ÄÄRELLISTEN RYHMIEN VAIHDANNAISUUSVERKOT

MIIKKA SILFVERBERG

PRO GRADU

HELSINGIN YLIOPISTON
MATEMATIIKAN LAITOS

TOUKOKUU 2008

SISÄLTÖ

1. Merkinnöistä ja määritelmistä

Tässä tutkielmassa noudatetaan algebran alalla yleistä käytäntöä kirjoittaa kuvaukset oikealta. Jos $f : X \to Y$ on kuvaus, niin alkion $x \in X$ kuvaa merkitään xf. Oletusarvoisesti sisin kuvaus sitoo vahvimmin, siis $xfg = (xf)g$.

Toisaalta monet ryhmien luokan operaatiot, kuten $\mathrm{Z}(G)$ ja $\mathrm{N}(G)$ kirjoitetaan vasemmalta. Kun H ja G ovat ryhmiä ja $\phi : H \to \mathrm{Aut}(G)$ on kuvaus, merkitään ryhmän H alkion h kuvaa useimmiten f_h. Ryhmä H siis indeksoi ryhmän G isomorfismeja. Homomorfismi ϕ on tavallisesti selvä asiayhteydestä.

Koska permutaatiot ovat kuvauksia, kerrotaan permutaatioita tässä tutkielmassa vasemmalta. Esimerkiksi on (1 2 3)(2 3) = (1 3) (jos permutaatioita kerrottaisiin oikealta se olisi (1 2)).

Usein n-kulmaisen monikulmion diedriryhmää merkitään D_n, mutta tässä tutkielmassa sitä merkitään D_{2n}.

$\sum_i G_i$	Ryhmien G_i suora summa.
S_n	Joukon {1, 2, ..., n} symmetrinen ryhmä.
S_X	Joukon X symmetrinen ryhmä.
Ker_f	Homomorfismin f ydin.
$\mathrm{C}(x)$	Alkion $x \in G$ keskittäjä ryhmässä G.
$\mathrm{N}(x)$	Alkion $x \in G$ normalisoija ryhmässä G.
H^g, h^g	$g^{-1}Hg$, $g^{-1}hg$, kun H on aliryhmä ja h jokin alkio, jossain ryhmässä.
C_n	Kertaluvun $n \in \mathbb{N}$ syklinen ryhmä.
D_{2n}	Diedriryhmä, jossa on $2n$ alkiota.
$\mathbb{H}$	Kvaternioiden kunnan yksiköiden ryhmä.
$\mathcal{W}_x$	Verkon $\mathcal{W}$ solmun x naapurusto.
$\mathcal{W}^G$	Ryhmän G vaihdannaisuusverkko.

2. Johdanto

Ryhmän G vaihdannaisuusrelaatiolla tarkoitetaan joukon G relaatiota R, missä xRy joss x ja y ovat vaihdannaisia ryhmässä G. Tämä tutkielma keskittyy ryhmien vaihdannaisuusrelaation, jota havainnollistetaan ns. *vaihdannaisuusverkkojen* avulla.

Binääriset relaatiot ja verkot ovat tietenkin lähestulkoon sama asia. Verkoilla on kuitenkin abstrakteihin relaatioihin verrattuna se etu, että niistä voi toisinaan piirtää kuvan – muutenkin ne tuovat perin abstraktiin vaihdannaisuusrelaation käsitteeseen konkretiaa.

Jo kaksikymmenalkioisten ryhmien vaihdannaisuusverkot ovat ikävä kyllä piirrettyinä varsin sotkuisia, koska vaihdannaisuusverkoissa on aina paljon kaaria. Isommissa ryhmissä avuksi voidaan siksi ottaa *keskuksen sivuluokkien vaihdannaisuusverkko*. Tämän määritelmä perustuu sille havainnolle, että ryhmän G alkioiden x ja y kuuluminen samaan keskuksen $\mathrm{Z}(G)$ sivuluokkaan takaa, että x ja y ovat keskenään vaihdannaisia.

Pro gradu -tutkielman varsinainen sisältö liittyy ryhmien maksimaalisiin Abelin aliryhmiin ja ehtoihin sille, että kahdella ryhmällä on isomorfiset vaihdannaisuusverkot. Kysymyksiä on tarkasteltu neljännessä luvussa aiemmissa luvuissa käsiteltyjen esitietojen pohjalta.

Ryhmien maksimaalisten Abelin aliryhmien käsittely nojaa vahvasti W. Burnsiden 1900-luvun vuosisadan alkupuoliskolla saamiin tuloksiin p-ryhmien isomorfismeista. Näitä käsitellään kolmannen luvun alaluvussa 3.8. Burnsiden tuloksen avulla voidaan löytää yläraja sellaisen p-ryhmän koolle, jonka jokainen Abelin aliryhmä on kertaluvultaan pienempi kuin p^n jollain $n \in \mathbb{N}$. Tästä saadaan helposti johtopäätös, että suurissa ryhmissä on aina suuria Abelin aliryhmiä. Siis jos $k \in \mathbb{N}$, niin voidaan löytää sellainen luku $M_k \in \mathbb{N}$ että jokaisessa ryhmässä, jonka kertaluku on suurempi kuin M_k on vähintään kertalukua k oleva Abelin aliryhmä.

Vaihdannaisuusverkkojen isomorfiaa tarkastellaan neljännessä luvussa. Päämääränä on löytää kaksi ryhmää, joilla on *samanlainen konjugaattirakenne* mutta epäisomorfiset vaihdannaisuusverkot. Ryhmillä on samanlainen konjugaattirakenne, mikäli niillä on samat määrät konjugaattiluokkia, joissa on samat määrät alkioita. Tällainen esimerkki löytyykin kertalukua 128 olevista ryhmistä.

Kysymystä käsiteltiin ohjelmallisesti GAP (Groups, Algorithms and Programming) ohjelmointiympäristössä ja saadut tulokset tarkistettiin NAUTY (No Automorphisms, Yes?) verkkojen käsittelyohjelmalla. Koska isomorfiakysymystä ei ratkaistu täydellisesti, voi olla ettei löydetty esimerkki ole pienintä mahdollista kertalukua (minusta se tuntuu peräti todennäköiseltä).

Keskeisten tulosten lisäksi tutkielmassa käydään tietenkin läpi paljon äärellisten ryhmien teoriaa (ja hiukan verkkojen teoriaa). Tutkielman ensimmäisessä sisältöluvussa eli kolmannessa luvussa käsitellään melkoinen määrä mielenkiintoista ryhmäteoriaa. Tarkastelu lähtee liikkeelle alkeista, mutta tahti on sangen kova. Niille, jotka eivät ole aiemmin ryhmäteoriaan tutustuneet, voin mitä lämpimimmin suositella J. Rosen oppikirjaa [8], joka soveltunee mainiosti ensimmäiseksi kosketukseksi aiheeseen.

Rosen oppikirja täyttää tämän tutkielman esitietovaatimukset erityisen hyvin, koska siinä painotetaan ryhmän toiminnan käsitettä (mikä lienee koko ryhmäteorian tärkein idea). Toiminnat muodostavat nimittäin keskeisen juonteen tässäkin tutkielmassa.

Tanskalainen matemaatikko, runoilija ja keksijä Piet Hein kirjoitti mielenkiintoisista kysymyksistä:

Problems worthy
of attack
prove their worth
by hitting back.

Tässä tutkielmassa käsiteltävät äärellisten ryhmien *vaihdannaisuusrelaatiot* ovat osoittautuneet sangen iskukykyisiksi ainakin itseäni kohtaan. Tutkielman kirjoittajana olen viettänyt huomattavasti aikaa yrittäen todistaa järjettömiksi osoittautuneita otaksumia. Vaivan palkkana tutkielmaan sisältyy kuitenkin muutamia yksinkertaisia, mutta mielestäni kiinnostavia, tuloksia vaihdannaisuudesta ryhmissä.

Haluaisin kiittää tutkielman ohjaajaa Kerkko Luostoa sekä hienosta aiheesta että mielenkiintoisista ryhmäteoriaa koskevista keskusteluista sekä ideoista ja avusta materiaalin etsimisessä. Tutkielman toista tarkastajaa Markku Niemenmaata haluan myös lämpimästi kiittää. Kiitoksia haluaisin osoittaa myöskin Onni Talaan säätiölle, jonka myöntämä stipendi ei aivan ehtinyt hyödyttää tämän tutkielman kirjoittamista, mutta helpottaa suuresti kirjoittamisen taloudellista jälkipyykkiä. Luova työ kun edellyttää joutilaisuutta, mistä ei makseta palkkaa. Tämä pro gradu olisi huomattavasti köyhempi ilman GAP- ja Nauty-ohjelmia, joiden kehittäjille kuuluu suuri kiitos.

Panu Kalliokoskea haluaisin kiittää paitsi vertaistuesta pro gradu -kirjoitusprosessin aikana, myös mentoroinnista viimeisen kuuden vuoden aikana. Lopuksi haluaisin kiittää Roosaa ja Ilyaa, jotka ystävällisesti tarjosivat työskentelypaikan, loistavaa seuraa ja aterian useana köyhänä päivänä.

3. Ryhmäteoriaa

Tässä luvussa käsitellään sen verran äärellisten ryhmien teoriaa kuin vaihdannaisuusverkkojen ymmärtämiseksi on hallittava. Vaikka käsittely alkaa perusteista, on se alkeiden osalta kursorista, joten lukijalta edellytetään melko paljon esitietoja (esim. Helsingin yliopiston Matematiikan laitoksen kurssit Algebra I ja II).

Käsiteltävät aiheet ja niiden järjestys noudattavat melko pitkälti Scottin [9] ja Rosen [8] esitystä. Varsinkin Rosen erinomaista oppikirjaa voi lämmöllä suositella kaikille ryhmäteoriasta kiinnostuneille. Alaluku 3.7. perustuu Burnsiden artikkeliin [4], jota on hieman modernisoitu, lähinnä merkintöjen osalta.

Kirjoittajaan omaa työtä on esimerkin 3.22 muokkaaminen paremmin tutkielmaan sopivaksi ja pääosa luvusta 3.5.

3.1. Ryhmät ja toiminnat

Ryhmä on pari $(G, \circ_G)$, missä G on joukko ja *ryhmäoperaatio* $\circ_G : G \times G \to G$ toteuttaa seuraavat *ryhmäaksioomat*

(1) Operaatio $\circ_G$ on liitännäinen. Ellei ole sekaannuksen vaaraa, merkitään $\circ_G = \circ$.
(2) On yksi sellainen alkio $1_G \in G$ että $1_G \circ g = g \circ 1_G = g$, kaikilla $g \in G$. Alkio 1_G on ryhmän G *neutraalialkio*. Ellei ole sekaannuksen vaaraa, merkitään lyhyesti $1_G = 1$.
(3) Jokaiselle $g \in G$ on sellainen $g^{-1} \in G$ että $g \circ g^{-1} = g^{-1} \circ g = 1$.

Jos ryhmä $(G, \circ)$ lisäksi toteuttaa aksiooman

(4) Kaikilla $x, y \in G$ on $x \circ y = y \circ x$.

sanotaan ryhmää *Abelin ryhmäksi*.

Ryhmää $(G, \circ)$ merkitään lyhyemmin G, koska ryhmäoperaatio on useimmiten selvä asiayhteydestä. Jos $g, h \in G$, niin alkiota $g \circ h$ merkitään lyhyesti gh. Kun joukko G on äärellinen, sanotaan, että ryhmä $(G, \circ_G)$ on äärellinen.

Olkoon loppuluvun ajan G äärellinen ryhmä.

Ryhmän $(G, \circ)$ osajoukkoa H sanotaan *aliryhmäksi*, jos $(H, \circ|_H)$ on ryhmä (tässä $\circ|_{H\times H}$ on operaation $\circ$ rajoittuma joukkoon $H \times H$). Tämä merkitään $H \leq G$. Jos H on joukon G aito osajoukko, sitä sanotaan *aidoksi aliryhmäksi* ja merkitään $H < G$.

3.1. **Lemma.** *Olkoon $(G, \circ)$ äärellinen ryhmä ja $H \subset G$. Tällöin $H \leq G$, joss $x, y \in H \Rightarrow x \circ y \in H$. Jos $H \leq G$, niin $1_H = 1_G$.* □

3.2. **Määritelmä.** Olkoot $(G, \circ_G)$ ja $(H, \circ_H)$ ryhmiä. Ryhmän G *homomorfismi* ryhmään H on kuvaus $f : G \to H$, joka toteuttaa ehdon

$$(g \circ_G g')f = (gf) \circ_H (g'f) \text{ kaikilla } g, g' \in G.$$

Ryhmän G osajoukko $\mathrm{Ker}_f = \{g \in G \mid gf = 1_H\}$ on homomorfismin f *ydin*.

Jos f on injektio, kutsutaan sitä *upotukseksi* ja mikäli se on lisäksi surjektio, sanotaan sitä *isomorfismiksi*. Mikäli ryhmien G ja H välillä on olemassa isomorfismi sanotaan, että ryhmät ovat *isomorfisia*.

3.3. **Lause.** *Olkoot G ja H ryhmiä. Surjektiivinen homomorfismi $f : G \to H$ on isomorfismi, joss* $\mathrm{Ker}_f = \{1_G\}$. □

Ryhmäteorian keskeisimpiin käsitteisiin kuuluu ryhmän toiminta jossain toisessa matemaattisessa rakenteessa, esimerkiksi joukossa, verkossa tai toisessa ryhmässä. Historiallisesti toiminnan käsite on ryhmäteoriassa erityisen tärkeä, koska koko oppialan voidaan katso saaneen alkunsa pyrkimyksistä rakentaa yleinen yhtälöiden ratkaisemisen teoria, mikä johti kuntien automorfismien ryhmien tarkastelemiseen ([3] sivu 687).

3.4. **Määritelmä.** Olkoon X jokin joukko. Merkinnällä S_X tarkoitetaan joukon X permutaatioiden joukkoa. Pari $(\mathrm{S}_X, \circ)$, missä $\circ$ on funktioiden yhdiste, muodostaa ryhmän, jota kutsutaan joukon X *symmetriseksi ryhmäksi*. Merkinnällä S_n, missä $n \in \mathbb{N}$ tarkoitetaan joukon $\{1, ..., n\}$ symmetristä ryhmää. Jos G on äärellinen ryhmä, ja ϕ on homomorfismi ryhmästä G ryhmään S_X, sanotaan, että G *toimii* joukossa X. Kuvaus ϕ on ryhmän G *toiminta* joukossa X. Kun sekaannuksesta ei ole vaaraa, merkitään alkiota $x(g\phi)$ lyhyesti xg. Jos $Y \subset X$ ja $g \in G$, merkitään $Yg = \{yg \mid y \in Y\}$.

Jos $Y \subset X$, on $Y_G = \{yg \mid g \in G \text{ ja } y \in Y\}$ osajoukon Y *rata*. Kun Y on pistejoukko $\{y\}$, merkitään lyhyesti y_G.

Jos $Y \subset X$, on

$$G_{(Y)} = \{g \in G \mid yg = y \text{ jokaiselle } y \in Y\}$$

osajoukon Y *pistekiinnittäjä* ja

$$G_{\{Y\}} = \{g \in G \mid yg \in Y \text{ jokaisella } y \in Y\}$$

osajoukon Y *joukkokiinnittäjä*. Kun Y on pistejoukko $\{y\}$, ovat piste- ja joukkokiinnittäjä samat ja merkitään G_y. Pistekiinnittäjää $G_{(X)}$ kutsutaan ryhmän G *toiminnan ytimeksi*.

Sellainen osajoukko $\Delta \subset X$, että $1 < |\Delta| < |X|$ ja jokaisella $g \in G$ on

$$\Delta g = \Delta \text{ tai } \Delta g \cap \Delta = \emptyset,$$

on ryhmän G *toiminnan lohko*.

Toiminta ϕ on

(1) *uskollinen*, jos $G_{(X)} = \{1\}$.
(2) *transitiivinen*, jos kaikille $s_1, s_2 \in S$ on $s_1 g = s_2$ jollain $g \in G$. Toiminta on *intransitiivinen* ellei näin ole.
(3) *primitiivinen*, ellei sillä ole lohkoja. Toiminta, jolla on lohkoja on *imprimitiivinen*.

Jos ryhmän G toiminta joukossa X on transitiivinen, mutta imprimitiivinen ja $\Delta \subset X$ on toiminnan lohko, on $\{\Delta g \mid g \in G\}$ joukon X ositus. Koska jokainen g on bijektio, on aina $|\Delta| = |\Delta g|$, joten lohkon Δ alkioiden lukumäärä on aina joukon X alkioiden lukumäärän tekijä.

Ositusta $\{\Delta g \mid g \in G\}$ kutsutaan ryhmän G toiminnan *lohkorakenteeksi*.

Jokaisella ryhmällä G on aliryhminä $\{1\}$ ja G. Toimintojen kielellä ilmaistuna on olemassa yleinen ehto sille, että ryhmän G osajoukko on sen aliryhmä. Tämä antaa tietoa äärellisen ryhmän aliryhmien kertaluvuista.

3.5. **Lemma.** *(Lagrangen lause) Olkoon G ryhmä. Määritellään funktio $\phi : G \to S_G$, missä $h(g\phi) = hg$, kaikilla $h \in G$. Kuvaus ϕ on toiminta ja sellainen osajoukko $H \subset G$ että $1 < |H| < |G|$ ja $1 \in H$ on tämän toiminnan lohko, joss $H < G$. Siispä $|H| \,\big|\, |G|$.* □

3.6. **Määritelmä.** Jos $H < G$, niin ryhmän G osajoukkoja Hg sanotaan aliryhmän H *oikeiksi sivuluokiksi* (vasemmat sivuluokat määritellään vastaavasti). Luku $[G : H] = |G|/|H|$ on aliryhmän H *indeksi*. Mikäli lohkorakenne

$$\{Hg \mid g \in G\}$$

on sellainen, että $(hg)(h'g') \in H(gg')$ kaikilla $h, h' \in H$ ja $g, g' \in G$, sanotaan, että aliryhmä H on *normaali* ja merkitään $H \lhd G$. Normaalin aliryhmän H lohkorakenne on itsessään ryhmä, kun määritellään $(Hg)(Hg') = H(gg')$. Tämä ryhmä on aliryhmän H *tekijäryhmä*, jota merkitään G/H.

3.7. **Lemma.** *Aliryhmä $H \leq G$ on normaali, joss $g^{-1}Hg = H$ kaikilla $g \in G$.* □

Myöhemmin merkitään $g^{-1}Hg = H^g$, kun H on jonkin ryhmän aliryhmä ja g jokin tämän ryhmän alkio.

3.8. **Lemma.** *Olkoot G ja H ryhmiä ja olkoon $f : G \to H$ isomorfismi. Tällöin* $\mathrm{Ker}_f \lhd G$. *Mikäli f on surjektiivinen, on* $G/\mathrm{Ker}_f \approx H$. □

Jos joukolla X on jonkinlainen sisäinen rakenne, ts. siihen liittyy erilaisia relaatioita R_1, ..., R_n voidaan toiminnan ehtoja tiukentaa. Saatetaan vaikkapa vaatia, että

(1) $\qquad xR_iy \Leftrightarrow xgR_iyg$ kaikilla R_i, $g \in G$ ja $x, y \in X$.

Tällä tavoin voidaan melkeinpä mihin vaan matemaattiseen rakenteeseen X liittää sen *symmetrioiden ryhmä*. On helppoa osoittaa, että sellaiset kuvaukset, jotka säilyttävät relaatiot R_i yhtälön (1) mielessä, muodostavat ryhmän S_X aliryhmän. Tätä ryhmää kutsutaan rakenteen X symmetrioiden ryhmäksi.

3.9. **Lause.** *Olkoon G äärellinen ryhmä, X äärellinen joukko, ϕ ryhmän G toiminta joukossa X, $x \in X$ ja $Y \subset X$. Tällöin*

(1) $|x_G| \cdot |G_x| = |G|$
(2) $G_{(X)} \lhd G$.
(3) $G_{(Y)} \leq G_{\{Y\}} \leq G$.

□

3.10. **Määritelmä.** Olkoon G ryhmä ja $H < G$. Aliryhmä H on *maksimaalinen*, ellei ole olemassa sellaista aliryhmää $K < G$, että $H < K$. Aliryhmä H on *maksimaalinen normaali* aliryhmä, jos se on ryhmän G normaali aliryhmä, eikä ole toista ryhmän G aitoa normaalia aliryhmää K, jonka aito aliryhmä H olisi. Käsitteet *maksimaalinen Abelin aliryhmä* ja *maksimaalinen normaali Abelin aliryhmä* määritellään vastaavasti paitsi, että aliryhmän K on lisäksi oltava Abelin aliryhmä.

3.11. **Lemma.** *Jokainen aliryhmä, jonka indeksi on alkuluku, on maksimaalinen.*

Todistus. Tämä seuraa suoraan Lagrangen lauseesta. □

3.12. **Lause.** *(Sylowin lause) Olkoon G ryhmä, $|G| = p^m r$, missä p ei jaa lukua r.*

(1) *Jokaiselle p^k, missä $k \leq m$, on ryhmällä G aliryhmiä, joiden kertaluku on p^k.*
(2) *Näiden kertalukua p^k olevien aliryhmien lukumäärä $n_k \equiv 1 \mod p$.*
(3) *Kaikki aliryhmät kertalukua p^m ovat konjugaatteja, joten ne ovat isomorfisia.*

Todistus. Katso [8] sivut 91-93 ja 108. □

3.13. **Määritelmä.** Olkoon ryhmä G kertalukua $p^m r$, missä $m \in \mathbb{N}$ ja p ei jaa lukua r. Sylowin lauseen mukaan ryhmällä G on $kp+1$ kappaletta kertalukua p^m olevaa aliryhmää

$$P_1, ..., P_{kp+1}$$

jollain $k \in \mathbb{N}$. Kaikki nämä aliryhmät ovat konjugaatteja ryhmässä G. Niitä kutsutaan ryhmän G *Sylowin p-aliryhmiksi*.

3.14. **Lemma.** *Jos G on ryhmä ja $M \lhd G$ on maksimaalinen aliryhmä, niin $|G/M|$ on alkuluku.*

Todistus. Oletetaan, että $|G/M| = n \in \mathbb{N}$ ei ole alkuluku, jolloin sillä on alkulukutekijä $p \neq n$. Nyt ryhmällä G/M on Sylowin lauseen nojalla kertalukua p oleva epätriviaali aliryhmä H/M, joten ryhmällä G on kertalukua $|M|p$ oleva epätriviaali aliryhmä, joka sisältää aliryhmän M aidosti, mikä on ristiriita. □

3.15. **Määritelmä.** Olkoon $\mathcal{H}$ ryhmän G maksimaalisten aliryhmien joukko. Ryhmän G *Frattinin aliryhmä* on

$$\mathrm{Frat}(G) = \bigcap_{H \in \mathcal{H}} H.$$

Alkio $x \in G$ on *merkityksetön*, jos jokaisella osajoukolla $S \subset G$ jolla $\langle S \rangle \neq G$ on $\langle S \cup \{x\} \rangle \neq G$.

3.16. **Lause.** *Olkoon G äärellinen ryhmä. Tällöin*

$$\mathrm{Frat}(G) = \{x \in G \mid x \text{ on ryhmän } G \text{ merkityksetön alkio.}\}.$$

Todistus. Jos $H < G$, niin induktiolla saadaan

$$\langle H \cup \{x \in G \mid x \text{ on ryhmän } G \text{ merkityksetön alkio.}\} \rangle < G,$$

joten merkityksettömien alkioiden joukko on jokaisen maksimaalisen aliryhmän osajoukko. Jos taas x ei ole merkityksetön, on olemassa sellainen $S \subset G$ että $\langle S \rangle \neq G$, mutta $\langle S \cup \{x\} \rangle = G$. Koska S sisältyy johonkin maksimaaliseen aliryhmään H, $x \notin H$, joten $x \notin \mathrm{Frat}(G)$. □

3.17. **Lemma.** *Olkoon G ryhmä. Tällöin* $\mathrm{Frat}(G) \lhd G$. *Itse asiassa jokainen ryhmän G automorfismi kiinnittää aliryhmän* $\mathrm{Frat}(G)$.

Todistus. Olkoon $f \in \mathrm{Aut}(G)$. Aliryhmä $H < G$ on maksimaalinen, joss Hf on maksimaalinen, joten $\mathrm{Frat}(G) \subset \mathrm{Frat}(G)f$. Koska f on bijektio, väite seuraa. □

3.18. **Lemma.** *Olkoon G äärellinen ryhmä ja $X = \{x_1 \operatorname{Frat}(G),, ..., x_n \operatorname{Frat}(G)\}$ jokin ryhmän $G/\operatorname{Frat}(G)$ virittäjistö. Tällöin $Y = \{x_1, ..., x_n\}$ on ryhmän G virittäjistö.*

Todistus. Jokainen ryhmän $G/\operatorname{Frat}(G)$ alkio on muotoa

$$x_1^{k_1} \ldots x_n^{k_n} \operatorname{Frat}(G), \text{ missä } k_i \in \mathbb{N} \text{ kaikilla } i,$$

koska X on ryhmän $G/\operatorname{Frat}(G)$ virittäjistö. Koska jokainen ryhmän G alkio sisältyy johonkin ryhmän $\operatorname{Frat}(G)$ sivuluokkaan on jokainen ryhmän G alkio muotoa

$$x_1^{k_1} \ldots x_n^{k_n} y, \text{ missä } k_i \in \mathbb{N} \text{ kaikilla } i \text{ ja } y \in \operatorname{Frat}(G).$$

Näin ollen joukko $Y \cup \operatorname{Frat}(G)$ virittää ryhmän G. Lauseesta 3.16 seuraa nyt, että Y virittää ryhmän G, koska G on äärellinen. □

3.2. Tulokonstruktiot

(Luvussa noudatetaan kirjan [9] esitystä.)

Jos äärellisellä ryhmällä G on sellaiset normaalit aliryhmät $N_1, ..., N_m$ että $G = N_1 N_2 \ldots N_m$ ja $N_i \cap (N_1 \ldots N_{i-1} N_{i+1} \ldots N_m) = \{1\}$ kaikilla i, sanotaan että ryhmä G on aliryhmiensä $N_1, ..., N_m$ suora summa.

3.19. **Lemma.** *Olkoon G normaalien aliryhmiensä $N_1, ..., N_m$ suora summa. Tällöin*

(1) *Jos $k \in N_i$ ja $l \in N_j$, missä $i \neq j$, niin $kl = lk$.*
(2) *Jokainen ryhmän G alkio voidaan esittää yksikäsitteisesti muodossa $n_1 \ldots n_m$, missä $n_i \in N_i$ kaikilla i.*
(3) *Olkoot $k_i, l_i \in N_i$ kaikilla i. Alkiot $k_1 \ldots k_m, l_1 \ldots l_m \in G$ ovat konjugaatteja ryhmässä G, joss k_i ja l_i ovat konjugaatteja ryhmässä N_i jokaisella i. Siispä jokainen ryhmän G konjugaattiluokka on muotoa*

$$\{k_1 \ldots k_m \mid k_i \in K_i, \text{ kaikilla } i\},$$

missä jokaisella i on K_i ryhmän N_i konjugaattiluokka.
(4) *Ryhmän G keskus on joukko*

$$\{z_1 \ldots z_m \mid z_i \in \mathrm{Z}(N_i) \text{ kaikilla } i\}.$$

□

Suoran summan käsitteen motivoimana voidaan esittää suoran tulon käsite. Olkoot $G_1, ..., G_n$ ryhmiä. Näiden ryhmien suora tulo on joukko $G_i \times \ldots \times G_n$ varustettuna kertolaskulla

$$(g_1, ..., g_n)(g_1', ..., g_n') = (g_1 \circ_{G_1} g_1', ..., g_n \circ_{G_n} g_n').$$

Varustettuna tällä kertolaskulla suora tulo on ryhmä. Jokainen G_i voidaan upottaa suoraan tuloon aliryhmäksi $\{1_{G_1}\} \times \ldots \times \{1_{G_{i-1}}\} \times G_i \times \{1_{G_{i+1}}\} \times \ldots \times \{1_{G_n}\}$ ja on helppoa osoittaa, että suora tulo on näiden aliryhmien suora summa, joten tässä mielessä suora tulo ja suora summa ovat sama asia.

Suoraa summa hiukan monimutkaisempi käsite on *jakolaajennus*. Jos G on ryhmä, jolla on sellainen normaali aliryhmä N ja sellainen aliryhmä H että $G = HN$ ja $N \cap H =$

{1}, sanotaan että ryhmä G on aliryhmänsä N jakolaajennus aliryhmällä H (engl. G is the split extension of N by H). Jokainen ryhmän G alkio on ilmaistavissa muodossa hn, missä $h \in H$ ja $n \in N$, koska $G = HN$. Jos $h_1n_1, h_2n_2 \in G$, missä $h_1, h_2 \in H$ ja $n_1, n_2 \in N$, niin

$$(h_1n_1)(h_2n_2) = h_1h_2(h_2^{-1}n_1h_2)n_2 = (h_1h_2)(n_1^{h_2}n_2).$$

Tässä $n_1^{h_2} \in N$, koska N on normaali aliryhmä. Helposti voi tarkistaa, että H toimii ryhmässä N säilyttäen ryhmän N laskuoperaation, joten ryhmään H liittyy homomorfismi $\phi : H \to \mathrm{Aut}(N)$. Tulo $(h_1h_2)(n_1^{h_2}n_2)$ voidaan siis kirjoittaa uudestaan $(h_1h_2)(n_1\phi_{h_2}n_2)$.

Jakolaajennuksen motivoimana voidaan määritellä *puolisuoran tulon* käsite. Jos N ja H ovat ryhmiä ja $\phi : H \to \mathrm{Aut}(N)$ on homomorfismi, niin ryhmän N puolisuora tulo ryhmällä H (engl. the semidirect product of N by H) on joukko $H \times N$ varustettuna tulolla

$$(h_1, n_1)(h_2, n_2) = (h_1 \circ_H h_2, n_1\phi_{h_2}n_2), \text{ kaikilla } h_1, h_2 \in H \text{ ja } n_1, n_2 \in N.$$

Tätä ryhmää merkitään $N \rtimes_\phi H$. Selvästikin $\{1\} \times N$ on tämän ryhmän normaali aliryhmä ja alkion $(x, y) \in N \rtimes_\phi H$ käänteisalkio on $(x^{-1}, (y^{-1})\phi_{x^{-1}})$

Puolisuoran tulon rakenne riippuu olennaisella tavalla homomorfismista ϕ, kuten seuraava esimerkki osoittaa.

3.20. **Esimerkki.** Olkoon $\tau : \mathrm{C}_2 \to \mathrm{Aut}(\mathrm{C}_3)$ määritelty kaavalla $x\tau_y = x$ kaikilla $x \in \mathrm{C}_3$ ja $y \in \mathrm{C}_2$. Tarkastellaan ryhmää $\mathrm{C}_3 \rtimes_\tau \mathrm{C}_2$. Huomattiin, että $(\{0\} \times \mathrm{C}_3) \lhd (\mathrm{C}_3 \rtimes_\tau \mathrm{C}_2)$. Osoitetaan, nyt, että myöskin $(\mathrm{C}_2 \times \{0\}) \lhd (\mathrm{C}_3 \rtimes_\tau \mathrm{C}_2)$. Olkoot $(x, y), (z, t) \in (\mathrm{C}_3 \rtimes_\tau \mathrm{C}_2)$, jolloin

$$(x, y)(z, t) = (xz, y\tau_z t) = (xz, yt), \text{ koska } \tau_z \text{ on identiteettikuvaus jokaisella } z \in \mathrm{C}_2\,.$$

Tästä nähdään heti, että $\mathrm{C}_3 \rtimes_\tau \mathrm{C}_2$ on ryhmien $\{0\} \times \mathrm{C}_3$ ja $\mathrm{C}_2 \times \{0\}$ suora summa, koska sekä $\{0\} \times \mathrm{C}_3$ että $\mathrm{C}_2 \times \{0\}$ ovat normaaleja aliryhmiä, $\mathrm{C}_3 \rtimes_\tau \mathrm{C}_2$ on niiden tulo ja niiden leikkaus on triviaali. Koska kumpikin näistä ryhmistä on vaihdannainen, on myöskin $\mathrm{C}_3 \rtimes_\tau \mathrm{C}_2$ vaihdannainen lemman 3.19 nojalla.

Olkoon nyt $\sigma : \mathrm{C}_2 \to \mathrm{Aut}(\mathrm{C}_3)$ homomorfismi $x\sigma_0 = x$ ja $x\sigma_1 = x^{-1}$ kaikilla $x \in \mathrm{C}_3$. Helposti nähdään, että $\sigma : \mathrm{C}_2 \to \mathrm{Aut}(\mathrm{C}_3)$ on homomorfismi. Tarkastellaan alkioiden $(0, 1), (1, 0) \in \mathrm{C}_3 \rtimes_\sigma \mathrm{C}_2$ tuloja

$$(1, 0)(0, 1) = (1, 1), \text{ mutta } (0, 1)(1, 0) = (1, 1\sigma_1) = (1, 2) \neq (1, 1),$$

joten $\mathrm{C}_3 \rtimes_\sigma \mathrm{C}_2$ ei ole vaihdannainen ryhmä, eikä siis myöskään isomorfinen ryhmien C_2 ja C_3 suoran tulon kanssa (tällöin se olisi vaihdannainen, koska ryhmät C_2 ja C_3 ovat vaihdannaisia).

3.3. Kommutaattorit ja kommutaattorialiryhmä

Jos $x, y \in G$, niin ei välttämättä ole $xy = yx$, ellei G ole Abelin ryhmä. Sellaista alkiota $[x, y] \in G$, jolla on ominaisuus

$$xy = yx[x, y],$$

kutsutaan alkioiden x ja y kommutaattoriksi. Helppo laskutoimitus osoittaa, että alkioiden x ja y kommutaattori on aina yksikäsitteisesti määritelty ja pätee, että $[x, y] = x^{-1}y^{-1}xy$.

Ryhmän G *kommutaattorialiryhmä* G' on $\langle\{[x,y] \mid x,y \in G\}\rangle$. Kuten seuraavasta lemmasta nähdään, kommutaattorialiryhmä on normaali ryhmässä G ja se on pienin aliryhmä, jonka tekijäryhmä on Abelin ryhmä.

3.21. **Lemma.** *Olkoon $H \leq G$. Pätee, että*

$$H \lhd G \text{ ja } G/H \text{ on Abelin ryhmä, joss } G' \leq H.$$

Todistus. Olkoon $H \lhd G$ ja G/H vaihdannainen. Olkoon $x, g \in G$, jolloin

$$H = (x^{-1}x)(g^{-1}g)H = x^{-1}HxHg^{-1}HgH = x^{-1}Hg^{-1}HxHgH = [x,g]H,$$

mistä seuraa, että $G' \leq H$.

Olkoon nyt $G' \leq H$, $g \in G$ ja $h \in H$, jolloin

$$h^g = g^{-1}hg(h^{-1}h) = [g,h^{-1}]h \in H,$$

siispä $H \lhd G$. Koska $xy = yx[x,y]$, niin

$$xy \in (xy)G' \cap (yx)G' \subset (xy)H \cap (yx)H,$$

joten G/H on vaihdannainen (koska eri sivuluokat ovat pistevieraita). □

Kommutaattorialiryhmä määriteltiin kommutaattoreiden joukon virittämäksi aliryhmäksi. Tämä on välttämätöntä, kuten seuraava esimerkki osoittaa, sillä kommutaattoreiden tulo ei aina ole kommutaattori.

3.22. **Esimerkki.** (Muokattu artikkelista [5]) Olkoon $\mathbb{F}_2$ kertaluvun kaksi Galois'n kunta. Olkoon G matriisien

$$M(f,g,h) = \begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix}$$

joukko, missä $f \in \mathbb{F}_2[x]$, $g \in \mathbb{F}_2[y]$ ja $h \in \mathbb{F}_2[x,y]$. Tavallisella matriisien kertolaskulla saadaan

(1) $M(f_1,g_1,h_1)M(f_2,g_2,h_2) = M(f_1+f_2, g_1+g_2, h_1+h_2+f_1g_2) \in G$,
(2) $M(f,g,h)^{-1} = M(f,g,h+fg) \in G$ ja
(3) neutraalialkio $M(0,0,0) \in G$

eli G on matriisien kertolaskun suhteen ääretön ryhmä. Alkioiden $M(f_1,g_1,h_1)$ ja $M(f_2,g_2,h_2)$ kommutaattori on

$$\begin{aligned}
[M(f_1,g_1,h_1), M(f_2,g_2,h_2)] &= M(f_1,g_1,h_1)^{-1}M(f_2,g_2,h_2)^{-1}M(f_1,g_1,h_1)M(f_2,g_2,h_2) \\
&= M(f_1,g_1,h_1+f_1g_1)M(f_2,g_2,h_2+f_2g_2)\cdot \\
&\quad M(f_1,g_1,h_1)M(f_2,g_2,h_2) \\
&= M(f_1+f_2, g_1+g_2, (h_1+h_2)+(f_1g_1+f_2g_2)+f_1g_2)\cdot \\
&\quad M(f_1+f_2, g_1+g_2, (h_1+h_2)+f_1g_2) \\
&= M(2(f_1+f_2), 2(g_1+g_2), 2(h_1+h_2)+2f_1g_1+ \\
&\qquad (f_1+f_2)(g_1+g_2)+(f_1g_1+f_2g_2)) \\
&= M(0,0,2f_1g_1+2f_2g_2+f_1g_2+f_2g_1) \\
&= M(0,0,f_1g_2+f_2g_1) \in \langle\{M(0,0,h) \mid h \in \mathbb{F}_2[x,y]\}\rangle.
\end{aligned}$$

Olkoon $N = \langle\{M(0,0,h) \mid h \in \mathbb{F}_2[x,y]\}\rangle$. Yllä osoitettiin, että $G' \leq N$. Koska

$$M(0,0,h_1)M(0,0,h_2) = M(0,0,h_1+h_2),$$

niin N on alkioiden $M(0,0,x^iy^j)$ virittämä, missä $i, j \in \mathbb{N}$ ja koska

$$[M(x^i,0,0), M(0,y^j,0)] = M(0,0,x^iy^j) \in G',$$

niin $G' = N$. Tarkastellaan kommutaattorialiryhmän alkiota $M(0,0,1+xy+x^2y^2+x^3y^3)$. Oletetaan, että se on kommutaattori, siis että on sellaiset polynomit $f_1, f_2 \in \mathbb{F}_2[x]$ ja $g_1, g_2 \in \mathbb{F}_2[y]$, että

$$1 + xy + x^2y^2 + x^3y^3 = f_1(x)g_2(y) + f_2(x)g_1(y).$$

Olkoot $f_1(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$ ja $f_2(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n$, jolloin kertomalla ja keräämällä termit yhteen saadaan

$$x^iy^i = x^i(a_ig_2(y) + b_ig_1(y)) \Rightarrow y^i = a_ig_2(y) + b_ig_1(y)$$

jokaisella $i \in \{0,1,2,3\}$. Koska kertoimet a_i ja b_i ovat kunnan $\mathbb{F}_2$ alkioita ei kuitenkaan ole kuin 3 erilaista vaihtoehtoa lausekkeen $a_ig_2(y) + b_ig_1(y) \neq 0$ arvolle, mikä on ristiriita, koska kaikki alkiot 1, y, y^2 ja y^3 ovat eri alkioita ja eroavat nollasta. Täten jokainen kommutaattorialiryhmän alkio ei ole itse kommutaattori.

3.23. **Lemma.** *Olkoon G ryhmä. Jos jokaisen $x \in G \setminus \mathrm{Z}(G)$ kertaluku on 2, on G Abelin ryhmä.*

Todistus. Olkoot $g, h \in G \setminus \mathrm{Z}(G)$. Jos $gh \in \mathrm{Z}(G)$, niin

$$[g,h] = g^{-1}h^{-1}gh = gh(gh) = g(gh)h = 1.$$

Muuten $o(gh) = 2$, joten

$$[g,h] = g^{-1}h^{-1}(gh) = (gh)(gh) = 1.$$

□

Jos $H, K \subset G$, voidaan määritellä osajoukkojen H ja K kommutaattorialiryhmä

$$[H,K] = \langle\{[h,k] \mid h \in H \text{ ja } k \in K\}\rangle.$$

Jos $h \in H$ ja $k \in K$, niin $[h,k]^{-1} = (h^{-1}k^{-1}hk)^{-1} = k^{-1}h^{-1}kh = [k^{-1},h^{-1}]$, mistä nähdään että $[H,K] = [K,H]$. Koko ryhmän G kommutaattorialiryhmä on $G' = [G,G]$.

Normaaliuden käsite liittyy kiinteästi vaihdannaisuuden käsitteeseen, kuten seuraava lause osoittaa

3.24. **Lemma.** *Pätee, että $N \lhd G$, joss $[G,N] \leq N$ (tai $[N,G] \leq N$).*

Todistus. Olkoon $g \in G$, $n \in N$ ja $[g,n] = n' \in N$. Nyt

$$[g,n] = n' \Leftrightarrow g^{-1}n^{-1}gn = n' \Leftrightarrow (n^{-1})^g = n'n^{-1} \text{ siispä } [G,N] \leq N \Leftrightarrow N \lhd G.$$

□

Tästä seuraa, että jos $M, N \lhd G$, niin $[M, N] \leq M \cap N$.

Olkoot $x \in G$, $h \in H$ sekä $k \in K$, jolloin

$$[h,k]^x = x^{-1}h^{-1}k^{-1}hkx = (x^{-1}h^{-1}x)(x^{-1}k^{-1}x)(x^{-1}hx)(x^{-1}kx) = [h^x, k^x] \in [H,K]$$

eli $[H,K] \lhd G$. Voidaan osoittaa (samalla tavalla kuin lemmassa 3.21), että $[H,K]$ on pienin normaali aliryhmä, jonka tekijäryhmässä jokaisella $h \in H$ ja $k \in K$ pätee $hk[H,K] = kh[H,K]$.

3.25. **Lemma.** *Pätee, että $G' \leq \mathrm{Frat}(G)$, joss ryhmän G jokainen maksimaalinen aliryhmä on normaali.*

Todistus. Jos $G' \leq \mathrm{Frat}(G)$, niin $G' \leq M$ jokaisella ryhmän G maksimaalisella aliryhmällä M. Lauseesta 3.21 seuraa nyt, että jokainen maksimaalinen aliryhmä $M \lhd G$.

Olkoon M ryhmän G maksimaalinen aliryhmä, joka on normaali. Tällöin ryhmän G/M kertaluku on alkuluku lauseen 3.14 nojalla. Siispä G/M on Abelin ryhmä, joten lemman 3.21 nojalla $G' \leq M$. Selvästikin $G' \leq \mathrm{Frat}(G)$, mikäli jokainen ryhmän G maksimaalinen aliryhmä on normaali. □

3.26. **Lemma.** *Jos $G' \subset \mathrm{Z}(G)$, niin jokainen ryhmän G alkio on vaihdannainen jokaisen konjugaattinsa kanssa.*

Todistus. Olkoon $G' \subset \mathrm{Z}(G)$ ja olkoon $g \in G$. Nyt $g^{-1}(y^{-1}gy) = g^{-1}g^y \in \mathrm{Z}(G)$ kaikilla $g, y \in G$ eli g ja g^y kuuluvat samaan keskuksen sivuluokkaan, joten ne ovat keskenään vaihdannaisia. □

3.4. Nilpotentit ryhmät

3.27. **Määritelmä.** Ryhmän *G alempi keskeinen sarja* on aliryhmien $\Gamma_i(G)$ sarja, missä

$$\Gamma_0(G) = G \text{ ja } \Gamma_{i+1}(G) = [\Gamma_i(G), G].$$

Jos $\Gamma_n(G) = \{1\}$ jollain $n \in \mathbb{N}$, niin sanotaan, että ryhmä G on *nilpotentti*.

Määritelmästä nähdään, että $\Gamma_1(G) = G'$. Jos $G' = \{1\}$, on ryhmä G nilpotentti, joten jokainen Abelin ryhmä on nilpotentti. Pienintä $n \in \mathbb{N}$, jolla $\Gamma_n(G) = \{1\}$ sanotaan nilpotentin ryhmän *nilpotenttisuusasteeksi*. Selvästikin epätriviaalin ryhmän nilpotenttisuusaste on 1, joss ryhmä on epätriviaali Abelin ryhmä.

3.28. **Lemma.** *Jokainen tekijä $\Gamma_i(G) \lhd G$, missä $0 \leq i < \infty$.*

Todistus. Selvästikin $\Gamma_0(G) = G \lhd G$. Olkoon $k \in \mathbb{N}$ ja $\Gamma_k(G) \lhd G$. Aliryhmän Γ_{k+1} virittävät alkiot muotoa $[\gamma, g]$, missä $\gamma \in \Gamma_k$ ja $g \in G$. Olkoon $x \in G$, jolloin

$$[\gamma, g]^x = [\gamma^x, g^x] \in \Gamma_{k+1}(G) = [\Gamma_k(G), G], \text{ koska } \Gamma_k \lhd G.$$

□

Olkoon ryhmän G nilpotenttisuusaste n, jolloin $[\Gamma_{n-1}(G), G] = \{1\}$, eli $\Gamma_{n-1} \subset \mathrm{Z}(G)$. Tästä seuraa helposti, että nilpotentin ryhmän keskus on epätriviaali.

3.29. **Lemma.** *Jos $G \neq \{1\}$ ja $\mathrm{Z}(G) = \{1\}$, ei G ole nilpotentti.*

Todistus. Oletetaan, että G on nilpotentti. Koska G ei ole triviaali ryhmä, on sen nilpotenttisuusaste $n > 0$ eli $\Gamma_{n-1}(G)$ on määritelty. Kuten yllä nähtiin, on

$$[\Gamma_{n-1}(G), G] = \Gamma_n(G) = \{1\} \Rightarrow \Gamma_{n-1} \subset \mathrm{Z}(G) = \{1\}$$

Tästä seuraa, että ryhmän G nilpotenttisuusaste on $< n$, mikä on ristiriita. □

Itse asiassa saadaan hieman parempikin tulos.

3.30. **Lemma.** *Jos G on nilpotentti ryhmä, $N \neq \{1\}$ ja $N \lhd G$, niin $N \cap \mathrm{Z}(G) \neq \{1\}$.*

Todistus. Olkoon $i+1 \in \mathbb{N}$ pienin luku, jolla $N \cap \Gamma_{i+1}(G) = \{1\}$, jolloin $N \cap \Gamma_i(G) \neq \{1\}$. Nyt $[N \cap \Gamma_i(G), G] \subset \Gamma_{i+1}(G)$. Koska $N \lhd G$, niin on lemman 3.24 nojalla on $[N \cap \Gamma_i(G), G] \subset N$. Niinpä

$$[N \cap \Gamma_i(G), G] = \{1\},$$

mutta $[N \cap \Gamma_i(G), G]$ on välttämättä epätriviaali, ellei $N \cap \Gamma_i(G) \subset \mathrm{Z}(G)$. □

3.31. **Lemma.** *Nilpotentin ryhmän G aliryhmät ja tekijäryhmät ovat nilpotentteja ja niiden nilpotenttisuusaste on korkeintaan ryhmän G nilpotenttisuusaste.*

Todistus. Jos G on nilpotentti ja $H \leq G$, niin $\Gamma_0(H) \leq \Gamma_0(G)$. Jos oletetaan, että $\Gamma_i(H) \leq \Gamma_i(G)$, niin $\Gamma_{i+1}(H) = [\Gamma_i(H), H] \leq [\Gamma_i(G), G] = \Gamma_{i+1}(G)$, joten jokaisella $k \in \mathbb{N}$ on $\Gamma_k(H) \leq \Gamma_k(G)$. Jollain $n \in \mathbb{N}$ on $\Gamma_n(G) = \{1\}$, joten $\Gamma_n(H) = \{1\}$. Siispä H on nilpotentti ja sen nilpotenttisuusaste on korkeintaan n.

Olkoon nyt G/N jokin ryhmän G tekijäryhmä. Olkoon $f : G \to G/N$ kanoninen surjektio. Osoitetaan, että tekijäryhmän G/N alempi keskeinen sarja on $\Gamma_0(G)f, \Gamma_1(G)f, \ldots$.

Selvästikin $\Gamma_0(G/N) = G/N = Gf = \Gamma_0(G)f$. Oletetaan, että väite pätee jollain $i \in \mathbb{N}$. Nyt

$$\Gamma_{i+1}(G/N) = [\Gamma_i(G/N), G/N] = [\Gamma_i(G)f, Gf] = [\Gamma_i(G), G]f = \Gamma_{i+1}(G)f,$$

joten väitteen ensimmäinen osa seuraa. Toinen osa seuraa siitä, että $\Gamma_n(G) = \{1\} \Rightarrow \Gamma_n(G/N) = \{N\}$. □

3.32. **Lemma.** *Ryhmä G on nilpotentti, joss $G/\mathrm{Z}(G)$ on nilpotentti.*

Todistus. Jos G on nilpotentti, on lemman 3.31 nojalla $G/\mathrm{Z}(G)$ nilpotentti.

Olkoon jokaisen $\Gamma_i(G/\mathrm{Z}(G))$ alkukuva ryhmässä G aliryhmä Γ_i, siis

$$\Gamma_i/\mathrm{Z}(G) = \Gamma_i(G/\mathrm{Z}(G)).$$

Huomataan heti, että $\Gamma_0(G) = \Gamma_0$. Oletetaan, että $\Gamma_i(G) \subset \Gamma_i$. Olkoon $\gamma \in \Gamma_i(G)$ ja $x \in G$, jolloin

$$[\gamma\,\mathrm{Z}(G), x\,\mathrm{Z}(G)] = [\gamma, x]\,\mathrm{Z}(G) \in \Gamma_{i+1}(G/\mathrm{Z}(G)) \text{ joten } \Gamma_{i+1}(G) \subset \Gamma_{i+1}.$$

Oletetaan nyt, että $G/\mathrm{Z}(G)$ on nilpotentti, jolloin on sellainen $n \in \mathbb{N}$ että $\Gamma_n(G/\mathrm{Z}(G) = \{Z(G)\}$, siis $\Gamma_n = \mathrm{Z}(G)$. Tästä seuraa, että $\Gamma_n(G) \subset \mathrm{Z}(G)$, mistä seuraa, että $\Gamma_{n+1}(G) = \{1\}$. □

3.33. **Lause.** *Jos G on nilpotentti ryhmä ja $H < G$, niin $H < \mathrm{N}(H)$.*

Todistus. Olkoon $i \in \mathbb{N}$ pienin sellainen luku, että $\Gamma_{i+1}(G) < H$, jolloin on joko $H = \Gamma_i(G)$ tai on alkio $x \in \Gamma_i(G) \setminus H$. Jos $H = \Gamma_i(G)$, niin $H \lhd G$ eli väite pätee. Jos taas $x \in \Gamma_i(G) \setminus H$ ja $h^{-1} \in H$, niin

$$(h^{-1})^x = (x^{-1}h^{-1}x)(hh^{-1}) = [x,h]h^{-1} \in \Gamma_{i+1}(G)H = H,$$

joten $x \in \mathrm{N}(H)$, eli $H < \mathrm{N}(H)$. □

3.34. **Korollaari.** *Jos G on äärellinen nilpotentti ryhmä ja $H \leq G$, niin on olemassa sellainen jono aliryhmiä H_0, ..., H_n että*

$$H = H_0 \lhd \ ... \ \lhd H_n = G.$$

Todistus. Olkoon $H_0 = H$ ja $H_{i+1} = N(H_i)$. Lauseen 3.33 nojalla on jokaisella i joko $H_i = G$ tai $H_i < H_{i+1}$. Koska ryhmä G on äärellinen ja

$$H_0 < \ ... \ < H_k \text{ jokaisella } k, \text{ jolla } H_k \text{ on aito aliryhmä,}$$

on välttämättä $H_i = G$ jollain i. □

3.35. **Lause.** *Nilpotentin ryhmän maksimaalinen normaali Abelin aliryhmä on maksimaalinen Abelin aliryhmä.*

Todistus. Olkoon G nilpotentti ryhmä. ja A sen maksimaalinen normaali Abelin aliryhmä. Aliryhmä $A \lhd \mathrm{C}(A)$. Koska $A \lhd G$, niin $\mathrm{C}(A) \lhd G$, joten $\mathrm{C}(A)/A \lhd G/A$. Tästä seuraa, että $\mathrm{C}(A)/A \cap \mathrm{Z}(G/A) \neq \{A\}$, mikäli $A < \mathrm{C}(A)$. Koska aliryhmän $\mathrm{Z}(G/A) \cap \mathrm{C}(A)/A$ alkukuva ryhmässä G on normaali Abelin ryhmä, niin $\mathrm{C}(A) = A$, sillä A on maksimaalinen normaali Abelin aliryhmä. Näin siis A on maksimaalinen Abelin ryhmä. □

3.36. **Lemma.** *Jos G on nilpotentti ryhmä, niin $G' \leq \mathrm{Frat}(G)$.*

Todistus. Lauseen 3.33 nojalla jokainen ryhmän G maksimaalinen aliryhmä on normaali, joten lauseen 3.25 nojalla $G' \leq \mathrm{Frat}(G)$. □

3.5. Ryhmien maksimaaliset Abelin aliryhmät

Äärellisen ryhmän G jokainen normaali Abelin aliryhmä sisältyy johonkin maksimaaliseen normaaliin Abelin aliryhmään. Jos A on normaali Abelin aliryhmä ja $x \in G$, niin x määrittelee konjugaatiolla ryhmän A isomorfismin. Alkiot $x \in G$ ja $y \in G$ määrittelevät saman isomorfismin, mikäli ne kuuluvat samaan aliryhmän A sivuluokkaan. Tämän takia voidaan määritellä ryhmän G/A toiminta ryhmässä A, missä jokainen sivuluokka (Ag) määrittelee saman permutaation kuin $g \in G$.

3.37. **Määritelmä.** Olkoon ryhmällä G ominaisuus: Jos $A \leq G$ on maksimaalinen normaali Abelin aliryhmä, niin A on maksimaalinen Abelin aliryhmä. Tällaista ryhmää G, joka ei ole Abelin ryhmä, kutsutaan *O-ryhmäksi*.

Edellisestä määritelmästä ja lauseessa 3.35 seuraa, että jokainen nilpotentti ryhmä, joka ei ole Abelin ryhmä on *O*-ryhmä.

3.38. **Lause.** *Olkoon G O-ryhmä. Tällöin sen normaali Abelin aliryhmä A on maksimaalinen normaali Abelin aliryhmä, joss ryhmä G/A toimii uskollisesti ryhmässä A.*

Todistus. Jos A on maksimaalinen normaali Abelin aliryhmä, on A maksimaalinen Abelin aliryhmä. Tästä seuraa, että ryhmän G/A toiminta aliryhmässä A on uskollinen (koska $\mathrm{C}(A) = A$).

Jos taas G/A toimii uskollisesti ryhmässä A, on jokaisella $x \in G \setminus A$ $a^x \neq a$ jollain $a \in A$, joten $\mathrm{C}(A) = A$. □

Jos G on O-ryhmä ja A sen maksimaalinen normaali Abelin aliryhmä kertalukua n, on $|G/A| \leq n!$, koska tätä suuremmalla joukolla ei ole uskollisia toimintoja joukossa A. Koska jokainen aliryhmän A automorfismi kiinnittää alkion 1, on itse asiassa $|G/A| \leq (n-1)!$, siispä $|G| \leq n!$.

3.39. **Esimerkki.** Osajoukko

$$A = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

muodostaa ryhmän S_4 aliryhmän. Kuten esim. laskemalla on helppo huomata, on tämä aliryhmä Abelin aliryhmä. Koska ryhmän S_4 alkiot ovat konjugaatteja, joss niillä on sama syklirakenne, on aliryhmä myöskin normaali. Se nimittäin sisältää jokaisen ryhmän S_4 permutaation, joka on kahden erillisen transposition tulo, eikä näiden lisäksi sisällä muuta kuin neutraalialkion. Olkoon $(a\ b)$ transpositio ja $c, d \notin \{a, b\}$. Nyt

$$a(a\ b)^{(a\ c)(b\ d)} = a \Rightarrow (a\ b) \notin \mathrm{C}(A).$$

Olkoon $(a\ b\ c)$ kolmisykli ja $d \notin \{a, b, c\}$. Nyt

$$a(a\ b\ c)^{(a\ b)(c\ d)} = d \Rightarrow (a\ b\ c) \notin \mathrm{C}(A).$$

Olkoon $(a\ b\ c\ d)$ nelisykli. Nyt

$$a(a\ b\ c\ d)^{(a\ d)(b\ c)} = d \Rightarrow (a\ b\ c\ d) \notin \mathrm{C}(A).$$

Koska ryhmän S_4 alkiot ($\neq 1$) ovat täsmälleen sen transpositiot, kahden transposition tulot, kolmi- ja nelisyklit, on A maksimaalinen Abelin aliryhmä.

Kahden erillisen transposition tulot muodostavat ryhmän S_4 ainoan epätriviaalin konjugaattiluokan, jonka kaikki alkiot ovat keskenään vaihdannaisia. Jos B on ryhmän S_4 normaali aliryhmä, joka sisältää jonkin alkion $g \notin A$, se sisältää koko alkion g konjugaattiluokan eli se ei voi olla Abelin aliryhmä. Koska A on ryhmän S_4 ainoa maksimaalinen normaali Abelin aliryhmä ja A on maksimaalinen Abelin aliryhmä, on S_4 O-ryhmä. Aliryhmän A indeksi on $|G/A| = 4!/4 = 3!$.

Edellinen esimerkki osoittaa, että O-ryhmissä yllä esitetty tulos on eräässä mielessä paras mahdollinen. Kuitenkin tuntuu selvältä, että useimmille kertaluvuille voidaan saada paljonkin parempia tuloksia. Harvan Abelin ryhmän H automorfismien ryhmän kertaluku on nimittäin $(|H| - 1)!$. Esimerkin aliryhmä A on isomorfinen Kleinin neliryhmän kanssa. Kleinin neliryhmällä tämä ominaisuus on. Sen lisäksi on vain kaksi muuta äärellistä ryhmää, joiden automorfismien joukko on yhtä iso. Nämä ovat kaksi- ja kolmialkioinen syklinen ryhmä.

Tämä todetaan seuraavasti. Olkoon H, sellainen ryhmä, että $|\operatorname{Aut}(H)| = (|H| - 1)!$. Nyt jokainen ryhmän $\operatorname{Aut}(H)$ kuvaus on samalla yksikäsitteinen joukon $H \setminus \{1\}$ permutaatio. Koska $|\operatorname{Aut}(H)| = |\operatorname{S}_{H\setminus\{1\}}|$, sisältää $\operatorname{Aut}(H)$ jokaisen joukon $H \setminus \{1\}$ permutaation. Olkoon $f \in \operatorname{Aut}(H)$ ja $x \in H \setminus \{1\}$. Nyt pätee että $x^2 f = (xf)^2$, joten f kiinnittää alkion x^2, mikäli se kiinnittää alkion x. Tästä seuraa

(1) jokainen permutaatio, joka kiinnittää alkion x on identiteettikuvaus, siis joukossa $H \setminus \{1\}$ on yksi tai kaksi alkiota eli ryhmässä H on kaksi tai kolme alkiota, tai
(2) jokaisella $x \in H$ on $x^2 = 1$ eli $|H| = 2^n$, jollain $n \in \mathbb{N}$.

Oletetaan jälkimmäisessä tapauksessa, että $x, y \in H \setminus \{1\}$ ja $x \neq y$. Nyt jos $xf = x$ ja $yf = y$, niin $(xy)f = xy$,. Kuten yllä voidaan, saadaan siksi, että joukossa $H \setminus \{1\}$ on kolme alkiota, tai $xy = 1$. Jälkimmäinen johtaa ristiriitaa, koska oletettiin, että $o(x) = o(y) = 2$ ja $x \neq y$. Siispä $n = 2$ tai $n = 1$. Siispä H on isomorfinen kaksi- tai kolmialkioisen syklisen ryhmän kanssa tai Kleinin neliryhmän kanssa.

Yllä oleva tulos sopii hyvin yhteen sen kanssa, että on olemassa ryhmä S_3, joka on kertalukua 6, mutta sen suurin Abelin aliryhmä on ainoastaan kertalukua 3.

Olkoon A ryhmän G maksimaalinen normaali Abelin aliryhmä, jonka kertaluku on n. Kuten nähtiin on $|G/A| < (n-1)!$. Koska G on nilpotentti ryhmä ja $|A| > 1$ on $\operatorname{Z}(G) \cap A \neq \{1\}$ lemman 3.30 nojalla. Jokainen ryhmän G/A alkio kiinnittää keskuksen pisteittäin, joten $|G/A| \leq (n-2)!$ eli $|G| \leq n \cdot (n-2)!$. Vaikka on olemassa p-ryhmiä, kuten D_8, missä tämä raja saavutetaan, voidaan isommille nilpotenteille ryhmille tätä rajaa parantaa käyttämällä hyväksi p-ryhmille saatavia tuloksia.

3.40. **Lause.** *Olkoon $n \in \mathbb{N}$. Olkoon G nilpotentti ryhmä ja $|G| > n \cdot (n-2)!$. Jos $A \lhd G$ on maksimaalinen normaali Abelin aliryhmä, on $|A| > n$. Erityisesti jokaisessa nilpotentissa ryhmässä, joka on suurempaa kertalukua kuin $n \cdot (n-2)!$ on vähintään kertalukua n olevia Abelin aliryhmiä.*

3.6. p-RYHMÄT

Sylowin lauseen nojalla on jokaiselle alkulukupotenssille p^n, joka jakaa ryhmän G kertaluvun, olemassa ryhmän G aliryhmiä, jotka ovat kertalukua p^n. Koska jokaisen ryhmän rakenne on vahvasti yhteydessä sen aliryhmiin, on tällaisten kertalukua p^n olevien ryhmien rakenteen tunteminen tärkeää. Näillä p-ryhmiksi kutsutuilla ryhmillä on myös erityisominaisuuksia, joita yleisillä ryhmillä ei ole. Tämä tekee niiden tutkimisesta jossain määrin helpompaa. Näiden seikkojen takia on p-ryhmiä ja niiden yleistyksiä nilpotentteja ryhmiä tutkittu varsin paljon ryhmäteorian piirissä.

Kirjoittajien Besche & al. [2] mukaan on korkeintaan kertalukua 2000 olevia ryhmiä 49.910.529.484, joista 49.487.365.422 eli yli 99%, on 2-ryhmiä joiden kertaluku on 2^{10}. On hyvin intuitiivinen ajatus, että kertalukua n olevien ryhmien lukumäärä on sitä suurempi, mitä jaollisempi luku n on ja luvut $2^m < n$ ovat kaikkein jaollisimpia kaikista lukua n pienemmistä luvuista. Siten tulos ei ehkä ole niin omituinen kuin miltä se ensi silmäyksellä näyttää. Tämä kuitenkin antaa hyvän perusteen p-ryhmien tutkimiselle. Suurin osa lukua n pienempien kertalukujen ryhmistä on p-ryhmiä.

Olkoon p loppuluvun ajan alkuluku.

3.41. **Määritelmä.** Ryhmä G on p-ryhmä, joss sen jokaisen alkion kertaluku on p^n jollain $n \in \mathbb{N}$.

3.42. **Lemma.** *Olkoon G ryhmä.*

(1) *Ryhmä G on p-ryhmä, joss sen jokainen aliryhmä ja tekijäryhmä ovat p-ryhmiä.*
(2) *Jos G on äärellinen, niin se on p-ryhmä, joss sen kertaluku on p^n.*

Todistus.

(1) Jos G on p-ryhmä ja $H \leq G$, niin jokaiselle $h \in H$ on $h \in G$ eli H on p-ryhmä. Jos $N \lhd G$ ja $x \in G$, niin $o(x) = p^n$ jollain $n \in \mathbb{N}$. Koska $(xN)^{p^n} = N$ on Lagrangen lauseen mukaan sivuluokan xN kertaluku luvun p^n tekijä eli alkuluvun p potenssi.
Jos ryhmän G jokainen aliryhmä on p-ryhmä on G omana aliryhmänään p-ryhmä. Koska G on isomorfinen ryhmän $G/\{1\}$ kanssa, pätee sama myös tekijäryhmille.
(2) Jos G on äärellinen ja jokin alkuluku $q \neq p$ on ryhmän G kertaluvun tekijä, on Sylowin lauseen nojalla ryhmällä G kertalukua q oleva alkio, mikä on ristiriita. Siispä ryhmän G kertaluku on p^n jollain $n \in \mathbb{N}$.
Jos ryhmän G kertaluku on p^n, on sen jokaisen alkion kertaluku Lagrangen lauseen mukaan alkuluvun p potenssi eli G on p-ryhmä.

□

p-ryhmillä on monia ominaisuuksia, joita yleisillä ryhmillä ei ole. Monet niistä tulevat parhaiten esiin, kun annetaan p-ryhmien toimia toisissa p-ryhmissä.

3.43. **Määritelmä.** Jos G toimii rakenteessa X ja $x \in X$ on sellainen alkio, että $xg = x$ jokaiselle $g \in G$, niin x on ryhmän G toiminnan *kiintopiste*. *Toiminnan kiintopisteiden joukko* on

$$\mathrm{Fix}_G(X) = \{x \in X \mid x \text{ on ryhmän } G \text{ toiminnan kiintopiste}\}.$$

3.44. **Lemma.** *Olkoon G äärellinen p-ryhmä ja X äärellinen joukko. Jos G toimii joukossa X, niin* $|\mathrm{Fix}_G(X)| \equiv |X| \mod p$.

Todistus. Jos $y \in X \setminus \mathrm{Fix}_G(X)$, niin $|yG| \,\big|\, |G|$, lauseen 3.9 nojalla, eli $|yG| = p^k$ jollain $k \in \mathbb{N}$ ja $k \neq 0$. Valitaan jokaisesta joukon $X \setminus \mathrm{Fix}_G(X)$ radasta edustajat. Olkoon saatu edustajisto $y_1, ..., y_m$. Tällöin

$$|X \setminus \mathrm{Fix}_G(X)| = |X| - |\mathrm{Fix}_G(X)| = \sum_i |y_i G| = kp, \text{ jollain } k \in \mathbb{N}.$$

Siispä $|\mathrm{Fix}_G(X)| \equiv |X| \mod p$. □

3.45. **Lemma.** *Jokaisen äärellisen epätriviaalin p-ryhmän keskus on epätriviaali.*

Todistus. Olkoon G äärellinen epätriviaali p-ryhmä, jonka kertaluku on p^k jollain $k \in \mathbb{N} \setminus \{0\}$. Jos G toimii itsellään konjugaatiolla, niin $\mathrm{Fix}_G(G) = \mathrm{Z}(G)$. Tiedetään, että $1 \in \mathrm{Fix}_G(G)$, mistä seuraa, että $\mathrm{Fix}_G(G) \neq \emptyset$. Lemmasta 3.44 Seuraa, että

$$|\mathrm{Fix}_G(G)| \equiv |G| \equiv 0 \mod p,$$

mistä seuraa, että $|\mathrm{Fix}_G(G)| > 1$. □

3.46. **Lemma.** *Jos G on p-ryhmä ja $H < G$, niin $H < N(H)$.*

Todistus. Olkoon X aliryhmän H oikeanpuoleisten sivuluokkien joukko. Ryhmä H toimii tässä joukossa oikealta kertoen. Jos $h \in H$ ja $Hx \in X$, niin

$$(Hx)h = H(xhx^{-1})x = Hx, \text{ joss } h^{x^{-1}} \in H,$$

siispä $Hx \in \mathrm{Fix}_H(X)$, joss $x \in N(H)$. Koska $H \in \mathrm{Fix}_H(X)$ ja H on p-ryhmä, niin $|Fix_H(X)| = |N(H)|/|H| > 1$, eli $H < N(H)$. □

Lemmalla 3.46 on erittäin hyödyllisiä korollaareja.

3.47. **Korollaari.** *Olkoon G p-ryhmä. Aliryhmä $H < G$ on maksimaalinen, joss $[G : H] = p$.*

Todistus. Lemman 3.11 nojalla H on maksimaalinen, jos sen indeksi on p. Olkoon nyt $[G : H] = p^n$ jollain $n > 1$. Jos H ei ole normaali, on $G < \mathbb{N}(H) < H$, eli H ei ole maksimaalinen. Jos taas H on normaali, sisältää G/H Sylowin lauseen mukaan kertalukua p olevan alkion gH. Koska $n > 1$ on $\langle gH \rangle < G/H$, joten $H < \langle H \cup \{g\} \rangle < G$. □

3.48. **Korollaari.** *Jos G on äärellinen p-ryhmä, niin aliryhmä, jonka indeksi on p, on normaali. Erityisesti korollaarin 3.47 nojalla on jokainen p-ryhmän maksimaalinen aliryhmä sen maksimaalinen normaali aliryhmä.*

Edelliset ominaisuudet ovat p-ryhmille ja nilpotenteille ryhmille yhteisiä ja itse asiassa jokainen p-ryhmä onkin nilpotentti ryhmä, kuten seuraava lause osoittaa

3.49. **Lause.** *Jokainen p-ryhmä G on nilpotentti.*

Todistus. Kertalukua 1 oleva ryhmä on Abelin ryhmä, siis nilpotentti. Olkoon $n \in \mathbb{N} \setminus \{0\}$. Oletetaan, että jokainen p-ryhmä, jonka kertaluku on $< p^n$ on nilpotentti. Olkoon ryhmän G kertaluku p^n. Lemman 3.45 nojalla $|G/\mathrm{Z}(G)| < |G|$, joten $G/\mathrm{Z}(G)$ on induktio-oletuksen nojalla nilpotentti. Nyt lemman 3.32 nojalla on G nilpotentti. □

Tarkastelemme nyt p-ryhmän Frattinin aliryhmää ja käytämme siitä saamaamme tietoa p-ryhmän automorfismien ryhmän koon arvioimiseen. Käsittely on pääpiirteissään sama kuin Scotilla ([9] sivut 160-162).

3.50. **Määritelmä.** Ryhmä A on elementaarinen Abelin ryhmä, jos se on muotoa $\mathrm{C}_p \times ... \times \mathrm{C}_p$ jollain alkuluvulla p. Sanotaan, että ryhmän A *eksponentti* on p. Abelin ryhmä A on siis elementaarinen Abelin ryhmä, jonka eksponentti on p, joss sen jokainen alkio paitsi neutraalialkio on kertalukua p.

Jos G on elementaarinen Abelin ryhmä, niin voidaan määritellä kunnan $\mathbb{F}_p$ skalaarikertolasku ryhmässä G. Olkoon $x \in G$ ja $f \in \mathbb{F}_p$. Alkio f on jonkin luonnollisen luvun k jaollisuusluokka jaettaessa luvulla p. Määritellään $fx = x^k$. Tämä operaatio on hyvin määritelty ja toteuttaa kaikki skalaarikertolaskun aksioomat. Koska G on Abelin ryhmä, on se $\mathbb{F}_p$-avaruus varustettuna äskeisellä skalaarikertolaskulla. Jos ryhmän G kertaluku on p^n, on se n kunnan $\mathbb{F}_p$ n-ulotteinen vektoriavaruus. On helppoa osoittaa, että jokainen $\mathbb{F}_p$-avaruuden G virittäjistö on ryhmän G virittäjistö ja päinvastoin. On myös helppoa osoittaa, että ryhmän G homomorfismi itseensä on automorfismi, joss se on avaruuden G automorfismi. Erityisesti ryhmä $\mathrm{Aut}(G)$ toimii transitiivisesti joukossa $G \setminus \{1\}$.

3.51. **Lemma.** *Elementaarisen Abelin ryhmän G Frattinin aliryhmä on* $\{1\}$.

Todistus. Jokainen ryhmän G automorfismi kiinnittää aliryhmän $\mathrm{Frat}(G)$ lauseen 3.17 nojalla ja $\mathrm{Frat}(G)$ on välttämättä aito aliryhmä. Näin ollen $\mathrm{Frat}(G)$ ei voi sisältää muita alkioita kuin neutraalialkion, koska $\mathrm{Aut}(G)$ toimii transitiivisesti joukossa $G \setminus \{1\}$. Väite on todistettu. □

3.52. **Lemma.** *Jos G on p-ryhmä ja $H \leq G$, niin* $\mathrm{Frat}(G) \leq H$*, joss $H \lhd G$ ja G/H on elementaarinen Abelin ryhmä.*

Todistus. Olkoon $H \lhd G$ ja G/H elementaarinen Abelin ryhmä. Olkoon

$$\mathcal{K} = \{K \leq G \mid H \leq K \text{ ja } K \text{ on maksimaalinen aliryhmä.}\}$$

Nyt $\mathrm{Frat}(G) \leq \cap\mathcal{K}$. Koska G/H on elementaarinen Abelin ryhmä, on lauseen 3.51 nojalla $\mathrm{Frat}(G/H) = \{1\}$, joten $\cap\mathcal{K} = H$.

Olkoon nyt $\mathrm{Frat}(G) \leq H$. Koska G on nilpotentti ryhmä, on lauseen 3.36 nojalla $G' \leq \mathrm{Frat}(G)$, joten $H \lhd G$ ja G/H on Abelin ryhmä. Jokaisen ryhmän G maksimaalisen aliryhmän M indeksi on p, joten $x^p \in M$ jokaisella $x \in G$. Siispä $G^p \subset H$, eli jokaisen ryhmän G/H alkion kertaluku on p, joten G/H on elementaarinen Abelin ryhmä. □

Edellinen lemma mahdollistaa Abelin p-ryhmän G Frattinin aliryhmän kuvailemisen. Jos $x \in G$, niin $x^p \in \mathrm{Frat}(G)$, koska $G/\mathrm{Frat}(G)$ on elementaarinen Abelin ryhmä. Siispä $G^p \leq \mathrm{Frat}(G)$, missä $G^p = \{x^p \mid x \in G\}$, joka on aliryhmä, koska G on Abelin ryhmä. Toisaalta G/G^p on elementaarinen Abelin ryhmä, joten $\mathrm{Frat}(G) \leq G^p$. Nyt siis $\mathrm{Frat}(G) = G^p$.

3.53. **Lemma.** *(Burnsiden kantalause) Jos G on p-ryhmä, niin jokainen ryhmän G virittäjistö x_1, ..., x_r sisältää alivirittäjistön x_{i_1}, ..., x_{i_n}, missä n on ryhmän $G/\mathrm{Frat}(G)$ minimaalisen virittäjistön alkioiden lukumäärä.*

Todistus. Jono $x_1\,\mathrm{Frat}(G)$, ..., $x_r\,\mathrm{Frat}(G)$ virittää ryhmän $G/\mathrm{Frat}(G)$. Ryhmä $G/\mathrm{Frat}(G)$ on elementaarinen Abelin aliryhmä, siis $\mathbb{F}_p$ avaruus, jonka jokaisella virittäjistöllä on vapaa alivirittäjistö, jossa on n alkiota. Siispä saadaan alkuperäisen jonon alijono $x_{i_1}\,\mathrm{Frat}(G)$, ..., $x_{i_n}\,\mathrm{Frat}(G)$, joka virittää ryhmän $G/\mathrm{Frat}(G)$. Lemman 3.18 nojalla x_{i_1}, ..., x_{i_n} virittää ryhmän G. □

Frattinin aliryhmä antaa mahdollisuuden arvioida p-ryhmien automorfismiryhmien kokoa.

3.54. **Lause.** *Jos G on p-ryhmä kertalukua p^n, jonka Frattinin aliryhmän kertaluku on p^{n-r}, niin*

$$|\operatorname{Aut}(G)| \,\Big|\, (p^{r(n-r)} \prod_{i=0}^{r-1} (p^r - p^i)).$$

Todistus. Olkoon $f \in \operatorname{Aut}(G)$. Lemman 3.17 nojalla $\operatorname{Frat}(G)f = \operatorname{Frat}(G)$, joten f permutoi ryhmän $G/\operatorname{Frat}(G)$ alkioita. Siispä saadaan homomorfismi $\operatorname{Aut}(G) \to \operatorname{Aut}(G/\operatorname{Frat})$. Koska $G/\operatorname{Frat}(G)$ on elementaarinen Abelin ryhmä, joka on $\mathbb{F}_p$-avaruus, on

$$|\operatorname{Aut}(G/\operatorname{Frat}(G))| = \prod_{i=0}^{r-1} (p^r - p^i).$$

Tarkastellaan nyt homomorfismin ydintä K, joka on niiden ryhmän G automorfismien joukko, jotka kiinnittävät ryhmän $G/\operatorname{Frat}(G)$ pisteittäin. Olkoon $x_1, ..., x_r$ jokin ryhmän G virittäjistö (tällainen on olemassa, koska $G/\operatorname{Frat}(G)$ on kertalukua p^r). Olkoon $S = \{(y_1, ..., y_r) \mid y_i \in x_i \operatorname{Frat}(G)\}$, jolloin jokainen $f \in K$ vastaa jotakin joukon S permutaatiota. Vain identiteettikuvaus kiinnittää ryhmän G virittäjistön pisteittäin. Siispä yksikään $f \in K \setminus \{1\}$ ei kiinnitä yhtäkään virittäjistöä $s \in S$. Lisäksi jokainen f on erillisten saman pituisten syklien tulo, sillä muuten olisi sellainen $i \in \mathbb{N}$, että f^i kiinnittäisi jonkin, muttei kaikkia virittäjistöjä, mikä on ristiriita. Koska $|S| = p^{r(n-r)}$ nähdään suoraan, että jokaisen f kertaluku on jokin luvun p potenssi. Saadaan, että $|K| = p^k$ jollain $k \in \mathbb{N}$, koska K on p-ryhmä.

Toisaalta, koska jokainen $f \in K$ on yksikäsitteisesti määrätty, kun tiedetään virittäjistön $x_1, ..., x_r$ kuva, on $|K| \leq |S|$. Siispä $|K| \,\big|\, |S| = p^{r(n-r)}$, joten $|\operatorname{Aut}(G)| \,\big|\, (p^{r(n-r)} \prod_i p^r - p^i)$, missä $0 \leq i < r$. □

3.55. **Korollaari.** *Olkoon G p-ryhmä kertalukua p^n. Ryhmän* $\operatorname{Aut}(G)$ *Sylowin p-ryhmien kertaluku on luvun $p^{r(2n-r-1)/2}$ tekijä, missä ryhmän G Frattinin aliryhmän indeksi on p^r.*

Todistus. Lauseen 3.54 nojalla $|\operatorname{Aut}(G)| \,\big|\, (p^{r(n-r)} \prod_i p^r - p^i)$. Luvun p suurin potenssi, joka jakaa luvun $(p^{r(n-r)} \prod_i p^r - p^i)$ on

$$p^{r(n-r)} \prod_i p^i, \text{ missä } 0 \leq i < r \text{ eli } p^{r(n-r)} p^{r(r-1)/2}.$$

Siispä Sylowin p-ryhmien kertaluku on luvun $p^{r(2n-r-1)/2}$ tekijä. □

3.7. Äärellisten Abelin ryhmien rakenne

(Noudattaen esitystä [9], sivut 89-94.) Olkoon G äärellinen Abelin ryhmä. Jokaiselle alkuluvulle p, joka on ryhmän G kertaluvun tekijä, on Sylowin lauseen mukaan olemassa alkioita, joiden kertaluku on p^n jollain $n \in \mathbb{N}$. Olkoon jokaiselle tällaiselle p joukko

$$G_p = \{g \in G \mid o(g) = p^n \text{ jollain } n \in \mathbb{N}\}.$$

Jos $g, h \in G_p$, niin $o(g) = p^{n_1}$ ja $o(h) = p^{n_2}$, joten $(gh)^{p^{n_1+n_2}} = 1$, siispä $o(gh) | p^{n_1+n_2}$ eli G_p on suljettu ryhmäoperaation suhteen. Koska G on äärellinen ryhmä, on G_p sen aliryhmä.

3.56. **Määritelmä.** Jos G on äärellinen Abelin ryhmä, niin jokaisella p, joka jakaa ryhmän kertaluvun on G_p ryhmän *p-tekijä*.

Ratkaistaan nyt äärellisten Abelin ryhmien rakenne. Seuraavien lauseiden korollaarina saadaan tiettyä kertalukua olevien Abelin ryhmien lukumäärä.

3.57. **Lemma.** *Jos G on äärellinen Abelin ryhmä, niin G on p-tekijöidensä suora tulo.*

Todistus. Olkoon ryhmän G kertaluku $p_1^{n_1} \cdot \ ... \ \cdot p_k^{n_k}$. Tulo

$$G_{p_1} \times \ ... \ \times G_{p_k}$$

on välttämättä suora, koska jos p ja q_1, ..., q_n ovat eri alkulukuja, niin $p^k = q_1^{k_1} \cdot \ ... \ \cdot q_n^{k_n}$, joss $k = k_1 = \ ... \ = k_n = 0$. Siispä aliryhmien G_p ja $G_{q_1} \times ... \times G_{q_n}$ leikkaus on triviaali.

Jos $x \in G$, niin $o(x) = p_{i_1}^{m_1} \cdot \ ... \ \cdot p_{i_j}^{m_j}$, missä i_1, ..., i_j on jonon 1, ..., k osajono. Olkoon $P_{i_h} = p_{i_1}^{m_1} \cdot \ ... \ \cdot p_{i_{h-1}}^{m_{h-1}} \cdot p_{i_{h+1}}^{m_{h+1}} \cdot \ ... \ \cdot p_{i_j}^{m_j}$. Tällöin on jokaiselle p_{i_h}

$$o(x^{P_{i_h}}) = p_{i_h}^{m_h} \text{ eli } x^{P_{i_h}} \in G_{p_{i_h}}.$$

Selvästikin

$$x^{P_{i_1}} \ ... \ x^{P_{i_k}} \in \langle G_{p_1}, ..., G_{p_j} \rangle \text{ ja } (x^{P_{i_1}} \ ... \ x^{P_{i_j}})^l = 1 \Rightarrow o(x) | \Big(l \cdot \sum_h P_{i_h} \Big),$$

Helposti nähdään, ettei luvuilla $o(x)$ ja $\sum_h P_{i_h}$ ole yhteisiä tekijöitä, joten $o(x)|l$ eli $x^{P_{i_1}} \ ... \ x^{P_{i_k}}$ on ryhmän $\langle x \rangle$ virittäjä. Siispä $x \in \langle G_{p_1}, ..., G_{p_k} \rangle$. Nyt $G = G_{p_1} \times , ..., \ \times G_{p_k}$. □

Abelin ryhmän p-tekijä voidaan edelleen jakaa syklisten aliryhmien suoraksi tuloksi, kuten lause 3.58 osoittaa. Tämä tekijöihin jako ei ole samalla tavalla yksikäsitteinen kuin jako p-tekijöihin, mutta tekijöiden lukumäärä ja kertaluvut ovat invariantteja, kuten nähdään lauseesta 3.59. Nämä tulokset mahdollistavat kaikkien tiettyä kertalukua olevien Abelin ryhmien laskemisen.

3.58. **Lemma.** *Jos G on Abelin ryhmä, jonka kertaluku on p^n jollain $n \in \mathbb{N}$, niin $G = (\mathrm{C}_{p^{k_1}} \times ... \ \times \mathrm{C}_{p^{k_m}})$, missä jokainen $\mathrm{C}_{p^{k_i}}$ on syklinen kertalukua p^{k_i}, $k_i > 0$ ja $\sum_i k_i = n$.*

Todistus. Edetään induktiolla. Jos $n = 0$, tulos on triviaalisti tosi.

Oletetaan, että $n > 0$ ja väite pätee jokaisella $k < n$. Sylowin lauseen mukaan ryhmässä on kertalukua p oleva alkio x. Koska G on Abelin ryhmä on funktio $f : G \to G$, $g \mapsto g^p$ homomorfismi. Kuvaus f ei ole injektio, koska $x \mapsto 1$. Se ei siis myöskään ole surjektio, koska G on äärellinen. Aliryhmä $Gf < G$, joten induktio-oletuksen mukaan on

$$Gf = \mathrm{C}_{p^{k_1}} \times ... \ \times \mathrm{C}_{p^{k_l}} .$$

Valitaan tekijöille $\mathrm{C}_{p^{k_i}}$ virittäjät y_i. Jokaiselle y_i voidaan valita $x_i \in y_i f^{-1}$. Ellei $\langle x_1, ..., x_l \rangle$ ole tekijöiden $\langle x_i \rangle$ suora tulo, on joillain x_{i_1}, ..., x_{i_r} relaatio

$$x_{i_1}^{n_1} \ ... \ x_{i_r}^{n_r} = 1 \text{ missä jokainen } x_{i_j}^{n_j} \neq 1. \tag{2}$$

Jos $p | n_j$ kaikilla j, niin yhtälöstä (2) saadaan

$$y_{i_1}^{n_1/p} \ ... \ y_{i_r}^{n_r/p} = 1, \text{ mistä seuraa } y_{i_j}^{n_j/p} = x_{i_j}^{n_j} = 1 \text{ kaikilla } j.$$

Voidaan siis olettaa, ettei p jaa lukua n_j jollain j. Nyt saadaan korottamalla yhtälö (2) potenssiin p ja järjestelemällä termit

$$y_{i_1}^{n_1} \ldots y_{i_j}^{n_j} \ldots y_{i_r}^{n_r} = 1,$$

jolloin välttämättä $y_{i_j}^{n_j} = 1$. Koska p ei jaa lukua n_j on $y_{k_j} = 1$, mikä on ristiriita. On siis osoitettu, että

$$\langle x_1, \ldots, x_l \rangle = \langle x_1 \rangle \times \ \ldots \ \times \langle x_l \rangle.$$

Olkoon nyt T kaikkien niiden ryhmän G kertalukua p olevien alirymien C_p joukko, joilla

$$\mathrm{C}_p \cap (\langle x_1 \rangle \times \ \ldots \ \times \langle x_l \rangle) = \{1\}$$

ja olkoon $K = \{\mathrm{C}_{p,1}, \ldots, \mathrm{C}_{p,h}\} \subset T$ sellainen maksimaalinen kokoelma näitä aliryhmiä että

$$M = \left\langle \bigcup K \cup (\langle x_1 \rangle \times \ \ldots \ \times \langle x_l \rangle) \right\rangle = \prod K \times \langle x_1 \rangle \times \ \ldots \ \times \langle x_l \rangle.$$

Jos $g \in G \setminus M$, niin $gf \in Gf$ eli

$$gf = y_1^{n_1} \ldots y_l^{m_l} = (x_1^{n_1} \ldots x_l^{m_l})^p = u^p, \text{ missä } u \in M.$$

Nyt on välttämättä $gu^{-1} \in G \setminus M$ (muuten $g \in M$). Pätee, että $(gu^{-1})^p = u^p u^{-p} = 1$, joten suora tulo

$$\langle gu^{-1} \rangle \times \prod K \times \langle x_1 \rangle \times \ \ldots \ \times \langle x_l \rangle$$

on olemassa. Tämä on ristiriidassa kokoelman K maksimaalisuuden kanssa. □

3.59. **Lemma.** *Olkoon p alkuluku. Jos*

$$\begin{aligned} G &= (\mathrm{C}_{p,1} \times \ldots \times \mathrm{C}_{p,i_1}) \times \ \ldots \ \times (\mathrm{C}_{p^n,1} \times \ldots \times \mathrm{C}_{p^n,i_n}) \\ &= (\mathrm{C}_{p,1} \times \ldots \times \mathrm{C}_{p,j_1}) \times \ \ldots \ \times (\mathrm{C}_{p^m,1} \times \ldots \times \mathrm{C}_{p^m,j_m}), \end{aligned}$$

missä $\mathrm{C}_{p^k,i}$ on kertaluvun p^k syklinen ryhmä, niin $m = n$ ja $i_k = j_k$ jokaisella k ($0 \leq k \leq m$).

Todistus. Todistetaan väite induktiolla. Jos

$$G = \mathrm{C}_{p,1} \times \ldots \times \mathrm{C}_{p,i_1} = (\mathrm{C}_{p,1} \times \ldots \times \mathrm{C}_{p,j_1}) \times \ \ldots \ \times (\mathrm{C}_{p^m,1} \times \ldots \times \mathrm{C}_{p^m,j_m}),$$

niin jokainen $g \in G$ on korkeintaan kertalukua p eli $m = 1$. Nyt $|G| = p^{i_1} = p^{j_1}$, mistä seuraa, että $j_1 = i_1$.

Oletetaan, että $n > 1$, $i_n \geq 1$ ja väite pätee kaikilla $l < n$. Nyt

$$G = (\mathrm{C}_{p,1} \times \ldots \times \mathrm{C}_{p,i_1}) \times \ \ldots \ \times (\mathrm{C}_{p^n,1} \times \ldots \times \mathrm{C}_{p^n,i_n}).$$

Oletetaan lisäksi, että

$$G = (\mathrm{C}_{p,1} \times \ldots \times \mathrm{C}_{p,j_1}) \times \ \ldots \ \times (\mathrm{C}_{p^m,1} \times \ldots \times \mathrm{C}_{p^m,j_m}).$$

Koska G on Abelin p-ryhmä (mikä seuraa siitä, että se on syklisten aliryhmien suora tulo), niin

$$o(gh) \leq \max\{o(g), o(h)\} \text{ kaikilla } g, h \in G. \tag{3}$$

Tämän takia ei voi olla sellaista $g \in G$ että $o(g) > p^m$ tai $o(g) > p^n$, joten $m = n$. Olkoot

$$M_i = (\mathrm{C}_{p,1} \times \ldots \times \mathrm{C}_{p,i_1}) \times \ \ldots \ \times (\mathrm{C}_{p^{n-1},1} \times \ldots \times \mathrm{C}_{p^{n-1},i_{n-1}}) \text{ ja } N_i = \mathrm{C}_{p^n,1} \times \ldots \times \mathrm{C}_{p^n,i_n}$$

sekä

$$M_j = (\mathrm{C}_{p,1} \times ... \times \mathrm{C}_{p,j_1}) \times \ ... \ \times (\mathrm{C}_{p^{n-1},1} \times ... \times \mathrm{C}_{p^{n-1},j_{n-1}}) \text{ ja } N_j = \mathrm{C}_{p^n,1} \times ... \times \mathrm{C}_{p^n,j_n}\,.$$

Olkoon kuvaus $\tau : G \to G$ määritelty $g\tau = g^{p^{(n-1)}}$. Selvästikin τ on homomorfismi ryhmältä G itseensä ja selvästikin $M_i, M_j \subset \mathrm{Ker}(\tau)$. Olkoon $y \in N_i$, jolloin alkiolla y on yksikäsitteinen esitys tulona $z_1 \ ... \ z_n$, missä $z_i \in \mathrm{C}_{p^n,i}$. Nyt on $y\tau = (z_1\tau) \ ... \ (z_{i_n}\tau) \neq 1$, joss joku z_i on kertalukua p^n.

Mikäli z ja z' ovat kertalukua p^n ja $z^{p^{(n-1)}} = (z')^{p^{(n-1)}}$, on $z = z'$. Niinpä pätee, että aliryhmän N_i alkioiden $y = z_1 \ ... \ z_{i_n}$ ja $y = z'_1 \ ... \ z'_{i_n}$ kuvat $y\tau$ ja $y'\tau$ ovat samat ryhmässä $G\tau$, joss $o(z_l) < p^n$ ja $o(z'_l) < p^n$ tai $z_l = z'_l$ jokaisella l. Koska jokaisessa aliryhmässä $\mathrm{C}_{p^n,l}$ on $p^n - n$ alkiota, joiden kertaluku on p^n, on ryhmässä $G\tau$ alkioita $(p^n - n + 1)^{i_n}$. Vastaava pätee aliryhmässä N_j, joten $(p^n - n + 1)^{i_n} = (p^n - n + 1)^{j_n}$ eli $i_n = j_n$.

Siirtymällä tekijäryhmiin, huomataan, että

$$M_i \approx G/N_i \approx G/N_j \approx M_j,$$

joten induktio-oletuksen nojalla $i_l = j_l$, kun $1 \leq l < n$. Nyt väite on todistettu. □

Olkoot $H_1, ..., H_n$ syklisiä p-ryhmiä, missä $|H_i| = p^{h_i}$. Jos

$$G = H_1 \times \ ... \ \times H_n,$$

sanotaan, että G on isomorfiatyyppiä $(h_1, ..., h_n)$ tai $G = (h_1, ..., h_n)$. Kun p tunnetaan, tämä määrittelee ryhmän G isomorfiatyypin yksikäsitteisesti.

Kerätään edelliset tulokset yhteen *Abelin ryhmien peruslauseeksi*.

3.60. **Lause.** *Olkoon $\mathcal{P}^*$ kaikkien alkulukujen positiivisten potenssien joukko. Jos G on Abelin ryhmä, niin G voidaan esittää muodossa*

$$G = H_1 \times \ ... \ \times H_m, \text{ missä jokainen } H_i \text{ on syklinen ja } o(H_i) \in \mathcal{P}^* \text{ kaikilla } i.$$

Jos G voidaan myös esittää muodossa

$$G = K_1 \times \ ... \ \times K_n, \text{ missä jokainen } K_i \text{ on syklinen ja } o(K_i) \in \mathcal{P}^* \text{ kaikilla } i,$$

niin $m = n$ ja on olemassa sellainen $\sigma \in \mathrm{S}_m$ että $H_i = K_{i\sigma}$ jokaisella i.

Todistus. Seuraa suoraan lauseista 3.57, 3.58 ja 3.59. □

3.61. **Määritelmä.** Jos $k \in \mathbb{N}\backslash\{0\}$, niin luvun k ositus on jono $(i_1, ..., i_n)$, missä $i_j \in \mathbb{N}\backslash\{0\}$, $i_l < i_m \Rightarrow l < m$ ja $\sum_j i_j = k$. Merkinnällä $i(k)$ tarkoitetaan luvun k ositusten lukumäärää.

3.62. **Korollaari.** *Olkoon $n = p_1^{m_1} \cdot \ ... \ \cdot p_n^{m_n}$, missä $p_i < p_j$, joss $i < j$. Kertalukua n olevien Abelin ryhmien lukumäärä on*

$$\prod_j i(m_j).$$

Todistus. Lauseesta 3.60 seuraa, että jokainen Abelin ryhmä kertalukua n on isomorfinen jonkin ryhmän

$$G = \mathrm{C}_{p_1^{k_{1,p_1}}} \times ... \times \mathrm{C}_{p_1^{k_{u,p_1}}} \times ... \ \mathrm{C}_{p_n^{k_{1,p_n}}} \times ... \times \mathrm{C}_{p_n^{k_{u',p_n}}}$$

kanssa, missä $(k_{1,p_i}, ..., k_{u,p_i})$ luvun m_i ositus jokaisella i, missä $0 < i \leq n$. Siitä seuraa myös, että ryhmä

$$H = \mathrm{C}_{p_1^{l_{1,p_1}}} \times ... \times \mathrm{C}_{p_1^{l_{v,p_1}}} \times ... \ \mathrm{C}_{p_n^{l_{1,p_n}}} \times ... \times \mathrm{C}_{p_n^{l_{v',p_n}}},$$

missä $(l_{1,p_i}, ..., l_{v,p_i})$ on luvun m_i ositus jokaisella i, missä $0 < i \leq n$, on isomorfinen ryhmän G kanssa joss, ositukset ovat jokaisella m_i samat.

Näin siis on $\prod_j i(m_j)$ kappaletta Abelin ryhmiä kertalukua n. □

3.8. p-ryhmien maksimaaliset Abelin aliryhmät

Olkoot G äärellinen p-ryhmä, $g \in G$ ja A ryhmän G maksimaalinen normaali Abelin aliryhmä. Sivuluokkaa gA vastaa ryhmän G/A konjugointitoiminnassa jokin ryhmän A automorfismi, jonka kertaluku on alkuluvun p potenssi. Tämä johtuu tietenkin siitä, että ryhmä G/A on p-ryhmä lemman 3.42 nojalla. Ryhmän A kertalukua p^n, jollain $n \in \mathbb{N}$, olevia automorfismeja kutsutaan *p-automorfismeiksi*.

Esimerkki 3.39 osoitti, että on olemassa kertalukua $n!$ olevia ryhmiä, joissa ei ole kertalukua n suurempia Abelin aliryhmiä. p-ryhmien tapauksessa tilanne ei ole ihan näin huono. Tämä johtuu siitä, ettei luku $(p^n - 1)!$ ole luvun p potenssi (ellei $n = 0$), joten $\mathrm{S}_{p^k-1} \not\approx G/A$. Tässä esitellään W. Burnsiden keksimä tapa hyödyntää tätä rajoitetta. Hän arvioi p-ryhmän maksimaalisen normaalin Abelin aliryhmän kertalukua alhaalta [4].

Olkoon G äärellinen p-ryhmä, joka ei ole Abelin ryhmä, ja A sen maksimaalinen normaali Abelin aliryhmä. Koska myöskin $\mathrm{Z}(G)A$ on ryhmän G maksimaalinen normaali Abelin aliryhmä, on $\mathrm{Z}(G) \subset A$.

Lemman 3.38 nojalla vastaa jokaista ryhmän G/A alkiota eri ryhmän $\mathrm{Aut}(A)$ alkio, koska p-ryhmät ovat nilpotentteja ryhmiä. Lisäksi jokaista sivuluokkaa gA vastaava ryhmän A automorfismi kiinnittää joukon $\mathrm{Z}(G)$ pisteittäin, sillä $z^g = z$ aina kun $z \in \mathrm{Z}(G)$ ja $g \in G$.

Selvitetään ensin yläraja sille, kuinka suuria ryhmän $\mathrm{Aut}(A)$ p-aliryhmiä voi olla, jotka kiinnittävät pisteittäin aliryhmän $\mathrm{Z}(G)$. Tätä varten tarvitaan seuraava lause.

3.63. **Lause.** *(Hilton) Olkoon G Abelin p-ryhmä kertalukua p^n. Ryhmän* $\mathrm{Aut}(G)$ *Sylowin p-aliryhmien kertaluku on luvun $p^{n(n-1)/2}$ tekijä.*

Todistus. Tämä seuraa suoraan lauseesta 3.55, kun huomataan, että Frattinin ryhmän indeksi on korkeintaan p^n. □

Olkoot nyt $|\mathrm{Z}(G)| = p^c$ ja $|A| = p^k$. Koska A on Abelin aliryhmä, on myöskin $A/\mathrm{Z}(G)$ kertalukua p^{k-c} Abelin ryhmä. Olkoon K sellainen ryhmän A p-automorfismien ryhmä, että K kiinnittää aliryhmän $\mathrm{Z}(G)$ pisteittäin.

Jos $f \in K$ sekä $x, y \in G$, niin $xf = yf$, mikäli x ja y kuuluvat samaan keskuksen $\mathrm{Z}(G)$ sivuluokkaan. Niinpä ryhmä K toimii ryhmässä $A/\mathrm{Z}(G)$. Olkoon K_1 tämän toiminnan ydin. Koska jokainen ryhmän K/K_1 alkio vastaa yksikäsitteistä Abelin ryhmän $A/\mathrm{Z}(G)$ automorfismia, jakaa lemman 3.63 nojalla $|K/K_1|$ luvun $p^{(k-c)(k-c-1)/2}$.

Jokainen ryhmän K_1 alkioista määräytyy yksikäsitteisesti, kun tiedetään ryhmän A jonkin virittäjistön alkioiden kuvat. Ryhmän $A/\mathrm{Z}(G)$ pienintä mahdollista kertalukua olevassa virittäjistössä on korkeintaan $k - c$ alkiota, kuten voidaan nähdä Abelin ryhmien

rakennelauseesta. Olkoon

$$X = \{ x_1 \mathrm{Z}(G), ..., x_{k-c} \mathrm{Z}(G) \}$$

jokin ryhmän $A/\mathrm{Z}(G)$ virittäjistö. Tällöin on $\{x_1, ..., x_{k-c}\} \cup \mathrm{Z}(G)$ ryhmän A virittäjistö.

Jokainen ryhmän K_1 kuvaus kiinnittää jokaisen aliryhmän $\mathrm{Z}(G)$ sivuluokan, joten virittäjän mahdollisia kuvia on korkeintaan $|\mathrm{Z}(G)| = p^c$. Jokainen ryhmän K_1 kuvaus kiinnittää jokaisen keskuksen $\mathrm{Z}(G)$ alkion, joten ryhmän K_1 kuvaus määräytyy yksikäsitteisesti, kun tiedetään alkioiden $x_1, ..., x_{k-c}$ kuvat, siispä $|K_1| \leq p^{(k-c)c}$. Näin siis $|K| \leq p^{(k-c)(k+c-1)/2}$.

Saadaan siis, että $|G/A| \leq p^{(k-c)(k+c-1)/2}$, missä p^c on ryhmän G keskuksen kertaluku ja p^k on ryhmän A kertaluku. Olkoon $|G| = p^n$, jolloin

$$p^{n-k} \leq p^{(k-c)(k+c-1)/2} \Rightarrow n - k \leq (k-c)(k+c-1)/2.$$

Ratkaisemalla syntynyt toisen asteen epäyhtälö luvun k suhteen, saadaan että

$$k \geq (2\sqrt{2n + c^2 - c + 1/4} - 1)/2.$$

3.9. Nilpotenttien ryhmien maksimaaliset Abelin aliryhmät

Nilpotenttien ryhmien maksimaaliset Abelin aliryhmät ovat niiden Sylowin aliryhmien maksimaalisten Abelin aliryhmien suoria tuloja, kuten alla osoitetaan.

3.64. **Lemma.** *Olkoon $G = H_1 \times ... \times H_n$. Olkoot ryhmillä $H_1, ..., H_n$ maksimaaliset Abelin aliryhmät $A_1, ..., A_n$. Tällöin on ryhmällä G maksimaalinen Abelin aliryhmä $A_1 \times ... \times A_n$.*

Todistus. Aliryhmä $A_1 \times ... \times A_n$ on selvästikin ryhmän G Abelin aliryhmä. Jos $x = (h_1, ..., h_n) \in G$, ja $(a_1, ..., a_n) \in A_1 \times ... \times A_n$, niin

$$(a_1, ..., a_n)^x = (a_1^{h_1}, ..., a_n^{h_n}) = (a_1, ..., a_n),$$

joss $h_i \in \mathrm{C}(a_i)$ jokaisella i. Siispä $x \in \mathrm{C}(A_1 \times ... \times A_n)$, joss $x \in A_1 \times ... \times A_n$ eli $A_1 \times ... \times A_n$ on ryhmän G maksimaalinen Abelin aliryhmä. □

3.65. **Lemma.** *Olkoon G nilpotentti ryhmä ja olkoon P sen Sylowin p-aliryhmä. Tällöin $P \lhd G$.*

Todistus. Selvästikin $P \leq \mathrm{N}(P) \leq \mathrm{N}(\mathrm{N}(P))$. Lemman 3.33 nojalla yhtäsuuruus $\mathrm{N}(P) = \mathrm{N}(\mathrm{N}(P))$ pätee, joss $P \lhd G$. Koska $P \lhd G$ ja Sylowin lauseen nojalla kaikki ryhmän $\mathrm{N}(P)$ Sylowin p-aliryhmät ovat konjugaatteja, on P ryhmän $\mathrm{N}(P)$ ainoa Sylowin p-aliryhmä. Tästä seuraa, että jokainen ryhmän $\mathrm{N}(P)$ automorfismi kiinnittää aliryhmän P, joten jokaisella $x \in \mathrm{N}(\mathrm{N}(P))$ on $P^x = P$ eli $P \lhd \mathrm{N}(\mathrm{N}(P))$, siispä $\mathrm{N}(P) = \mathrm{N}(\mathrm{N}(P))$ ja $P \lhd G$. □

3.66. **Lause.** *Nilpotentti ryhmä G on Sylowin aliryhmiensä suora tulo.*

Todistus. Lemman 3.65 nojalla on jokainen ryhmä G Sylowin aliryhmä normaali. Selvästikin kahden eri alkuluvun Sylowin aliryhmän leikkaus on triviaali.

Olkoon $|G| = p_1^{n_1} ... p_k^{n_k}$ ja olkoon jokaista p_i vastaava ryhmän G Sylowin aliryhmä P_i. Olkoon $x \in G$ ja olkoon $M_i = |G|/p_1^{n_i}$ jokaisella i. Koska $x^{|G|} = 1$, on $o(x^{M_i})|p_i^{n_i}$. Koska

P_i on normaali ja ryhmän G/P_i kertaluku ei selvästikään voi olla jaollinen luvulla p_i on $x^{M_i} \in P_i$. Nyt siis alkio

$$y = x^{M_1 + \ldots + M_k} \in P_1 \times \ldots \times P_k.$$

Nähdään helposti, että $p_i | h \cdot (M_1 \ldots M_k)$, joss $p_i | h$ eli $o(x) = o(y)$, joten $x = y^j$ jollain $j \in \mathbb{N}$, siispä $x \in P_1 \times \ldots \times P_k$. □

Lauseella 3.66 yhdistettynä lauseeseen 3.64 on monia helppoja korollaareja, joista muutamia luetellaan tässä:

- Nilpotentti ryhmä G, jonka kertaluku ei ole jaollinen yhdenkään alkuluvun kuutiolla on Abelin ryhmä. (Jos $|G|$ ei ole jaollinen yhdenkään alkuluvun kuutiolla, on jokainen sen Sylowin p-aliryhmistä Abelin aliryhmä.)
- Diedriryhmä D_{2n} on nilpotentti, joss n on luvun 2 potenssi. (Jos n on luvun 2 potenssi on D_{2n} 2-ryhmä, siis nilpotentti. Jos taas n on jaollinen jollain $p > 2$ ja oletetaan, että D_{2n} on nilpotentti, on ryhmän D_{2n} Sylowin p-ryhmä sen keskuksessa, mikä on mahdotonta, koska $|\mathrm{Z}(\mathrm{D}_{2n})|$ on joko 1 tai 2.)
- Jokainen nilpotentin ryhmän maksimaalinen Abelin aliryhmä on sen Sylowin p-aliryhmien maksimaalisten Abelin aliryhmien suora tulo. (Tämä seuraa suoraan yllä olevista lauseista.)

Kolmas korollaari on parantaa monissa tapauksissa huomattavasti aiemmin saatua arviota nilpotentin ryhmän maksimaalisille Abelin aliryhmille.

3.67. **Esimerkki.** Olkoon G nilpotentti ryhmä, jonka kertaluku on $6! = 5 \cdot 3^2 \cdot 2^4$. Lause 3.40 takaa, että ryhmässä G on Abelin aliryhmä, jonka kertaluku on vähintään 7. Edellisen luvun nojalla ryhmän G Sylowin 2-aliryhmällä on Abelin aliryhmä, jonka koko on vähintään $2^{(2\sqrt{8+1/4}-1)/2} > 2^2$. Sen Sylowin 5- ja 3-aliryhmät ovat Abelin ryhmiä, joten ryhmällä G on Abelin aliryhmä, jonka kertaluku on vähintään $2^2 \cdot 3^2 \cdot 5 = 180$, mikä on melko huomattava parannus edelliseen arvioon nähden.

4. Vaihdannaisuusverkon määritelmä sekä sen ominaisuuksia

4.1. Verkoista

Käsitteellä *verkko* tarkoitetaan tässä tutkielmassa paria $\mathcal{W} = (V, E)$, jossa V on joukko ja E on tämän joukon symmetrinen ja refleksiivinen relaatio. Tässä poiketaan yleisestä käytännöstä määritellä verkot irrefleksiivisiksi. Joukon V alkioita nimitetään verkon *solmuiksi* ja relaation E alkioita verkon *kaariksi*.

Kaksi verkkoa $\mathcal{W} = (V, E)$ ja $\mathcal{M}' = (V', E')$ ovat isomorfiset, joss on olemassa sellainen bijektio $f : V \to V'$ että kaikille $v, w \in V$ pätee

$$f(v)E'f(w) \Leftrightarrow vEw.$$

Verkko $\mathcal{W} = (V, E)$ voidaan *upottaa* verkkoon $\mathcal{W}' = (V', E')$, joss on olemassa sellainen injektio $i : V \to V'$ että kaikille $v, w \in V$ pätee.

$$viE'wi \Leftrightarrow vEw.$$

Funktiota i sanotaan upotukseksi.

4.1. **Lemma.** *Jos verkko $\mathcal{W} = (V, E)$ voidaan upottaa verkkoon $\mathcal{W}' = (V', E')$ ja $\mathcal{W}'$ voidaan upottaa verkkoon $\mathcal{W}'' = (V'', E'')$, niin $\mathcal{W}$ voidaan upottaa verkkoon $\mathcal{W}''$*

Todistus. On olemassa upotukset $i_1 : V \to V'$ ja $i_2 : V' \to V''$. Kompositio $i_1 i_2 : V \to V''$ on injektio ja koska

$$xEy \Leftrightarrow xi_1E'xi_1 \Leftrightarrow (xi_1)i_2E''(yi_1)i_2 \Leftrightarrow x(i_1i_2)E''y(i_1i_2),$$

on se upotus. □

Verkon $\mathcal{W} = (V, E)$ solmujen joukon osajoukkoa W, jossa kaikille $x, y \in W$ pätee xEy kutsutaan *klikiksi*. Klikki W on *maksimaalinen klikki*, joss

$$\text{jokaiselle } v \in V \setminus W \text{ on sellainen } x \in W \text{ että } \neg(vEx).$$

Verkon *suurimmilla klikeillä* tarkoitetaan maksimaalisia klikkejä, joiden alkioiden lukumäärä on suurin mahdollinen.

Verkon $\mathcal{W} = (V, E)$ solmun x naapurustolla tarkoitetaan joukkoa

$$\mathcal{W}_x = \{y \in V \mid xEy\}.$$

4.2. **Propositio.** *Verkon $\mathcal{W} = (V, E)$ maksimaalinen klikki on solmujensa naapurustojen leikkaus.*

Todistus. Olkoon W verkon (V, E) maksimaalinen klikki. Koska kaikille $x, y \in W$ pätee, että xEy, niin jokaisella $x \in W$ on $W \subset \mathcal{W}_x$. Siispä

$$W \subset \bigcap_{x \in W} \mathcal{W}_x .$$

Toisaalta jokaiselle $v \in V \setminus W$ on sellainen $x \in W$ että $\neg(vEx)$ eli $v \notin \mathcal{W}_x$. Tämän takia

$$\bigcap_{x \in W} \mathcal{W}_x \subset W$$

joten väite seuraa. □

Olkoon $\mathcal{W} = (V, E)$ sellainen verkko, että sen solmujen joukko voidaan osittaa osiin $F_1, ..., F_n$ siten, että kaikilla F_i ja F_j pätee

Jos on sellaiset $x \in F_i$ ja $y \in F_j$, että xEy, niin kaikilla $s \in F_i$ ja $t \in F_j$ on sEt.

Tällöin voidaan muodostaa *tekijäverkko* $\mathcal{W}' = (V', E')$, missä

$$V' = \{F_1, ..., F_n\} \text{ ja } E' = \{(F_i, F_j) \mid \text{on sellaiset } x \in F_i \text{ ja } y \in F_j \text{ että } xEy\}.$$

4.2. Vaihdannaisuusverkot

Ryhmän $(G, \circ)$ *vaihdannaisuusverkko* on verkko $\mathcal{W}^G = (G, \mathrm{C}_G)$, missä

$$\mathrm{C}_G = \{(x, y) \in G^2 \mid [x, y] = 1\}.$$

Kun puhutaan ryhmän G vaihdannaisuusverkkosta, tarkoitetaan yllä olevaa verkkoa, missä solmujen joukko on ryhmän G alkioiden joukko. Ryhmän *vaihdannaisuusosamäärä* on luku $|\mathrm{C}_G|/|G|^2$.

4.3. **Esimerkki.** Jokaisen n-alkioisen Abelin ryhmän vaihdannaisuusverkko on n-klikki, koska kaikki alkiot ovat pareittain vaihdannaisia. Kun n ei ole neliötön (eli n on jaollinen jonkin alkuluvun neliöllä), on Abelin ryhmien rakennelauseen nojalla olemassa useampi kuin yksi Abelin ryhmä kertalukua n. Tämä on yksinkertaisin esimerkki siitä, että ryhmillä voi olla isomorfiset vaihdannaisuusverkot, vaikka ryhmät eivät olisikaan isomorfisia.

4.4. **Esimerkki.** Ryhmän S_3 alkiot ovat 1, transpositiot (1 2), (1 3) sekä (2 3) ja kolmisyklit (1 2 3) sekä (1 3 2).

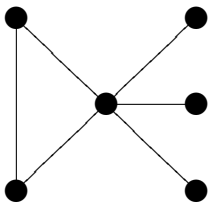
Neutraalialkio 1 on vaihdannainen ryhmän kaikkien alkioiden kanssa.

Kolmisyklit ovat keskenään vaihdannaisia, koska ne kuuluvat samaan kolmialkioiseen sykliseen aliryhmään $\langle(1\ 2\ 3)\rangle$. Koska

$$(1\ 2\ 3)(1\ 2) = (2\ 3) \neq (1\ 3) = (1\ 2)(1\ 2\ 3),$$

niin aliryhmä $\langle(1\ 2\ 3)\rangle$ on Lagrangen lauseen nojalla oma keskittäjänsä eli kumpikaan kolmisykleistä ei ole yhdenkään ryhmän S_3 transposition kanssa vaihdannainen.

Lopuksi eri transpositiot ovat vaihdannaisia, joss ne ovat erillisiä. Kolmialkioisen joukon transpositiot eivät koskaan ole erillisiä, joten ne eivät ole keskenään vaihdannaisia. Saadaan alla oleva vaihdannaisuusverkko. Siihen ei ole piirretty muotoa xEx olevia kaaria.

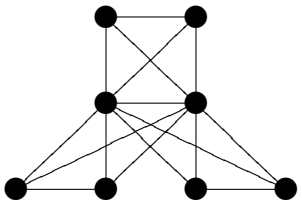


4.5. **Esimerkki.** Olkoon G ryhmä, jonka keskuksen indeksi on p^2 jollakin alkuluvulla p. Ryhmän alkiot voidaan jakaa keskuksen alkioihin, joita on $|\mathrm{Z}(G)|$ kappaletta ja muihin alkioihin, joita on $|G| - |\mathrm{Z}(G)| = (p^2 - 1)|\mathrm{Z}(G)|$ kappaletta. Jos $z \in \mathrm{Z}(G)$, niin $\mathrm{C}(z) = G$, jos taas $x \in G \setminus \mathrm{Z}(G)$, niin $\{x\} \cup \mathrm{Z}(G) \subset \mathrm{C}(x)$. Koska $\mathrm{Z}(G)$ on keskittäjän $\mathrm{C}(x) \neq G$ aito aliryhmä, on $[G : C(x)] = p$ lemman 3.11 ja Lagrangen lauseen nojalla. Lisäksi $\mathrm{C}(x) = \langle x,\ \mathrm{Z}(G)\rangle$, koska $|\langle x,\ \mathrm{Z}(G)\rangle| = |\mathrm{C}(x)|$.

Olkoot $x, y \in G \setminus \mathrm{Z}(G)$ ja $[x, y] = 1$, jolloin $\langle x,\ \mathrm{Z}(G)\rangle = \mathrm{C}(x) \subset \mathrm{C}(y)$. Koska $|\mathrm{C}(x)| = |\mathrm{C}(y)|$, niin $\mathrm{C}(x) = \mathrm{C}(y)$.

Olkoot $x, y \in G \setminus \mathrm{Z}(G)$ ja $[x, y] \neq 1$, jolloin $\mathrm{C}(x) \neq \mathrm{C}(y)$. Koska $\mathrm{Z}(G) \subset \mathrm{C}(x)$, $\mathrm{Z}(G) \subset \mathrm{C}(y)$ ja $[\mathrm{C}(x) : \mathrm{Z}(G)] = [\mathrm{C}(y) : \mathrm{Z}(G)] = p$, niin lemman 3.11 nojalla on $\mathrm{C}(x) \cap \mathrm{C}(y) = \mathrm{Z}(G)$.

Vaihdannaisuusverkon rakenne tunnetaan nyt täysin. Esimerkkinä on alla oleva ryhmien D_8 ja $\mathbb{H}$ vaihdannaisuusverkko (tyyppiä xEx olevat kaaret on taaskin jätetty pois). Samaa kertalukua olevilla ryhmillä voi siis olla isomorfiset vaihdannaisuusverkot, vaikka ryhmät eivät olisikaan Abelin ryhmiä.



Alkion $x \in G$ naapurusto verkossa $\mathcal{W}^G$ on kaikkien niiden alkioiden $y \in G$ joukko joilla

$$[x, y] = 1 \text{ eli } y \in \mathrm{C}_x\,.$$

Tästä seuraa, että jokaisella alkiolla $x \in G$ on $\mathcal{W}^G_x = \mathrm{C}(x)$. Erityisesti jokaisella $x \in G$ pätee $|\mathcal{W}^G_x| \;\big|\; |G|$ Lagrangen lauseen nojalla.

4.6. **Lemma.** *Indeksi* $[G : \mathrm{Z}(G)]$ *ei koskaan ole alkuluku.*

Todistus. Olkoon $x \notin \mathrm{Z}(G)$ ja $[G : \mathrm{Z}(G)]$ alkuluku, jolloin $\{x\} \cup \mathrm{Z}(G) \subset \mathrm{C}(x)$ eli $[G : \mathrm{C}(G)] \;\big|\; [G : \mathrm{Z}(x)]$ ja $[G : \mathrm{C}(x)] \neq [G : \mathrm{Z}(G)]$, jolloin $[G : \mathrm{C}(x)] = 1$ eli $x \in \mathrm{Z}(G)$, mikä on ristiriita. □

Koska $\mathrm{C}(x^y) = \mathrm{C}(x)^y$, niin konjugaattien naapurustot vaihdannaisuusverkoissa ovat saman kokoiset.

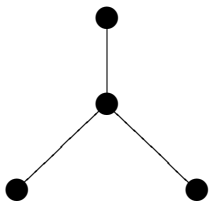
4.7. **Lause.** *Ryhmän vaihdannaisuusverkon maksimaaliset klikit ovat ryhmän maksimaalisia Abelin aliryhmiä.*

Todistus. Ryhmän maksimaaliset Abelin aliryhmät ovat alkioidensa keskittäjien leikkauksia, joten väite seuraa suoraan lemmasta 4.2. □

Olkoon G ryhmä, $x, y \in G$ ja $z \in \mathrm{Z}(G)$, jolloin

$$[x, y] = x^{-1}y^{-1}xy = z^{-1}zx^{-1}y^{-1}xy = (z^{-1}x^{-1})y^{-1}(xz)y = [xz, y] = [x, yz]$$

eli x ja y ovat vaihdannaisia, joss $x\,\mathrm{Z}(G)$ ja $y\,\mathrm{Z}(G)$ ovat pisteittäin vaihdannaisia eli voidaan muodostaa vaihdannaisuusverkon tekijäverkko, jonka solmut ovat ryhmän keskuksen sivuluokat, siis *keskuksen sivuluokkien vaihdannaisuusverkko* eli $\mathcal{W}^{\{G/\,\mathrm{Z}\}}$. Esimerkkinä tästä ryhmän D_8 keskuksen sivuluokkien vaihdannaisuusverkko. Tähän liittyy kanoninen surjektio ryhmän vaihdannaisuusverkolta sen keskuksen sivuluokkien vaihdannaisuusverkolle $x \mapsto x\,\mathrm{Z}(G)$.



On tärkeää olla sekoittamatta tätä verkkoa ryhmän $G/\,\mathrm{Z}(G)$ vaihdannaisuusverkkoon $\mathcal{W}^{G/\,\mathrm{Z}(G)}$, koska nämä eivät tyypillisesti ole isomorfisia. Esimerkiksi ryhmän $\mathrm{D}_8\,/\,\mathrm{Z}(D_8)$ vaihdannaisuusverkko on neliklikki.

Verkossa $\mathcal{W}^{\{G/\,\mathrm{Z}\}}$ on kaari solmujen välillä, mikäli solmut, siis keskuksen sivuluokat, ovat pisteittäin vaihdannaisia. Tämä voidaan ilmaista toisin, nimittäin jos $x\,\mathrm{Z}(G)$ ja $y\,\mathrm{Z}(G)$ ovat keskuksen sivuluokkia, on niiden väillä kaari, mikäli $y\,\mathrm{Z}(G) \subset \mathrm{C}(x)$ eli $[x, y] = 1$. Verkossa $\mathcal{W}^{G/\,\mathrm{Z}(G)}$ taas riittää että $[x, y] \in \mathrm{Z}(G)$. Tästä tietenkin seuraa, että jos solmujen välillä on kaari verkossa $\mathcal{W}^{\{G/\,\mathrm{Z}\}}$, on niiden välillä kaari myös verkossa $\mathcal{W}^{G/\,\mathrm{Z}(G)}$.

Olkoon G äärellinen ryhmä ja $A \leq G$ maksimaalinen Abelin aliryhmä. Jos $x \in G$ ja $[x, a] = 1$ kaikilla $a \in A$, niin $x \in A$, koska A on maksimaalinen klikki. Siispä jokaisen verkon $\mathcal{W}^{\{G/Z\}}$ maksimaalisen klikin kuva keskuksen sivuluokkien vaihdannaisuusverkossa on maksimaalinen klikki. Näin ei kuitenkaan aina ole verkossa $\mathcal{W}^{G/\,\mathrm{Z}(G)}$, mistä taaskin esimerkkinä D_8.

Jos $x \notin \mathrm{Z}(G)$, niin on sellainen $y \in G$ että $[x, y] \neq 1$ eli $x\,\mathrm{Z}(G)$ ja $y\,\mathrm{Z}(G)$ eivät ole pisteittäin vaihdannaiset, siis jokaiselle keskuksen sivuluokalle on jokin sellainen $y\,\mathrm{Z}(G)$ että sivuluokkien välillä ei ole kaarta keskuksen sivuluokkien vaihdannaisuusverkossa.

4.8. **Lemma.** *Olkoon G ryhmä, joka ei ole vaihdannainen. Tällöin $[G : \mathrm{Z}(G)] \geq 4$.*

Todistus. Tämä seuraa lemmasta 4.6, koska pienin luonnollinen luku, joka ei ole 1 tai alkuluku on 4. □

Etsitään nyt yläraja ryhmän vaihdannaisuusosamäärälle, kun ryhmä ei ole Abelin ryhmä. Olkoon G ryhmä, joka ei ole Abelin ryhmä ja $\omega = \sum_{x\in G} |\mathrm{C}(x)|/|G|^2$ ryhmän G vaihdannaisuusosamäärä [7]. Nyt

$$\begin{aligned}
\omega &= |\{(x,y) \in G^2 \mid [x,y] = 1\}|/|G|^2 \\
&= (|\{(x,y) \in G^2 \mid x \in \mathrm{Z}(G)\}| + |\{(x,y) \in G^2 \mid x \notin \mathrm{Z}(G),\, [x,y] = 1\}|)/|G|^2 \\
&= (|\mathrm{Z}(G)| \cdot |G| + \sum_{x\notin \mathrm{Z}(G)} |\mathrm{C}(x)|)/|G|^2 \\
&\leq (|\mathrm{Z}(G)| \cdot |G| + (|G| - |\mathrm{Z}(G)|)(\frac{1}{2}|G|)/|G|^2 \\
&= (|\mathrm{Z}(G)| + \frac{1}{2}(|G| - |\mathrm{Z}(G)|))/|G|.
\end{aligned}$$

Olkoon $t = |\mathrm{Z}(G)|/|G| > 0$. Lemmasta 4.8 seuraa, että $t \leq \frac{1}{4}$. Koska $t \mapsto t + \frac{1}{2} - \frac{1}{2}t)$ on kasvava funktio on

$$\omega \leq t + \frac{1}{2}(1-t) \leq \frac{1}{4} + \frac{1}{2} \cdot \frac{3}{4} = \frac{5}{8}.$$

Kuten tarkastelemalla ryhmän D_8 vaihdannaisuusverkkoa on helppo huomata, tämä raja myös saavutetaan.

4.9. **Propositio.** *Jokaisen n-solmuisen verkon voi upottaa ryhmän S_{3n} vaihdannaisuusverkkoon.*

Todistus. Olkoon $\mathcal{W} = (\{x_1, ..., x_n\}, E)$ verkko. Olkoon $N = \{1, ..., n\}$. Määritellään jokaisella $i \in N$ transpositiot

$$s_i = \Big((3(i-1)+1)\ \ (3(i-1)+2)\Big) \text{ ja } t_i = \Big((3(i-1)+1)\ \ (3(i-1)+3)\Big).$$

Jos $i \neq j$, niin

$$[s_i, s_j] = [t_i, t_j] = [s_i, t_j] = 1,$$

koska nämä transpositiot ovat erillisiä. Huomataan, että

$$\begin{aligned}
(4) \qquad s_i t_i &= \Big((3(i-1)+1)\ \ (3(i-1)+2)\ \ (3(i-1)+3)\Big) \\
&\neq \Big((3(i-1)+1)\ \ (3(i-1)+3)\ \ (3(i-1)+2)\Big) = t_i s_i
\end{aligned}$$

Määritellään sitten jokaiselle verkon $\mathcal{W}$ solmulle permutaatio

$$\tau_i = s_i \prod_{j\in N\setminus\{i\}} r_{i,j},$$

missä

$$r_{i,j} = \begin{cases} I, & \text{jos } x_i E x_j \\ t_j, & \text{muuten.} \end{cases}$$

Huomataan, että τ_i on tällä tavalla esitetty erillisten transpositioiden tulona.

Oletetaan, että x_i ja x_j ovat verkon $\mathcal{W}$ solmuja.

Olkoon $x_i E x_j$, jolloin

$$\tau_i = s_i r_{i,1} \ldots r_{i,j-1} r_{i,j+1} \ldots r_{i,n} \text{ ja } \tau_j = s_j r_{j,1} \ldots r_{j,i-1} r_{j,i+1} \ldots r_{j,n}.$$

Kuten ei-vastaavuudesta 4 ja permutaatioiden r_k määritelmästä nähdään on $[\tau_i, \tau_j] = 1$.

Olkoon $\neg x_i E x_j$, jolloin

$$\tau_i = s_i r_1 \ldots r_j \ldots r_n \text{ ja } \tau_j = s_j r_1 \ldots r_i \ldots r_n.$$

Koska transpositiot tässä esityksessä ovat erillisiä, niin voidaan helposti laskea

$$\begin{aligned} [3(i-1)+1]\tau_i\tau_j &= [3(i-1)+1]s_i t_i = [3(i-1)+2] \\ &\neq [3(i-1)+3] = [3(i-1)+1]t_i s_i = [3(i-1)+1]\tau_j\tau_i \end{aligned}$$

$\Rightarrow [\tau_i, \tau_j] \neq 1$. Siispä on osoitettu, että $x_i E x_j$, joss $[\tau_i, \tau_j] = 1$. Koska $x_i \mapsto \tau_i$ on selvästikin injektio, on se upotus. □

4.3. Vaihdannaisuusverkon maksimaaliset klikit

Alaluvuissa 3.8 ja 3.9 tutkittiin p-ryhmien ja nilpotenttien ryhmien maksimaalisia Abelin aliryhmiä. Saatiin selville, että näiden koon alaraja on ryhmän kertaluvun kasvava funktio. Tämän luvun tarkoituksena on osoittaa, että jokaisessa tarpeeksi suuren ryhmän vaihdannaisuusverkossa on tarpeeksi suuria klikkejä. Täsmällisemmin tämä tarkoittaa, että jokaiselle $n \in \mathbb{N}$ on olemassa sellainen $M_n \in \mathbb{N}$ että jokaisen kertalukua M_n suuremman ryhmän G vaihdannaisuusverkossa on klikkejä, joiden koko on suurempi kuin n.

Olkoon jokaisella $n \in \mathbb{N}$ joukko X_n niiden ryhmien joukko, joiden jokainen maksimaalinen Abelin aliryhmä on korkeintaan kertalukua $n-1$. Jos jollekin n voidaan osoittaa, että X_n on äärellinen, on olemassa yläraja joukon X_n ryhmien kertaluvuille, siis sellainen luku M_n, että jokaisessa kertalukua M_n suuremmassa ryhmässä on n-klikki. Mikäli tämä voidaan osoittaa jokaiselle $n \in \mathbb{N}$, on luvun väite todistettu.

4.10. **Määritelmä.** Olkoon $\omega_{p,n}$, missä p on alkuluku ja $n \in \mathbb{N}$, niiden ryhmien kertalukujen joukko, jotka

(1) eivät ole jaollisia yhdelläkään lukua p suuremmalla alkuluvulla.
(2) eivät ole jaollisia yhdenkään alkuluvun q potenssilla q^m ($m \in \mathbb{N}$), missä $m > n$.

Joukko $\omega_{p,n}$ on äärellinen jokaisella alkuluvulla p ja luonnollisella luvulla n. Tämä seuraa siitä, että jokainen $u \in \omega_{p,n}$ jakaa luvun $(q_1 \cdot \ldots \cdot q_k \cdot p)^n$, missä $\{q_1, \ldots, q_k\}$ on alkulukua p pienempien alkulukujen joukko. Siispä se on ylhäältä rajoitettu joukon $\mathbb{N}$ osajoukko eli äärellinen.

Luvun 3.8 nojalla tiedetään, että p-ryhmässä, jonka kertaluku on p^k ($k \in \mathbb{N}$) on maksimaalisten Abelin aliryhmien koolla alaraja. Tämä on luku p^h, missä

$$h = \frac{2\sqrt{2k + 1/4} - 1}{2}.$$

4.11. **Lemma.** *Funktio $f : \mathbb{N} \to \mathbb{R}$, missä*

$$k \mapsto \frac{2\sqrt{2k + 1/4} - 1}{2} \text{ jokaisella } k \in \mathbb{N}$$

ei ole ylhäältä rajoitettu.

Todistus. Olkoon $R \in \mathbb{R}$ ja $R > 0$. Valitaan sellainen $N \in \mathbb{N}$, että $N > (R+1)^2$, jolloin

$$\frac{2\sqrt{2N+1/4}-1}{2} > \frac{2\sqrt{2(R+1)^2+1/4}-1}{2} > \frac{2(R+1)-1}{2} > \frac{2R}{2} = R$$

eli väite seuraa. □

4.12. **Lause.** *Olkoon $n \in \mathbb{N}$. On olemassa sellainen $M_n \in \mathbb{N}$ että ryhmässä G on Abelin aliryhmä, jonka kertaluku on vähintään n, kunhan $|G| > M_n$.*

Todistus. Olkoon q alkuluku, joka on suurempi kuin n. Mikäli ryhmän kertaluku on jaollinen alkuluvulla q, on siinä Sylowin lauseen mukaan kertalukua q oleva syklinen aliryhmä, joten siinä on vähintään kertalukua n oleva Abelin aliryhmä.

Voidaan löytää sellainen $k \in \mathbb{N}$, että

$$f_k = \frac{2\sqrt{2k+1/4}-1}{2} > \log_2(n),$$

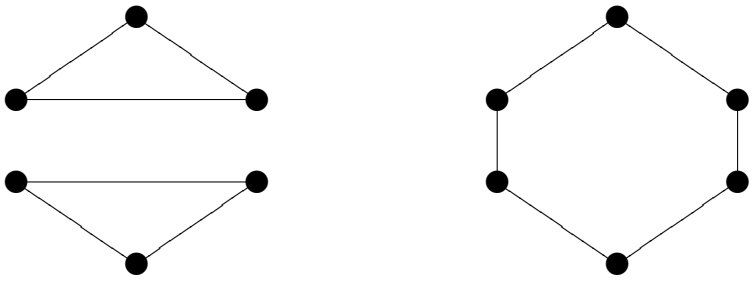
mikä seuraa lemmasta 4.11. Nyt $p^{f_k} \geq 2^{f_k} > n$ jokaisella alkuluvulla p. Näin ollen jokainen ryhmä, jonka kertaluku on jaollinen jonkin alkuluvun potenssilla, jonka eksponentti on suurempi kuin f_k, sisältää luvun 3.8 nojalla Abelin aliryhmän, jonka kertaluku on vähintään n.

Olkoon $f \in \mathbb{N}$ pienin luonnollinen luku, joka on suurempi kuin f_n. Jokainen ryhmä, jossa ei ole kertalukua n olevaa Abelin aliryhmää on joukon $\omega_{q,f}$ jäsen. Kuten määritelmässä 4.10 todetaan, on $\omega_{q,f}$ äärellinen joukko, joten voidaan löytää pienin sellainen luku $M_n \in \mathbb{N}$ ettei yksikään ryhmä, jonka kertaluku on $\geq M_n$, kuulu joukkoon $\omega_{q,f}$. □

4.4. Konjugaattiluokat ja vaihdannaisuusverkot

Kun halutaan testata kahden verkon isomorfisuutta, lasketaan melko usein ensimmäiseksi verkkojen solmujen asteluvut. Jos nimittäin verkoissa on eri määrät solmuja, joilla on samat asteluvut, eivät verkot voi olla isomorfiset. Ei kuitenkaan ole mitään takeita siitä, että verkot olisivat isomorfiset, vaikka niissä olisikin samat määrät samanasteisia solmuja.

Vastaesimerkki löytyy kuusialkioisista verkoista. Alla olevissa verkoissa jokainen solmu on yhteydessä kolmeen solmuun, itseensä ja kahteen muuhun solmuun (kaaret solmusta itseensä on jätetty kuvasta pois), mutta verkot eivät ole isomorfiset (kuten helposti näkee, sillä ensimmäinen verkko on epäyhtenäinen, mutta toinen on yhtenäinen).



Jonkin ryhmän G vaihdannaisuusverkossa voidaan solmun $x \in G$ naapurusto samastaa sen keskittäjien aliryhmän $\mathrm{C}(x)$ kanssa. Niinpä alkion x asteluku on sen keskittäjän kertaluku. Jos siis ryhmillä H_1 ja H_2 on isomorfiset vaihdannaisuusverkot, on niillä samat lukumäärät alkioita, joilla on samaa kertalukua olevat keskittäjät. Koska alkion $x \in G$ konjugaattiluokan kertaluku on $|G|/|\mathrm{C}(x)|$, on ryhmillä H_1 ja H_2 samat määrät samankokoisia konjugaattiluokkia.

4.13. **Määritelmä.** Ryhmillä H_1 ja H_2 on *samanlaiset konjugaattirakenteet*, mikäli niillä on samat lukumäärät samankokoisia konjugaattiluokkia.

Herää kysymys, onko mahdollista löytää kaksi ryhmää, joilla on samanlaiset konjugaattirakenteet, mutta epäisomorfiset vaihdannaisuusverkot. Kysymys on mielenkiintoinen, koska kielteinen vastaus tarkoittaisi, että vaihdannaisuusverkot ovat yleisiä verkkoja yksinkertaisempia (kuten yllä nähtiin).

Tutkielmassa ongelmaan otettiin kokeellinen lähestymistapa, koska sen ratkaiseminen muulla tavoin ei kirjoittajalta onnistunut. Vaihdannaisuusverkkoja käytiin läpi tietokoneella n.s. GAP -ympäristössä (Groups Programming and Algebra [6]) toteutetulla ohjelmalla, joka on tämän tutkielman liitteenä (LIITE A).

Ensimmäinen ratkaisuyritys perustui sille, että pyrittiin käymään kertalukuja läpi ja etsimään ryhmiä, joilla on samanlainen konjugaattirakenne. Kun tällainen pari H_1 ja H_2 löytyi, käytiin läpi kaikki bijektiot, jotka kuvaavat jokaisen $m \in \mathbb{N}$ alkiota sisältävän ryhmän H_1 konjugaattiluokan jollekin ryhmän H_2 konjugaattiluokalle, jossa on m alkiota (kaikilla $m \in \mathbb{N}$). Jos ryhmien H_1 ja H_2 vaihdannaisuusverkot eivät olleet isomorfiset ei yksikään bijektioista ollut vaihdannaisuusverkkojen isomorfismi.

Tällaisen lähestymistavan ongelma on se, että bijektioiden lukumäärä on jo melko pienissä ryhmissä valtava. Esimerkiksi kahdeksanalkioisessa diedriryhmässä D_8 ja kvaternioiden yksiköiden ryhmässä $\mathbb{H}$ on molemmissa viisi konjugaattiluokkaa, joista kolmessa on kaksi ja kahdessa yksi alkio. Bijektioita, jotka säilyttävät konjugaattirakenteen, on näin ollen $3! \cdot 2^3 \cdot 2 = 96$.

Jos $f : H_1 \to H_2$ ja $g : H_1 \to H_2$ ovat bijektioita, $xf = xg$ ja $yf = yg$ joillekin $x, y \in H_1$, niin on luonnollisesti

$$([xg, yg] = 1 \Leftrightarrow [x, y] = 1) \Leftrightarrow ([xf, yf] = 1 \Leftrightarrow [x, y] = 1).$$

Niinpä se, että osoitetaan ettei jokin ryhmien H_1 ja H_2 välinen bijektio f ole isomorfismi (löytämällä sellaiset $x, y \in H_1$ että $[x, y] = 1 \nLeftrightarrow [xf, yf] = 1$) osoittaa että moni muukaan bijektio ei tätä ole. Tämä helpottaa laskentaa jonkin verran, muttei tarpeeksi. Lisäksi se vaikeuttaa ohjelmointitehtävää, joten tulokset käyvät epävarmemmiksi.

Laskennallisten ongelmien takia päätettiin käyttää ns. verkkojen värittämiseen perustuvaa Babai-Erdös-Selkow isomorfia-algoritmia ([1]). Se on parannus yllä esitettyyn solmujen astelukuja vertailevaan menetelmään.

Värittämisen tarkoituksena on tuottaa molempiin verkkoihin lineaarisesti järjestetyt ekvivalenssirelaatiot. Nämä *väritykset* ovat siis sellaisia ekvivalenssirelaatioita, joiden ekvivalenssiluokilla on järjestysluvut. Menetelmä on rekursiivinen siinä mielessä, että väritystä hienonnetaan asteittain. Tätä hienontamista jatketaan, kunnes ekvivalenssirelaation luokat eivät enää muutu.

Kun vertaillaan ryhmien H_1 ja H_2 vaihdannaisuusverkkoja, ositetaan ryhmien alkioiden joukko ensin luokkiin

$$K_1, K_2, \ldots \subset H_1 \text{ ja } L_1, L_2, \ldots \subset H_2,$$

yksi jokaista luonnollista lukua kohti. Jokainen alkio kuuluu siihen luokkaan, jonka indeksi on sen keskittäjän kertaluku. Vaihdannaisuusverkko siis ositetaan solmujen astelukujen mukaan.

Muodostunut ekvivalenssiluokkien joukko perii lineaarisen järjestysrelaation luonnollisilta luvuilta. Näin on esimerkiksi

$$K_l < K_m \Leftrightarrow l < m.$$

Mikäli verkot ovat isomorfiset, pätee jokaisella luvulla $n \in \mathbb{N}$, että $|K_n| = |L_n|$. Olkoon nimittäin $n \in \mathbb{N}$ sellainen luonnollinen luku, että $|K_n| \neq |L_n|$. Voidaan olettaa, että $|K_m| > |L_m|$, koska tilanne on symmetrinen. Mikä tahansa bijektio $f : H_1 \to H_2$ kuvaa nyt jonkin alkion $x \in K_m$ alkiolle $y \in L_h \neq L_m$. Niinpä on mahdollista löytää joko sellainen $x' \in H_1$ että $[x, x'] = 1$, mutta $[y, x'f] \neq 1$ (jos $h < m$), tai sellainen $y' \in H_2$ että $[x, y'f^{-1}] \neq 1$, mutta $[y, y'] = 1$ (jos $h > m$). Tällöin vaihdannaisuusverkot eivät ole isomorfiset.

Tämä verkkojen osittaminen solmujen astelukujen mukaan on väritysalgoritmin ensimmäinen askel.

Tarkastellaan nyt ekvivalenssiluokkaa $K_l \subset H_1$. Jokainen tämän luokan alkioista on yhteydessä samaan määrään $m \in \mathbb{N}$ alkioita vaihdannaisuusverkossa $\mathcal{W}^{H_1}$. Luokan K_l alkiot voidaan järjestää järjestysrelaatiolla $<_l$ sen mukaan kuinka suuria niiden naapureiden ekvivalenssiluokkien järjestysnumerot ovat. Olkoot $x, y \in K_l$ ja alkion x naapurit $s_{x,1}, \ldots, s_{x,m}$ sekä alkion y naapurit $s_{y,1}, \ldots, s_{y,m}$. Olkoot naapurustot järjestettyinä laskevaan järjestykseen ekvivalenssiluokkansa järjestysluvun mukaan. Nyt $x <_l y$, joss on sellainen i, että $1 \leq i \leq m$ jokaisella luonnollisella luvulla $j < i$ kuuluvat $s_{x,j}$ ja $s_{y,j}$ samaan ekvivalenssiluokkaan, mutta $s_{x,i}$ kuuluu matalampaa järjestyslukua olevaan luokkaan kuin $s_{y,i}$.

Jokainen ekvivalenssiluokka K_l voidaan nyt osittaa esijärjestyksensä $<_l$ mukaan uusiin ekvivalenssiluokkiin ja näin saadaan vanhan järjestetyn ekvivalenssirelaation hienonnus. Olkoot R_1 ja R_2 ryhmien H_1 ja H_2 tällaiset järjestetyt ekvivalenssirelaatiot ja S_1 sekä S_2 näiden hienonnukset. Olkoot ryhmien H_1 sekä H_2 vaihdannaisuusverkot isomorfiset ja olkoot relaatiot R_1 ja R_2 sellaiset, että jokainen verkkoisomorfismi säilyttää jokaisen alkion $x \in H_1$ ekvivalenssiluokan järjestysluvun. Jos siis $f : H_1 \to H_2$ on isomorfismi, on jokaisen $x \in H_1$ ekvivalenssiluokan järjestysluku relaatiossa R_1 sama kuin sen kuvan xf ekvivalenssiluokan järjestysluku relaatiossa R_2. Tästä seuraa, että relaatioiden R_1 ja R_2 samaa järjestyslukua olevissa ekvivalenssiluokissa on samat määrät alkioita.

Muodostetaan nyt uudet, relaatioita R_1 ja R_2 hienommat, järjestetyt ekvivalenssirelaatiot S_1 sekä S_2 yllä kuvatulla tavalla. Jokainen ryhmien H_1 ja H_2 vaihdannaisuusverkkojen isomorfismi säilyttää relaation R_1 ekvivalenssiluokkien järjestysluvut siirryttäessä relaatioon R_2. Siksi säilyy myös jokaisen alkion $x \in H_1$ naapuruston ekvivalenssiluokkien järjestyslukujen jono (relaatiossa R_1), joten alkion x kuvan ekvivalenssiluokan järjestysluku on relaatiossa S_1 sama kuin alkion x ekvivalenssiluokan järjestysluku relaatiossa S_2. Tästä seuraa, että samaa järjestyslukua vastaavissa ekvivalenssiluokissa on samat määrät

alkioita relaatiossa S_1 sekä S_2. Induktiolla nähdään helposti, että tämä pätee jokaisessa hienonnuksessa.

Yllä olevaa menetelmää voidaan soveltaa niin kauan, kunnes ekvivalenssirelaatio ei enää hienone. Jos voidaan löytää sellaiset ryhmät H_1 ja H_2 että niillä on samanlaiset konjugaattirakenteet, mutta yllä oleva prosessi antaa niille erilaiset ekvivalenssiluokkiin jaot, on löydetty kaivattu vastaesimerkki.

Etsinnässä käytettiin hyväksi GAP -ohjelman kirjastoa `SmallGroups`. Kertaluku 128 oli pienin kertaluku, josta käytetyllä menetelmällä löydettiin vastaesimerkkipari. Löydettyihin ryhmiin pääsee GAP -ympäristössä käsiksi komennolla `SmallGroup(128,134)` ja `SmallGroup(128,931)`. Käyttämällä *GAP* -ympäristön funktiota `StructureDescrption( Group )` saadaan ryhmälle `SmallGroup(128,134)` esitys

$$((\mathrm{C}_4 \rtimes \mathrm{C}_8) \rtimes \mathrm{C}_2) \rtimes \mathrm{C}_2$$

ja ryhmälle `SmallGroup(128,931)` esitys

$$(((\mathrm{C}_8 \rtimes \mathrm{C}_2) \rtimes \mathrm{C}_2) \rtimes \mathrm{C}_2) \rtimes \mathrm{C}_2 \,.$$

Kummassakin ryhmässä on

- kolme konjugaattiluokkaa, joissa on 16 alkiota.
- kahdeksan konjugaattiluokkaa, joissa on kahdeksan alkiota.
- kolme konjugaattiluokkaa, joissa on neljä alkiota.
- yksi konjugaattiluokka, jossa on kaksi alkiota.
- kaksi konjugaattiluokka, joissa on yksi alkio.

Ryhmän `SmallGroup(128,134)` vaihdannaisuusverkko hajoaa kuitenkin kymmeneen epätyhjään ekvivalenssiluokkaan, kun taas ryhmän `SmallGroup(128,931)` vaihdannaisuusverkko hajoaa ainoastaan seitsemään epätyhjään ekvivalenssiluokkaan, joten verkot eivät voi olla isomorfiset. Alla olevassa taulukossa on kuvattuna ryhmien järjestysrelaatioiden ekvivalenssiluokkien alkioiden lukumäärät. Taulukon sarakkeet vastaavat tietyn kokoiseen konjugaattiuokkaan kuuluvien alkioiden joukkoja, joiden välillä on bijektiivinen vastaavuus, kuten yllä on todettu. Sarakejako siis kuvaa ryhmien konjugaattirakennetta.

	Alkioiden lukumäärä ekvivalenssiluokissa (niiden konjugaattien lukumäärän mukaan)				
	16	8	4	2	1
`SmallGroup(128,931)`	48	24, 16, 24	12	2	2
`SmallGroup(128,134)`	32, 16	8, 16, 8, 32	4, 8	2	2

Kaiken kaikkiaan käytetyllä menetelmällä löytyi 120 vastaesimerkkiä kertalukua 128 olevien ryhmien joukosta. Ensimmäisen vastaesimerkin löytämiseksi jouduttiin käymään läpi 36825 samanlaiset konjugaattirakenteet omaavien ryhmien paria. Näistä 30155 eli noin 81% oli kertalukua 128. Kaiken kaikkiaan käsiteltiin 498513 ryhmien paria (näistä ainakaan toinen ei ole Abelin ryhmä), joista 430324 eli noin 86% oli kertaluvun 128 ryhmiä.

Laskennassa kiinnitettiin huomiota siihenkin, kuinka hyvin käytetty Babai-Erdös-Selkow-algoritmi soveltuu ryhmien vaihdannaisuusverkkojen isomorfisuuden selvittämiseen. Tärkein kriteeri lienee se, kuinka hienoksi lopullinen järjestetty ekvivalenssirelaatio ryhmissä muodostuu. Mikäli jokaisessa ekvivalenssiluokassa on ainoastaan yksi alkio, ei tarvitse kokeilla kuin yhtä kuvausta vaihdannaisuusverkkojen välillä, jotta saadaan tietää ovatko ne isomorfisia.

Ekvivalenssiluokkien kokoja ei suoraan laskettu, mutta se selvitettiin, mitä kertalukua on ensimmäinen ryhmä, jonka järjestetty ekvivalenssirelaatio hienonee useammin kuin kerran. Tämäkin ryhmä on kertalukua 128, nimittäin ryhmä `SmallGroup(128,1997)`.

Ryhmän `SmallGroup(128,1997)` konjugaattirakenne sisältää neljä luokkaa, mutta se hajoaa yhdeksään luokkaan Babai-Erdös-Selkow-algoritmin avulla. Tämäkään ei ole kovin hieno ositus, koska luokassa on keskimäärin 14 alkiota.

Ryhmien vaihdannaisuusverkoissa Babai-Erdös-Selkow algoritmi ei siis luultavasti ole kovinkaan tehokas. Tämä on hieman yllättävää, koska Babai-Erdös-Selkow algoritmi tuottaa lineaarisen järjestyksen melkein kaikkiin verkkoihin (siis muodostuvan ekvivalenssirelaation jokainen luokka on yksiö). Tämän ovat osoittaneet Babai Erdös ja Selkow artikkelissaan [1]. On kuitenkin huomattava, ettei algoritmi pysty erottelemaan sellaisia alkioita, jotka voivat kuvautua toisikseen jossain verkkojen isomorfismissa (tämä seuraa suoraan siitä, että isomorfismin on säilytettävä jokaisen alkion järjestysluku). Näin ollen, se ei pysty erottamaan toisistaan konjugaattialkioita, koska jokainen ryhmän konjugointi, jollain alkiolla voidaan tulkita sen vaihdannaisuusverkon isomorfismiksi (kuten tietenkin mikä vaan muukin ryhmäautomorfismi). Tässä mielessä vaihdannaisuusverkot siis ovat melko vaikeita erityistapauksia verkoista.

5. Johtopäätöksiä

Ryhmien vaihdannaisuusrelaatioita ei liene aikaisemmin tarkasteltu ihan tässä tutkielmassa esitetyllä tavalla. Aiemmin on käytetty numeerisia mittoja vaihdannaisuudelle kuten vaihdannaisuusosamäärää ([7]). Vaihdannaisuusverkkojen kaltainen rakenteellinen vaihdannaisuuden mitta tietenkin mutkistaa vaihdannaisuuden tarkastelua, mutta tuo esiin kaikenlaisia uusia mielenkiintoisia kysymyksiä. Voidaan esimerkiksi kysyä voiko epäisomorfisilla ryhmillä olla samanlaiset vaihdannaisuusrelaatio, kuten tehtiin luvussa 4 ja saatiin myönteinen vastaus.

Luvuissa 3 ja 4 käsitelty kysymys ryhmien maksimaalisista Abelin aliryhmistä liittyy olennaisella tavalla siihen, mitkä verkot voivat olla jonkin ryhmän vaihdannaisuusverkkoja. Käytetyllä p-ryhmien maksimaalisiin Abelin aliryhmiin nojautuvalla tarkastelutavalla ei voi saada kovinkaan hyviä numeerisia tuloksia. Periaate kuitenkin on selvä. Tarpeeksi suurissa ryhmissä on isoja Abelin aliryhmiä. Riittävän suurissa vaihdannaisuusverkoissa on siis isoja klikkejä. Tätä kysymystä olisi mielenkiintoista selvittää edelleen. Olisi esimerkiksi hauska tietää, kuinka isoja Abelin aliryhmiä on yksinkertaisissa ryhmissä.

Luvussa 4 saatua tulosta, että konjugaattirakenne ei määrää ryhmän vaihdannaisuusverkkoa, voi pitää tutkielman päätuloksena. Käytetty menetelmä ei takaa, että löydetty vastaesimerkkipari on pienintä mahdollista kertalukua, mikä on vähän ongelmallista. Löydetyt vastaesimerkit ovat kertalukua 128 eli niin isoja, ettei niiden alkeellinen tarkastelu ole kovinkaan helppoa. Tämän takia olisi syytä pohtia toisenlaisia isomorfismialgoritmeja.

Babai-Erdös-Selkow algoritmin tuottama väritys on alla oleville verkoille sama.

Nämä ovat kuitenkin selvästikin epäisomorfisia. Ensimmäisen verkon automorfismien ryhmä on ainoastaan yksi-, mutta toisen peräti nelitransitiivinen. Babai-Erdös-Selkow algoritmi ei kuitenkaan pysty näihin verkkoihin.

Eräs ratkaisu edelliseen ongelmaan voisi olla tuloverkkojen muodostaminen näistä verkoista. Jos $G = (V, R)$ on verkko, voidaan siitä muodostaa uusi verkko $G' = (V', R')$, jonka solmuiksi otetaan kaikki verkon G eri noodien parit, siispä

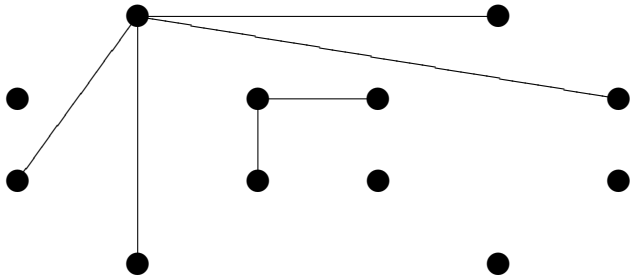
$$V' = \{(x, y) \mid x, y \in V \text{ ja } x \neq y\}.$$

Verkon G' solmujen (x, y) ja (z, t) välillä on kaari, joss ensimmäisillä ja toisilla jäsenillä on yhteydet toisiinsa eli

$$R' = \{((x, y), (z, t)) \mid xRz \text{ ja } yRt\}.$$

Nähdään helposti, että edellisen esimerkin toisesta verkosta muodostuu tällä menetelmällä 12-klikki, koska minkä tahansa noodiparin välillä on kaaret. Siispä Babai-Erdös-Selkow-algoritmin tuottama ositus on yksi iso ekvivalenssiluokka. Esimerkin toisessa verkossa taas on kahdenlaisia noodipareja. Niitä joiden välillä on kaari ja niitä joiden

välillä ei ole kaarta. Ensimmäinen tyyppi on uudessa verkossa yhteydessä neljään noodiin, kun taas toinen on yhteydessä ainoastaan kahteen noodiin. Alla olevaan verkkoon on selkeyden vuoksi piirretty vain kahdesta solmusta lähtevät kaaret.



Babai-Erdös-Selkow algoritmi antaa siis osituksen ainakin kahteen luokaan.

Tällainen menetelmä on riittävän hyvä erottamaan yksi- ja useampitransitiivisen automorfismien ryhmän omaavat verkot toisistaan. Vaikka äärellisten ryhmien vaihdannaisuusverkkojen automorfismien ryhmät eivät olekaan transitiivisia (paitsi Abelin ryhmien tapauksessa) uskoisin yllä olevan kaltaisesta tarkastelusta olevan hyötyä. Olisikin hauska selvittää löytyykö tämän tapaisella menetelmällä pienempää kertalukua kuin 128 olevaa vastaesimerkkiparia.

Kysymys siitä, millaiset verkot voivat olla vaihdannaisuusverkkoja jää vastaamatta tässä tutkielmassa. Se kuitenkin on ilmeistä, että vaihdannaisuusverkot ovat poikkeuksellisia. Tämä näkyy mm. siitä, ettei Babai-Erdös-Selkow algoritmi toimi niille kovinkaan hyvin, toisin kuin tyypillisille verkoille. Ehkä tämä ei kuitenkaan ole niin omituista. Mielenkiintoiset verkot kun yleensä eivät taida olla tyypillisiä.

LIITE A OHJELMALISTAUS

Tässä on luvussa 4 käytetty GAP-ohjelma, jolla etsittiin ryhmien paria, joilla on samanlaiset konjugaattirakenteet, mutta epäisomorfiset vaihdannaisuusverkot. Ohjelmassa on kiinnitetty huomiota selkeyteen pikemminkin kuin optimointiin, jota olisi voinut harjoittaa melko paljon. Kommenteissa on pyritty siihen, että funktioiden käyttötarkoitus käy ilmi mahdollisimman hyvin. Itse ohjelmaa ei ole kommentoitu, mutta muuttujien nimissä on pyritty selkeyteen. Lisäksi GAP-ohjelman erinomaisen kuvaavat operaatioiden ja funktioiden nimet auttavat ohjelman lukemisessa.

```
#
# makeList ( elem, order )
#
# param: elem type
#        An element of some type.
#
#        order int
#        Order of the list produced.
#
# return l [ type, ... ]
#        The list l has length order. Every one of its element is a copy of elem.
#
# description:
#
# notice: ShallowCopy is used, so this might not work, if the structure of elem is
#         intricate.
#
makeList := function( elem, order )
        local i, l;

        l := [];

        for i in [ 1 .. order ] do
                Add( l, ShallowCopy( elem ) );
        od;

        return l;
end;

#
# comm ( group )
#
# Let G be an indexed group. Let g_i, g_j and g_k in G.
#
# param: group Group
#        An indexed group G.
#
# returns: commTable [ [ int, ... ], ... ]
#          The commutativity table of the group G. The list commTable[i] corresponds
#          to g_i in G. The elements of commTable[i] = [ j, k, ... ] correspond to the
#          elements of the centralizer of g_i namely g_j, g_k, ...
#
# description: Return the commutativity graph of G represented as a table.
#
comm := function( group )
```

```
        local i, j, length, commTable, table;

        table := MultiplicationTable( group );
        length := Length( table );

        commTable := makeList( [], length );

        for i in [ 1 .. length ] do
                Add( commTable[i], i );
                for j in [ ( i + 1 ) .. length ] do
                        if table[i][j] = table[j][i] then
                                Add( commTable[i], j );
                                Add( commTable[j], i );
                        fi;
                od;
        od;
        return commTable;
end;

#
# classes ( commTable )
#
# Let G be an indexed group. Let g_i, g_j and g_k in G.
#
# param: commTable [ [ int, ... ], ... ]
#        The commutativity table of the group G. The list commTable[i] corresponds
#        to g_i in G. The elements of commTable[i] = [ j, k, ... ] correspond to the
#        elements of the centralizer of g_i namely g_j, g_k, ...
#
# returns: centralizerOrders [ int, ... ]
#          The element centralizerOrders[i] corresponds to the order of  C(g_i).
#
classes := function( commTable )
        local elem,centralizerOrders;

        centralizerOrders := [];

        for elem in commTable do
                Add( centralizerOrders, Size( elem ) );
        od;
        return centralizerOrders;
end;

#
# neighbourHoodOrders ( commTable, classList )
#
# Let G be an indexed group. Let g_i in G.
#
# param: commTable [ [ int, ... ], ... ]
#        The list commTable[i] = [ j, k, ... ] corresponds to an element g_i in the indexed
#        group G. The elements j, k, ... in commTable[i] correspond to the elements, in G
#        g_j, g_k, ... that commute with g_i.
#
#        classList [ int, ... ]
#        The list classList describes an equivalence relation on the indexed group G. The
#        equivalence-classes of the relation are linearly ordered. The element classList[i]
#        corresponds to the ordinal of the equivalence-class of the element g_i in G.
#
# returns: neighbourOrders [ [ int, ... ], ... ]
#          The element neighbourOrders[i] = [ m, n, ...] corresponds to the element g_i
```

```
#          in the indexed group G. The elements m, n, ... correspond to the ordinals of
#          the equivalence classes of the elements g_m, g_n, ... in the centralizer of g_i.
#          The list neighbourOrders[i] is sorted in ascending order.
#
# description: Given the indexed group G, and an ordered equivalence-relation on G,
#              return a list representing the order-structure of the neighbourhood of every
#              element in G.
#
neighbourHoodOrders := function( commTable, classList )

        local neighbourOrders, element, centralizerElement, l;

        neighbourOrders := [];

        for element in commTable do
                l := [];
                for centralizerElement in element do
                        Add( l, classList[ centralizerElement ] );
                od;

                Sort( l );
                Add( neighbourOrders, l);

        od;

        return neighbourOrders;

end;

#
# formPartition ( classList )
#
# Let G be an indexed group, Let R be an ordered equivalence-relation. Let g_i, g_j and g_k in G.
#
# param: classList [ int, ... ]
#        The element classList[i] corresponds to the order of the equivalence-class of g_i in
#        the relation R.
#
# returns: classes [ [ int, ... ], ... ]
#          The list classes[i] = [ j, k, ... ] corresponds to the set of elements g_j, g_k, ...
#          that form the equivalence-class of R, whcih has order i.
#
# description: Return the ordered partition of G, correpsonding to the equivalence-relation R.
#
formPartition := function( classList )
        local partition, i, class, classes;

        partition := makeList( [], Size( classList ) );

        for i in [ 1 .. Size( classList ) ] do
                Add( partition[ classList[i] ], i );
        od;

        classes := [];

        for class in partition do
                if not class = [] then
                        Add(classes,class);
                fi;
        od;
```

```
        return classes;
end;

#
# preOrdering ( commTable, classList )
#
# Let G be an indexed group. Let g_i in G.
#
# param: commTable [ [ int, ... ], ... ]
#        The list commTable[i] = [ j, k, ... ] corresponds to an element g_i in the indexed
#        group G. The elements j, k, ... in commTable[i] correspond to the elements, in G
#        g_j, g_k, ... that commute with g_i.
#
#        classList [ int, ... ]
#        The list classList describes an equivalence relation R  on the indexed group G. The
#        equivalence-classes of the relation are linearly ordered. The element classList[i]
#        corresponds to the ordinal of the equivalence-class of the element g_i in G.
#
# returns: newClassList [ int, ... ]
#          A refinement of classList.
#
# description: Given the indexed group G and an ordered equivalence-relation R on G, a new relation
#              can be built. The relation is as follows: An element g_i in G belongs to
#              an equivalence-class of lower order, than g_j in G, iff
#
#              1. g_i belonged to a lower equivalence-class than g_j in the relation R or
#              2. g_i and g_j belonged to the same equivalence relation in R, but there exists
#                 such an order n, that g_i and g_j have the same number of neighbours belonging to
#                 equvialence-classes of R of orders higher than n, but g_i has less elements of
#                 belonging to the equivalence-class of order n than g_j.
#
#              The new relation is clearly a refinement of the old relation R, and is an equivalence-
#              relation. Return this relation.
#
preOrdering := function( commTable, classList )

        local class, i, j, classSize, partition, oldPartition, partitions, neighbourOrders ,
              newClassList, foundClass;

        partitions := [];
        oldPartition := formPartition( classList );

        neighbourOrders := neighbourHoodOrders( commTable, classList );

        for class in oldPartition do

                classSize := Size( class );

                if classSize < 2 then Add( partitions, class ); continue; fi;

                partition := [ [ class[1] ] ];

                for i in [ 2 .. classSize ] do

                        foundClass := false;

                        for j in [1 .. Size( partition ) ] do

                                if neighbourOrders[ class[i] ] < neighbourOrders[ partition[j][1] ] then
```

```
                                        Add( partition, [ class[i] ], j );
                                        foundClass := true;
                                        break;
                                fi;

                                if neighbourOrders[ class[i] ] = neighbourOrders[ partition[j][1] ] then
                                        Add( partition[j], class[i] );
                                        foundClass := true;
                                        break;
                                fi;
                         od;

                        if not foundClass then Add( partition, [ class[i] ] ); fi;

                od;
                Append( partitions, partition );
        od;

        newClassList := makeList( 0, Size( classList ) );

        for i in [ 1 .. Size(partitions) ] do

                for j in [ 1 .. Size( partitions[i] ) ] do
                        newClassList[ partitions[i][j] ] := i;
                od;
        od;

        return newClassList;
end;

#
# refiningPreOrdering ( commTable, classList )
#
# Let G be an indexed group. Let g_i, g_j and g_k in G.
#
# param: commTable [ [ int, ... ], ... ]
#        The list commTable[i] = [ j, k, ... ] corresponds to an element g_i in the indexed
#        group G. The elements j, k, ... in commTable[i] correspond to the elements, in G
#        g_j, g_k, ... that commute with g_i.
#
#        classList [ int, ... ]
#        The list classList describes an equivalence relation R  on the indexed group G. The
#        equivalence-classes of the relation are linearly ordered. The element classList[i]
#        corresponds to the ordinal of the equivalence-class of the element g_i in G.
#
# returns: order [ int, ... ]
#          A list, that describes the ordered equivalence-relation, that is achieved by
#          iteratively refining the equivalence-relation classList.
#
# description: This function applies the method preOrder (above) iteratively on a group G and
#              an equivalence-relation of thet group R, until the equivalence-relation can't be
#              refined further.
#
refiningPreOrdering := function( commTable, classList )
        local order, old_order;

        old_order := preOrdering( commTable, classList );
        order := preOrdering( commTable, old_order );

        while not old_order = order do
```

```
                Print("Hey found an order, that was refined!\n");
                old_order := order;
                order := preOrdering( commTable, order );
        od;

        return order;
end;

#
# isom ( order )
#
# param: order int
#        An order to be investigated.
#
# returns: void
#
# description: Check, if there are two such groups of size order G_1 and G_2, that
#
#              1. They have the same amounts of equivalence-classes with the same amount
#                 of elements.
#              2. The colorings of their commutativity-classes, given by the Babai-Erdös-Selkow
#                 algorithm, are different.
#
#              If such pairs of groups can be found, display their indices in the SmallGroups
#              library.
#
isom := function( order )

        local commTable, conjList, orderList, ordering, number, i, j, k, gp, l, class;

        number := NumberSmallGroups( order );

        conjList := [];
        orderList := [];

        Print("Order: ",order,"\n");

        for i in [ 1 .. number ] do
                gp := SmallGroup( order, i );
                if IsAbelian( gp ) then

                        Add( conjList, [] );
                        Add( orderList, [] );
                else


                        l := [];

                        for class in ConjugacyClasses( gp ) do
                                Add( l, Size( class ) );
                        od;
                        Sort( l );
                        Add( conjList, l );

                        commTable := comm( gp );
                        ordering := refiningPreOrdering( commTable, classes( commTable ) );
                        Sort( ordering );
                        Add( orderList, ordering );

                        for j in [ 1 .. (i - 1) ] do
```

```
                                if conjList[j] = l then

                                        if not orderList[i] = orderList[j] then
                                                Print(i, ", ", j,".\n");
                                        fi;


                                fi;
                        od;
                fi;
        od;
end;
```

VIITTEET

[1] L. Babai, P. Erdös, S. M. Selkow: Random Graph Isomorphism SIAM Journal on Computing, volyymi 9, numero 3 (1980)
[2] H. U. Besche, B. Eick, E. A. O'Brien: A Millennium Project: Constructing Small Groups citeseer.ist.psu.edu/634986.html (haettu 19. lokakuuta 2007).
[3] C. Boyer: Matematiikan historia osa II
Art House, Suomi, 1994.
[4] W. Burnside: On some Properties of Groups whose Orders are Powers of Primes
Proceedings of the London Mathematical Society volyymi 2 numero 11 (1932), sivut 225-245.
[5] P. J. Cassidy: Products of Commutators are Not Always Commutators: An Example
The American Mathematical Monthly, volyymi 86, numero 9 (Marraskuu, 1979), sivu 772
[6] The GAP Group: GAP Reference Manual
http://www-gap.mcs.st-and.ac.uk/Manuals/doc/ref/manual.pdf (haettu 20. tammikuuta 2008).
[7] W. H. Gustafson: What is the Probability that Two Group Elements Commute?
The American Mathematical Monthly, volyymi 80, numero 9 (Marraskuu, 1973), sivut 1031-1034.
[8] J. S. Rose: A Course on Group Theory
Dover Publications, Yhdysvallat, 1994.
[9] W. R. Scott: Group Theory
Dover Publications, Yhdysvallat, 1987.