# 3 Ryhmäteorian peruskäsitteet ja pienet ryhmät, $C_2$

Olen valinnut kunkin luvun teemaksi yhden ryhmän. Ensimmäisen luvun teema on pienin epätriviaali ryhmä, eli ryhmä, jossa on kaksi alkiota. Merkitsen sitä $C_2$. Tämä voidaan nähdä musteläiskätestin symmetriaryhmänä ja on syklinen. Toisaalta, jos lähdemme rakentelemaan tästä kahden alkion ryhmästä monimutkaisempia ryhmiä, rakenne muuttuukin pian vaikeaksi, kuten luvun loppupuolella havaitsemme. Rehellisyyden vuoksi minun on tässä vaiheessa jo sanottava, että ryhmästä $C_2$ rakennettujen ryhmien luokittelu on erittäin vaikea avoin ongelma.

## 3.1 Peruskäsitteet

**Määritelmä 3.1.** Ryhmä on joukko $G$, jossa on binäärioperaatio $*$, joka toteuttaa seuraavat ehdot

(i) jos $g_1, g_2 \in G$ niin $g_1 * g_2 \in G$ (operaatio on suljettu)

(ii) $g * (h * k) = (g * h) * k$, (operaatio on liitännäinen)

(iii) on olemassa $e \in G$, joka toteuttaa $g * e = e * g = g$ kaikille $g \in G$, (on olemassa ykkösalkio, yleensä 0 tai 1)

(iv) jokaiselle $g \in G$ on olemassa $g^{-1} \in G$, joka toteuttaa $g * g^{-1} = g^{-1} * g = e$ (on olemassa käänteisalkio).

**Esimerkki 3.2.** Otetaan joukko $\{0, 1\}$ ja operaatioksi yhteenlasku siten, että $1 + 1 = 0$. Tämä on ryhmä, sillä se on suljettu em. säännön nojalla. Ykkösalkio on nolla, ja koska $1 + 1 = 0$, on alkiolla 1 myös yksiselitteinen käänteisalkio. Koska yhteenlasku on liitännäinen, on myös tämän ryhmän operaatio liitännäinen. Jos otamme joukoksi $1, a$ ja tarkastelemme binäärioperaationa kertolaskua siten, että $a^2 = 1$, saamme täysin saman ryhmärakenteen. Keksitkö lisää esimerkkejä kahden alkion ryhmästä?

**Esimerkki 3.3.** Kolmen alkion permutaatioryhmä on helpoin esimerkki epäkommutatiivisesta ryhmästä. Tämä ryhmä koostuu kaikista bijektioista $\tau : \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$. Näitä bijektioita on yhteensä kuusi

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, (13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$(23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, (123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, (132) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Jos merkitsemme tasasivuisen kolmion kulmia $1, 2, 3$, voimme visualisoida tämän ryhmän tasasivuisen kolmion symmetriaryhmänä. Ryhmän kertolasku on näiden bijektioiden kompositio. $(12)(13) = (123)$ tai

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

**Tehtävä 1.** Laske $(12)(23)$, $(123)(132)$ ja $(12)(123)$. Löydä sellainen pari, että $ab \neq ba$.

**Tehtävä 2.** Osoita, että ykkösalkio on yksikäsitteinen. Osoita myös, että käänteisalkio on yksikäsitteinen.

**Määritelmä 3.4.** Ryhmän $G$ aliryhmä $H$ on $G$:n osajoukko, joka on suljettu ryhmäoperaation suhteen. Algebrallisesti kirjoittaen, $1 \in H$, jos $a \in H$, on myös $a^{-1} \in H$ ja jos $a, b \in H$ on myös $ab \in H$.

**Määritelmä 3.5.** Ryhmän kertaluku on ryhmän alkioiden määrä, eli ryhmän $G$ koko. Merkitsemme tätä $|G|$.

Kertaluku voi olla äärellinen tai ääretön, jopa ylinumeroituva.

**Määritelmä 3.6.** Alkion kertaluku on pienin sellainen $n \geq 1$, jolle $g^n = 1$. Tällöin alkion kertaluku on $o(g) = n$.

Ykkösalkion kertaluku on yksi, muitten alkioitten kertaluku on suurempi kuin yksi. Huomaa, että myös alkion kertaluku voi olla äärellinen tai ääretön. Jos alkion kertaluku on äärellinen, toisinaan kutsumme sitä torsioalkioksi. Jos ryhmän jokaisen alkion kertaluku on ääretön, kutsumme ryhmää torsiovapaaksi (torsiottomaksi).

**Määritelmä 3.7.** Olkoon $G$ ryhmä ja $H$ sen aliryhmä. Merkitsemme $|G : H| = \frac{|G|}{|H|}$ ja kutsumme tätä lukua $H$:n indeksiksi $G$:ssä.

Äärellisen ryhmän aliryhmiän indeksi on aina kokonaisluku Lagrangen lauseen perusteella, jonka todistamme seuraavalla sivulla.

Varsinkin äärettömien ryhmien tapauksessa, indeksi on tärkeä invariantti. Aliryhmät, joiden indeksi on äärellinen, poikkeavat rakenteeltaan huomattavasti aliryhmistä, joiden indeksi on ääretön. Samaan tapaan kuin kuntalaajennuksissa.

**Tehtävä 3.** Osoita, että

(i) Luonnolliset luvut $\mod 5$ muodostavat ryhmän yhteenlaskun suhteen.

(ii) Luonnolliset luvut $\mod 8$ eivät muodosta ryhmää kertolaskun suhteen.

(iii) Miten käy, kun poistamme edellisestä kohdasta alkion 0?

(iv) Onko mahdollista konstruoida luonnollisten lukujen $\mod 8$ osajoukko, niin, että se muodostaa ryhmän kertolaskun suhteen? Kuinka monta tällaista osajoukkoa löydät? Ovatko jotkut näistä toistensa aliryhmiä? Määrittele nämä aliryhmät ja niiden indeksit.

(v) Onko $\{\pm 1, \pm i\}$ ryhmä normaalin kompleksilukujen kertolaskun suhteen? Mitkä ovat sen alkioitten kertaluvut? Onko mahdollista valita yksi alkio niin, että koko ryhmä on tämän alkion potensseista koostuva.

(vi) Osoita, että $2 \times 2$ kääntyvien matriisien joukko muodostaa ryhmän kertolaskun suhteen minkä tahansa kunnan $k$ yli. Merkitsemme tätä ryhmää $\mathrm{GL}_2(k)$. Onko sama totta mille tahansa renkaalle? Miksi?

(vii) Tarkastellaan kääntyviä matriiseja kuten yllä, nyt $p$:n alkion kunnan yli. Tämä ryhmä on luonnollisesti äärellinen, sillä on olemassa vain $p^4$ erilaista matriisia tämän kunnan yli. Kuinka monta niistä kuuluu kääntyvien matriisien ryhmään?

(viii) Nyt vaadimme, että kääntyvien matriisien determinantti on yksi. Osoita, että tämä on kääntyvien matriisien ryhmän aliryhmä. Merkitsemme tätä ryhmää $\mathrm{SL}_2(p)$. Montako alkiota tässä ryhmässä on, kun kunnan koko on edelleen $p$? Mikä on tämän aliryhmän indeksi?

**Määritelmä 3.8.** Ryhmää kutsutaan Abelin ryhmäksi tai kommutatiiviseksi, jos kaikille alkioille $a, b \in G$ pätee $ab = ba$.

**Tehtävä 4.** Mitkä ylläolevista ryhmistä ovat Abelin ryhmiä?

**Tehtävä 5.** Osoita, että $G$:n ollessa Abelin ryhmä, pätee kaikille $n \in \mathbb{Z}$ identiteetti $(ab)^n = a^n b^n$. Olkoon $G$ ryhmä, jossa pätee $(ab)^2 = a^2 b^2$ kaikille $a, b \in G$. Osoita, että tällainen $G$ on Abelin ryhmä.

**Määritelmä 3.9.** Kutsumme kahta ryhmän $G$ alkiota $h_1$ ja $h_2$ toistensa konjugaateiksi, jos on olemassa sellainen alkio $g \in G$, joka toteuttaa identiteetin $g^{-1} h_1 g = h_2$.

**Tehtävä 6.** Osoita, että matriisit $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ ja $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ ovat toistensa konjugaatteja ryhmässä $\mathrm{GL}_2(\mathbb{Z})$.

**Tehtävä 7.** Osoita, että alkiot $(12), (13), (23)$ ovat keskenään konjugaatteja ryhmässä $S_3$, kuten myös $(123), (132)$.

**Määritelmä 3.10.** Kaikkia niitä ryhmän $G$ alkioita, jotka ovat keskenään konjugaatteja, kutsutaan $G$:n konjugaattiluokaksi.

Yllä olevan esimerkin nojalla on ryhmässä $S_3$ kolme konjugaattiluokkaa: ykkösalkio, kakkossyklit ja kolmossyklit. On yleisemmin totta, että symmetrisen ryhmän $S_n$ konjugaattiluokan määrittelee yksikäsitteisesti alkion syklityyppi.

Tiettyjen konjugaattiluokkien unioni on myös toisinaan mielenkiintoinen aliryhmä.

**Määritelmä 3.11.** Ryhmän $G$ normaali aliryhmä $N$ on aliryhmä, jolle pätee $g^{-1}Ng = N$ kaikille $g \in G$.

Normaalin aliryhmän määritelmässä siis tarkastelemme konjugaatiota joukon suhteen. Aliryhmän $N$ tulee olla suljettu konjugaation suhteen, mutta emme vaadi, että kullekin $n \in N$ pätee $g^{-1}ng = n$. Huomaa, että Abelin ryhmässä jokainen aliryhmä on normaali.

**Tehtävä 8.** Miksi joukko $\{1, (123), (132)\} = A_3$ muodostaa ryhmän $S_3$ normaalin aliryhmän, mutta joukko $\{1, (12), (13), (23)\}$ ei?

**Tehtävä 9.** Osoita, että jos $A \lhd G$ ja $B \lhd G$, silloin $AB \lhd G$, missä $AB = \{ab : a \in A, b \in B\}$. Huomaa, että on hyvinkin mahdollista, että $A \lhd B$ ja $B \lhd C$, ja $A \ntriangleleft C$. Normaalin aliryhmän ominaisuus ei siis ole transitiivinen.

**Määritelmä 3.12.** Olkoon $G$ ryhmä ja $H$ aliryhmä. Kutsumme joukkoa

$$gH = \{gh : h \in H\}$$

$H$:n (vasemmaksi) sivuluokaksi.

Oikea sivuluokka määritellään vastaavasti

$$Hg = \{hg : h \in H\}.$$

**Tehtävä 10.** Osoita, että $H$ on $G$:n normaali aliryhmä, jos $|G : H| = 2$.

**Tehtävä 11.** Olemme osoittaneet, että $A_3 \lhd S_3$. Sivuluokat ovat $A_3 = \{1, (123), (132)\}$ ja $(12)A_3 = \{(12), (13), (23)\}$ (miksi?). Osoita, että $(12)A_3 = (13)A_3 = (23)A_3$, eli ei ole väliä, minkä alkion valitsemme esittämään sivuluokkaa.

**Lause 3.13** (Lagrange)**.** *Olkoon $G$ ryhmä ja $H$ aliryhmä. Silloin $H$:n kertaluku jakaa $G$:n kertaluvun.*

*Todistus.* Olkoon $H$ aliryhmä, ja sen sivuluokat $g_i H$. Jokainen sivuluokka on yhtäsuuri, ja koska $H$ on itsessään sivuluokka, voimme olettaa, että $|g_i H| = |H|$ jokaiselle $g_i \in G$. Sivuluokat ovat erillisiä, mutta toisaalta myös kattavat $G$:n alkiot $\bigcup_i g_i H = G$. Tästä seuraa, että $i \times |H| = |G|$. Joten $|H| \mid |G|$. □

**Korollaari 3.14.** *Olkoon $g \in G$. Silloin $g$:n kertaluku jakaa $G$:n kertaluvun.*

*Todistus.* Tarkastellaan alkion $g$ potensseja. Nämä virittävät aliryhmän $\langle g \rangle$ (tehtävä!). Nyt tulos seuraa Lagrangen lauseesta, sillä $o(g) = |\langle g \rangle|$. □

**Lause 3.15.** *Jos $G$ on ryhmä, ja $N$ on sen normaali aliryhmä, myös $N$:n sivuluokat muodostavat ryhmän, jota kutsutaan tekijäryhmäksi ja merkitään $G/N$.*

*Todistus.* Tehtävä. Tarkastele aksioomia. □

**Määritelmä 3.16.** Olkoot $G$ ja $H$ kaksi ryhmää. Kuvaus

$$\phi : G \to H$$

on homomorfismi, jos kaikille $g_1, g_2 \in G$ pätee $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

Homomorfismi on siis kuvaus, joka kuvaa sekä alkiot, että säilyttää ryhmäoperaation.

**Esimerkki 3.17.** Perusesimerkkejä homomorfismeista ovat:

(i) Kuvaus $\phi : G \longrightarrow 1$ on homomorfismi, mille tahansa ryhmälle $G$. Tätä kutsutaan triviaaliksi homomorfiksi.

(ii) Kuvaus $\det : \mathrm{GL}_2(\mathbb{R}) \longrightarrow \mathbb{R}^*$ on homomorfismi.

(iii) $\psi : G \longrightarrow G/N$, missä $N \lhd G$ on homomorfismi.

**Määritelmä 3.18.** Homomorfismin $\phi : G \longrightarrow H$ ydin on joukko

$$Ker(\phi) := \{g \in G : \phi(g) = 1\},$$

ja homomorfismin kuva, joukko

$$Im(\phi) := \{h \in H : \phi(g) = h\}.$$

**Tehtävä 12.** Tarkastellaan homomorfismia $\rho_k : \mathbb{Z} \longrightarrow \mathbb{C}^*$ jossa $n \mapsto e^{2ni\pi/k}$. Tässä $\mathbb{Z}$ on ryhmä yhteenlaskun suhteen ja $\mathbb{C}^*$:ssa operaatio on normaali kertolasku. Osoita, että tämä on homomorfismi. Mikä on sen ydin ja mikä kuva? Miten kuva ja ydin riippuvat $k$:sta.

**Tehtävä 13.** Osoita, että minkä tahansa homomorfismin

$$\phi : G \to H$$

ydin on $G$:n normaali aliryhmä ja että kuva on $H$:n aliryhmä.

**Määritelmä 3.19.** Ryhmien välistä bijektiota, joka on myös homomorfismi, kutsutaan isomorfismiksi.

**Lause 3.20** (Ensimmäinen isomorfialause)**.** *Olkoot $G$ ja $H$ ryhmiä, ja $\phi$ epimorfismi,*

$$\phi : G \to H.$$

*Olkoon $N$ homomorfismin ydin. Silloin $G/N \cong H$.*

Yleisesti, jos kyseessä ei ole epimorfismi, $G/Ker(\phi) \cong Im(\phi)$.

**Lause 3.21** (Toinen isomorfialause)**.** *Kun $H \leq G$ ja $K \lhd G$, silloin $HK \leq G$ ja $H \bigcap K \lhd K$ sekä*

$$HK/K \cong H/(H \bigcap K).$$

Tämän isomorfialauseen muistisääntönä toimii suunnikas.

**Lause 3.22** (Kolmas isomorfialause)**.** *Jos $N \leq G$ ja $N \leq M \lhd G$, silloin $M/N \lhd G/N$ ja*

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

**Tehtävä 14.** $S_3$ on kolmen kirjaimen permutaatioryhmä. Se koostuu $3! = 6$ alkiosta. Jos käytämme syklinotaatiota, voimme merkitä sen alkiota 1, (12), (23), (13), (123), (132). Tässä kahden pituiset syklit ovat involuutioita (eli niiden kertaluku on 2), ja syklit (123) ja (132) ovat toistensa käänteisalkioita. Osoita, että

1. $S_3$ sisältää kolme aliryhmää, joitten kertaluku on 2, ja yhden, jonka kertaluku on 3. Osoita, että kertalukua kolme oleva ryhmä on syklinen ja normaali $S_3$:ssa. Kutsumme tätä ryhmää nimellä $A_3$.

2. Osoita, että $S_3/A_3 \cong C_2$. Miltä tämän ryhmän alkiot näyttävät?

3. Määritellään permutaatio parilliseksi, jos se voidaan kirjoittaa parillisena määränä involuutioita, esimerkiksi $(12)(13) = (123)$, joten $(123)$ on parillinen permutaatio. Kun taas alkio $(13)$ on pariton permutaatio. Määritellään kuvaus
$$\psi : S_3 \longrightarrow \{1, -1\},$$
missä $\psi(a) = 1$ jos $a$ on parillinen ja $-1$ jos $a$ on pariton. Osoita, että tämä kuvaus on homomorfismi, kun joukon $\{\pm 1\}$ ryhmäoperaatio on normaali kertolasku, ja totea edellisen kohdan isomorfismi tätä kautta.

**Tehtävä 15.** Olkoon $D_6$ kolmion symmetriaryhmä. Kuvaile ryhmä geometrisesti. Osoita konstruoimalla sopiva kuvaus, että $S_3$ on isomorfinen ryhmän $D_6$ kanssa.

## 3.2 Kertalukua 6 olevien ryhmien luokittelu

Jo vuonna 1854 Cayley määritteli kaikki ryhmät, joitten kertaluku on korkeintaan kuusi. Seuratkaamme hänen jalanjäljissään ja tutkikaamme näitä ryhmiä.

Määrittelimme edellisessä kappaleessa alkion kertaluvun. Olkoon $g$ alkio, jonka kertaluku on $m$, silloin
$$\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}.$$

**Tehtävä 16.** Osoita, että $\langle g \rangle$ on ryhmä. Kutsumme ryhmää $\langle g \rangle$ sykliseksi ryhmäksi. Osoita, että $\langle g \rangle$ on Abelin ryhmä. Jokainen syklisen ryhmän aliryhmä on myös syklinen.

Tarkastelemme ryhmiä, joiden kertaluku on alkuluku $p$. Olkoon $g$ tällaisen ryhmän alkio, joka ei ole ykkösalkio. Koska alkion kertaluku jakaa ryhmän koon, tästä seuraa, että $g^p = 1$, ja koska $g^1 \neq 1$, on alkion $g$ kertaluku $p$ ja näin ollen $G \cong \langle g \rangle$. Itseasiassa kaikki ykkösalkiosta eroavat alkiot ovat kertalukua $p$. Tämä ryhmä on syklinen. Kertalukua 2,3,5,7 olevia ryhmiä on näin ollen kutakin vain yksi. Jäljelle jäävät kertaluvut 4,6.

**Propositio 3.23.** *Kertalukua neljä oleva ryhmä on Abelin ryhmä.*

*Todistus.* Ainakin yksi alkio on kertalukua kaksi, sillä jos paritamme alkiot aina niiden käänteisalkioitten kanssa, jää yksi pariton, joka on siis kertalukua kaksi. Merkitään tätä alkiota $a$. Ja merkitään kahta muuta ei-triviaalia alkiota $b$ ja $c$. Koska $a$ ja $b$ eivät ole toistensa käänteisalkioita, eivätkä ykkösalkioita, täytyy olla $ab = c$, mutta sama pätee myös tulolle $ba = c$. Tästä seuraa, että $a$ ja $b$ kommutoivat. Toisaalta vaihtamalla $b$:n tilalle $c$:n, seuraa myös, että $a$ ja $c$ kommutoivat. Lopuksi näytämme, että $b$ ja $c$ kommutoivat. Nyt $b$ ja $c$ ovat joko toistensa käänteisalkioita, missä tapauksessa $bc = cb = 1$, tai kummankin kertaluku on kaksi. Tässä tapauksessa väistämättä $bc = a = cb$. Joten ryhmä, jonka alkiot ovat $1, a, b, c$ on väistämättä Abelin ryhmä.

□

Kertalukua neljä oleva ryhmä on joko $C_4$ tai $C_2 \times C_2$.

Yllä totesimme, että $a$ on kertalukua kaksi. Jos $b$ ja $c$ ovat kertalukua kaksi, saamme ryhmäksi $C_2 \times C_2$. Tätä ryhmää kutsutaan toisinaan myös nimellä Klein Viergruppe, $V_4$. Jos $b$ ja $c$ ovat toistensa käänteisalkioita, ryhmä on $C_4$.

**Tehtävä 17.** Kirjoita Cayleyn taulukot näille ryhmille ja vakuutu siitä, että pelkästään kertalukua kaksi olevien alkioiden määrä erottaa ryhmät toisistaan.

On siis jäljellä vain kertaluku kuusi.

**Propositio 3.24.** *Kertalukua 6 oleva ryhmä sisältää aliryhmän, jonka kertaluku on kaksi, sekä aliryhmän, jonka kertaluku on kolme.*

*Todistus.* Yllä kuvatulla alkioiden parituksella saamme selville, että on olemassa alkio, jonka kertaluku on kaksi. Tämä alkio virittää syklisen kahden alkion aliryhmän. Todistamme, että on olemassa alkio, jonka kertaluku on kolme, ja tämä virittää kolmen alkion syklisen ryhmä. Jos ryhmässä on alkio $a$, jonka kertaluku on kuusi, virittää alkio $a^2$ vaaditun aliryhmän. Voimme siis lopullista ristiriitaa varten olettaa, että jokaisen alkion kertaluku on kaksi. Merkitään alkioita $1, a, b, c, d, e$. Voimme valita alkiot niin, että $ab = c$, tästä seuraa, että $bc = a$ ja $ac = b$, koska kaikki alkiot ovat kertalukua kaksi, ovat ne itsensä käänteisalkioita. Nyt $ad = e$ ja $ae = d$, koska kyseessä on ryhmä. Toisaalta $ba = c$ ja $bc = a$, joten $bd = e$ (koska $b \neq 1$) ja $be = d$. Nyt $bd = ad = e$, mistä seuraa supistussäännön nojalla, että $a = b$, mikä on ristiriita. □

Kuuden alkion ryhmällä on siis kaksi syklistä aliryhmää $C_2$ ja $C_3$, joiden leikkaus on tämälleen ykkösalkio. Jos ryhmä on Abelin ryhmä, ovat kaikki aliryhmät normaaleja ja tällöin se on isomorfinen $C_2 \times C_3$ kanssa. Tarkastelemme tapausta, jossa ryhmä ei ole Abelin ryhmä, erikseen. Merkitään ryhmän tähän mennessä määriteltyjä alkiota $a$, $b$, $b^2 = e$. Koska ryhmä ei ole Abelin ryhmä, on $ab = c$ ja $ba = d$. Tästä seuraa, että $a^2b = ac = b$ ja $ba^2 = da = b$. Nyt myös $cd = abba = aea = b$, ja $dc = baab = b^2 = e$ jne.

Nämä voidaan koota Cayleyn taulukkoon 1.

Tämä päättää kertalukua kuusi olevien ryhmien luokittelun. Tarkista, että tämän ryhmän Cayleyn taulukko on sama kuin $S_3$:n Cayleyn taulukko.

Taulukko 1: Kuuden alkion epäkommutatiivinen ryhmä

| * | 1 | a | c | d | b | e |
|---|---|---|---|---|---|---|
| 1 | 1 | a | c | d | b | e |
| a | a | 1 | b | e | c | d |
| c | c | e | 1 | b | d | a |
| d | d | b | e | 1 | a | c |
| b | b | d | a | c | e | 1 |
| e | e | c | d | a | 1 | b |

## 3.3 2-ryhmät

Äärellisiä ryhmiä, joiden kertaluku on joku kakkosen potenssi kutsutaan 2-ryhmiksi. Helpoimmat epätriviaalit 2-ryhmät olivat ryhmän $C_2$ lisäksi Kleinin neliryhmä $V_4$ ja neljän alkion syklinen ryhmä $C_4$, molemmat Abelin ryhmiä.

Kertalukua kahdeksan olevia ryhmiä on yhteensä viisi. Kolme Abelin ryhmää $C_8$, $C_4 \times C_2$ ja $C_2 \times C_2 \times C_2$, sekä epäkommutatiiviset diedriryhmä ja kvarternioniryhmä. Abelin ryhmien lukumäärä ja luokittelu käydään läpi seuraavassa luvussa kokonaan, joten emme paneudu siihen tällä erää. Esittelemme kuitenkin diedriryhmän ja kvarternioni ryhmän ja todistamme, että nämä ovat ainoat vaihtoehdot.

Huomaamme myös, että jos ryhmä on epäkommutatiivinen, siinä ei voi olla alkiota, jonka kertaluku on kahdeksan, sillä jos näin olisi, olisi ryhmä syklinen kahdeksan alkion ryhmä ja siis kommutatiivinen. Alkioitten kertaluvut ovat siis joko neljä tai kaksi.

**Tehtävä 18.** Osoita, että jos jokaisen alkion kertaluku on kaksi, on ryhmä kommutatiivinen.

Näin ollen ryhmässä on alkio, jonka kertaluku on neljä. Koska ryhmän kertaluku on parillinen, on ryhmässä myös ainakin yksi involuutio. Voimme laskea nyt involuutioitten ja alkioitten, joiden kertaluku on neljä, lukumäärän. Jos alkion $a$ kertaluku on neljä, on myös alkion $a^3$ kertaluku neljä, ja kumpikin virittää saman syklisen aliryhmän $C_4$. Kertalukua neljä olevien alkioitten määrä on siis parillinen. Niitä on joko kaksi, neljä tai kuusi. Vastaavasti involuutioiden määrät ovat viisi, kolme tai yksi. Kaksi neljän alkion syklistä aliryhmää leikkaavat joko triviaalisti tai niiden leikkaus on $C_2$

**Tehtävä 19.** Osoita, että jos kahdeksan alkion joukko, jossa on täsmälleen neljä alkiota, joiden kertaluku on neljä, ja kolme, joiden kertaluku on kaksi, ei voi olla ryhmä. Vihje: kirjoita Cayleyn taulukko, jonka ensimmäisessä kulmassa on neljän alkion syklinen ryhmä $1, a, a^2, a^3$, merkitse muita alkioita $b, b^2, b^3$ ja $c$ ja johda ristiriita.

Todistamme nyt laskun avulla, että kumpikin jälkimmäinen vaihtoehto antaa vain yhden mahdollisen ryhmärakenteen. Parempien työkalujen puutteessa, käymme läpi taas Cayleyn taulukkoa.

Ensin käsitellään tapaus, että ryhmässä on kaksi alkiota, joiden kertaluku on neljä, ja viisi involuutiota. Olkoon alkio, jonka kertaluku on 4, nimeltään $a$, tällöin toinen alkio, jonka kertaluku on neljä on $a^3$. Merkitään sellaista involuutiota, joka ei ole muotoa $a^2$ nimellä $r$, loput kolme alkiota voivat olla nimeltään $ar$, $a^2r$ ja $a^3r$, ja myös nämä ovat involuutioita.

Taulukko 2: kertolaskutaulu kahdeksan alkion epäkommutatiiviselle ryhmälle

| $*$ | $1$ | $a$ | $a^2$ | $a^3$ | $r$ | $ar$ | $a^2r$ | $a^3r$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $a$ | $a^2$ | $a^3$ | $r$ | $ar$ | $a^2r$ | $a^3r$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $1$ | $ar$ | $a^2r$ | $a^3r$ | r |
| $a^2$ | $a^2$ | $a^3$ | $1$ | $a$ | $a^2r$ | $a^3r$ | $r$ | $ar$ |
| $a^3$ | $a^3$ | $1$ | $a$ | $a^2$ | $a^3r$ | $r$ | $ar$ | $a^2r$ |
| $r$ | $r$ | | | | $1$ | | | |
| $ar$ | $ar$ | | | | $a$ | | | |
| $a^2r$ | $a^2r$ | | | | $a^2$ | | | |
| $a^3r$ | $a^3r$ | | | | $a^3$ | | | |

Koska $arar = 1$, $a^2ra^2r = 1$ ja $a^3ra^3r = 1$, seuraa lopputaulukko yksikäsitteisesti.

Muussa tapauksessa ryhmässä on yksi involuutio ja kuusi alkiota, joiden kertaluku on neljä. Tämä ryhmä on väistämättä isomorfinen kvarternioniryhmän

$$\{\pm 1, \pm i, \pm j, \pm k\}$$

kanssa, jossa pätevät kvarternionien (tämä on yksi kompleksilukujen yleistys, Hamiltonin käsialaa) normaalit laskusäännöt $i^2 = j^2 = k^2 = ijk = -1$ ja $ij = k, jk = i, ki = j$.

**Tehtävä 20.** Täydennä päättely ja taulukko 3.

**Määritelmä 3.25.** Määritellään ryhmän keskus

$$Z(G) := \{g \in G : gh = hg \forall h \in G\}.$$

Taulukko 3: kertolaskutaulu kvarternioniryhmälle

| * | 1 | -1 | i | -i | j | -j | k | -k |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | -1 | i | -i | j | -j | k | -k |
| -1 | -1 | 1 | -i | i | -j | j | -k | k |
| i | | | | | | | | |
| -i | | | | | | | | |
| j | | | | | | | | |
| -j | | | | | | | | |
| k | | | | | | | | |
| -k | | | | | | | | |

Ykkösalkio kuuluu aina ryhmän keskukseen, joten keskus on epätyhjä. Huomaa myös, että Abelin ryhmälle pätee, että $Z(G) = G$.

**Tehtävä 21.** Osoita, että $Z(G) \lhd G$.

**Väite 1.** *Kertalukua kahdeksan olevan ryhmän keskus on epätriviaali.*

**Tehtävä 22.** Todista väite laskemalle näiden ryhmien keskus.

Olemme nyt luokitelleet kaikki ryhmät, joitten kertaluku on 8. Miten vaikeata olisi jatkaa vielä pidemmälle? Äskettäin Besche, Eick ja O'Brien luokittelivat kaikki ryhmät kertalukuun 2000 saakka. Tästä johtuen he kutsuivat projektiaan eräänlaiseksi Millennium-projektiksi.

**Määritelmä 3.26.** Ryhmää, jonka jokaisen alkion kertaluku on määrätyn alkuluvun $p$ potenssi, kutsutaan $p$-ryhmäksi. Tämä määritelmä on ekvivalentti sen kanssa, että äärellisen ryhmän kertaluku on $p^n$.

Heidän luokittelustaan seuraa, että suurin osa ryhmistä on 2-ryhmiä. Hankalin osa luokittelusta, oli laskea kaikki 49 487 365 422 ryhmää, joiden kertaluku on $2^{10}$. Muita ryhmiä, joiden kertaluku on alle 2000, oli tämän jälkeen jäljellä vain 423 164 062.

Tämä taulukko on otettu artikkelista

The groups of order at most 2000 Hans Ulrich Besche; Bettina Eick; E. A. O'Brien Electron. Res. Announc. Amer. Math. Soc. 7 (2001), 1-4.

## 3.4 Arviot $p$-ryhmien lukumäärästä

Higman ja Sims jo kuusikymmenluvulla laskivat asymptoottisen arvion sille, miten monta $p$-ryhmää kertalukua $p^m$ on olemassa. Heidän arvionsa on, että

Taulukko 4: Kymmenen hankalinta kertalukua luokittelun kannalta

| Kertaluku | Lukumäärä |
|---|---:|
| $2^{10}$ | 49 487 365 422 |
| $2^9 \cdot 3$ | 408 641 062 |
| $2^9$ | 10 494 213 |
| $2^8 \cdot 5$ | 1 116 461 |
| $2^8 \cdot 3$ | 1 090 235 |
| $2^8 \cdot 7$ | 1 083 553 |
| $2^7 \cdot 3$ | 5 241 004 |
| $2^7 \cdot 3^2$ | 157 877 |
| $2^8$ | 56 092 |
| $2^6 \cdot 3^3$ | 47 937 |

kertalukua $p^m$ olevia ryhmiä on noin $p^{2m^3/27+O(m^{8/3})}$. Lisäksi on huomattava, että jos laskemme ryhmiä, joitten kertaluku on joku yhdistetty luku $n$, näiden lukumäärä riippuu $n$ alkulukuhajotelmasta. Jos $e(n)$ on suurin eksponentti alkulukuhajotelmassa, tiedämme Pyberin todistaneen, että kertalukua $n$ olevien ryhmien kokonaismäärä on enintään. $n^{(\frac{2}{27}+o(1))e(n)^2}$.

p-ryhmien luokittelu on avoin matemaattinen ongelma. Itseasiassa matemaatikot eivät edes haaveile lopullisesta luokittelusta, sillä näitä ryhmiä on yksinkertaisesti liikaa.