja $H = G$, niin saadaan Frobeniuksen lause. Edelleen seurauksena saadaan Frobeniuksen lauseen yleistys. Seuraavassa Frobeniuksen lause on erikoistapaus $\phi = I$.

Seuraus 4.10 (Hall, 1935)**.** *Olkoon G äärellinen ryhmä ja ϕ ryhmän G automorfismi, jolle $\phi^n = I$. Tällöin yhtälön*

$$x \cdot \phi(x) \cdot \phi^2(x) \cdot \ldots \cdot \phi^{n-1}(x) = 1 \qquad (*)$$

ratkaisujen lukumäärä on luvun $(n, |G|)$ monikerta.

Todistus. Olkoon $G^l = \{L_g : g \in G\}$ ryhmän G tavallinen (vasen) permutaatioesitys. Nyt siis $L_g : G \to G$, missä $x \mapsto gx$ kaikilla $x \in G$. Tarkastellaan ryhmää $G \cong G^l$ ja yhtälön (*) ratkaisuja ryhmän $H = \langle G^l, \phi \rangle$ sisällä.

Kaikilla $x \in G$ pätee $L_{\phi(x)} = \phi L_x \phi^{-1}$, joten $\phi G^l \phi^{-1} = G^l$ ja $\phi \in N_H(G^l)$. Lisäksi tämän perusteella yhtälö (*) pätee jos ja vain jos

$$L_x \cdot (\phi L_x \phi^{-1}) \cdot (\phi^2 L_x \phi^{-2}) \cdot \ldots \cdot (\phi^{n-1} L_x \phi^{-(n-1)}) = I$$

mikä pätee jos ja vain jos $(L_x\phi)^n = I$, sillä $\phi^{-n} = I$. Näin ollen yhtälön (*) ratkaisujen lukumäärä on yhtälön $X^n = 1$ ratkaisujen lukumäärä sivuluokassa $G^l\phi$. Koska $\phi \in N_H(G^l)$, niin seurauksen 4.9 nojalla ratkaisujen määrä on luvun $(n, |G|)$ monikerta.

□

4.3 Sanayhtälöiden ratkaisut

Vuonna 1935 Philip Hall julkaisi artikkelin [13], jossa hän yleistää Frobeniuksen lauseen hyvin yleisille yhtälöryhmille. Tuloksien todistukset ovat pitkiä ja vaativat paljon etenkin p-ryhmiin liittyvää teoriaa, joten käymme tässä osiossa läpi ainoastaan päätulokset ilman todistuksia.

Olkoon G ryhmä ja olkoot $X_1, X_2, \ldots$ muuttujia, jotka kuvaavat ryhmän G alkioita. Tällöin *sanafunktio* muuttujien X_i suhteen on kuvaus f, jolle $f(X_1, X_2, \ldots)$ määräytyy muuttujien X_i ja niiden käänteisalkioiden X_i^{-1} äärellisenä tulona, eli

$$f(X_1, X_2, \ldots) = X_{i_1}^{\alpha_1} X_{i_2}^{\alpha_2} \ldots X_{i_t}^{\alpha_t}$$

missä $i_k \geq 1$ ja $\alpha_k \in \mathbb{Z}$. Muuttujan X_i aste sanafunktiossa f on yllä olevassa tulossa esiintyvien muuttujan X_i potenssien summa. Esimerkiksi $f(X_1, X_2) = X_1^2 X_2 X_1 X_2^{-1}$ on sanafunktio muuttujien X_1 ja X_2 suhteen. Tässä muuttujan X_1 aste on 3 ja muuttujan X_2 aste on 0.

Olkoon nyt X muuttuja, $a_i \in G$ vakioita ja $f_1, f_2, \ldots$ sanafunktioita. Tarkastelemme seuraavaa yhtälöryhmää.

$$\begin{aligned} f_1(X, a_1, a_2, \ldots) &= 1 \\ f_2(X, a_1, a_2, \ldots) &= 1 \\ f_3(X, a_1, a_2, \ldots) &= 1 \\ &\ldots \end{aligned} \qquad (*)$$

Yhtälöryhmän (*) ratkaisuille saadaan lauseen 4.3 yleistys. Lisäksi ratkaisuille kaksoissivuluokissa HyH saadaan seurausta 4.9 vastaava tulos.

Lause 4.11 (Hall, 1935)**.** *Jos n jakaa muuttujan X asteen kaikissa yhtälöryhmässä (*) esiintyvissä sanoissa f_i, niin yhtälöryhmän ratkaisujen lukumäärä on luvun (n, c) monikerta, missä c on aliryhmän $C_G(a_1, a_2, \ldots) = \cap_i C_G(a_i)$ kertaluku.*

Lause 4.12 (Hall, 1935)**.** *Olkoon $H \leq C_G(a_1, a_2, \ldots)$ ja oletetaan, että n jakaa muuttujan X asteen kaikissa yhtälöryhmässä (*) esiintyvissä sanoissa*

f_i. Tällöin kaikilla $y \in G$ yhtälöryhmän (*) ratkaisujen lukumäärä kaksoissivuluokassa HyH on luvun $(n, |H|)$ monikerta.

Sehgal [15] on yleistänyt Hallin tulokset useamman muuttujan yhtälöryhmille. Myös Hall esittää omassa artikkelissaan tiettyjä useamman muuttujan yleistyksiä [13, Lemma 4.21].

Olkoot G ja H ryhmiä ja olkoon n_H niiden ryhmän G aliryhmien lukumäärä, jotka ovat isomorfisia ryhmän H kanssa. Tuloksiensa sovelluksena Hall onnistuu määrittämään kongruensseja luvulle n_H joissakin erikoistapauksissa. Nyt ryhmälle H löytyy aina joukko generoivia alkioita jotka toteuttavat tietyt relaatiot. Olkoon esimerkiksi $H \cong (\mathbb{Z}_p)^k$. Tällöin jos $H = \langle x_1, \ldots, x_k \rangle$, niin alkiot x_i toteuttavat yhtälöt

$$\begin{aligned} X_i^p &= 1 \\ X_i^{-1} X_j^{-1} X_i X_j &= 1 \end{aligned}$$

kaikilla $i, j = 1, \ldots, k$. Hallin tuloksia soveltamalla saadaan kongruenssi yllä olevan yhtälöryhmän ratkaisujen lukumäärälle. Jokainen ratkaisu generoi aliryhmän joka on isomorfinen ryhmän $(\mathbb{Z}_p)^l$ kanssa, missä $l \leq k$. Induktiolla luvun k suhteen Hall onnistuu todistamaan tietyn kongruenssin luvulle n_H, joka riippuu ryhmän G Sylowin p-aliryhmien rakenteesta. Yksityiskohdat löytyvät Hallin artikkelista [13, Theorem 4.3].

Sanayhtälöllä ei välttämättä ole ratkaisua lainkaan. Esimerkiksi jos $G = \{(1), (12)(45), (13)(45), (23)(45), (123), (132)\}$, niin yhtälöllä $X^2 = (12)(45)$ ei ole ratkaisua ryhmässä G. Ryhmä G on kuitenkin symmetrisen ryhmän Sym(5) aliryhmä, jossa yhtälöllä on ratkaisu (1425). Ryhmää G laajentamalla saadaan siis yhtälölle ratkaisu, vastaavasti kuten rationaalilukujen kuntaa $\mathbb{Q}$ laajentamalla saadaan yhtälölle $x^2 = 2$ ratkaisu.

Tälläinen laajennus ei kuitenkaan ole aina mahdollista, kuten seuraava esimerkki [18] osoittaa. Olkoon G ryhmä ja a ja b eri kertalukua olevia ryhmän G alkioita. Voidaan esimerkiksi valita $G = S_3$, $a = (12)$ ja $b = (123)$. Tarkastellaan yhtälöä

$$xax^{-1}b^{-1} = 1.$$

Jos $G \leq G^*$ ja $x \in G^*$ on tämän yhtälön ratkaisu, niin $b = xax^{-1}$. Koska alkion a konjugaateilla on sama kertaluku kuin alkiolla a, tämä on ristiriita. Näin ollen yhtälöllä ei ole ratkaisua ryhmässä G, eikä ratkaisua myöskään löydy ryhmää G laajentamalla.

On kuitenkin yksi yleinen tapaus, jossa yhtälölle saadaan ratkaisu. Frank Levin [17] on todistanut seuraavan tuloksen, joka pätee myös äärettömille ryhmille.

Lause 4.13 (Levin, 1962). *Olkoon G ryhmä ja $g_i \in G$ ryhmän G alkioita. Olkoot $n_1, n_2, \ldots, n_t > 0$ kokonaislukuja ja olkoon*

$$x^{n_1} g_1 x^{n_2} g_2 \ldots x^{n_t} g_t = 1$$

yhtälö muuttujan x suhteen. Tällöin on olemassa sellainen ryhmä G^*, että $G \leq G^*$ ja yllä olevalla yhtälöllä on ratkaisu ryhmässä G^*.

Tuloksen yleistys on Kervaire-Laudenbachin otaksuma, joka on edelleen avoin ongelma. Huomaa, että edellä mainittu yhtälö $xax^{-1}b = 1$ ei toteuta otaksuman oletusta.

Otaksuma 4.14 (Kervaire-Laudenbachin otaksuma). *Lause 4.13 pätee myös heikommalla oletuksella $n_1 + n_2 + \ldots + n_t \neq 0$.*

4.4 Homomorfismit $A \to G$

Jos G ja A ovat ryhmiä, niin olkoon $\mathrm{Hom}(A, G)$ kaikkien homomorfismien $A \to G$ muodostama joukko. Yoshida [19] on todistanut seuraavan tuloksen, joka on Frobeniuksen lauseen yleistys.

Lause 4.15 (Yoshida, 1993). *Olkoon G ryhmä ja A Abelin ryhmä. Tällöin*

$$|\mathrm{Hom}(A, G)| \equiv 0 \mod (|A|, |G|)$$

Emme perehdy tämän tuloksen todistamiseen tässä tutkielmassa. Osoitetaan kuitenkin, että Frobeniuksen lause on erikoistapaus $A \cong \mathbb{Z}_n$. Jokainen homomorfismi $\phi : \mathbb{Z}_n \to G$ määräytyy generoivan alkion x kuvan $\phi(x)$ perusteella. Kuva-alkiolle pätee aina $\phi(x)^n = \phi(x^n) = \phi(1) = 1$. Lisäksi jos $g^n = 1$ jollakin $g \in G$, niin alkiota g vastaa homomorfismi $x^i \mapsto g^i$. Tämän perusteella $|\mathrm{Hom}(\mathbb{Z}_n, G)| = a_n(G) = a_{(n,|G|)}(G)$.

Lauseessa oletus, että A on Abelin ryhmä on välttämätön, sillä esimerkiksi $|\mathrm{Hom}(S_3, S_3)| = 10 \equiv 4 \mod (|S_3|, |S_3|)$. Yleistyksenä saadaan kuitenkin seuraava otaksuma, jonka Asai ja Yoshida esittivät artikkelissaan [20].

Otaksuma 4.16 (Asai, Yoshida, 1993). *Olkoot A ja G mitä tahansa äärellisiä ryhmiä. Tällöin*

$$|\mathrm{Hom}(A, G)| \equiv 0 \mod (|A/A'|, |G|)$$

Otaksuma on todistettu joissakin erikoistapauksissa, mutta on tällä hetkellä vielä avoin ongelma [21].

5 Frobeniuksen otaksuma

Vuonna 1893 Frobenius [9] osoitti, että jos ryhmän kertaluku on neliövapaa[5], niin ryhmä on ratkeava. Frobeniuksen todistus perustui seuraavaan lemmaan[6].

Lemma 5.1. *Olkoon G ryhmä, jonka kertaluku $|G|$ on neliövapaa, eli $|G| = p_1 p_2 \dots p_t$ missä $p_1 < p_2 < \dots < p_t$ ovat eri alkulukuja. Tällöin jos $m = p_j p_{j+1} \dots p_t$, niin yhtälöllä $X^m = 1$ on tarkalleen m ratkaisua ryhmässä G.*

Tarkastelemme tätä tulosta ja sen yleistystä tarkemmin luvussa 7. Kun $m = p_t$, niin lemman perusteella nähdään, että ryhmässä G on normaali Sylowin p_t-aliryhmä. Tämän tiedon avulla voidaan osoittaa, että ryhmä G on ratkeava. Lisäksi nähdään, että jos m on kuten lemman oletuksessa, niin ryhmässä G on yksikäsitteinen kertalukua m oleva aliryhmä H. Koska H on ainoa kertalukua m oleva aliryhmä, niin H on normaali aliryhmä. Tämän tuloksen motivoimana on luonnollista pohtia seuraavaa ongelmaa, jota kutsutaan Frobeniuksen otaksumaksi.

Otaksuma 5.2 (Frobeniuksen otaksuma)**.** *Olkoon G äärellinen ryhmä ja n ryhmän G kertaluvun tekijä. Jos yhtälöllä $X^n = 1$ on tarkalleen n ratkaisua, niin ratkaisujen joukko muodostaa normaalin aliryhmän.*

Otaksuma oli pitkään avoin ongelma, kunnes se viimein todistettiin 90-luvulla [31]. Todistus perustuu olennaisella tavalla äärellisten yksinkertaisten ryhmien luokitteluun. Todistamme tässä kappaleessa Frobeniuksen otaksuman joissakin erikoistapauksissa. Käsittelemme ensin erikoistapauksia ryhmän G suhteen ja todistamme otaksuman ratkeaville ryhmille. Lisäksi käsittelemme erikoistapauksia luvun n suhteen ja todistamme otaksuman muun muassa kun n on neliövapaa. Lopuksi osoitamme Zemlinin [23] tuloksen, jonka mukaan jos Frobeniuksen otaksuma ei pidä paikkansa, niin pienintä mahdollista kertalukua oleva vastaesimerkki otaksumalle on yksinkertainen ryhmä.

Tarkennetaan vielä joitakin käsitteitä. Sanotaan, että

(i) *Frobeniuksen otaksuma pätee ryhmälle G*, jos kaikilla kokonaisluvuilla n ehdoista $n \mid |G|$ ja $a_n(G) = n$ seuraa, että $A_n(G) \leq G$.

[5]Sanotaan, että positiivinen kokonaisluku n on *neliövapaa*, jos se ei ole jaollinen minkään alkuluvun p toisella potenssilla p^2. Toisin sanoen n on neliövapaa jos ja vain jos se on eri alkulukujen tulo.

[6]Itseasiassa Frobenius todisti tätä lemmaa yleisemmän tuloksen (kts. lause 7.4), mutta esitetään tässä selkeyden vuoksi vain tapaus, jossa ryhmän kertaluku on neliövapaa.

(ii) *Frobeniuksen otaksuma pätee luvulle n*, jos millä tahansa ryhmällä G ehdoista $n \mid |G|$ ja $a_n(G) = n$ seuraa, että $A_n(G) \leq G$.

(iii) *Frobeniuksen otaksuma pätee parille* (n, G), jos joko (a) $n \nmid |G|$, (b) $a_n(G) \neq n$ tai (c) $n \mid |G|$ ja $a_n(G) = n$ sekä $A_n(G) \leq G$.

5.1 Erikoistapaukset ryhmän G suhteen

Otaksumassa oletus että n jakaa ryhmän G kertaluvun on välttämätön Lagrangen lauseen nojalla. Esimerkiksi symmetrisessä ryhmässä S_3 on tarkalleen neljä alkiota jotka toteuttavat yhtälön $X^4 = 1$, mutta ratkaisujen joukko ei muodosta aliryhmää. Nyt jos $x^n = 1$, niin kaikilla $g \in G$ pätee $(gxg^{-1})^n = gx^ng^{-1} = 1$. Näin ollen ratkaisujen joukko on suljettu konjugoinnin suhteen. Riittää siis osoittaa, että ratkaisut muodostavat aliryhmän. Koska ehdosta $x^n = 1$ seuraa $(x^{-1})^n = 1$, niin riittää osoittaa, että ehdosta $x^n = 1$ ja $y^n = 1$ seuraa $(xy)^n = 1$. Esimerkiksi Abelin ryhmien tapauksessa tämä pitää paikkansa, sillä tällöin $(xy)^n = x^ny^n$.

Jos H on kertalukua n oleva ryhmän G aliryhmä, niin jokainen $x \in H$ toteuttaa yhtälön $x^n = 1$. Näin ollen jos G toteuttaa otaksuman oletukset, niin ratkaisujen joukko on tarkalleen aliryhmä H. Otaksuman todistamiseksi riittää siis osoittaa, että ryhmässä G on jokin kertalukua n oleva aliryhmä H. Tällöin H on tietysti ainoa kertalukua n oleva aliryhmä ryhmässä G, jolloin H on myös karakteristinen aliryhmä ja normaali aliryhmä. Sanotaan, että ryhmä G on *CLT-ryhmä* (Converse of Lagrange's Theorem) jos jokaiselle luvun $|G|$ tekijälle d pätee, että ryhmässä G on ainakin yksi kertalukua d oleva aliryhmä. Edellisen perusteella saadaan siis tulos

Lause 5.3. *Frobeniuksen otaksuma pätee kun G on CLT-ryhmä.*

Näin ollen Frobeniuksen otaksuma pätee erityisesti silloin kun G on nilpotentti. Kaikki ryhmät eivät kuitenkaan ole CLT-ryhmiä, sillä esimerkiksi alternoivalla ryhmällä A_4 ei ole kertalukua 6 olevaa aliryhmää. Todistamme seuraavaksi, että Frobeniuksen otaksuma pätee ratkeaville ryhmille. Tämä sisältää edellisen tuloksen, sillä voidaan osoittaa, että CLT-ryhmät ovat aina ratkeavia [38]. Todistus perustuu Marshall Hallin kirjan esitykseen [1, Theorem 9.4.1., s.145-146].

Lause 5.4. *Frobeniuksen otaksuma pätee kun G on ratkeava.*

Todistus. Induktiolla ryhmän G kertaluvun suhteen. Väite pitää paikkansa kun $|G| = 1$, joten oletetaan että se pätee kaikille ratkeaville ryhmille joiden kertaluku on $< |G|$. Olkoon N ryhmän G minimaalinen normaali aliryhmä.

Koska G on ratkeava, niin lemman 2.25 nojalla aliryhmä N on Abelin ryhmä, $|N| = p^i$ on alkuluvun potenssi ja $x^p = 1$ kaikilla $x \in N$. Lisäksi voidaan olettaa että N on aito aliryhmä, sillä Frobeniuksen otaksuma pätee kun G on Abelin ryhmä. Näin ollen induktio-oletusta voidaan jatkossa soveltaa ryhmään G/N, joka on ratkeavan ryhmän tekijäryhmänä ratkeava. Jaetaan väitteen todistus kahteen tapaukseen: joko $p \mid n$ tai $p \nmid n$.

Tapaus 1: $p \mid n$.

Nyt ryhmässä N pätee $x^p = 1$ kaikilla $x \in N$, joten jokainen ryhmän N alkio toteuttaa yhtälön $X^n = 1$. Olkoon $u \mid |G/N|$ ja $up \mid n$. Frobeniuksen lauseen nojalla ryhmässä G/N yhtälöllä $X^u = 1$ on ku ratkaisua, missä $k \geq 1$ on kokonaisluku. Lisäksi jos aN on ratkaisu, niin $a^u \in N$ jolloin $a^{up} = 1$. Koska $up \mid n$, niin a toteuttaa yhtälön $X^n = 1$. Näin ollen jos sivuluokka aN toteuttaa yhtälön $X^u = 1$ ryhmässä G/N, niin jokainen sivuluokan alkioista toteuttaa yhtälön $X^n = 1$ ryhmässä G. Tämän perusteella saadaan siis ainakin kup^i ratkaisua yhtälölle $X^n = 1$ ryhmässä G. Nyt $n = p^j n_1$, missä $j \geq 1$ ja $p \nmid n_1$. Valitsemalla $u = n_1$ saadaan edellisen perusteella ainakin $kn_1 p^i \geq p^i n_1$ ratkaisua yhtälölle $X^n = 1$ ryhmässä G. Näin ollen $j \geq i$, sillä muutoin saataisiin $> p^j n_1 = n$ ratkaisua. Siispä voidaan valita $u = p^{j-i} n_1$, jolloin ryhmän G/N ratkaisuista yhtälölle $X^u = 1$ saadaan ainakin $kup^i = kn$ ratkaisua yhtälölle $X^n = 1$ ryhmässä G. Oletuksen nojalla $k = 1$, ja tällöin induktio-oletuksen nojalla ryhmässä G/N on kertalukua u oleva aliryhmä H/N. Tässä aliryhmän H kertaluku on $up^i = n$, joten väite pätee ryhmälle G.

Tapaus 2: $p \nmid n$.

Nyt $n \mid |G/N|$, joten ryhmässä G/N yhtälöllä $X^n = 1$ on kn ratkaisua Frobeniuksen lauseen nojalla. Jos $aN \neq bN$ ovat sivuluokkia jotka toteuttavat yhtälön $X^n = 1$ ryhmässä G/N, niin $a^n, b^n \in N$ ja siten $a^{np} = b^{np} = 1$, eli a^p ja b^p ovat yhtälön $X^n = 1$ ratkaisuja ryhmässä G. Nyt jos $a^p = b^p$, niin $a^p N = b^p N$ ja $a^n N = b^n N$. Koska $(p, n) = 1$, niin $aN = bN$, mikä on ristiriita. Näin ollen $a^p \neq b^p$. Siispä ryhmän G/N kahdesta eri ratkaisusta yhtälöön $X^n = 1$ saadaan kaksi eri ratkaisua yhtälöön $X^n = 1$ ryhmässä G. Näin ollen saadaan ainakin kn ratkaisua yhtälöön $X^n = 1$ ryhmässä G. Koska $k \geq 1$, niin oletuksen nojalla $k = 1$. Siispä ryhmässä G/N on tarkalleen n ratkaisua yhtälöön $X^n = 1$, joten induktio-oletuksen nojalla ryhmässä G/N on aliryhmä H/N jonka kertaluku on n. Tällöin aliryhmän H kertaluku on np^i. Koska $p \nmid n$, niin Hallin lauseen (2.26) nojalla ryhmällä H on kertalukua n oleva aliryhmä K. Koska K on tällöin myös ryhmän G aliryhmä, niin väite on todistettu. □

Entä jos G ei ole ratkeava? Richard Zemlin [23] osoitti vuonna 1954, että jos Frobeniuksen otaksuma ei pidä paikkansa, niin minimaalinen vastaesimerkki Frobeniuksen otaksumalle on yksinkertainen ryhmä. Todistamme tämän tuloksen myöhemmin tässä luvussa. Zemlinin tuloksen nojalla riittää siis todistaa otaksuma yksinkertaisille ryhmille. Olkoon d ryhmän G kertaluvun tekijä. Frobeniuksen lauseen nojalla yhtälön $X^d = 1$ ratkaisuja on ainakin d kappaletta. Jos ratkaisuja olisi tarkalleen d kappaletta, niin Frobeniuksen otaksuman pätiessä ratkaisut muodostaisivat ei-triviaalin normaalin aliryhmän. Näin ollen jos G on yksinkertainen ryhmä, niin Frobeniuksen otaksuman todistamiseksi ryhmälle G pitää osoittaa, että kaikilla luvun $|G|$ tekijöille d, missä $1 < d < |G|$, yhtälöllä $X^d = 1$ on enemmän kuin d kappaletta ratkaisuja. Siispä jos otaksuma pitää paikkansa, niin Frobeniuksen lauseen nojalla ratkaisuja on ainakin $2d$ kappaletta.

Tunnetusti alternoiva ryhmä Alt(5) on yksinkertainen ryhmä. Laskemalla nähdään, että ryhmässä Alt(5) yhtälöllä $X^d = 1$ on tarkalleen d ratkaisua ainoastaan kun $d = 1$ tai $d = 60$ (kts. taulukko 1). Toisin sanoen Frobeniuksen otaksuma pätee kun $G = \mathrm{Alt}(5)$. Näin ollen on olemassa myös ryhmiä jotka eivät ole ratkeavia, mutta joille Frobeniuksen otaksuma pätee.

d	$a_d(\mathrm{Alt}(5)) = kd$	k
1	1	1
2	16	8
3	21	7
4	16	4
5	25	5
6	36	6
10	40	4
12	36	3
15	45	3
20	40	2
30	60	2
60	60	1

Taulukko 1: Yhtälön $X^d = 1$ ratkaisujen lukumäärä ryhmässä Alt(5), missä $d \mid 60$.

5.2 Erikoistapaukset luvun n suhteen

Toiseen suuntaan voidaan tarkastella erikoistapauksia joissa luku n on tiettyä muotoa. Esimerkiksi tapaukset $n = 1$ ja $n = |G|$ pätevät mille tahansa

ryhmälle G. Näin ollen Frobeniuksen otaksuma pätee ryhmälle G jos se pätee kaikille luvun $|G|$ tekijöille d, missä $1 < d < |G|$.

Jos $n = p^k$ on alkuluvun potenssi, niin Sylowin lauseen nojalla ryhmässä G on kertalukua p^k oleva aliryhmä. Näin ollen saadaan

Lause 5.5. *Frobeniuksen otaksuma pätee kun $n = p^k$ on alkuluvun potenssi.*

Vastaavalla tavalla ei voida jatkaa, sillä jos n ei ole alkuluvun potenssi, niin on aina olemassa ryhmä G jonka kertaluku on jaollinen luvulla n, mutta joka ei sisällä kertalukua n olevaa aliryhmää [39]. Muihin tapauksiin tarvitaan siis erilainen lähestymistapa. Useita erikoistapauksia saadaan todistettua laskemalla alkioitten lukumääriä.

Lause 5.6. *Frobeniuksen otaksuma pätee kun $n = pq$, missä p ja q ovat alkulukuja.*

Todistus. Väite seuraa myös myöhemmin todistettavasta lauseesta 5.11, mutta esitetään tässä erilainen todistus. Rajoituksetta voidaan olettaa, että $p < q$. Cauchyn lauseen nojalla ryhmässä G on kertalukua p oleva aliryhmä P ja kertalukua q oleva aliryhmä Q. Jos Q on ainoa kertalukua q oleva aliryhmä, niin Q on normaali ja tällöin PQ on kertalukua pq oleva aliryhmä. Muutoin Sylowin lauseen yleistyksen nojalla ryhmässä G on ainakin $q+1$ kertalukua q olevaa aliryhmää. Nyt q on alkuluku, joten eri aliryhmien leikkaukset ovat triviaaleja. Näistä aliryhmistä saadaan siis ainakin $(q+1)(q-1) \geq (q+1)p > pq$ ratkaisua yhtälöön $X^n = 1$, mikä on ristiriita.

□

Lause 5.7. *Frobeniuksen otaksuma pätee kun $n = 12$, $n = 20$ tai $n = 30$.*

Todistus. $n = 12 = 2^2 \cdot 3$:

Sylowin lauseen nojalla ryhmässä G on aliryhmä P jonka kertaluku on 2^2 ja aliryhmä Q jonka kertaluku on 3. Jos Q on ryhmän G ainoa kertalukua 3 oleva aliryhmä, niin Q on normaali ja tällöin PQ on kertalukua 12 oleva aliryhmä. Muutoin Sylowin lauseen yleistyksen nojalla ryhmässä G on ainakin 4 eri aliryhmää, joiden kertaluku on 3. Näistä aliryhmistä saadaan siis ainakin 8 alkiota, jotka kaikki toteuttavat yhtälön $X^{12} = 1$. Tilaa on siis vain yhdelle kertalukua 2^2 olevalle aliryhmälle, koska niiden alkiot toteuttavat myös yhtälön $X^{12} = 1$. Näin ollen P on normaali ja PQ on kertalukua 12 oleva aliryhmä.

$n = 20 = 2^2 \cdot 5$:

Kuten aiemmin, ryhmästä G löytyy kertalukua 2^2 oleva aliryhmä P ja kertalukua 5 oleva aliryhmä Q. Jos ryhmässä G olisi enemmän kuin yksi kertalukua 5 oleva aliryhmä, niin Sylowin lauseen yleistyksen nojalla niitä olisi

ainakin 6 kappaletta. Niistä saataisiin näin ollen ainakin 24 eri alkiota, jotka kaikki toteuttavat yhtälön $X^{20} = 1$. Tämä on ristiriita, sillä oletuksen nojalla ratkaisuja on tarkalleen 20 kappaletta. Näin ollen Q on normaali aliryhmä ja PQ on kertalukua 20 oleva aliryhmä.

$n = 30 = 2 \cdot 3 \cdot 5$:
Tämäkin seuraa myöhemmin todistettavan lemman 5.11 avulla, mutta voidaan osoittaa myös seuraavasti. Frobeniuksen lauseen nojalla yhtälön $X^{15} = 1$ ratkaisujen lukumäärä on luvun 15 monikerta. Jos ratkaisuja on enemmän kuin 15, niin niitä saataisiin ainakin 30. Nämä ratkaisut toteuttavat yhtälön $X^{30} = 1$, joten enempää ratkaisuja ei voi olla. Ryhmässä G on kuitenkin Cauchyn lauseen nojalla kertalukua 2 oleva alkio, joka ei voi toteuttaa yhtälöä $X^{15} = 1$. Tämä on ristiriita, joten yhtälöllä $X^{15} = 1$ on tarkalleen 15 ratkaisua. Lauseen 5.6 nojalla ryhmässä G on kertalukua 15 oleva normaali aliryhmä H. Tällöin jos P on kertalukua 2 oleva aliryhmä, niin aliryhmän PH kertaluku on 30.

□

Näin ollen Frobeniuksen otaksuma pätee kaikille kertalukua 60 oleville ryhmille. Jos $|G| = 60$, niin tapaus $n = |G|$ on selvä ja muille luvun 60 tekijöille n väite pätee yllä olevan perusteella. Erityisesti on todistettu jo aiemmin todettu tulos

Esimerkki 5.8. Frobeniuksen otaksuma pätee kun G on alternoiva ryhmä Alt(5).

Alkuluvun potenssien lisäksi on vielä yksi yleinen joukko lukuja, joille Frobeniuksen otaksuma saadaan suhteellisen helposti todistettua. Osoitetaan seuraavaksi, että otaksuma pätee kun n on neliövapaa. Tätä varten tarvitaan seuraava lemma, joka on hyödyllinen myös jatkossa.

Lemma 5.9. *Olkoon G ryhmä, p alkuluku ja pm luvun $|G|$ tekijä. Oletetaan lisäksi, että p on luvun pm pienin alkulukutekijä. Tällöin jos $a_m(G) < a_{pm}(G)$ ja $a_{pm}(G) = pm$, niin $a_m(G) = m$. Näin ollen erityisesti jos $p \nmid m$ ja $a_{pm}(G) = pm$, niin $a_m(G) = m$.*

Todistus. Frobeniuksen lauseen nojalla $a_m(G) = km$, missä $k \geq 1$ on kokonaisluku. Oletuksen nojalla $km < pm$, eli $1 \leq k < p$. Lemman 3.4 nojalla $p - 1 \mid a_{pm}(G) - a_m(G) = (p - k)m$. Koska p on luvun pm pienin alkulukutekijä, niin $(p - 1, m) = 1$ ja näin ollen $(p - 1) \mid (p - k)$. Koska $1 \leq k < p$, niin ainoa vaihtoehto on $k = 1$.

Oletetaan, että $p \nmid m$ ja $a_{pm}(G) = pm$. Koska p on luvun $|G|$ tekijä, niin ryhmässä G on kertalukua p oleva alkio x. Nyt $x^m \neq 1$, sillä muutoin

$p = |x| \mid m$. Näin ollen $a_m(G) < a_{pm}(G)$, joten $a_m(G) = m$ seuraa edellä olevasta. □

Seuraus 5.10. *Olkoon p alkuluku ja m kokonaisluku jonka alkulukutekijät ovat suurempia kuin p. Tällöin jos Frobeniuksen otaksuma pätee luvulle m, niin Frobeniuksen otaksuma pätee myös luvulle pm.*

Todistus. Oletetaan, että ryhmälle G pätee $pm \mid |G|$ ja $a_{pm}(G) = pm$. Nyt p on luvun pm pienin alkulukutekijä ja $p \nmid m$, joten lemman 5.9 nojalla $a_m(G) = m$. Koska Frobeniuksen otaksuma pätee luvulle m, niin ryhmässä G on kertalukua m oleva normaali aliryhmä M. Cauchyn lauseen nojalla ryhmässä G on myös kertalukua p oleva aliryhmä P. Tällöin PM on aliryhmä jonka kertaluku on pm. □

Seuraus 5.11. *Frobeniuksen otaksuma pätee kun $n = p_1 p_2 \dots p_t q^k$, missä $p_1 < p_2 < \dots < p_t < q$ ovat alkulukuja. Erityisesti siis otaksuma pätee kun n on neliövapaa.*

Todistus. Aiemmin todettiin, että Sylowin lauseen nojalla Frobeniuksen otaksuma pätee luvulle q^k, joten seurauksen 5.10 nojalla Frobeniuksen otaksuma pätee myös luvulle $p_t q^k$. Edelleen seurauksen 5.10 nojalla otaksuma pätee luvulle $p_{t-1} p_t q^k$. Näin jatkamalla nähdään, että Frobeniuksen otaksuma pätee luvulle $n = p_1 p_2 \dots p_t q^k$. □

5.3 Otaksuman todistaminen ja yksinkertaiset ryhmät

Siirrymme seuraavaksi tarkastelemaan Frobeniuksen otaksumaa yleisessä tapauksessa.

Lause 5.12. *Olkoon G ryhmä ja n luvun $|G|$ tekijä. Olkoon $H \trianglelefteq G$ ja merkitään $d = (n, |H|)$, $n = n_1 d$ sekä $|H| = h_1 d$. Tällöin*

(i) Jos $a_n(G) = n$, niin $a_{n_1}(G/H) = n_1$ ja $a_d(H) = d$.

(ii) Jos ryhmällä H on kertalukua d oleva karakteristinen aliryhmä T ja ryhmällä G/H on kertalukua n_1 oleva normaali aliryhmä K/H, niin ryhmällä G on kertalukua n oleva aliryhmä.

Todistus. (i) (Zemlin) Frobeniuksen lauseen nojalla $a_{n_1}(G/H) = kn_1$, missä $k \geq 1$ on kokonaisluku. Nyt jos $yH \in A_{n_1}(G/H)$, niin $y^{n_1} \in H$ ja tällöin $(y^{n_1})^{|H|} = 1$. Koska $n_1|H| = h_1 n$, niin $y^{h_1} \in A_n(G)$. Olkoon $yH, y'H \in A_{n_1}(G/H)$. Jos $y^{h_1}H = (y')^{h_1}H$, niin $y^{n_1}H = (y')^{n_1}H = H$ ja $(n_1, h_1) = 1$ nojalla $yH = y'H$. Näin ollen $A_{n_1}(G/H)$ eri alkioista saadaan muodostettua

eri sivuluokkia, jotka sisältävät joukon $A_n(G)$ alkioita. Tämän perusteella on olemassa ainakin kn_1 aliryhmän H sivuluokkaa jotka sisältävät joukon $A_n(G)$ alkioita.

Olkoot $y_1H, y_2H, \ldots, y_lH$ ne aliryhmän H sivuluokat jotka sisältävät joukon $A_n(G)$ alkioita, ja asetetaan $y_1 = 1$. Tällöin edellisen perusteella $l \geq kn_1$. Koska H on normaali aliryhmä, niin $HyH = y(y^{-1}Hy)H = yHH = yH$ kaikilla $y \in G$. Siispä seurauksen 4.9 nojalla kaikilla i pätee $a_n(y_iH) = \alpha_i d$, missä $\alpha_i \geq 1$ on kokonaisluku. Näin saadaan

$$n = a_n(G) = \sum_{i=1}^{l} a_n(y_iH) = \sum_{i=1}^{l} \alpha_i d \geq ld \geq kn_1 d = kn$$

joten $k = 1$ ja $\alpha_i = 1$. Näin ollen $a_{n_1}(G/H) = n_1$ ja $a_d(H) = \alpha_1 d = d$.

(ii) Koska K/H on ryhmän G/H normaali aliryhmä, niin K on ryhmän G normaali aliryhmä. Lisäksi koska T on karakteristinen, niin T on myös normaali ryhmässä K. Nyt $|K| = n_1 h_1 d$, jolloin $|K/T| = n_1 h_1$ ja $|H/T| = h_1$. Koska $(n_1, h_1) = 1$ ja H/T on normaali ryhmässä K/T, niin Schur-Zassenhausin lauseen (2.18) nojalla ryhmällä K/T on kertalukua n_1 oleva aliryhmä Q/T. Tällöin aliryhmän Q kertaluku on $n_1 d = n$. □

Seuraus 5.13. *Olkoon G ryhmä ja $H \trianglelefteq G$. Jos Frobeniuksen otaksuma pätee ryhmille H ja G/H, niin Frobeniuksen otaksuma pätee ryhmälle G.*

Todistus. Jos $n \mid |G|$ ja $a_n(G) = n$, niin soveltamatta lausetta 5.12 (i) saadaan $a_d(H) = d$ ja $a_{n_1}(G/H) = n_1$, missä $d = (n, |H|)$ ja $n = n_1 d$. Koska Frobeniuksen otaksuma pätee ryhmille H ja G/H, niin lauseen 5.12 (ii) nojalla ryhmällä G on kertalukua n oleva aliryhmä. □

Tämän seurauksen avulla saadaan helposti myös erilainen todistus Frobeniuksen otaksumalle ratkeavien ryhmien tapauksessa. Jos G on yksinkertainen ja ratkeava, niin $G \cong \mathbb{Z}_p$, missä p on alkuluku. Muutoin ryhmällä G on ei-triviaali normaali aliryhmä. Koska ratkeavan ryhmän aliryhmät ja tekijäryhmät ovat myös ratkeavia, Frobeniuksen otaksuma ratkeaville ryhmille saadaan seurauksen 5.13 ja induktion avulla. Lisäksi jos Frobeniuksen otaksuma ei päde ryhmälle G mutta pätee kaikille ryhmille joiden kertaluku on $< |G|$, niin seurauksen 5.13 nojalla G on yksinkertainen. Toisin sanoen

Seuraus 5.14 (Zemlin, 1954)**.** *Jos Frobeniuksen otaksuma ei pidä paikkansa, niin pienintä mahdollista kertalukua oleva vastaesimerkki Frobeniuksen otaksumalle on ei-kommutatiivinen yksinkertainen ryhmä.*

Itseasiassa seurauksen 5.13 todistusta tarkastelemalla huomataan, että samalla todistuksella saadaan vastaava tulos, jonka nojalla Frobeniuksen otaksuma voidaan todistaa luvulle n todistamalla se yksinkertaisille ryhmille.

Seuraus 5.15. *Olkoon n positiivinen kokonaisluku. Oletetaan, että Frobeniuksen otaksuma pätee kaikille luvun n tekijöille d joilla $d < n$. Olkoon G sellainen ryhmä, että Frobeniuksen otaksuma pätee parille (n, H) kaikilla ryhmillä H, joilla $|H| < |G|$. Jos G ei ole yksinkertainen, niin Frobeniuksen otaksuma pätee parille (n, G). Näin ollen pienintä mahdollista kertalukua oleva vastaesimerkki Frobeniuksen otaksumalle luvun n tapauksessa on ei-kommutatiivinen yksinkertainen ryhmä.*

Esimerkki 5.16. Frobeniuksen otaksuma pätee kun $n = 24 = 2^3 \cdot 3$.

Todistus. Olkoon G pienintä mahdollista kertalukua oleva vastaesimerkki Frobeniuksen otaksumalle luvun 24 tapauksessa. Aiemmin on osoitettu, että Frobeniuksen otaksuma pätee luvun 24 tekijöille jotka ovat < 24. Seurauksen 5.15 nojalla G on ei-kommutatiivinen yksinkertainen ryhmä. Koska G on yksinkertainen, niin ryhmällä G on ainakin kaksi kertalukua 8 olevaa aliryhmää, jotka sisältävät yhteensä ainakin $8+8-4 = 12$ alkiota. Jos k on ryhmän G kertalukua 3 olevien aliryhmien lukumäärä, niin tällöin $2k$ on kertalukua 3 olevien alkioiden lukumäärä. Näin ollen $12 + 2k \leq 24$, jolloin $k \leq 6$. Koska kertalukua 3 olevien aliryhmien lukumäärä on $\equiv 1 \mod 3$, niin $k = 1$ tai $k = 4$. Koska G on yksinkertainen, niin $k = 4$. Olkoot $P \leq G$ jokin kertalukua 3 oleva aliryhmä. Tällöin aliryhmän P konjugaattien kertaluku on 3, joten $[G : N_G(P)] \leq 4$. Näin ollen lemman 2.13 nojalla G on isomorfinen ryhmän $\mathrm{Sym}(r)$ aliryhmän kanssa, missä $r \leq 4$. Tämä on kuitenkin ristiriita, sillä tällöin $\mathrm{Sym}(r)$ on ratkeava ja G ei ole ratkeava. Näin ollen vastaesimerkkiä ei ole olemassa ja Frobeniuksen otaksuma pätee luvulle 24. □

Vastaavalla tekniikalla voidaan todistaa Frobeniuksen otaksuma monille luvuille. Esimerkiksi Robert McKean [25] osoitti vuonna 1973, että Frobeniuksen otaksuma pätee kun $n \leq 1000$. Esimerkin 5.16 tuloksen todistamista voi yrittää myös ilman seurauksen 5.15 apua, mutta näinkin pienen luvun tapauksessa tehtävä vaikuttaa vaikealta.

Seurauksen 5.13 nojalla Frobeniuksen otaksuman todistamiseksi riittää todistaa se yksinkertaisille ryhmille. Miten tämä onnistuu? Yksinkertaisten ryhmien tapauksessa induktiolla todistaminen ei toimi enää yhtä hyvin, sillä ei löydy normaalia aliryhmää H ja tekijäryhmää G/H joihin induktio-oletusta voitaisiin soveltaa.

Yksinkertaisten ryhmien luokittelun mukaan jokainen äärellinen yksinkertainen ryhmä on isomorfinen ryhmän kanssa, joka on jokin seuraavista [35]:

(i) $\mathbb{Z}_p$, missä p on alkuluku

(ii) Alternoiva ryhmä $\mathrm{Alt}(n)$, missä $n \geq 5$

(iii) Yksinkertainen Lie-tyypin ryhmä

(iv) Jokin 26 sporadisesta ryhmästä

Ainoa helppo tapaus on $\mathbb{Z}_p$. James Rust [24] todisti Frobeniuksen otaksuman alternoiville ryhmille vuonna 1966. Tällöin yksinkertaisten ryhmien luokittelu oli vielä pahasti kesken, ja seuraavan kerran ongelma eteni vasta 80-luvulla kun luokittelun uskottiin olevan valmis[7]. Tällöin Yamaki [28] [29] todisti tietokoneohjelman avulla otaksuman sporadisille ryhmille. Lisäksi Yamaki ja Iiyori todistivat otaksuman yksinkertaisille Lie-tyypin ryhmille. Todistus käytiin läpi neljässä artikkelissa, joista viimeinen [30] valmistui vuonna 1991. Tällöin Yamaki ja Iiyori [31] saattoivat ilmoittaa otaksuman todistetuksi, miltei sata vuotta sen jälkeen kun Frobenius todisti lauseensa.

Tällä hetkellä luokitteluun perustuva todistus on ainoa tunnettu todistus Frobeniuksen otaksumalle. Yksinkertaisten ryhmien luokittelu on kuitenkin valtava, satoja artikkeleita ja kymmeniä tuhansia sivuja kattava tulos. Todistuksen nojalla Frobeniuksen otaksuma pätee, mutta luokitteluun pohjautuvan todistuksen perusteella on hankalaa sanoa miksi näin on. Miksi yhtälön $X^n = 1$ ratkaisujen joukko muodostaa aliryhmän kun ratkaisuja on tasan n kappaletta?

Ongelma 5.17. *Voidaanko Frobeniuksen otaksuma todistaa ilman yksinkertaisten ryhmien luokittelua?*

Vaikuttaa siltä, että ainakin ryhmien esitysteoria on välttämätöntä Frobeniuksen otaksuman todistuksessa. Frobenius todisti yli sata vuotta sitten seuraavan tuloksen, jolle ei vieläkään tunneta todistusta ilman esitysteoriaa. Iiyori ja Yamaki huomauttavat artikkelissa [32], että tulos voidaan kuitenkin todistaa Frobeniuksen otaksuman avulla.

Lause 5.18 (Frobenius, 1901)**.** *Olkoon G ryhmä ja H ryhmän G aliryhmä, jolle $H \cap xHx^{-1} = \{1\}$ kaikilla $x \in G - H$. Tällöin $(|H|, [G : H]) = 1$ ja joukko*

$$N = \{1\} \cup (G - \bigcup_{g \in G} gHg^{-1})$$

[7]Gorenstein ilmoitti vuonna 1980 että yksinkertaisten ryhmien luokittelu oli valmis, mutta todellisuudessa todistuksessa oli vielä joitakin puutteita jotka huomattiin 80-luvun loppupuolella. Nämä puutteet paikattiin vuonna 2004 Aschbacherin ja Smithin toimesta, ja nykyään luokittelulausetta pidetään todistettuna (kts. [35]).

muodostaa kertalukua $[G : H]$ *olevan normaalin aliryhmän.*

Todistus. Jos $(|H|, [G : H]) \neq 1$, niin luvulla $(|H|, [G : H])$ on jokin alkulukutekijä p. Olkoon P ryhmän H Sylowin p-aliryhmä ja $|P| = p^k$, jolloin p^{k+1} jakaa ryhmän G kertaluvun. Voidaan osoittaa (esim. 2.15 (i) ja 2.16 avulla), että tällöin P sisältyy johonkin kertalukua p^{k+1} olevaan aliryhmään Q. Olkoon $x \in Q$. Nyt $P \triangleleft Q$ (lemma 2.16), joten $P \leq H \cap xHx^{-1}$. Näin ollen $H \cap xHx^{-1} \neq \{1\}$, ja oletuksen nojalla $x \in H$. Koska $\langle x \rangle \leq N_H(P)$ on p-ryhmä, niin $\langle x \rangle \leq P$ (lemma 2.15). Erityisesti $x \in P$, minkä nojalla $P = Q$. Tämä on ristiriita, joten $(|H|, [G : H]) = 1$.

Merkitään $n = [G : H]$. Oletuksen nojalla $H = N_G(H)$ ja $gHg^{-1} \cap g_0Hg_0^{-1} = \{1\}$ aina kun $gHg^{-1} \neq g_0Hg_0^{-1}$. Näin ollen yhdisteessä $\cup_{g \in G} gHg^{-1}$ on tarkalleen $[G : H](|H|-1)+1 = |G|-[G : H]+1$ alkiota, ja siten joukossa N on tarkalleen $1 + |G| - (|G| - [G : H] + 1) = [G : H] = n$ alkiota.

Nyt jos $x^n = 1$ ja $x \in gHg^{-1}$, niin $x^{|H|} = 1$ ja tällöin $x = 1$ koska $(|H|, n) = 1$. Näin ollen jos $x^n = 1$ ja $x \neq 1$, niin $x \in N$. Siispä $A_n(G) \subseteq N$ ja siten $N = A_n(G)$ koska joukossa $A_n(G)$ on ainakin n alkiota Frobeniuksen lauseen nojalla. Lopulta voidaan soveltaa Frobeniuksen otaksumaa. Koska $a_n(G) = n$, niin $A_n(G) = N$ muodostaa normaalin aliryhmän. □

Aiemmin osoitettiin, että Frobeniuksen otaksuma pätee ratkeaville ryhmille. Näin ollen yllä olevan todistuksen avulla nähdään ilman esitysteoriaa ja yksinkertaisten ryhmien luokittelua, että lause 5.18 pätee kun G on ratkeava. Tämä ei kuitenkaan ole mitään uutta, sillä puhtaan ryhmäteorian avulla voidaan osoittaa, että lause pätee muun muassa kun H on ratkeava tai kun $|H|$ on parillinen [36, Lemma 2.2].

5.4 Frobeniuksen otaksuma muille yhtälöille

Frobeniuksen otaksuman voi tietysti yleistää ja tarkastella sitä muillekin yhtälöille kuin $X^n = 1$. Olkoon G ryhmä, $\phi \in \mathrm{Aut}(G)$ ja $\phi^n = I$. Luvussa 4 tarkasteltiin yhtälöä

$$x \cdot \phi(x) \cdot \phi^2(x) \cdot \ldots \cdot \phi^{n-1}(x) = 1.$$

Käytetään yhtälön ratkaisujen joukosta merkintää $L_n(G, \phi)$. Kuten aiemmin todettiin, niin tällöin yhtälön ratkaisujen lukumäärä on luvun $(n, |G|)$ monikerta. Voidaanko Frobeniuksen otaksuma yleistää tälle yhtälölle? Toisin sanoen: jos n jakaa luvun $|G|$ ja $|L_n(G, \phi)| = n$, niin muodostaako $L_n(G, \phi)$ aliryhmän? Frobeniuksen otaksuman perusteella tämä pätee kun $\phi = I$.

Seuraava vastaesimerkki [22] osoittaa, että yleisesti väite ei päde. Olkoon $G = \mathrm{Alt}(4)$ ja $\phi \in \mathrm{Aut}(G)$ konjugointi transpoosilla (12), eli toisin sanoen

$\sigma \mapsto (12)\sigma(12)$ kaikilla $\sigma \in G$. Tällöin $\phi^6 = I$ ja $|L_6(G, \phi)| = 6$. Nyt $L_6(G, \phi)$ ei kuitenkaan muodosta aliryhmää, sillä ryhmällä Alt(4) ei ole kertalukua 6 olevaa aliryhmää.

Murai ja Takegahara ovat kuitenkin osoittaneet artikkelissa [22], että jos G on nilpotentti, niin väite pätee. Lisäksi väite pätee myös ratkeaville ryhmille tietyillä lisäoletuksilla.

6 Aliryhmä $B_n(G)$

Olkoon G ryhmä ja n positiivinen kokonaisluku. Määritellään

$$B_n(G) = \langle x \in G : x^n = 1 \rangle.$$

Nyt siis $B_n(G) = \langle A_n(G) \rangle$ on yhtälön $X^n = 1$ ratkaisujen generoima aliryhmä. Jos ϕ on ryhmän G automorfismi, niin $\phi(x)^n = 1$ jos ja vain jos $x^n = 1$. Näin ollen $B_n(G)$ on ryhmän G karakteristinen aliryhmä ja erityisesti siis normaali aliryhmä.

Lemma 6.1. *Olkoon G ryhmä ja n luvun $|G|$ tekijä. Tällöin aliryhmän $B_n(G)$ kertaluku on jaollinen luvulla n.*

Todistus. Olkoon p^k suurin alkuluvun p potenssi joka jakaa luvun n. Sylowin lauseen nojalla ryhmässä G on kertalukua p^k oleva aliryhmä H. Koska p^k on luvun n tekijä, niin $H \leq B_n(G)$, joten Lagrangen lauseen nojalla $p^k \mid |B_n(G)|$. Tämän perusteella $|B_n(G)|$ on luvun n monikerta. □

Olkoon G on pienintä mahdollista kertalukua oleva vastaesimerkki Frobeniuksen otaksumalle. Nyt siis Frobeniuksen otaksuma pätee ryhmille joiden kertaluku on $< |G|$, ja lisäksi löytyy kokonaisluku n jolle $n \mid |G|$ ja $a_n(G) = n$, mutta $A_n(G)$ ei ole aliryhmä. Lemman nojalla $B_n(G) = G$, sillä muutoin $B_n(G)$ sisältää kertalukua n olevan aliryhmän ryhmän G minimaalisuuden nojalla. Koska $B_n(G)$ on normaali aliryhmä, niin tämä tietysti seuraa myös siitä, että ryhmän G täytyy olla yksinkertainen (seuraus 5.14).

Osoitetaan seuraavaksi, että ryhmän $B_n(G)$ alkiot voidaan asettaa tiettyyn muotoon. Tämän avulla saadaan yläraja ryhmän $B_n(G)$ kertaluvulle. Tulos on luultavasti Zemlinin, joka todisti sen väitöskirjassaan [23, 2.3, s. 5]. Todistus on kuitenkin hieman monimutkainen ja pitkä, joten todistamme sen tässä erilaisella tavalla.

Lause 6.2. *Olkoon G ryhmä ja n positiivinen kokonaisluku. Merkitään $a = a_n(G)$. Olkoon $A_n(G) = \{x_1, x_2, x_3, \ldots, x_a\}$, missä $x_1 = 1$. Tällöin jokainen ryhmän $B_n(G)$ alkio x on muotoa $x = x_2^{d_2} x_3^{d_3} \cdots x_a^{d_a}$, missä $d_i \in \{0, 1\}$.*

Todistus. Nyt kaikilla alkioilla x_i ja kokonaisluvuilla s pätee

$$(x_i)^s = x_j \qquad (*)$$

jollekin x_j, sillä $(x_i^s)^n = (x_i^n)^s = 1$. Lisäksi koska $A_n(G)$ on suljettu konjugoinnin suhteen, niin kaikilla x_i ja x_j pätee

$$x_j x_i = x_i x_k \qquad (**)$$

jollakin x_k.

Olkoon $x \in B_n(G)$. Koska $A_n(G)$ generoi ryhmän $B_n(G)$, niin lemman 2.11 nojalla x on joukon $A_n(G)$ alkioiden tulo, eli $x = x_{i_1}x_{i_2}\cdots x_{i_t}$. Valitaan tälläinen esitys niin, että luku $t \geq 1$ on pienin mahdollinen. Nyt yhtälöä (**) soveltamalla voidaan tulon tekijää x_{i_α} siirtää askel vasemmalle ilman, että tekijöiden määrä muuttuu. Lisäksi siirron jälkeen tulon tekijät pysyvät samana, lukuunottamatta mahdollisesti tekijää $x_{i_{\alpha-1}}$.

Näin ollen $x_{i_\alpha} \neq x_{i_\beta}$ kaikilla $i_\alpha \neq i_\beta$. Jos tulossa esiintyisi kaksi samaa tekijää, niin nämä tekijät voidaan siirtää vierekkäin yhtälön (**) avulla ilman että tekijöiden määrä muuttuu, mutta tämän jälkeen yhtälön (*) avulla saadaan alkiolle x esitys, jossa on vähemmän kuin t tekijää.

Tämän perusteella alkiolle x saadaan sellainen tuloesitys, että $i_1 < i_2 < \ldots < i_t$. Tämä pätee kun $t = 1$, joten olkoon $t > 1$ ja oletetaan että tuloesitys on osoitettu kun tulon termien lukumäärä on $< t$. Valitaan t alkion tuloesitys alkiolle x siten, että $\min\{i_1, i_2, \ldots, i_t\} = i_\alpha$ on pienin mahdollinen. Yhtälön (**) avulla x_{i_α} voidaan siirtää tulon vasempaan reunaan, ja tällöin x saadaan muotoon $x = x_{i_\alpha}x_{j_2}\cdots x_{j_t}$. Induktiolla alkio $x_{j_2}\cdots x_{j_t}$ saadaan sellaiseen muotoon, että $j_2 < \ldots < j_t$. Koska i_α on pienin mahdollinen, niin täytyy olla $i_\alpha < j_2 < \ldots < j_t$. Näin ollen alkio x on muotoa $x = x_{i_1}x_{i_2}\cdots x_{i_t}$, missä $i_1 < i_2 < \ldots < i_t$, ja siten

$$x = x_1^{d_1}x_2^{d_2}x_3^{d_3}\cdots x_a^{d_a}$$

missä $d_j = 1$ jos $j = i_k$ jollakin k ja $d_j = 0$ muulloin. Koska $x_1 = 1$, niin tuloesitys on haluttua muotoa.

□

Zemlinin alkuperäinen todistus on konstruktiivinen. Hän osoittaa, että yhtälöitä (*) ja (**) soveltamalla mikä tahansa ryhmän $B_n(G)$ alkio saadaan lauseen 6.2 muotoon.

Seuraus 6.3. *Olkoon G ryhmä, n positiivinen kokonaisluku ja $a = a_n(G)$. Tällöin $|B_n(G)| \leq 2^{a-1}$.*

Tässä seurauksena saatu yläraja on tietysti hyvin heikko, eikä yleensä ole yhtään parempi kuin triviaali yläraja $|B_n(G)| \leq |G|$. Nyt $|G| > 2^{a-1}$ jos ja vain jos $a < \log_2(|G|) + 1$. Tämän perusteella $B_n(G)$ on aito aliryhmä jos $a_n(G) < \log_2(|G|) + 1$.

Jos n on alkuluku, niin saadaan hieman parempi yläraja.

Seuraus 6.4. *Olkoon G ryhmä, p alkuluku ja $a = a_p(G)$. Tällöin $|B_p(G)| \leq p^{\frac{a-1}{p-1}}$.*

Todistus. Nyt $a = t(p-1)+1$, missä t on kertalukua p olevien syklisten aliryhmien lukumäärä. Valitaan kustakin aliryhmästä yksi generoiva alkio y_i, jolloin kaikki joukon $A_p(G)$ alkiot voidaan esittää alkioiden $y_1, y_2, \ldots, y_t$ potensseina. Toisin sanoen

$$A_n(G) = \{1, y_1, y_1^2, \ldots, y_1^{p-1}, \ldots, y_t, y_t^2, \ldots, y_t^{p-1}\}$$

joten lauseen 6.2 nojalla jokainen ryhmän $B_p(G)$ alkio on muotoa

$$y_1^{d_1} y_2^{d_2} \cdots y_t^{d_t},$$

missä $d_i \in \{0, 1, \ldots, p-1\}$. Näin ollen ryhmässä $B_p(G)$ on korkeintaan p^t alkiota. Koska $t = \frac{a-1}{p-1}$, niin väite on todistettu.

□

Entä päteekö vastaava epäyhtälö mille tahansa kokonaisluvulle n? Onko siis $|B_n(G)| \leq n^{\frac{a_n(G)-1}{n-1}}$? Tämä on yleistys Frobeniuksen otaksumasta, sillä tapauksessa $a_n(G) = n$ epäyhtälöstä seuraa $|B_n(G)| \leq n$, jolloin $|B_n(G)| = n$.

Ongelma 6.5. *Päteekö* $|B_n(G)| \leq n^{\frac{a_n(G)-1}{n-1}}$ *mille tahansa ryhmälle* G *ja kokonaisluvulle* $n > 1$*?*

Tämä ongelma ei ole ilmeisesti esiintynyt kirjallisuudessa. Yleisen tapauksen sijaan aliryhmän $B_n(G)$ ominaisuuksia onkin tarkasteltu enemmän p-ryhmien tapauksessa. Kun G on p-ryhmä, ryhmän G *omega-aliryhmät* ovat aliryhmät

$$\Omega_a(G) = \langle x \in G : x^{p^a} = 1 \rangle$$

ja vastaavasti määritellään *agemo-aliryhmät* asettamalla

$$\mho_a(G) = \langle x^{p^a} : x \in G \rangle.$$

Tässä siis $\Omega_a(G) = B_{p^a}(G)$. Nämä aliryhmät esiintyivät ensimmäisen kerran Philip Hallin p-ryhmiin liittyvissä tutkimuksissa [14]. Niiden avulla saadaan erittäin paljon tietoa tiettyjen p-ryhmien rakenteesta.

7 Sovelluksia ja esimerkkejä

7.1 Lukuteoreettinen sovellus

Olkoon G ryhmä jonka kertaluku on jaollinen luvulla n. Frobeniuksen lauseen nojalla saadaan kongruenssi $a_n(G) \equiv 0 \mod n$. Näin ollen jos luvulle $a_n(G)$ löytyy kaava tiettyjen ryhmien joukossa, niin kyseinen kaava on aina $\equiv 0 \mod n$. Esimerkiksi symmetrisille ryhmille ja alternoiville ryhmille tälläinen kaava voidaan usein määrätä, sillä permutaation kertaluku määräytyy sen syklirakenteen perusteella.

Esimerkiksi jos p on alkuluku ja $n \geq p$ on kokonaisluku, niin symmetrisessä ryhmässä $\mathrm{Sym}(n)$ yhtälön $X^p = 1$ ratkaisut ovat tarkalleen kaikki erillisten p-syklien tulot sekä neutraalialkio. Nyt erillisten p-syklien tuloja, joissa tekijöitä on k kappaletta, löytyy symmetrisestä ryhmästä $\mathrm{Sym}(n)$ tarkalleen

$$\frac{n!}{p^k(n-pk)!k!}$$

kappaletta. Tässä $1 \leq k \leq \lfloor \frac{n}{p} \rfloor$, missä $\lfloor \frac{n}{p} \rfloor$ on suurin kokonaisluku $\leq \frac{n}{p}$. Näin ollen Frobeniuksen lauseesta seuraa kongruenssi

$$\sum_{k=1}^{\lfloor \frac{n}{p} \rfloor} \frac{n!}{p^k(n-pk)!k!} \equiv -1 \mod p.$$

Huomaa, että tapauksessa $n = p$ saadaan $(p-1)! \equiv -1 \mod p$ (Wilsonin lause). Vastaavanlaisia kongruensseja löytyy lisää laskemalla tiettyä kertalukua olevien alkioiden lukumääriä muissa ryhmissä.

7.2 Z-ryhmät

Jos ryhmän G jokainen Sylowin aliryhmä on syklinen, niin sanotaan, että G on *Z-ryhmä* (engl. Z-group). Tällöin ryhmän G rakenteesta voidaan kertoa paljon. Yleensä Z-ryhmien ratkeavuus todistetaan oppikirjoissa Burnsiden lauseen avulla, katso esimerkiksi [4, s. 197, Theorem 7.5.3.]. Tulos seuraa myös Frobeniuksen lauseen avulla.

Lause 7.1. *Olkoon G ryhmä kertalukua $|G| = p_1^{a_1} \dots p_t^{a_t}$, missä $p_1 < p_2 < \dots < p_t$ ovat alkulukuja. Oletetaan, että ryhmän G Sylowin aliryhmät ovat syklisiä. Tällöin kaikilla $m = p_j^{b_j} p_{j+1}^{a_{j+1}} \dots p_t^{a_t}$, missä $b_j \leq a_j$, yhtälöllä $X^m = 1$ on ryhmässä G tarkalleen m ratkaisua. Lisäksi G on ratkeava ja sen Sylowin p_t-aliryhmä on normaali aliryhmä.*

Todistus. Ensimmäinen väite pätee kun $j = 1$, $b_1 = a_1$, sillä tällöin $m = |G|$. Oletetaan, että väite on todistettu kaikille luvuille jotka ovat annettua muotoa ja suurempia kuin m. Olkoon p luvun $|G|/m$ suurin alkulukutekijä. Oletuksen nojalla yhtälöllä $x^{pm} = 1$ on tarkalleen pm ratkaisua. Olkoon p^{a-1} suurin alkuluvun p potenssi joka jakaa luvun m. Koska ryhmän G Sylowin p-aliryhmät ovat syklisiä, niin ryhmässä G on kertalukua p^a oleva alkio x. Tällöin $x^m \neq 1$, sillä $p^a \nmid m$. Näin ollen $a_m(G) < a_{mp}(G)$, ja lemman 5.9 nojalla yhtälöllä $x^m = 1$ on tarkalleen m ratkaisua. Induktiolla väite pätee siis kaikille luvuille m jotka ovat annettua muotoa.

Erityisesti ensimmäinen väite pätee kun $m = p_t^{a_t}$, joten ryhmässä G on normaali Sylowin p_t-aliryhmä P_t. Jos $t = 1$, niin ryhmä G on syklinen ja siten ratkeava. Olkoon $t > 1$ ja kaikilla $1 \leq i < t$ aliryhmä P_i jokin Sylowin p_i-aliryhmä. Tällöin P_iP_t/P_t on ryhmän G/P_t Sylowin p_i-aliryhmä. Lisäksi $P_iP_t/P_t \cong P_i/P_i \cap P_t$, joten P_iP_t/P_t on syklinen koska P_i on syklinen. Näin ollen ryhmän G/P_t kaikki Sylowin aliryhmät ovat syklisiä ja induktiolla G/P_t on ratkeava. Koska P_t on syklisenä ryhmänä ratkeava, niin myös G on ratkeava. □

Lisää Z-ryhmien rakenteesta löytyy esimerkiksi lähteestä [1, s.146-148, Theorem 9.4.3.], johon yllä oleva todistus perustuu. Aiemmin todistettiin, että Frobeniuksen otaksuma pätee ratkeaville ryhmille. Näin ollen lauseesta 7.1 saadaan

Seuraus 7.2. *Olkoon G kuten edellä. Tällöin ryhmässä G on yksikäsitteinen kertalukua m oleva aliryhmä H kaikille $m = p_j^{b_j} p_{j+1}^{a_{j+1}} \dots p_t^{a_t}$, missä $b_j \leq a_j$. Erityisesti H on siis normaali aliryhmä.*

Erityisesti seurauksena saadaan aiemmin mainittu Frobeniuksen [9] tulos, sillä jos ryhmän kertaluku on alkuluku, niin ryhmä on syklinen.

Seuraus 7.3 (Frobenius, 1893)**.** *Jos ryhmän G kertaluku on neliövapaa, niin G on ratkeava.*

Frobenius itse todisti tämän tuloksen seuraavan lauseen avulla. Kuten edellä, todistus perustuu lemman 5.9 käyttöön. Frobeniuksen alkuperäinen todistus oli monimutkaisempi, sillä hän todisti Frobeniuksen lauseen vasta myöhemmin.

Lause 7.4 (Frobenius, 1893)**.** *Olkoon G ryhmä, jonka kertaluku $|G| = mn$, missä $m = p_1p_2 \dots p_t$, $n = q_1^{a_1}q_2^{a_2} \dots q_s^{a_s}$ ja $p_1 < p_2 < \dots < p_t < q_1 < q_2 < \dots < q_s$ ovat alkulukuja. Tällöin yhtälöllä $X^n = 1$ on tarkalleen n ratkaisua ryhmässä G.*

Todistus. Nyt $a_{mn}(G) = mn = p_1(\frac{m}{p_1}n)$, joten lemman 5.9 nojalla $a_{\frac{m}{p_1}n}(G) = \frac{m}{p_1}n = p_2(\frac{m}{p_1p_2}n)$. Edelleen lemman 5.9 nojalla $a_{\frac{m}{p_1p_2}n}(G) = \frac{m}{p_1p_2}n = p_3\frac{m}{p_1p_2p_3}n$. Koska $n = \frac{m}{p_1p_2\ldots p_t}n$, niin induktiolla nähdään, että $a_n(G) = n$.

□

7.3 Sylowin aliryhmistä

Olkoon p alkuluku ja $n \geq 1$ kokonaisluku. Oletetaan jatkossa, että G on ryhmä jonka Sylowin p-aliryhmien kertaluku on p^n. Olkoon lisäksi $n_p(G)$ ryhmän G Sylowin p-aliryhmien lukumäärä.

Kuinka paljon eri alkioita on ryhmän G Sylowin p-aliryhmissä? Toisin sanoen, mikä on ryhmän G kaikkien Sylowin p-aliryhmien yhdisteen kertaluku? Nyt alkio $x \in G$ kuuluu johonkin Sylowin p-aliryhmään jos ja vain jos $x^{p^n} = 1$, joten Sylowin p-aliryhmien yhdisteen kertaluku on $a_{p^n}(G)$. Tarkastelemme seuraavaksi miten Sylowin p-aliryhmien lukumäärä $n_p(G)$ vaikuttaa lukuun $a_{p^n}(G)$.

Lause 7.5 (G. A. Miller, 1916)**.** *Merkitään $n_p(G) = kp + 1$. Tällöin*

(i) Jos $k = 0$, niin $a_{p^n}(G) = p^n$.

(ii) Jos $k = 1$, niin $a_{p^n}(G) = p^{n+1}$.

(iii) Jos $k \geq 2$, niin $a_{p^n}(G) \geq (2p-1)p^n$.

Todistus. Huomaa, että Sylowin lauseen nojalla oletus $n_p(G) \equiv 1 \mod p$ on järkevä. Lisäksi lause käy läpi kaikki mahdolliset tapaukset. Tapauksessa (i) Sylowin p-aliryhmiä on tarkalleen yksi, joten eri alkioita Sylowin p-aliryhmissä on tarkalleen p^n kappaletta.

Olkoon P jokin Sylowin p-aliryhmä. Jos Sylowin p-aliryhmiä on $p+1$ kappaletta, niin Sylowin lauseen ja lemman 2.13 nojalla tällöin on olemassa homomorfismi $\phi : G \to S_{p+1}$, missä

$$\operatorname{Ker}(\phi) = \bigcap_{g \in G} N_G(gPg^{-1}).$$

Homomorfismien peruslauseen nojalla $|G|/|\operatorname{Ker}(\phi)|$ jakaa ryhmän S_{p+1} kertaluvun. Koska p on alkuluku, niin $p \mid (p+1)!$ ja $p^2 \nmid (p+1)!$. Näin ollen $p^{n-1} \mid |\operatorname{Ker}(\phi)|$. Sylowin lauseen nojalla löytyy aliryhmä $T \leq \operatorname{Ker}(\phi)$, missä $|T| = p^{n-1}$. Tällöin kaikilla $g \in G$ pätee $T \leq N_G(gPg^{-1})$, jolloin $T \leq gPg^{-1}$ koska T on p-ryhmä (lemma 2.15). Näin ollen T sisältyy jokaiseen Sylowin p-aliryhmään. Tämän perusteella kaikkien Sylowin p-aliryhmien leikkauksen

kertaluku on p^{n-1}, joten niiden yhdisteessä on yhteensä $(p+1)(p^n - p^{n-1}) + p^{n-1} = p^{n+1}$ alkiota. Näin ollen (ii) pätee.

Tarkastellaan lopuksi vielä tapaus (iii), jossa Sylowin p-aliryhmiä on enemmän kuin $p+1$ kappaletta. Osoitetaan ensin, että $a_{p^n}(G) > p^{n+1}$. Olkoot $P_1 \neq P_2$ Sylowin p-aliryhmiä joiden leikkaus $D = P_1 \cap P_2$ on kertaluvultaan suurin mahdollinen, ja merkitään $|D| = p^k$. Koska p-ryhmät toteuttavat normalisoijaehdon (lause 2.16), niin $D < N_{P_1}(D)$. Voidaan siis valita $g \in N_{P_1}(D)$ jolle pätee $g \notin D$, ja tällöin $g \notin P_2$. Merkitään $H = \langle g \rangle$. Nyt muotoa xP_2x^{-1}, missä $x \in H$, olevia aliryhmän P_2 konjugaatteja on $[H : N_G(P_2) \cap H] = [H : P_2 \cap H]$ kappaletta, sillä $N_G(P_2) \cap H = P_2 \cap H$ (lemma 2.15). Tälläisiä konjugaatteja on siis ainakin p kappaletta, ja jokainen niistä sisältää aliryhmän D koska $H \leq N_{P_1}(D)$. Lisäksi koska $P_1 \neq P_2$, niin mikään konjugaateista ei voi olla aliryhmä P_1.

Olkoon $P_1, P_2, \ldots, P_s$ aliryhmän D sisältävät Sylowin p-aliryhmät, jolloin $s \geq p+1$ edellisen perusteella. Aliryhmän D kertaluvun maksimaalisuuden nojalla $P_i \cap P_j = D$ kaikilla $i \neq j$, joten yhdistessä $P_1 \cup P_2 \cup \ldots \cup P_s$ on tarkalleen $s(p^n - p^k) + p^k$ alkiota. Jos $s > p+1$ tai $k < n-1$, niin tämä lukumäärä on $> p^{n+1}$.

Voidaan siis olettaa, että $s = p+1$ ja $k = n-1$, jolloin yhdisteessä on tarkalleen p^{n+1} alkiota. Tällöin D on normaali aliryhmässä P_i kaikilla i (lause 2.16). Näin ollen jos $g \in P_1 \cup P_2 \cup \ldots P_s$, niin kaikilla i pätee $gP_ig^{-1} = P_j$ jollain j, sillä $D \leq gP_ig^{-1}$. Olkoon P jokin Sylowin p-aliryhmä joka ei ole mikään aliryhmistä P_i. Nyt riittää osoittaa, että löytyy $x \in P$ jolle xP_1x^{-1} ei ole mikään aliryhmistä P_i. Tällöin $x \notin P_1 \cup P_2 \cup \ldots \cup P_s$ edellisen perusteella. Koska yhdisteessä on tarkalleen p^{n+1} alkiota, niin tästä seuraa $a_{p^n}(G) > p^{n+1}$.

Aliryhmän P_1 konjugaattien xP_1x^{-1}, missä $x \in P$, lukumäärä on tarkalleen $[P : P \cap P_1] \geq p$. Jos $[P : P \cap P_1] > p$, niin tällöin konjugaatteja on enemmän kuin $p+1$ kappaletta, jolloin jokin xP_1x^{-1} ei ole mikään aliryhmistä P_i. Jos $[P : P \cap P_1] = p$, niin löytyy ainakin yksi P_i joka ei ole muotoa xP_1x^{-1}, missä $x \in P$. Tällöin aliryhmällä P_i on konjugaatteja xP_ix^{-1}, missä $x \in P$, tarkalleen $[P : P \cap P_i] \geq p$ kappaletta. Koska $p \geq 2$, niin jokin näistä konjugaateista ei ole mikään aliryhmistä P_i.

Frobeniuksen lauseen nojalla $a_{p^n}(G) = tp^n$, missä $t > p$ äskeisen perusteella. Nyt $a_{p^n}(G) - 1$ on niiden alkioiden lukumäärä, joiden kertaluku on p^k jollakin $1 \leq k \leq n$. Lemman 3.3 nojalla $a_{p^n}(G) - 1$ on siis luvun $p-1$ monikerta. Näin ollen $0 \equiv tp^n - 1 = (t-1)p^n + p^n - 1 \equiv (t-1)p^n \mod p-1$, jolloin $t-1 \equiv 0 \mod p-1$ koska $(p^n, p-1) = 1$. Tämän perusteella $t-1$ on luvun $p-1$ monikerta. Koska $t > p$, niin $t-1 \geq 2(p-1)$ ja tällöin $t \geq 2p-1$. Tämän avulla saadaan $a_{p^n}(G) = tp^n \geq (2p-1)p^n$.

□

Todistus osoittaa, että $a_{p^n}(G) = tp^n$ ei voi olla mikä tahansa luvun p^n monikerta, kun ryhmän G Sylowin aliryhmien kertaluku on p^n. Erityisesti nähdään, että koskaan ei päde $1 < t < p$ ja jos $t > p$, niin $t \geq 2p-1$. Tämän lisäksi luvun $t-1$ täytyy olla luvun $p-1$ monikerta.

Kun Sylowin p-aliryhmien määrä kasvaa, niin myös alkioiden määrä Sylowin p-aliryhmien joukossa kasvaa. Koska jokainen Sylowin p-aliryhmä sisältää p^n kappaletta joukon $A_{p^n}(G)$ alkioita, niin saadaan epäyhtälö

$$a_{p^n}(G)^{p^n} \geq \binom{a_{p^n}(G)}{p^n} \geq n_p(G).$$

Tämän perusteella

$$a_{p^n}(G) \geq n_p(G)^{p^{-n}}$$

ja $a_{p^n}(G) \to \infty$ kun $n_p(G) \to \infty$. Tämä on tietysti erittäin heikko alaraja, mutta on silti vakioalarajaa $(2p-1)p^n$ parempi kun $n_p(G)$ on erittäin suuri. Seuraavaa ongelmaa on siis mielenkiintoista pohtia.

Ongelma 7.6. *Paranna lauseen 7.5 alarajaa luvulle $a_{p^n}(G)$ tapauksessa $k > 2$.*

Lähteissä [3, §32, s. 79-81] ja [12] G. A. Miller todistaa lauseen 7.5, mutta ei vie tarkastelua sen pidemmälle. Muuta ongelmaan liittyvää ei vaikuta löytyvän kirjallisuudesta. Olisi kuitenkin mielenkiintoista selvittää, miten $a_{p^n}(G)$ kasvaa kun Sylowin p-aliryhmien lukumäärä kasvaa. Onko kasvu esimerkiksi lineaarista Sylowin p-aliryhmien lukumäärän suhteen? Seuraavassa huomioita joistakin erikoistapauksista.

Tapauksessa $k = 2$ lauseen 7.5 alaraja on paras mahdollinen. Emme käy tässä läpi yksityiskohtia, mutta tämä nähdään seuraavalla tavalla. Olkoon $n_p(G) = 2p+1$. Tällöin $a_{p^n}(G) = tp^n$, missä $t \geq 2p-1$. Lisäksi on selvää, että $t < 2p+1$, joten $t = 2p-1$ tai $t = 2p$. Jos p on pariton alkuluku, niin $2p$ ei ole jaollinen luvulla $p-1$, joten tällöin $t = 2p-1$. Riittää siis tarkastella tapausta $p = 2$. Olkoon $H = \mathrm{AGL}(1,5)$ kunnan $\mathbb{Z}_5$ kääntyvien affiinien muunnoksien muodostama ryhmä. Tässä siis ryhmän H alkiot ovat kaikki kuvaukset $x \mapsto ax + b$, missä $a, b \in \mathbb{Z}_5$ ja $a \neq 0$. Näin ollen ryhmän H kertaluku on 20. Nähdään, että ryhmälle H pätee $n_p(H) = 5 = 2p+1$ ja $a_{p^n}(H) = 6 = p(2p-1)$. Tällöin jos $G = \mathbb{Z}_{2^{n-1}} \times H$, niin ryhmän G Sylowin 2-aliryhmien kertaluku on 2^n. Voidaan osoittaa, että jos A ja B ovat ryhmiä ja q on alkuluku, niin tällöin pätee $n_q(A \times B) = n_q(A)n_q(B)$ sekä $a_{q^n}(A \times B) = a_{q^n}(A)a_{q^n}(B)$. Näin ollen $n_p(G) = 2p+1$ ja $a_{p^n}(G) = (2p-1)p^n$ ja G saavuttaa lauseen 7.5 alarajan.

Kun $k \geq 2$, niin ongelmia saattaa aiheuttaa se, että tällöin ei välttämättä ole olemassa ryhmää G jolle pätee $n_p(G) = kp + 1$. Jos $p = 2$ niin tätä ongelmaa ei ole, mutta millä tahansa parittomalla alkuluvulla p joudutaan vaikeuksiin. Marshall Hall on tutkinut lukuja r joille pätee $r \equiv 1 \mod p$, mutta $n_p(G) \neq r$ millä tahansa ryhmällä G. Hall todistaa artikkelissa [37] tuloksen, jonka avulla nähdään, että on olemassa ryhmä G jolle $n_p(G) = 2p+1$ jos ja vain jos $2p+1$ on alkuluvun potenssi [37, Theorem 3.1]. Tapauksessa $k = 3$ tilanne on vielä rajoitetumpi: on olemassa ryhmä G jolle $n_p(G) = 3p+1$ jos ja vain jos $p = 2$, $p = 3$ tai $p = 5$ [37, Theorem 3.2]. Näiden tulosten todistaminen vaatii melko paljon työtä, joten parhaan mahdollisen alarajan löytäminen kaikille $k > 2$ on varmasti vaikea ongelma.

Jos ryhmän G Sylowin p-aliryhmät ovat syklisiä, niin tällöin jokainen Sylowin p-aliryhmän generoiva alkio sisältyy tarkalleen yhteen Sylowin p-aliryhmään. Tässä tapauksessa saadaan alaraja $a_{p^n}(G) \geq n_p(G)\varphi(p^n) + p^{n-1} = n_p(G)(p^n - p^{n-1}) + p^{n-1}$. Tämä alaraja ei kuitenkaan välttämättä päde jos ryhmän G Sylowin p-aliryhmät eivät ole syklisiä. Lisäksi on olemassa ryhmiä G, joissa jokainen Sylowin p-aliryhmän alkio sisältyy ainakin kahteen Sylowin p-aliryhmään, ja joissa epäyhtälö $a_{p^n}(G) \geq n_p(G)$ ei päde. Sivuutamme todistuksen, mutta voidaan osoittaa, että ryhmässä $G = \mathrm{PSL}(2, 19)$ Sylowin 2-aliryhmillä on tämä ominaisuus[8]. Ryhmän G Sylowin 2-aliryhmien kertaluku on 2^2 ja tietokoneohjelmalla (esim. GAP [41]) voidaan tarkistaa, että $a_{2^2}(G) = 172$ ja $n_2(G) = 285$, joten $a_{2^2}(G) < n_2(G)$. Pienin esimerkki vaikuttaa olevan eräs kertalukua 180 oleva ryhmä, joka löytyy GAP-ohjelmiston komennolla `SmallGroup(180, 30)`. Myös tämän ryhmän Sylowin 2-aliryhmillä on mainittu ominaisuus.

7.4 Kertalukua p^k olevien aliryhmien lukumäärä

Kun Frobenius [10] ensimmäisen kerran todisti lauseensa vuonna 1895, ei artikkelin päätulos ollut tässä tutkielmassa käsiteltävä Frobeniuksen lause. Sen sijaan Frobenius sovelsi sitä seuraavan Sylowin lauseen yleistyksen todistamiseen, jonka todistamme seuraavaksi. Todistus on käytännössä samanlainen kuin Frobeniuksen alkuperäinen todistus.

Lause 7.7 (G. Frobenius, 1895)**.** *Olkoon p alkuluku. Ryhmässä G kertalukua p^k olevien aliryhmien lukumäärä on $\equiv 1 \mod p$ kaikilla $1 \leq k \leq n$, missä p^n on ryhmän G Sylowin p-aliryhmien kertaluku.*

Todistus. Olkoon s_k ryhmän G kertalukua p^k olevien aliryhmien lukumäärä.

[8] Olkoon q alkuluvun potenssi. Tällöin $\mathrm{PSL}(2, q)$ on projektiivinen erityinen lineaarinen ryhmä astetta 2 kertalukua q olevan äärellisen kunnan yli [4, Chapter 8, s.224-227].

Frobeniuksen lauseen nojalla $s_1(p-1)+1 \equiv 0 \mod p$, joten $s_1 \equiv 1 \mod p$. Artikkelissaan [10] Frobenius osoittaa, että

$$s_k \equiv s_{k+1} \mod p \qquad (*)$$

kaikilla $k = 1, 2, \ldots, n-1$. Tämä riittää lauseen todistamiseen, sillä tällöin

$$1 \equiv s_1 \equiv s_2 \equiv \ldots \equiv s_n \mod p.$$

Olkoot $A_1, \ldots, A_{s_k}$ ryhmän G kaikki kertalukua p^k olevat aliryhmät ja olkoot $B_1, \ldots, B_{s_{k+1}}$ ryhmän G kaikki kertalukua p^{k+1} olevat aliryhmät. Olkoon lisäksi a_i niiden aliryhmien B_j lukumäärä, joihin A_i sisältyy. Vastaavasti olkoon b_i niiden aliryhmien A_j lukumäärä, jotka sisältyvät aliryhmään B_i. Tällöin

$$a_1 + a_2 + \ldots + a_{s_k} = b_1 + b_2 + \ldots + b_{s_{k+1}}$$

sillä yhtälön molemmat puolet antavat sellaisten parien (A_α, B_β) lukumäärän, joille $A_\alpha \leq B_\beta$. Näin ollen kongruenssin (*) todistamiseksi riittää osoittaa, että $a_i \equiv 1 \mod p$ kaikilla $i = 1, \ldots, s_k$ sekä $b_j \equiv 1 \mod p$ kaikilla $j = 1, \ldots, s_{k+1}$.

Olkoot A kertalukua p^k oleva aliryhmä ja $P_1, \ldots, P_a$ kertalukua p^{k+1} olevat aliryhmät jotka sisältävät aliryhmän A. Halutaan siis osoittaa, että $a \equiv 1 \mod p$. Nyt A on normaali kaikissa aliryhmissä P_i, joten P_i/A on aliryhmän $N_G(A)/A$ kertalukua p oleva aliryhmä. Lisäksi jos aliryhmän $P/A \leq N_G(A)/A$ kertaluku on p, niin P sisältää aliryhmän A ja on kertalukua p^{k+1}. Lisäksi ehdosta $P_i/A = P_j/A$ seuraa $P_i = P_j$, joten a on kertalukua p olevien ryhmien lukumäärä ryhmässä $N_G(A)/A$. Näin ollen $a \equiv 1 \mod p$ tapauksen $k = 1$ nojalla, joka todistettiin aiemmin.

Olkoot B kertalukua p^{k+1} oleva aliryhmä ja $Q_1, \ldots, Q_b$ kertalukua p^k olevat aliryhmät jotka sisältyvät aliryhmään B. Nyt jokainen Q_i on ryhmän B normaali aliryhmä, joten myös $D_i = Q_1 \cap Q_i$ on normaali aliryhmä. Lisäksi $Q_1 Q_i = B$ kun $i > 1$, joten tällöin $|D_i| = p^{k-1}$. Nyt B/D_i ei voi olla syklinen, sillä kertalukua p^2 olevalla syklisellä ryhmällä olisi yksikäsitteinen kertalukua p oleva aliryhmä. Aliryhmillä Q_1/D_i ja Q_i/D_i on molemmilla kuitenkin kertaluku p. Näin ollen $B/D_i \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Nyt kertalukua p^k olevia aliryhmiä T joille pätee $D_i < T < B$ on tarkalleen yhtä paljon kuin ryhmällä B/D_i on kertalukua p olevia aliryhmiä. Niitä on $p+1$ kappaletta, sillä $x^p = 1$ kaikilla $x \in \mathbb{Z}_p \times \mathbb{Z}_p$. Nyt jokaiselle Q_i pätee $D_i < Q_i < B$. Lisäksi jos $D_i < Q_i < B$ ja $D_j < Q_i < B$, niin $D_i = D_j$. Olkoon $D_{i_1}, D_{i_2}, \ldots, D_{i_\rho}$ kaikki eri aliryhmät listassa $D_2, D_3, \ldots, D_b$. Jokaista D_{i_m} vastaa $p+1$ kertalukua p^k olevaa aliryhmää Q_i, joista yksi on Q_1. Näin ollen saadaan tarkalleen $\rho p + 1 \equiv 1$

mod p kertalukua p^k olevaa aliryhmää jotka sisältyvät aliryhmään B. Toisin sanoen saadaan $b \equiv 1 \mod p$.

□

Aliryhmien lukumäärälle voidaan todistaa myös vahvempi kongruenssi, joka riippuu Sylowin p-aliryhmien rakenteesta. Esimerkiksi parittomien alkulukujen tapauksessa saadaan seuraava yleistys.

Lause 7.8. *Olkoon p pariton alkuluku ja s_k ryhmän G kertalukua p^k olevien aliryhmien lukumäärä. Tällöin*

(i) ([13, Lemma 4.6.1]) Jos ryhmän G Sylowin p-aliryhmät ovat syklisiä, niin $s_k \equiv 1 \mod p^{n-k+1}$ kaikilla $0 \leq k \leq n$.

(ii) (Kulakoff [13, Theorem 4.6]) Jos ryhmän G Sylowin p-aliryhmät eivät ole syklisiä, niin $s_k \equiv 1 + p \mod p^2$ kaikilla $1 \leq k \leq n-1$.

7.5 Ratkaisujen lukumäärän vaikutus ryhmän rakenteeseen

Millä tavalla yhtälön $X^n = 1$ ratkaisujen lukumäärä vaikuttaa ryhmän rakenteeseen? Frobeniuksen otaksuman nojalla jos ratkaisuja on tarkalleen n kappaletta, niin ryhmällä on yksikäsitteinen kertalukua n oleva aliryhmä. Frobeniuksen lauseen nojalla jos n jakaa ryhmän kertaluvun, niin ratkaisujen lukumäärä on luvun n monikerta ja siten $\geq n$. Seuraavan tuloksen nojalla ratkaisujen lukumäärä on tarkalleen n kaikilla ryhmän kertaluvun tekijöillä n jos ja vain jos ryhmä on syklinen.

Lause 7.9 (G. A. Miller, 1916)**.** *Jos ryhmässä G yhtälöllä $X^n = 1$ on korkeintaan n ratkaisua kaikilla kokonaisluvulla n, niin ryhmä G on syklinen.*

Yleinen sovellus esimerkille on eräs kuntateoriaan liittyvä tulos. Olkoon K on kunta ja K^* sen kertolaskuryhmä. Tällöin esimerkin 7.9 avulla voidaan osoittaa, että ryhmän K^* jokainen äärellinen aliryhmä on syklinen. Esimerkki 7.9 saadaan seuraavasta Cohnin [40] yleisemmästä tuloksesta, jonka todistamme tässä.

Lause 7.10 (J. H. E. Cohn, 1972)**.** *Jos ryhmässä G kaikilla alkuluvuilla p ja positiivisilla kokonaisluvuilla k yhtälöllä $X^{p^k} = 1$ on korkeintaan $p^{k+1} - 1$ ratkaisua, niin ryhmä G on syklinen.*

Todistus. Olkoon P jokin ryhmän G Sylowin p-aliryhmä ja p^k suurin alkuluvun potenssi joka jakaa ryhmän G kertaluvun. Jos P ei ole syklinen, niin jokainen ryhmän P alkio toteuttaa yhtälön $X^{p^{k-1}} = 1$, eli ratkaisuja on enemmän kuin $p^k - 1$ kappaletta. Tämä on ristiriidassa oletuksen kanssa, joten P on syklinen.

Osoitetaan seuraavaksi, että P on normaali aliryhmä. Jos näin ei ole, niin Sylowin lauseen nojalla ryhmässä G on ainakin $p + 1$ Sylowin p-aliryhmää. Koska Sylowin p-aliryhmät ovat syklisiä, niin jokaisesta saadaan $\varphi(p^k)$ kertalukua p^k olevaa alkiota. Eri aliryhmillä on eri generoivat alkiot, joten näin saadaan $\varphi(p^k)(p+1) = p^{k+1} - p^{k-1}$ kertalukua p^k olevaa alkiota. Lisäksi kaikissa aliryhmissä on $p^k - \varphi(p^k) = p^{k-1}$ alkiota, joiden kertaluku on pienempi on pienempi kuin p^k. Näin ollen kaikista Sylowin p-aliryhmistä saadaan ainakin p^{k+1} alkiota, jotka kaikki toteuttavat yhtälön $X^{p^k} = 1$. Tämä on ristiriita, joten P on normaali aliryhmä.

Nyt siis ryhmän G kaikki Sylowin p-aliryhmät ovat normaaleja aliryhmiä, joten G on Sylowin p-aliryhmiensä suora tulo [5, 8.6 Theorem, s. 166]. Koska ryhmän G Sylowin p-aliryhmät ovat lisäksi syklisiä, niin myös G on syklinen. Tämä nähdään esimerkiksi sen perusteella, että kahden syklisen ryhmän suora tulo $H \times K$ on syklinen jos ja vain jos $(|H|, |K|) = 1$. □

Näin ollen $a_n(G) \leq n$ kaikilla $n \mid |G|$ jos ja vain jos G on syklinen ryhmä. Meng ja Shi ovat luokitelleet artikkelissa [33] ne ryhmät, joilla $a_n(G) \leq 2n$ kaikilla $n \mid |G|$. Syklisten ryhmien lisäksi tälläinen ryhmä on esimerkiksi mikä tahansa suora tulo $\mathbb{Z}_m \times Q_8$, missä $m \geq 1$ on pariton kokonaisluku ja Q_8 on kvaternioryhmä[9]. Myöhemmässä artikkelissa [34] Meng ja Shi luokittelivat ne ryhmät, joilla $a_n(G) \leq 3n$ kaikilla $n \mid |G|$. Yleisemmin voidaan tarkastella ongelmaa

Ongelma 7.11 (W. Meng, J. Shi, 2011)**.** *Olkoon k positiivinen kokonaisluku. Luokittele kaikki ryhmät G, joille $a_n(G) \leq kn$ kaikilla $n \mid |G|$.*

Huomaa, että ongelmassa 7.11 esiintyville ryhmille pätee $a_n(G) \leq kn$ millä tahansa positiivisella kokonaisluvulla n. Lisäksi millä tahansa aliryhmällä $H \leq G$ on vastaava ominaisuus, sillä $a_n(H) \leq a_n(G)$. Meng ja Shi tarkastelevat artikkeleissaan [33] ja [34] ainoastaan tapauksia $k = 2$ ja $k = 3$, mutta ehdottavat kuitenkin yllä olevaa yleisempää ongelmaa. Seuraavassa joitakin huomioita ongelmaan 7.11 liittyen.

Lause 7.12. *Oletetaan, että $a_n(G) \leq kn$ kaikilla $n \mid |G|$. Olkoon p jokin luvun $|G|$ alkulukutekijä. Tällöin*

[9] $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, missä $i^2 = j^2 = k^2 = ijk = -1$ sekä $ij = -ji = k$, $jk = -kj = i$ ja $ki = -ik = j$. Kyseessä on siis kertalukua 8 oleva ei-kommutatiivinen ryhmä.

(i) *Jos $k < p$, niin ryhmän G Sylowin p-aliryhmä on syklinen ja normaali aliryhmä.*

(ii) *Jos $k < p^2$, niin ryhmän G Sylowin p-aliryhmät ovat syklisiä tai ryhmällä G on normaali Sylowin p-aliryhmä.*

Todistus. Olkoon p^α suurin alkuluvun p potenssi joka jakaa luvun $|G|$ ja olkoon $P \leq G$ jokin Sylowin p-aliryhmä.

Jos $k < p$, niin $a_{p^{\alpha-1}}(P) \leq a_{p^{\alpha-1}}(G) \leq kp^{\alpha-1} < p^\alpha$, joten ryhmässä P on alkio x jolle $x^{p^\alpha} = 1$ mutta $x^{p^{\alpha-1}} \neq 1$. Tällöin $P = \langle x \rangle$ ja kaikki Sylowin p-aliryhmät ovat syklisiä. Kuten lauseen 7.10 todistuksessa (tai lauseen 7.5 avulla), ehdon $a_{p^\alpha}(G) < p^{\alpha+1}$ nojalla ryhmässä G on tarkalleen yksi Sylowin p-aliryhmä.

Jos $k < p^2$ ja ryhmän G Sylowin p-aliryhmät eivät ole syklisiä, niin $a_{p^\alpha}(G) = a_{p^{\alpha-1}}(G) \leq kp^{\alpha-1} < p^{\alpha+1}$. Millerin lauseen (7.5) nojalla ryhmässä G on tarkalleen yksi Sylowin p-aliryhmä. □

Seuraus 7.13. *Olkoon $a_n(G) \leq kn$ kaikilla $n \mid |G|$. Olkoon $|G| = p_1^{a_1} \dots p_t^{a_t} b$, missä $p_1 < \dots < p_t \leq k$ ovat alkulukuja ja missä jokainen luvun b alkulukutekijä on $> k$. Tällöin ryhmällä G on kertalukua b oleva syklinen ja normaali aliryhmä N. Lisäksi $G = MN$, missä $|M| = p_1^{a_1} \dots p_t^{a_t}$.*

Todistus. Voidaan olettaa, että $b > 1$, joten olkoon luvun b alkulukuesitys $b = q_1^{b_1} \dots q_s^{b_s}$. Lauseen 7.12 nojalla ryhmällä G on kertalukua $q_i^{b_i}$ oleva normaali syklinen aliryhmä Q_i. Tällöin $N = Q_1 \cdots Q_t$ on kertalukua b oleva normaali aliryhmä. Nyt ryhmän N jokainen Sylowin aliryhmä on syklinen ja normaali aliryhmä. Kuten lauseen 7.10 todistuksessa nähtiin, tällöin N on syklinen. Aliryhmän M olemassaolo seuraa Schur-Zassenhausin lauseen avulla, sillä $(|N|, [G : N]) = 1$. □

Jos $a_n(G) \leq kn$ kaikilla $n \mid |G|$, niin mitä voidaan päätellä ryhmän G rakenteesta? Seurauksen 7.13 nojalla ryhmä G voidaan esittää kahden aliryhmän tulona (puolisuora tulo [4, Chapter 7, s. 167-172]), joista toinen on syklinen ja normaali aliryhmä. Seurauksen 7.13 ja aiemmin todistetun lauseen 7.5 sovelluksena saadaan seuraava ratkeavuuskriteeri.

Lause 7.14. *Olkoon $a_n(G) \leq 6n$ kaikilla $n \mid |G|$. Tällöin G on ratkeava.*

Todistus. Olkoon G pienintä mahdollista kertalukua oleva vastaesimerkki väitteelle. Nyt G ei ole ratkeava, mutta jokainen ryhmän G aito aliryhmä on ratkeava. Näin ollen jos p on alkuluku ja $p \mid |G|$, niin ryhmällä G ei voi olla normaalia Sylowin p-aliryhmää P. Muutoin Schur-Zassenhausin lauseen

nojalla $G = PM$, missä $G/P \cong M$ ja G on ratkeava koska P ja M ovat aitoja aliryhmiä. Siispä lauseen 7.12 perusteella $|G| = 2^\alpha 3^\beta 5^\gamma$.

Jos $3 \mid |G|$, niin ryhmän G Sylowin 3-aliryhmä ei ole normaali ja siten jokainen Sylowin 3-aliryhmä on syklinen lauseen 7.12 (ii) nojalla. Näin ollen Sylowin 3-aliryhmistä saadaan ainakin $n_3(G)\varphi(3^\beta)+3^{\beta-1}$ alkiota. Koska tämä lukumäärä on $\leq 6 \cdot 3^\beta$, niin $n_3(G) \leq \frac{17}{2}$ ja $n_3(G) \leq 8$. Näin ollen $n_3(G) = 1, 4$ tai 7 koska $n_3(G) \equiv 1 \mod 3$. Koska $7 \nmid |G|$ ja ryhmän G Sylowin 3-aliryhmä ei ole normaali, niin $n_3(G) = 4$. Nyt siis $[G : H] = 4$, missä H on Sylowin 3-aliryhmän normalisoija. Täten on olemassa homomorfismi $\phi : G \to \mathrm{Sym}(4)$, missä $K = \mathrm{Ker}(\phi) \leq H$ (lemma 2.13). Koska $\mathrm{Sym}(4)$ on ratkeava, niin homomorfismien peruslauseen nojalla G/K on ratkeava ja K on aitona aliryhmänä ratkeava. Tämä on ristiriita, joten $3 \nmid |G|$.

Nyt ryhmän G Sylowin 5-aliryhmät ovat syklisiä lauseen 7.12 (ii) nojalla. Vastaavasti kuten aiemmin, Sylowin 5-aliryhmistä saadaan ainakin $n_5(G)\varphi(5^\gamma) + 5^{\gamma-1}$ alkiota. Tämä lukumäärä on $\leq 6 \cdot 5^\gamma$, joten $n_5(G) \leq \frac{29}{4}$ ja $n_5(G) \leq 7$. Näin ollen $n_5(G) = 1$ tai $n_5(G) = 6$ Sylowin lauseen nojalla. Koska $6 \nmid |G|$, niin $n_5(G) = 1$. Tämä on ristiriita, sillä ryhmällä G ei ole normaalia Sylowin 5-aliryhmää. □

Voidaanko lauseen 7.14 tulosta parantaa? Jos $G = \mathrm{Alt}(5)$, niin G ei ole ratkeava ja $a_n(G) \leq 8n$ kaikilla $n \mid |G|$. Entä jos $a_n(G) \leq 7n$ kaikilla $n \mid |G|$?

Ongelma 7.15. *Olkoon $a_n(G) \leq 7n$ kaikilla $n \mid |G|$. Onko G ratkeava?*

Viitteet

[1] M. Hall, Jr., *The theory of groups*, Macmillan, New York, (1959).

[2] W. Burnside, *Theory of Groups of Finite Order*, Cambridge, (1897).

[3] G. A. Miller, H. F. Blichfeldt, L. E. Dickson, *Theory and applications of finite groups*, New York: John Wiley sons, (1916).

[4] J. J. Rotman, *An introduction to the theory of groups* (neljäs painos), New York. Springer-Verlag (1994).

[5] J. S. Rose, *A Course on Group Theory*, Mineola, New York, Dover Publications, (1978).

[6] H. Finkelstein, *Solving equations in groups: A survey of Frobenius' theorem*, Periodica Mathematica Hungarica, Vol. 9, Iss. 3, 187-204, (1978).

[7] I. M. Isaacs, G. R. Robinson, *On a Theorem of Frobenius: Solutions of* $x^n = 1$ *in finite groups*, Amer. Math. Monthly, Vol. 99, No. 4, 352-354, (1992).

[8] R. Brauer, *On a Theorem of Frobenius*, Amer. Math. Monthly, Vol. 76, No. 1, 12-15, (1969).

[9] F. G. Frobenius, *Über auflösbare Gruppen*, Sitzungsberichte der Königl. Preuß. Akad. Wissenschaften (Berlin), 337-345, (1893).

[10] F. G. Frobenius, *Verallgemeinerung des Sylow'schen Satzes*, Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften (Berlin), 981-993, (1895).

[11] F. G. Frobenius, *Über einen Fundamentalsatz der Gruppentheorie*, Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften (Berlin), 987-991, (1903).

[12] G. A. Miller, *Some deductions from Frobenius' Theorem*, Proc. Nat. Acad. Sci. U.S.A., 28, 251–254, (1942).

[13] P. Hall, *On a Theorem of Frobenius*, Proc. London Math. Soc, vol. 40, 468-501, (1935).

[14] P. Hall, *A contribution to the theory of groups of prime power order*, Proc. London Math. Soc., vol. 36, 29-95, (1934).

[15] S. K. Sehgal, *On P. Hall's Generalization of a Theorem of Frobenius*, Vol. 5, 97-100, (1962)

[16] I. M. Isaacs, *Systems of equations and generalized characters in groups*, Canad. J. Math., 22, 1040-1046, (1970).

[17] F. Levin, *Solutions of Equations Over Groups*, Bull. Amer. Math. Soc., Vol. 68, No. 6, 603-604, (1962).

[18] R. J. Lipton, *Equations Over Groups: A Mess*, Gödel's Lost Letter and P = NP, `http://rjlipton.wordpress.com/2010/11/03/equations-over-groups-a-mess/`, (2010).

[19] T. Yoshida, $|\mathrm{Hom}(A, G)|$, J. Algebra, 156, 125–156, (1993).

[20] T. Asai, T. Yoshida, $|\mathrm{Hom}(A, G)|, II$, J. Algebra, 160, 273–285, (1993).

[21] T. Asai, Y. Takegahara, $|\mathrm{Hom}(A, G)|, IV$, J. Algebra, 246, 543-563, (2001).

[22] M. Murai, Y. Takegahara, *Hall's Relations in Finite Groups*, J. Algebra, 271, 312-326, (2004).

[23] R. Zemlin, *On a conjecture arising from a theorem of Frobenius*, Väitöskirja, Ohio State Univ., (1954).

[24] J. Rust, *On a Conjecture of Frobenius*, Väitöskirja, Univ. of Chicago, (1966).

[25] R. G. McKean, *On Frobenius' Conjecture*, Väitöskirja, The University of Wisconsin, (1973).

[26] Z. Arad, D. Chillag, M. Herzog, *On a Problem of Frobenius*, J. Algebra, Vol. 74, Iss. 2, 516–523, (1982).

[27] K. Fenchel, *On a theorem of Frobenius*, Math. Scand., 42, 243–250 (1978).

[28] H. Yamaki, *A conjecture of Frobenius and the sporadic simple groups, I*, Comm. Algebra 11, 2513-2518, (1983).

[29] H. Yamaki, *A conjecture of Frobenius and the sporadic simple groups, II*, Math. Comp., 46, 609-611,(1986).

[30] N. Iiyori, *A conjecture of Frobenius and the simple groups of Lie type, IV*, J. Algebra, 154, 188-214, (1993).

[31] N. Iiyori, H. Yamaki, *On a Conjecture of Frobenius*, Bull. Amer. Math. Soc. (N.S.), Vol. 25, Num. 2, 413-416, (1991).

[32] N. Iiyori, H. Yamaki, *A Problem of Frobenius*, Representations of Algebras, CMS Conference Proceedings, Vol. 14, 237-244, (1992).

[33] W. Meng, J. Shi, *On an inverse problem to Frobenius' theorem*, Archiv der Mathematik, vol. 96, no. 2, pp. 109-114, (2011).

[34] W. Meng, J. Shi, K. Chen, *On an inverse problem to Frobenius' theorem II*, J. Algebra Appl., Vol. 11, Iss. 5, (2012).

[35] M. Aschbacher, *The status of the classification of the finite simple groups*, Notices of the AMS, Vol. 51, Num. 7, 736-740, (2004).

[36] P. Flavell, *A Note on Frobenius Groups*, J. Algebra, 228, 367-376, (2000).

[37] M. Hall, Jr., *On the number of Sylow subgroups in a finite group*, J. Algebra, Vol. 7, Iss. 3, 363–371, (1967)

[38] H. G. Bray, *A note on CLT groups*, Pacific J. Math. Volume 27, Number 2, 229-231, (1968).

[39] D. McCarthy, *Sylow's theorem is a sharp partial converse to Lagrange's theorem*, Mathematische Zeitschrift, Vol. 113, Iss. 5, 383-384, (1970).

[40] J. H. E. Cohn, *A condition for a finite group to be cyclic*, Proc. Amer. Math. Soc., Vol. 32, No. 1 (1972).

[41] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.4.12, `http://www.gap-system.org` (2008).