Ryhmäteoria

Pirita Paajanen
pirita.paajanen@helsinki.fi

26. marraskuuta 2008

Sisältö

1 Merkinnät

$\mathbb{N}$	luonnollisten lukujen joukko $\{0, 1, 2, \dots\}$
$\mathbb{Z}$	kokonaislukujen joukko, ääretön syklinen ryhmä
$\mathbb{Z}_p$	p-adiset kokonaisluvut, huom. ei äärellinen syklinen ryhmä!
$\mathbb{Z}_n$	merkintä, jota tällä kurssilla ei saa käyttää
C_n	n:n alkion syklinen ryhmä
V_4	Kleinin neliryhmä $\cong C_2 \times C_2$
S_n	n:n alkion symmetrinen ryhmä
A_n	alternoiva (vaihtuva) ryhmä
D_{2n}	diedriryhmä, n-kulmion symmetriaryhmä
Q_n	kvarternioniryhmä

2 Alkusanat

Ryhmäteoria voidaan tiivistää sanomalla, että se on symmetrioiden matemaattista tutkimista. Tällä ei tarkoiteta yksinomaan kadunmiehen käsitystä siitä, että joku esine on symmetrinen, jos sille voidaan piirtää symmetria-akseli niin, että kumpikin puoli näyttää toistensa peilikuvilta, kuten nyt esimerkiksi musteläikkätestin kuvat. Peilisymmetria on tietysti yksi symmetrian laji, mutta ei ainoa symmetriatyyppi. Esimerkiksi lumihiutale on symmetrinen. On totta, etta siinä on kuusi symmetria-akselia, joiden ympäri lumihiutale voidaan peilata itselleen, mutta koska lumihiutale on täydellinen säännöllinen kuusikulmio, on sillä myös kiertosymmetrioita, itseasiassa yhteensä kuusi kappaletta. Kuusi? Miten niin kuusi? Sitä voidaan kiertää $n \times \pi/3$ radiaania, $n = 1, \ldots 5, 6$, mutta $6\pi/3 = 2\pi$ eikä se oikeastaan ole kierto. Sovimme kuitenkin, että tämä on neutraalikierto, ja ekvivalentti sen kanssa, etta lumihiutale nostetaan tasosta (ja toivotaan ettei se sula tässä käsittelyssä) ja lasketaan tasolle samaan asentoon. Oikeastaan ryhmäteoria ei itsessään ole symmetrioita, vaan se kuvaa symmetrisiä toimintoja. Musteläikän tapauksessa, se kuvasi peilaustoimintaa. Ja lumihiutaleen tapauksessa nostoja ja kiertoja peilausten lisäksi. Ryhmäteoriassa ryhmä itse ja sen toiminnat – yllä olevassa tapauksessa kaksiuloitteisessa avaruudessa – ovat erottamattomasti yhteydessä toisiinsa. Kahdessa ulottuvuudessa ja toisinaan kolmessakin, pystymme vielä näkemään, ellemme itse ryhmää, ainakin sen toiminnat, esimerkiksi lineaarikuvaukset tasolla. Kun ulottuvuuksia on enemmän kuin kolme, on syytä turvautua algebralliseen merkintätapaan, sillä ihmismieli ei pysty enää hahmottamaan näitä symmetrioita geometrisesti. Symmetrioita on siis näkyviä että abstrakteja näkymättömiä. Vaikka ryhmäteoria tuntuisikin kuivalta algebralta, joka seuraa neljästä tylsästä aksioomasta, se ei ole sitä. Jotenkin ryhmäteoria on samantyyppinen kuin esimerkiksi elliptiset käyrät. Jostain syystä genus ykkösen käyrillä on tavattoman rikas teoria, jota ei ole muun genuksen käyrillä. Samaan tapaan myös monistot kolmessa ulottuvuudessa ovat valtavan paljon mielenkiintoisempia kuin monistot kahdessa, tai neljää korkeammissa ulottuvuuksissa. Ryhmillä on siis tarpeeksi rakennetta olla mielenkiintoisia tavalla, jota yhtäältä esimerkiksi puoliryhmät (joukko, jossa on liitännäinen operaatio) tai monoidi (joukko, jossa on liitännäinen operaatio sekä ykkösalkio) eivät ole. Yksinkertaisesti liian vähät aksioomat tuottavat tylsyyttä. Toisaalta kuntien teoria on hyvin paljon paremmin ymmärretty kuin ryhmien. Kunnan määritelmässä on enemmän aksioomia ja ne tuottavat rajoitetumpia rakenteita – vaikka on kunnissa myös hyvin villejä lukuteoreetikkojen tuottamia esimerkkejä. Toisaalta nämä villit kunnat tuottavat myös villejä ryhmiä, joten ehkä ryhmäteoreetikot olivat tässäkin yhteydessä asialla ensin. Tämä yhteys tulee tietysti Galois'n teorian kautta.

Tällä kurssilla saatamme päästä Galois'n teorian kautta tutkimaan proäärellisiä ryhmiä, jos osanottajat hallitsevat Galois'n teorian perusteet, mutta kuten jokaisella ryhmäteorian peruskurssilla, aloitamme pienistä äärellisistä ryhmistä ja erityisesti tutustumme esimerkkeihin, jotka ovat epäkommutatiivisia. Kun ryhmän kertaluku on pieni, seuraa näistä neljästä aksioomasta jo sangen helppo luokittelu ryhmille. Tutkimme tarkemmin kertalukua kuusi ja kahdeksan olevia ryhmiä. Toisinaan myös pelkkä kertaluku rajoittaa ryhmän rakennetta radikaalisti. Todistamme esimerkiksi, että pelkästään Sylowin lauseesta seuraa, että voi olla olemassa vain kaksi yksinkertaista (epäkommutatiivista) äärellistä ryhmää, joiden kertaluku on alle kolmesataa. Tavallaan ryhmäteorian hienous on siinä, että olioita voidaan luokitella.

Ryhmäteoria on edelleen hyvin aktiivinen matematiikan tutkimuksen ala, joka edelleen jakautuu useisiin alahaaroihin. Tällä kurssilla tutustumme muutamiin hyvin tuoreisiinkin tuloksiin (emme kuitenkaan yleisesti ottaen niiden todistuksiin, sillä kuten on lukuteorian tapauksessa, jotkut ryhmäteoreettiset lauseet on helppo esittää, mutta erittäin hankala todistaa). Opetuksen periaate ei ole kuivan teorian laajentaminen, vaan yritän tehdä ryhmäteoriaa eläväksi matematiikan alaksi. Sitä varten olen valinnut noin kymmenen suosikkiryhmääni. Ne ovat sangen konkreettisia esimerkkejä, joiden kautta voimme oppia teoriaa ja ymmärtää, miksi jokin teoreettinen määritelmä on hyödyllinen tai järkevä. Esimerkit on valittu hyvin erilaisilta matematiikan ja ryhmäteorian aloilta, jotta saamme hieman makua siitä, miten monipuolista ryhmäteoria on. Tarkastelemme myös ryhmäteorian yhteyksiä eri puolille puhdasta matematiikkaa.

Vaikka aloitamme äärellisistä ryhmistä, on hyvä pitää mielessä että äärelliset ryhmätkin voivat olla todella suuria. Jopa yksinkertaiset ryhmät, joita voidaan pitää kaikkien äärellisten ryhmien rakennuspalikoina, voivat olla valtavia. Suurin nk. sporadinen ryhmä tässä luokittelussa, jota myös Hirvióksi kutsutaan, on kertalukua $808017424794512875886459904961710757005754368000000000 = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$, mikä tarkoittaa ryhmän alkioiden määrää.

Yksinkertaiset ryhmät määrittelemme myöhemmin tällä kurssilla. Hirviön tarkempi määritelmä vaatisi kokonaisen kurssin. Palatkaamme siis alkeisiin.

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 2×2 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 $A \not\lhd C$. 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_iH. Jokainen sivuluokka on yhtäsuuri, ja koska H on itsessään sivuluokka, voimme olettaa, että $|g_iH| = |H|$ jokaiselle $g_i \in G$. Sivuluokat ovat erillisiä, mutta toisaalta myös kattavat G:n alkiot $\bigcup_i g_iH = G$. 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 $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$.

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 ϕ 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 kak-

si, 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.

4 Abelin ryhmät

Ensimmäisellä ryhmäteorian kurssilla käytiin läpi lähinnä syklisiä ryhmiä. Tällä kurssilla keskitymme epäkommutatiivisiin esimerkkeihin. On kuitenkin niin, että äärellisesti viritettyjen Abelin ryhmien teoria on syytä nähdä ainakin kerran elämässä ja se on suhteellisen helppo myös, joten käykäämme se tässä lyhyesti läpi. Tämän teorian perusteella saamme myös helposti luokiteltua loput ryhmät, joiden kertaluku on kahdeksan ja näemme, että nämä kolme ovat epäisomorfisia.

4.1 Suorat tulot ja summat

4.1.1 Ulkoinen suora tulo

Olkoot $G_1, \ldots, G_n$ ryhmiä. Muodostamme karteesisen tulon $G := G_1 \times G_2 \times \cdots \times G_n$ ja tälle joukolle määrittelemme kaksipaikkaisen operaation yksinkertaisesti $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$, eli jokaisessa komponentissa i tulo noudattaa ryhmän G_i tuloa.

Tehtävä 23. Todista, että tämä on ryhmä.

Kutsumme ryhmää $G = G_1 \times G_2 \times \cdots \times G_n$ ryhmien $G_1, \ldots, G_n$ (ulkoiseksi) suoraksi tuloksi. Huomaa, että komponenttien G_i järjestyksellä ei ole ryhmän määritelmässä mitään väliä.

Ryhmällä $G = G_1 \times G_2 \times \cdots \times G_n$ on seuraavat ominaisuudet

(i) Jokaista indeksiä i kohden, on olemassa $H_i \leq G$, ja $H_i \cong G_i$, eli

$$H_i = \{(1, \ldots, g_i, \ldots, 1) : g_i \in G_i\}.$$

Lisäksi huomaamme, että

$$G/H_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

(ii) Jokainen $g \in G$ voidaan kirjoittaa yksikäsitteisesti $g = h_1 \ldots h_n$, jossa jokainen $h_i \in H_i$. Eli jos $g = (g_1, \ldots, g_n)$, niin $h_i = (1, \ldots, g_i, \ldots, 1)$ jokaiselle i. Tästä seuraa, että jos jokainen G_i on äärellinen, niin $|G| = |G_1||G_2| \ldots |G_n|$.

Tämä konstruktio toimii mille tahansa ryhmille G_i.

4.1.2 Sisäinen suora tulo

Olettakaamme nyt vuorostamme, että G on ryhmä, ja sillä on aliryhmät $H_1, \ldots, H_n$ ja niillä ominaisuudet.

(i) $H_i \lhd G$, kaikille $i = 1, \ldots, n$.

(ii) Jokainen $g \in G$ voidaan yksikäsitteisesti kirjoittaa muodossa $g = h_1 \ldots h_n$, jossa jokainen $h_i \in H_i$

Huomaamme, että näistä kahdesta seuraa

(iii) $G = H_1 \ldots H_n$.

(iv) $H_i \bigcap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n = 1$ jokaiselle indeksille i.

(v) Jos $i \neq j$, silloin H_i:n ja H_j:n alkiot kommutoivat keskenään.

(vi) Jos $g = h_1 \ldots h_n$ ja $g' = h'_1 \ldots h'_n$, jossa $h_i, h'_i \in H_i$ jokaiselle i:lle, silloin $gg' = (h_1 h'_1) \ldots (h_n h'_n)$.

Huomaamme, että voimme määritellä yksikäsitteisen isomorfismin $\tau : G \longrightarrow H_1 \times H_2 \times \cdots \times H_n$, jossa siis jokainen $H_i \mapsto 1 \times \cdots \times H_i \times \cdots \times 1$.

Kutsumme tällöin ryhmää G:tä aliryhmiensä $H_1, \ldots, H_n$ (sisäiseksi) suoraksi tuloksi. Toisinaan merkitsemme myös $G = H_1 \times H_2 \times \cdots \times H_n$, vaikka tämä onkin lievää merkintätavan väärinkäyttöä.

Tästä seuraa lause

Lause 4.1 (Kiinalainen jäännösluokkalause)**.** *Olkoon* $n = p_1^{k_1} \cdots p_m^{k_m}$. *Silloin*

$$C_n \cong C_{p_1^{k_1}} \times \cdots \times C_{p_m^{k_m}}.$$

Todistus. Määritellään kaikille $1 \leq i \leq m$ ryhmä $P_i = \langle x_i \rangle \cong C_{p_i^{m_i}}$. Nyt alkion $(x_1, \ldots, x_n) \in P_1 \times \cdots \times P_m$ kertaluku on $p_1^{k_1} \times \cdots \times p_m^{k_m} = n$, joten $P_1 \times \cdots \times P_m \cong C_n$, koska ryhmä on syklinen. □

Korollaari 4.2. *Jos* $m = pq$, *kahden erillisen alkuluvun tulo, on* $C_m \cong C_p \times C_q$.

Esimerkiksi totesimme kertalukua kuusi olevien ryhmien luokittelussa, että $C_6 \cong C_2 \times C_3$.

Huomaa, että tämä on sama kiinalainen jäännösluokkalause kuin alkeellisessa lukuteoriassa.

Olkoot $n_1, \ldots, n_k$ pareittain suhteellisia alkulukuja. Silloin mille tahansa kokonaisluvuille $a_1, \ldots, a_k$ on olemassa kokonaisluku x, joka toteuttaa kongruenssiyhtälöryhmän

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_k \mod n_k. \end{aligned}$$

Lisäksi kaikki ratkaisut x ovat kongruentteja modulo N, missä $N = n_1 n_2 \ldots n_k$.

Tämä siis syklisten ryhmien lauseessa todistaa, että kuvaus

$$C_n \longrightarrow C_{p_1^{k1}} \times \cdots \times C_{p_m^{km}}$$

on surjektiivinen.

Teoreeman julkaisi ensimmäisen kerran kiinalainen matemaatikko Sun Tzu kolmannella vuosisadalla. Alkuperäinen Sun Tsun ongelma kuuluu seuraavasti. Kuinka monta sotilasta on Han Xingin armeijassa? Jos sotilaat marssivat kolmen riveissä, kaksi sotilasta jää yli. Jos he marssivat viiden riveissä, kolme jää yli, ja jos he marssivat seitsemän riveissä, kaksi jää yli?

Ongelma voidaan ilmaista kongruenssiyhtälöryhmänä:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 2 \mod 7 \end{aligned}$$

Luvut 3, 5 ja 7 ovat pareittain keskenään jaottomia, joten voimme soveltaa kiinalaista jäännöslausetta.

Ensimmäisestä yhtälöstä saamme, että $x = 3t+2$, jollekin kokonaisluvulle t. Sijoitamme tämän toiseen yhtälöön ja saamme, $3t + 2 \equiv 3 \mod 5$. Tästä seuraa, että $t \equiv 2 \mod 5$, joten $t = 5u+2$, ja siis $x = 3(5u+2)+2 = 15u+8$, jonka voimme sijoittaa viimeiseen yhtälöön $15u + 8 \equiv 2 \mod 7$. Tämän kongruenssin ratkaisu on $u \equiv 1 \mod 7$, joten $u = 7v + 1$, mikä lopulta tuottaa vastauksen $x = 15(7v + 1) + 8 = 105 + 23$. Joten $x \equiv 23 \mod 105$. Sotilaiden määrä voi siis olla 23, 128, 233, 338 jne.

Tehtävä 24. Ratkaise ryhmä

$$\begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 6 \\ x &\equiv 3 \mod 7. \end{aligned}$$

Kiinalainen jäännösluokkalause ei kuitenkaan auta Abelin ryhmien luokittelussa kovinkaan pitkälle, sillä tiedämme esimerkiksi, että kaikki äärelliset Abelin ryhmät eivät ole muotoa C_{p^n}, esimerkiksi $C_4 \ncong C_2 \times C_2$. On siis kaksi äärellistä Abelin ryhmää, joiden kertaluku on neljä.

Miten tästä eteenpäin luokittelun kanssa?

4.2 Ryhmän virittäjät

Syklinen ryhmässä C_n on alkio g, jonka kertaluku on n ja $C_n = \langle g \rangle$. Kutsumme alkiota g ryhmän C_n virittäjiksi. Voimme yleistää virittäjän käsitettä useampiin virittäjiin.

Määritelmä 4.3. Olkoon S ryhmän G osajoukko. Joukon S virittämä aliryhmä on

$$\langle S \rangle := \bigcap_{S \subset H \leq G} H.$$

Jos $\langle S \rangle = G$, kutsumme joukon S alkioita ryhmän G virittäjiksi tai generaattoreiksi. Jos virittäjäjoukko on äärellinen, kutsutaan ryhmää G äärellisesti viritetyksi.

Propositio 4.4. *Ryhmän G osajoukon S virittämä aliryhmä koostuu kaikista tuloista*

$$\langle S \rangle = \{ s_1^{e_1} s_2^{e_2} \dots s_l^{e_l} : s_i \in S, e_i = \pm 1, l = 1, 2, \dots \},$$

jos $l = 0$, määrittelemme tyhjäksi tuloksi ykkösalkion.

Todistus. Merkitään yhtälön oikeanpuoleista joukkoa H:lla. $S \subseteq H$ ja koska $H \leq G$, saamme $\langle S \rangle \subseteq H$. Toisaalta, jos M on mikä tahansa aliryhmä, joka sisältää joukon S, niin sisältää aliryhmä M kaikki tulot, jotka saadaan muodostettua joukosta S, joten $H \leq M$, kaikille $S \subseteq M \leq G$. Niinpä

$$H \subseteq \bigcap_{S \subset M \leq G} H = \langle S \rangle.$$

□

Esimerkki 4.5. Alkiot r ja a virittivät edellisen luvun esimerkissä ryhmän D_8. Ryhmä D_8 on siis kahden alkion virittämä.

Huomaa, että ryhmällä voi olla monta virittäjäjoukkoa. Virittäjäjoukkoa kutsutaan minimaaliseksi, jos jonkun alkion poisto tarkoittaa sitä, että ryhmä ei enää virity. Myöskään minimaalinen virittäjäjoukko ei ole yksikäsitteinen. Minimaalinen ei tarkoita, että alkioitten määrä olisi minimaalinen.

Tehtävä 25. (i) Mitkä alkiot virittävät äärettömän syklisen ryhmän $\mathbb{Z}$?

(ii) Etsi ryhmän S_3 minimaaliset virittäjäjoukot.

(iii) Osoita, että kumpikin joukko $(12), (13), (14)$ ja $(12), (1234)$ ovat ryhmän S_4 minimaalinen virittäjäjoukko. Löydätkö vielä lisää minimaalisia virittäjäjoukkoja? Yleistä tulos koskemaan kaikkia ryhmiä S_n.

4.3 Vapaa Abelin ryhmä

Olkoon $\mathbb{G}$ ryhmäluokka (esimerkiksi kaikki ryhmät, Abelin ryhmät, ratkeavat ryhmät, äärelliset ryhmät). Olkoon G mikä tahansa ryhmä luokassa $\mathbb{G}$, joka on joukon $\{a_i : i \in I\}$ virittämä. Ryhmää $F := \langle x_i : i \in I\rangle$ kutsutaan vapaaksi luokassa $\mathbb{G}$ jos jokainen virittäjäkuvaus $x_i \mapsto a_i$ laajenee ryhmähomomorfismiksi $F \longrightarrow G$. Toisinaan ryhmää F kutsutaan myös joukon $\{x_i : i \in I\}$ vapaasti virittämäksi. Indeksijoukon I mahtavuutta kutsutaan vapaan ryhmän rankiksi. Rankki voi olla äärellinen tai ääretön.

Intuitiivisesti ajatellen vapaa ryhmä on siis sellainen ryhmä, jossa ei ole yhtään relaatioita virittäjien välillä. Koska jos, sanokaamme $x_1x_2 = 1$ ryhmässä F, voi olla, että kuvaus $x_i \mapsto a_i$ ei ole homomorfismi, jos ryhmässä G $a_1a_2 \neq 1$.

Kaikki ryhmäluokat eivät sisällä vapaata ryhmää. Kaikkien ryhmien luokka sisältää vapaan ryhmän, jota käsittelemme myöhemmin tällä kurssilla. Myös Abelin ryhmät sisältävät vapaan ryhmän. Abelin ryhmissä yleensä käytetään additiivista merkintätapaa. Siksi yleensä merkitsemme ääretöntä syklistä ryhmää nimellä $\mathbb{Z}$, emmekä C_∞. Edellä käsitellyt suorat tulot ymmärretään tällä merkintätavalla suoriksi summiksi. Huomaa, että additiivisessa merkinnässä g^n on muodossa ng, ja jokaista suoran summan alkiot merkitään $a = \sum n_k a_k$, eikä $(a_1^{n_1}, \ldots, a_k^{n_k})$.

Lemma 4.6. *Olkoon G Abelin ryhmä. Oletamme, että tekijäryhmä G/N hajoaa äärettömien syklisten ryhmien suoraksi summaksi*

$$G/N = \bigoplus_{i\in I}(A_i/N),$$

$A_i = \langle a_i + N\rangle$. Silloin G on aliryhmiensä N ja $A = \langle a_i : i \in I\rangle$ suora summa.

Todistus. Ensiksikin huomaamme, että $G = N + A$. Oletetaan ristiriitaa varten, että $A \bigcap N$:ssa on epätriviaali alkio a. Tällöin $a = \sum n_k a_{i_k}$, koska tämä alkio kuuluu A:n. Kun siirrytään tekijäryhmään G/N saadaan

$$N = a + N = \sum(n_k a_{i_k} + N),$$

(koska $a \in N$) ja nyt seuraa suoran summan määritelmästä, että $n_k a_{i_k} + N = N$ kaikilla k. Koska A_{i_k}/N on ääretön syklinen ryhmä, tästä seuraa, että jokainen $n_k = 0$, mutta silloin $a = 0$, mikä on vaadittu ristiriita. □

Lause 4.7. *Abelin ryhmien luokassa vapaat ryhmät ovat täsmälleen äärettömien syklisten ryhmien suoria summia.*

Todistus. Olkoon $G = \bigoplus_{i \in I} \langle x_i \rangle$ äärettömien syklisten ryhmien $\langle x_i \rangle$ suora summa, ja olkoon A mikä tahansa ryhmä, jonka virittäjät ovat $a_i, i \in I$. Nyt voimme luonnollisella tavalla laajentaa virittäjäkuvauksen $x_i \mapsto a_i$ ryhmäepimorfismiksi $\sum n_k x_{i_k} \mapsto \sum n_k a_{i_k}$. Olemme siis todistaneet, että G on vapaa Abelin ryhmä, jonka rankki on äärettömien syklisten ryhmien määrä.

Olkoon G nyt vapaa Abelin ryhmä ja $\{x_i : i \in I\}$ vapaa virittäjäjoukko tälle ryhmälle. Vapaan ryhmän määritelmän mukaan, on olemassa epimorfismi τ ryhmästä F äärettömien syklisten ryhmien suoraan summaan $A = \bigoplus_{i \in I} \langle a_i \rangle$, joka laajentaa virittäjäkuvauksen $x_i \mapsto a_i$ ryhmäepimorfismiksi. Ensimmäisen isomorfialauseen perusteella $F/N \cong A$, jossa $N = Ker(\tau)$, joten tekijäryhmä F/N hajoaa (i.e. on sisäisesti isomorfinen) äärettömien syklisten ryhmien $\langle x_i + N \rangle, i \in I$ suoraksi summaksi. Edellisen lemman perusteella $F = N \bigoplus B$, jossa $B = \langle x_i : i \in I \rangle$. Kuitenkin aliryhmä B on saman joukon $\{x_i : i \in I\}$ virittämä kuin F, joten homomorfismin τ ytimen N pitää olla nolla, joten homomorfismi τ olikin isomorfismi. □

Tämä todistus myös osoittaa, että vapaan Abelin ryhmän rankki ei riipu ryhmän kannasta. Ryhmän rankki riippuu vain siitä, miten monen äärettömän syklisen ryhmän suora summa vapaa Abelin ryhmä on.

4.4 Äärellisesti viritetyt Abelin ryhmät

Lause 4.8 (Abelin ryhmien peruslause)**.** *Olkoon F_n vapaa Abelin ryhmä, jonka rankki n on äärellinen, ja olkoon $0 \neq A \leq F_n$. Silloin A on vapaa, ja ryhmillä A ja F_n on kannat $\{a_1, \ldots, a_k\}$ ja $\{f_1, \ldots, f_n\}$, joilla on seuraavat ominaisuudet: $k \leq n$, $a_i = m_i f_i$ kaikille $1 \leq i \leq k$ ja m_i jakaa m_{i+1}:n, kun $1 \leq i \leq k-1$.*

Todistus. Todistus on induktio ryhmän F_n rankin suhteen. Jos $n = 1$, on ryhmä syklinen ja isomorfinen $\mathbb{Z}$:n kanssa, joten väite on tosi. Olkoon $n > 1$. Oletetaan nyt, että väite on totta vapaille Abelin ryhmille, joiden rankki on $n - 1$.

Huomaamme ensin, että jos $\{x_1, \ldots, x_n\}$ on mikä tahansa ryhmän F_n (järjestetty) kanta, ja a mikä tahansa F_n:n alkio, silloin on olemassa yksikäsitteinen kokonaislukujen ännäkkö $(t_1, \ldots, t_n)$, joka määrittää

$$a = t_1 x_1 + \cdots + t_n x_n,$$

tämän kannan suhteen.

Valitaan nyt joku kanta ja $a_1 \in A$, siten että, tämän kannan ännäkön ensimmäinen kerroin on positiivinen ja pienin mahdollinen, kutsutaan tätä nimellä m_1. Merkitään tätä uutta kantaa $\{b_1, \ldots, b_n\}$, joten

$$a_1 = m_1 b_1 + t_2 b_2 + \cdots + t_n b_n.$$

Haluamme todistaa, että m_1 jakaa kaikki kertoimet t_i. Jakoyhtälön perusteella, voimme kirjoittaa $t_i = q_i m_1 + r_i, (0 \leq r_i < m_1)$. Määritellään uusi kanta

$$\{f_1 = b_1 + q_2 b_2 + \cdots + q_n b_n, b_2, \ldots, b_n\}. \tag{1}$$

Tämän kannan suhteen $a_1 = m_1 f_1 + r_2 b_2 + \cdots + r_n b_n$. Koska olimme valinneet m_1:n minimaaliseksi, jokainen $r_i = 0$. Niinpä $a_1 = m_1 f_1$.

Kirjoitetaan $B = A \bigcap F_{n-1}$, jossa $F_{n-1} = \langle b_2, \ldots, b_n \rangle$. Aiomme todistaa, että A on aliryhmiensä $\langle a_1 \rangle$ ja B:n suora summa. Koska $\langle a_1 \rangle \bigcap B = 0$, riittää todistaa, että $A = a_i + B$. Jos $a = mf_1 + b \in A$ missä $b \in F_{n-1}$ ja taas jakoyhtäkön perusteella $m = qm_1 + r, (0 \leq r < m_1)$. Tarkastelemme alkiota $a - qa_1 = mf_1 + b - qa_1 = (qm_1 + r)f_1 + b - q(m_1 f_1) = rf_1 + b \in A$, joten sillä on esitys kannassa (1). Jakoyhtäkön perusteella kanta-alkion f_1 kerroin on $r < m_1$, joten $r = 0$. Tästä seuraa, että $b = a - qa_1 \in A$ ja $b \in B$. Koska a oli mielivaltainen A:n alkio, saamme

$$A = \langle a_1 \rangle \oplus B.$$

Induktiivisen hypoteesin perusteella aliryhmällä B ja ryhmällä F_{n-1} on kannat $\{a_2, \ldots a_k\}$ ja $\{f_2, \ldots, f_n\}$, missä $k \leq n$, $a_i = m_i f_i, (2 \leq i \leq k)$ ja $m_i \mid m_{i+1}$ kaikille $2 \leq i < k$. Luonnollisesti joukot $\{a_1, \ldots, a_n\}$ ja $\{f_1, \ldots, f_n\}$ ovat kannat ryhmille A ja F_n. Jotta nämä kannat toteuttavat halutut ominaisuudet, riittää todistaa, että $m_1 \mid m_2$.

Olkoon $m_2 = \hat{q} m_1 + \hat{r}$, $0 \leq r < m_1$. Jos kirjoitamme alkion $a_2 - a_1 \in A$ uuden kannan $\{\hat{q} f_2 - f_1, f_2, \ldots, f_n\}$ mukaisesti, saamme

$$a_2 - a_1 = m_1(\hat{q} f_2 - f_1) + \hat{r} f_2.$$

Koska f_2:n kerroin on $\hat{r} < m_1$, voimme päätellä, kuten aina ennenkin, että $\hat{r} = 0$, joten $m_1 \mid m_2$, kuten vaadittua. □

Lause 4.9. *Jokainen äärellisesti viritetty Abelin ryhmä on syklisten aliryhmien suora summa. Eli se voidaan kirjoittaa muotoon*

$$A = C_{m_1} \bigoplus C_{m_2} \bigoplus \cdots \bigoplus C_{m_k} \bigoplus \mathbb{Z} \bigoplus \mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z},$$

jossa $1 < m_1 \mid m_2 \mid m_3 \mid \cdots \mid m_k \neq 0$. Hajotelmassa m_i:t on määritelty yksikäsitteisesti, kuten myös äärettömien syklisten ryhmien $\mathbb{Z}$ määrä, jota kutsutaan äärettömän Abelin ryhmän torsio-vapaaksi rankiksi..

Todistus. Olkoon G äärellisesti viritetty Abelin ryhmä, jonka virittää n alkiota. Silloin G on isomorfinen jonkun vapaan ryhmän F_n tekijäryhmän F_n/A kanssa. Edellisen lauseen perusteella, ryhmät F_n ja A sisältävät kannat $f_1, \ldots, f_n$ ja $a_1, \ldots, a_k$, jolle pätee $a_i = m_i f_i$ kaikille $1 \leq i \leq k$. Koska $G \cong F_n/A$, lauseen todistukseen riittää osoittaa, että F_n/A on syklisten aliryhmiensä $< f_i + A >$ suora summa.

Ensiksikin, on selvää, että F_n/A on aliryhmien $< f_i + A >$ virittämä. Seuraavaksi oletamme, että nolla-alkio tekijäryhmässä F_n/A voidaan kirjoittaa muotoon $A = l_1 f_1 + \cdots + l_n f_n + A$. Tästä seuraa, että $l_1 f_1 + \cdots + l_n f_n = a \in A$. Kun kirjoitamme alkion a ylläolevan A:n kannan mukaan ja käytämme yhtälöä $a_i = m_i f_i$, voimme kirjoittaa seuraavat yhtälöt

$$l_1 f_1 + \cdots + l_n f_n = s_1 a_1 + \cdots + s_k a_k = s_1 m_1 f_1 + \cdots + s_k m_k f_k.$$

Koska jokainen alkio voidaan esittää yksikäsitteisesti vapaitten generaattorien f_i avulla, saamme, että $l_i = s_i m_i$ $(1 \leq i \leq k), l_j = 0, k < j \leq n$.

Tämä kuitenkin tarkoittaa, että kaikki alkiot $l_i f_i$ kuuluvat A:n, eli $l_i f_i + A = A$. Tämä antaa vaaditun yksikäsitteisyyden nolla-alkion esitykselle aliryhmän $< f_i + A >$ alkioitten summana. □

Esimerkki 4.10. Kuinka monta Abelin ryhmää on, joiden kertaluku on $243 = 3^5$? Abelin ryhmien peruslauseen nojalla, kukin tällainen ryhmä $A = C_{d_1} \bigoplus \cdots \bigoplus C_{d_k}$, missä $d_1 \mid d_2 \mid \cdots \mid d_k$ ja $d_1 d_2 \ldots d_k = 3^5$. Vaihtoehdot ovat

$$\begin{aligned}
C_3 \bigoplus C_3 \bigoplus C_3 \bigoplus C_3 \bigoplus C_3 \\
C_3 \bigoplus C_3 \bigoplus C_3 \bigoplus C_9 \\
C_3 \bigoplus C_9 \bigoplus C_9 \\
C_3 \bigoplus C_3 \bigoplus C_{27} \\
C_9 \bigoplus C_{27} \\
C_3 \bigoplus C_{81} \\
C_{243}
\end{aligned}$$

Ryhmiä on siis täsmälleen yhtä paljon kuin luvun 5 osituksia.

Tehtävä 26.

1. Luokittele Abelin ryhmät, joiden koko on 60.
2. Kuinka monta Abelin ryhmää on, joiden koko on 17^7?
3. Kuinka monta Abelin ryhmää on, joiden koko on 2^{10}?

4.5 Vapaitten Abelin ryhmien aliryhmät

Äärettömällä syklisellä ryhmällä $\mathbb{Z}$ on vain yksi aliryhmä kutakin äärellistä indeksiä n, eli tietysti $n\mathbb{Z}$. Kuinka monta aliryhmää on $\mathbb{Z}^2$:ssa? Luokittelu ei äärettömien ryhmien tapauksessa ole järkevää, tai mahdollista. Äärellisesti viritetyissä ryhmissä voimme kuitenkin laskea aliryhmien määrän indeksin mukaan.

Määritelmä 4.11. Määritellään funktio $a_n(G)$ kirjoittamaan muistiin niiden aliryhmien määrä, joiden indeksi on täsmälleen n.

Esimerkki 4.12. Ylläolevan nojalla $a_n(\mathbb{Z}) = 1$ kaikille $n \geq 1$, koska jokaista indeksiä kohden on täsmälleen yksi aliryhmä.

Tarkastelemme $\mathbb{Z} \bigoplus \mathbb{Z}$:n aliryhmiä. Kuinka monta niitä on kutakin indeksiä n? Ensimmäinen epätriviaalitapaus on indeksi 2. Ainakin $2\mathbb{Z} \bigoplus \mathbb{Z}$ ja $\mathbb{Z} \bigoplus 2\mathbb{Z}$ ovat kumpainenkin indeksiltään kaksi. Onko muita? Itseasiassa on vielä kolmas aliryhmä, jonka indeksi on kaksi. Huomaa nimittäin, että suoran summan (tai tulon) kaikki aliryhmät eivät ole yksinkertaisesti pelkästään jommankumman komponentin aliryhmiä. Muistamme, että esimerkissä $C_2 \times C_2$ löysimme yhteensä kolme aliryhmää, jotka olivat indeksiltään kaksi ja isomorfisia C_2:n kanssa, eli $(1,0), (0,1), (1,1)$ generoimat aliryhmät. Vain kaksi ensimmäistä saadan suoraan komponenttien aliryhmänä. Tarvitsemme järeämpiä työkaluja.

Ensiksikin olemme todistaneet Lauseessa 4.8, että jos A on vapaan Abelin ryhmän F_k aliryhmä, on A:n kanta on rankiltaan pienempi tai yhtäsuuri kuin k. Eli tässä tapauksessa $\mathbb{Z} \bigoplus \mathbb{Z}$:n aliryhmän virittää korkeintaan kaksi alkiota. Koska tarkastelemme aliryhmiä, joiden indeksi on äärellinen luku n, huomaamme, että yhden alkion virittämä aliryhmä ei kelpaa, sillä sen tekijäryhmä on ääretön, $\mathbb{Z} \bigoplus \mathbb{Z}/m\mathbb{Z}$ ja näin ollen myös indeksi on ääretön. Äärellistä indeksiä olevan aliryhmän tulee siis kahden alkion virittämä.

Voimme esittää tämän kannan 2×2-matriisin lineaarisesti riippumattomina riveinä (ajattele taas vektoriavaruuksia ja aliavaruuksia), joten ongelma kutistuu matriisien laskemiseen joukossa $\mathbb{M}_2(\mathbb{Z})$. On toisaalta mahdollista, että kaksi matriisia M ja N virittävät saman aliryhmän, mutta eri kannassa. Tämä tapahtuu täsmälleen silloin kun voimme riviredusoita (vastaa kannan vaihtoa) kummankin matriisin samaksi yläkolmiomatriisiksi. Huomaa, että riviredusoinnissa $\mathbb{Z}$:n yli saa kertoa matriisin rivin vain ± 1:llä (tämä on edelleen kanta), vaihtaa rivien järjestystä (uudelleenjärjestää kannan) ja lisätä kokonaisluku-kertaa rivin toiseen riviin (osoita, että tämäkin on kanta). Kaikki nämä operaatiot pitävät matriisin determinantin vakiona, ja matriisin determinantti määrää täsmälleen aliryhmän indeksin. Näillä operaatioilla

(erityisesti jakoyhtälöä käyttämällä), kukin matriisi saadaan yläkolmiomuotoon

$$\begin{pmatrix} m_{11} & m_{12} \\ 0 & m_{22} \end{pmatrix},$$

missä $0 \leq m_{12} < m_{22}$. Joten tällaiset yläkolmiomatriisit siis esittävät kunkin aliryhmän yksikäsitteisesti. Tällaisen matriisin determinantti on tietysti $m_{11}m_{22}$, joten indeksiä kaksi olevat aliryhmät ovat sellaisia, joissa $m_{11}m_{22} = 2$. Jos valitsemme $m_1 1 = 1$, niin $m_{22} = 2$, mikä jättää alkiolle m_{12} kaksi vaihtoehtoa. Jos $m_{11} = 2$ ja $m_{22} = 1$, on $m_{12} = 0$, joten on vain yksi vaihtoehto. Yhteensä on kolme vaihtoehtoa.

Yleisemmin saamme kertoimeksi $a_n(n) = \sigma(n)$.

Määritelmä 4.13. Olkoon n luonnollinen luku. Määrittelemme funktion $\sigma(n)$ laskemaan niiden luonnollisten lukujen summan, jotka jakavat luvun n. Esimerkiksi $\sigma(p) = p + 1$ kaikille alkuluvuille p ja $\sigma(p^n) = 1 + p + \cdots + p^n$. Toisaalta $\sigma(6) = 1 + 2 + 3 + 6 = 10$.

Tehtävä 27. Osoita, että σ on multiplikatiivinen, eli jos $(n, m) = 1$, silloin $\sigma(nm) = \sigma(n)\sigma(m)$.

Tehtävä 28. Numeroimalla sopivat kaksi kertaa kaksi yläkolmiomatriisit, todista, että ryhmälle $\mathbb{Z} \bigoplus \mathbb{Z}$, funktio $a_n(n) = \sigma(n)$. Helpointa on varmastikin lähteä pienistä erikoistapauksista liikkeelle.

4.5.1 Esseen aihe

Jos haluamme laskea aliryhmiä yleisemmin $\mathbb{Z}^d$:ssä, on hyödyllistä määritellä generoiva funktio

$$\zeta_{\mathbb{Z}^d}(s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

missä kertoimet a_n ovat kuten määritelmässä 4.11, ja $s \in \mathbb{C}$. Tämä voidaan aluksi mieltää formaalina summana, mutta itseasiassa Abelin ryhmille tämä funktio suppenee aina kun $\Re(s) > d$.

Esimerkki 4.14. Laskujemme nojalla

$$\zeta_{\mathbb{Z}}(s) = \sum_{n=1}^{\infty} n^{-s} = \zeta(s),$$

joka on siis Riemannin zeeta-funktio. Toisaalta

$$\zeta_{\mathbb{Z}^2}(s) = \sum_{n=1}^{\infty} \sigma(n) n^{-s} = \zeta(s)\zeta(s-1).$$

Todista, että

$$\zeta_{\mathbb{Z}^d}(s) = \zeta(s)\zeta(s-1)\dots\zeta(s-(d-1)).$$

Tälle tulokselle on ainakin viisi todistusta. Osoita myös, että tällä funktiolla on Eulerin tulo, sekä ryhmäteoreettisesti, että lukuteoreettisesti. Määrittele aliryhmäin kasvu ja sen indeksi. Lähteeksi sopii esim. du Sautoy, The quest for order vs flight from ennui. Artikkelin löytää verkosta sivulta www.maths.ox.ac.uk/ dusautoy/newright.htm valikosta Preprints.

5 Platonin kappaleet ja niiden symmetriaryhmät

Ensimmäisissä luvussa käsittelimme ryhmäteorian peruskonsepteja niin kuin ne on 1800- ja 1900-luvuilla määritelty. Nyt palaamme ajassa taaksepäin, ja tutkimme, mitä antiikin kreikkalaiset tiesivät symmetriasta.

Pythagoras tunsi kolme säännöllistä kolmiulotteista kappaletta. Kuutio ja tetraedri olivat hyvin tuttuja, ja näiden perusteella hän myöhemmin konstruoi myos dodekaedrin.

Platon tai hänen oppilaansa lisäsivät joukkoon oktaedrin ja ikosaedrin, sekä todistivat, että nämä ovat ainoat säännölliset monitahokkaat kolmessa ulottuvuudessa. On tavallaan mielenkiintoista, että Pythagoras ei konstruoinut oktaedria, sillä se on kuitenkin kuution duaalikappale.

Määritelmä 5.1. Platonin kappale on säännöllinen monitahokas, jonka tahkot ovat keskenään yhteneviä säännöllisiä monikulmioita, ja jonka jokaisesta kärjestä lähtee yhtä monta särmää.

Lause 5.2. *Platonin kappaleita on korkeintaan viisi.*

Todistus. Oletetaan, että säännöllinen monikulmio on n-kulmio, ja jokaisesta kärjestä lähtee k särmää. Todistamme, että mahdollisia pareja (n, k) on korkeintaan viisi.

Merkitään säännöllisen n-kulmion sisäkulmaa α:lla, ja tämän komplementtikulmaa β:lla. Tällöin $\beta = \frac{2\pi}{n}$, joten $\alpha = \pi - \beta = \pi(1 - \frac{2}{n})$.

Jokaisesta kärjestä lähtee k särmää. Koska nämä särmät eivät kohtaa tasossa, saamme epäyhtälön $k\alpha < 2\pi$, josta seuraa

$$k\pi(1 - \frac{2}{n}) < 2\pi$$

$$k(n-2) < 2n$$

$$(k-2)(n-2) < 4.$$

Koska monitahokas on kolmiulotteinen, $k, n \geq 3$. Ainoat kokonaislukuparit (n, k), jotka toteuttavat ylläolevan epäyhtälön ovat $(3,3), (3,4), (4,3), (3,5), (5,3)$. □

Merkitään K monitahokkaan kärkien määrää, S särmien lukumäärää ja T tahkojen lukumäärää. Kokoamme taulukkoon ylläolevat viisi lukuparia, sekä kärkien, särmien ja tahkojen määrä kullekin monitahokkaalle.

Taulukko 5: Platonin kappaleet

nimi	K	S	T	n	k
tetraedri	4	6	4	3	3
kuutio	8	12	6	4	3
oktaedri	6	12	8	3	4
dodekaedri	20	30	12	5	3
ikosaedri	12	30	20	3	5

Huomautus 5.3. Platonin kappaleet toteuttavat Eulerin kaavan $K - S + T = 2$. Tämän näkee helpohkosti projisoimalla kunkin kappaleen tasoon planaariverkoksi.

Koska Platonin kappaleet elävät kolmiuloitteisessa avaruudessa on niiden symmetriaryhmä äärellinen $\mathrm{GL}_3(\mathbb{R})$:n aliryhmä. Symmetriaryhmä ei myöskään saa muuttaa etäisyyksiä joten ainoastaan alkiot, joiden determinantti on ± 1 kelpaavat. Jos rajoitamme etsintämme vain kiertosymmetrioihin, voimme tutkia vain $\mathrm{SL}_3(\mathbb{R})$:n äärellisiä aliryhmiin. Helpoiten hahmotamme nämä ryhmät kuitenkin ryhmän toimintojen ja ratojen avulla kuten alkusanoissa mainittiin. Joten ennen kuin pääsemme käsiksi ryhmiin, tarvitsemme lisää teoriaa. Jotkut teistä varmasti oppivat nämä asiat jo Algebra II:ssa, mutta kertaus ei liene pahitteeksi.

Esimerkkinä toiminnasta katsokaamme säännöllisiä monitahokkaita seuraavasta näkökulmasta. Huomaamme yleisesti, että mikä tahansa symmetria, jonka determinantti on 1, on kierto jonkun suoran L ympäri. Jos symmetria on epätriviaali, tämä suora L leikkaa Platonin kappaleen pinnan täsmälleen kahdessa pisteessä P ja Q. Mitä vaihtoehtoja on pisteelle P?

Oletetaan että P on jollain tietyllä sivutahkolla. Silloin se voi olla kärjessä, särmällä tai tahkon sisäpinnassa. Jos P on särmällä, mutta ei kärjessä, huomaamme ensin, että kiertosymmetria kiinnittää sekä pisteen P että särmän, jolla P sijaitsee, mutta se vaihtaa särmän päissä olevat kärjet (muussa tapauksessa symmetria ei ole kierto), joten P:n pitää olla särmän keskipisteessä.

Samalla tavalla voimme argumentoida, että jos P on tahkon sisäpinnalla, on sen pakko olla tahkon keskipisteessä.

Määritelmä 5.4. Olkoon G ryhmä ja Ω joukko. Ryhmä G toimii joukossa Ω, jos on olemassa kuvaus $\Omega \times G \to \Omega$, jossa $(\omega, g) \mapsto \omega * g$ joka toteuttaa seuraavat ehdot: (i)

$$\omega * 1 = \omega$$

(ii)
$$\omega * (gh) = (\omega * g) * h$$

Tätä kutsutaan vasemmaksi toiminnaksi, koska kohdassa (ii) vasemmanpuoleinen alkio toimii ensin. Oikeanpuoleinen toiminta määritellään vastaavalla tavalla.

Lemma 5.5. *Toimikoon G joukossa Ω. Tällöin jokainen $g \in G$ indusoi kuvauksen*

$$\begin{aligned} \phi_g : \quad & \Omega \to \Omega, \\ & \alpha \mapsto \alpha * g \end{aligned}$$

joka määrittää joukon Ω permutaation.

Tämän lisäksi, kuvaus

$$\begin{aligned} \phi : \quad & G \to Sym(\Omega) \\ & g \mapsto \phi_g \end{aligned}$$

on ryhmähomomorfismi. Tätä kutsutaan myös G:n permutaatioesitykseksi.[1]

Todistus. On selvää, että kuvauksen ϕ_g käänteiskuvaus on $\phi_{g^{-1}}$, koska jokaiselle $\alpha \in \Omega$ pätee

$$\alpha(\phi_g \phi_{g^{-1}}) = (\alpha * g) * g^{-1} = \alpha * g * g^{-1} = \alpha * 1 = \alpha.$$

Olemme todistaneet, että kuvaus $\phi_g : \Omega \to \Omega$ on bijektio, ja näin ollen se on permutaation määritelmän mukaan Ω:n permutaatio. Ryhmän toiminnan määritelmän kohdasta (i) seuraa, että

$$\phi(g_1 g_2) = \phi_{g_1 g_2} = \phi_{g_1} \phi_{g_2} = \phi(g_1)\phi(g_2),$$

joten $\phi : G \to Sym(\Omega)$ on homomorfismi. □

Tehtävä 29. 1. Olkoon G ryhmä, G toimii itsessään konjugaation kautta. Tarkemmin, kiinnitetään $h \in G$, nyt jokaiselle $g \in G$ toiminta määritellään $g \mapsto h^{-1}gh$ kautta. Osoita, että tämä on toiminta. Onko tämä vasen vai oikea? Jos haluamme määritellä vastakkaistoiminnan, mikä on oikea määritelmä?

[1] Permutaatioesitykset ovat tärkeitä esitysteoriassa. Valitettavasti tällä kurssilla meillä ei ole aikaa perehtyä ryhmien esitysteoriaan. Jos joku haluaa, voi tästä aiheesta laatia esseen.

2. Olkoon $\mathrm{GL}_n(\mathbb{R})$ kääntyvien $n \times n$-matriisien ryhmä. Määrittele $\mathrm{GL}_n(\mathbb{R})$:lle luonnollinen toiminta avaruudessa $\mathbb{R}^n$ ja osoita, että tämä on toiminta. Miten toimii ortogonaalisten matriisien ryhmä $O_n(\mathbb{R})$ avaruudessa $\mathbb{R}^n$.

3. G toimii omissa sivuluokissaan. Tarkemmin, olkoon $H \leq G$, ja olkoon $(G : H)$ oikeitten sivuluokkien joukko. Määrittelemme toiminnan

$$Hx * g = Hxg.$$

   Osoita, että tämä on toiminta.

4. Olkoon D_{2n} diedriryhmä. Osoita, että tämä toimii säännöllisen n-kulmion symmetriaryhmänä.

Monet ryhmäteorian lauseet on helppo todistaa toimintojen avulla. Tässä yksi esimerkki klassisesta lauseesta.

Lause 5.6 (Cayley)**.** *Jokainen äärellinen ryhmä G, jonka kertaluku on pienempi tai yhtäsuuri kuin n, on ryhmän S_n aliryhmä.*

Todistus. Jos $k \leq n$, on $S_k \leq S_n$. Todistukseen riittää, että oletamme G:n kertaluvun olevan tasan n. Nyt meidän täytyy enää osoittaa, että ryhmä, jonka kertaluku on n on symmetrisen ryhmän S_n aliryhmä. Voimme määritellä G-toiminnan triviaalin aliryhmän $\{1\}$ sivuluokissa. Näitä sivuluokkia on luonnollisesti n kappaletta ja ne vastaavat G:n alkioita. Yllä olevan lemman perusteella toiminta määrittelee homomorfismin $\phi : G \to S_n$. Homomorfismin ytimeen kuuluvat sellaiset G:n alkiot, jotka kiinnittävät jokaisen sivuluokan. Näin ollen vain ykkösalkio kuuluu ytimeen ja kuvaus ϕ on injektio. Tästä seuraa ensimmäisen isomorfialauseen perusteella

$$G \cong G/\{1\} \cong G/Ker\phi \cong Im\phi \leq S_n.$$

□

Olkoon $H \leq G$. Jos G toimii joukossa Ω, myös H määrittää toiminnan joukossa Ω. Tämä aliryhmän toiminta hajottaa joskus Ω:n palasiksi. Kutsumme tätä toimintaa H-toiminnaksi.

Määritelmä 5.7. Olkoon G ryhmä, ja toimikoon se joukossa Ω. Olkoon $H \leq G$. Kun $\omega \in \Omega$, silloin ω:n rata H-toiminnassa on

$$orb_H(\omega) = \{\omega * g : g \in H\}$$

Propositio 5.8. *Kun G toimii joukossa Ω ja $H \leq G$, joukko Ω hajoaa H-ratojen pistevieraaksi unioniksi.*

Todistus. Tehtävä. Käytiin luennolla läpi. □

Määritelmä 5.9. Kutsumme ryhmän G toimintaa joukossa Ω transitiiviseksi, jos jokaiselle $\omega_1, \omega_2 \in \Omega$, on olemassa $g \in G$ ja $\omega_1 * g = \omega_2$.

Jos jokaiselle parille pätee sama kuin yllä, kutsumme toimintaa 2-transitiiviseksi, ja edelleen n-transitiiviseksi.

Määritelmä 5.10. Toimikoon ryhmä G joukossa Ω, ja olkoon $\omega \in \Omega$. Alkion ω vakauttaja on joukko

$$G_\omega = \{g \in G : \omega * g = \omega\}.$$

Määritelmä 5.11. Ryhmän G toimintaa joukossa Ω kutsutaan uskolliseksi, jos ainoa alkio $g \in G$, jolle pätee $\omega * g = \omega$ kaikille $\omega \in \Omega$ on $g = 1$.

Tehtävä 30.

1. Osoita, että G_ω on G:n aliryhmä.

2. Olkoon $\omega = \alpha * g$, kun G toimii Ω:ssa. Osoita, että G_ω ja G_α ovat toistensa konjugaatteja.

3. Toimikoon G joukossa $\Omega = G$ konjugoimalla. Osoita, että alkion ω vakauttaja on alkion keskittäjä.

4. Osoita, että G:n toiminta oikeissa sivuluokissaan on transitiivinen, ja määrittele sivuluokkien H ja Hg vakauttajat.

Määritelmä 5.12. Toiminnan ydin on $G_{(\Omega)} = \cap_{\alpha \in \Omega} G_\alpha$.

Tehtävä 31. Osoita, että toiminta on uskollinen, jos toiminnan ydin on triviaali.

Yksi hyödyllisimmistä lausesta ryhmäteoriassa on rata-vakauttajalause.

Lause 5.13. *Olkoon G äärellinen ryhmä ja Ω äärellinen joukko. Kun G toimii Ω:ssa, jokaiselle $\alpha \in \Omega$, on voimassa*

$$|Orb_G(\alpha)| = |G : Stab_G(\alpha)|.$$

Määritellään ensin morfismi kahden toiminnan välillä.

Määritelmä 5.14. Kun ryhmä G toimii joukoissa Ω ja Δ kuvaus

$$\psi : \Omega \longrightarrow \Delta$$

on G-morfismi, jos

$$(\alpha *_\Omega g)\psi = \alpha\psi *_\Delta g,$$

kaikille $\alpha \in \Omega, g \in G$. Kuvausta ψ kutsutaan G-isomorfismiksi, jos se on bijektiivinen.

Tämän jälkeen rata-vakauttajalause seuraa seuraavasta lemmasta.

Lemma 5.15. *Jos G toimii transitiivisesti Ω:ssa ja $\omega \in \Omega$. Pisteen ω vakauttajaa merkitään G_ω. Silloin G:n toiminta Ω:ssa ja G:n toiminta G_ω:n sivuluokissa $(G : G_\omega)$ ovat isomorfisia.*

Todistus. Määritellään kuvaus $\psi : \Omega \longrightarrow (G : G_\omega)$ lähettämällä $\omega x \mapsto G_\omega x$. Tämä kuvaus on hyvinmääritelty ja injektiivinen, sillä

$$\omega x_1 = \omega x_2 \Leftrightarrow \omega x_1 x_2^{-1} = \omega \Leftrightarrow x_1 x_2^{-1} \in G_\omega \Leftrightarrow G_\omega x_1 = G_\omega x_2.$$

Kuvaus on myös selvästi surjektiivinen. Lopuksi tarkistetaan, että se on G-morfismi:

$$((\omega x) * g)\psi = (\omega * xg)\psi = G_\omega xg = (G_\omega x)g = (\omega x)\psi * g$$

kaikille pisteille $\omega x \in \Omega$. □

Todistetaan nyt rata-vakauttajalause.

Todistus. Olkoon $\alpha \in \Omega$, ja toimikoon G joukossa $Orb_G(\alpha)$. Tämä toiminta on luonnollisesti transitiivinen, sillä mikä tahansa radan alkio αg_1 voidaan kuvata mihin tahansa toiseen saman radan alkioon αg_2:n käyttämällä alkiota $g_1^{-1} g_2$. Nyt edellisen lemman perusteella G:n toiminnat radalla $Orb_G(\alpha)$ ja G_α:n sivuluokissa ovat isomorfiset, joten näiden kahden joukon välillä on bijektiivinen kuvaus. Tästä seuraa

$$|Orb(\alpha) = [G : G_\alpha].$$

□

Yksi sovellutus rata-vakauttajalauseelle on Cauchyn lause. Tämä voidaan nähdä eräänlaisena Lagrangen lauseen käänteistuloksena.

Lause 5.16 (Cauchyn lause)**.** *Jakakoon p ryhmän kertaluvun $|G|$. Tällöin G sisältää alkion, jonka kertaluku on p.*

Todistus. Määritellään $\Omega = \{(x_1, \ldots, x_p) : x_i \in G \text{ ja } x_1 x_2 \ldots x_p = 1\}$. Olkoon $H = \langle \sigma \rangle \cong C_p$, missä σ toimii Ω:ssa

$$\sigma : (x_1, \ldots, x_p) \to (x_2, \ldots, x_p, x_1).$$

Rata-vakauttajalause sanoo, että H-radan mahtavuus jakaa H:n kertaluvun. Niinpä saamme, että H-radan mahtavuus on joko 1 tai p. Lisäksi $|\Omega| = |G|^{p-1}$, koska voimme valita ensimmäiset $p-1$ alkiota vapaasti. Nyt p jakaa $|G|$:n, jakaa p myös $|\Omega|$:n. Siispä Ω on H-ratojen pistevieras unioni, ja kukin radoista on joko kokoa p tai 1. Huomaa, että $(1, 1, \ldots, 1)$ muodostaa oman ratansa, joten ainakin yksi rata on mahtavuutta yksi. Olkoon kokoa yksi olevien ratojen määrä a ja kokoa p olevien ratojen lukumäärä b. Silloin $|\Omega| = a \cdot 1 + b \cdot p$. Koska p jakaa $|\Omega|$:n, jakaa p myös a:n. Niinpä on olemassa ainakin p rataa, joiden koko on 1. Jotta α:n rata olisi kokoa 1, täytyy olla niin, että $x_1 = x_2 = \cdots = x_p \neq 1$. Mutta $x_1 x_2 \cdots x_p = 1$, joten $x_1^p = 1$ ja olemme löytäneet alkion, jonka kertaluku on p. □

Määritelmä 5.17. Ryhmän G keskus on joukko

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

Tästä huomaamme heti, että ykkösalkio kuuluu ryhmän keskukseen. Toisinaan ryhmän keskus on kuitenkin ykkösalkiota suurempi.

Tehtävä 32. (i) Osoita, että keskus on normaali aliryhmä.

(ii) Imitoimalla ylläolevaa todistusta, osoita, että p-ryhmän keskus on epätriviaali (suurempi kuin ykkösalkio). Tässä tarvittava toiminta on konjugaatiotoiminta.

Rata-vakauttajalauseen avulla pystymme nyt tutkimaan Platonin kappaleiden symmetriaryhmiä tarkemmin.

5.1 Ryhmä S_4

Tutkimme ryhmää S_4. Tämä on neljän alkion joukon permutaatioryhmä. Neljä alkiota voidaan permutoida yhteensä $4! = 24$ eri tavalla. Niinpä joukossa S_4 on yhteensä 24 alkiota. Symmetriselle ryhmälle on olemassa erityinen tapa merkitä alkioita, eli syklinotaatio, jossa alkiot esitetään erillisten syklien tulona.

Esimerkki 5.18. Permutaatiot

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

voidaan syklinotaatiossa kirjoittaa muotoon (13)(24) ja (134).

Kutsumme sykliä, jonka pituus on kaksi, transpositioksi. Voimme hajottaa jokaisen n:n pituisen syklin aina transpositioiden (ei välttämättä erillisten) tuloksi. Jos transpositiohajotelmassa on parillinen määrä termejä, kutsumme permutaatiota parilliseksi, muussa tapauksessa parittomaksi. Molemmat ylläolevat permutaatiot ovat parillisia, sillä $(134) = (13)(34)$.

Määritelmä 5.19. Symmetrisen ryhmän alkion syklityyppi määräytyy sen alkiovieraan syklihajotelman perusteella. Syklityyppi listaa yksinkertaisesti eripituisten syklien määrät.

Esimerkki 5.20. Alkion (14) syklityyppi on 2, kun taas alkion $(125)(346)(78)(9)$ syklityyppi on $3^2, 2, 1$, huomaa, että 3+3+2+1=9. Monesti ykkössyklejä ei kirjoiteta ollenkaan.

Lause 5.21. *Kaksi symmetrisen ryhmän S_n alkiota ovat toistensa konjugaatteja, jos ja vain jos niillä on sama syklityyppi.*

Todistus. Olkoon $(a_1 \dots a_m)$ m-sykli ja $\rho \in S_n$, silloin $\rho^{-1}(a_1 \dots a_m)\rho = (a_1\rho \dots a_m\rho)$ (vakuutu tästä esimerkkien avulla).

Olkoon nyt $\tau = \tau_1\tau_2 \dots \tau_r$ syklihajotelma. Silloin

$$\rho^{-1}\tau\rho = \rho^{-1}\tau_1 \dots \tau_r\rho = \rho^{-1}\tau_1\rho\rho^{-1}\tau_2\rho \dots \rho^{-1}\tau_r\rho,$$

missä jokainen $\rho^{-1}\tau_i\rho$ on sykli, jonka pituus on sama kuin τ_i:n pituus. Niinpä $\rho^{-1}\tau\rho^{-1}$:lla ja τ:lla on sama syklityyppi.

Jos taas τ:lla ja σ:lla on sama syklityyppi, meidän täytyy konstruoida ρ, joka konjugoi nämä alkiot keskenään. Kirjoitetaan τ ja σ sellaiseen järjestykseen, että samanpituiset syklit ovat samassa järjestyksessä.

$$\begin{aligned} \sigma &= (a_1 \dots a_m)(a_{m+1} \dots a_r)(a_{r+1} \dots)() \\ \tau &= (b_1 \dots b_m)(b_{m+1} \dots b_r)(b_{r+1} \dots)() \end{aligned}$$

Nyt luomme alkion ρ kuvaamaan $a_i \mapsto b_i$ mukaan lukien ykkössyklit. Tällainen ρ permutoi $\{1, \dots, n\}$ ja on siis ryhmän S_n alkio, kuten vaadittua. □

Tehtävä 33. Osoita, että ryhmän S_n parilliset permutaatiot muodostavat normaalin aliryhmän A_n, jota kutsutaan alternoivaksi ryhmäksi. [2] Osoita, että tasan puolet S_n:n alkioista on parillisia, ja päättele, että A_n:n indeksi on kaksi.

Huomautus 5.22. Syklityyppi ei määritä konjugaatiota alternoivassa ryhmässä. Joskus S_n:n konjugaatioluokat, voivat hajota, kun konjugoimme niitä ryhmässä A_n.

[2] Minun mielestäni parempi termi olisi kutsua sitä vuorottelevaksi ryhmäksi. Tai vuorotteluryhmäksi.

Tehtävä 34. Etsi alkion (123) konjugaatit ryhmässä A_4.

Kokoamme taulukkoon S_4:n alkiot konjugaatioluokkien mukaan

Taulukko 6: Ryhmän S_4 alkiot

Konjugaatioluokka	1	2	3	4	5
edustaja	1	(12)	(12)(34)	(123)	(1234)
alkion kertaluku	1	2	2	3	4
konjugaattien määrä	1	6	3	8	6
keskittäjän koko	24	4	8	3	4

Koska syklityyppi määrittää konjugaatioluokan, on luonnollista, että normaalit aliryhmät ovat konjugaatioluokkien yhdisteitä. S_4:ssä on kaksi normaalia aliryhmää. V_4 on konjuvaatioluokkien 1 ja 3 yhdiste ja alternoiva ryhmä A_4 on konjugaatioluokkien 1,3 ja 4 yhdiste.

Kokoamme myös ryhmän A_4 vastaavat tiedot taulukkoon.

Taulukko 7: Ryhmän A_4 alkiot

Konjugaatioluokka	1	2	3a	3b
edustaja	1	(12)(34)	(123)	(134)
alkion kertaluku	1	2	3	3
konjugaattien määrä	1	3	4	4
keskittäjän koko	12	4	3	3

5.2 Platonin kappaleiden symmetriaryhmät

Lause 5.23. *Kuution kiertosymmetriaryhmä on S_4.*

Todistus. Etsimme siis ryhmää

$$G = \{g \in SO(3) : g : \Omega \longrightarrow \Omega\},$$

missä

$$\Omega = \{(a, b, c) : a, b, c \in \{1, -1\}\}.$$

Jaamme todistuksen kolmeen eri osaan.

1. Aloitamme tarkastelemalla symmetriaryhmän kokoa. Koska symmetriaryhmä toimii transitiivisesti kuution kärjissä, ja jokaisen kärjen vakauttaa kolme alkiota, saamme rata-vakauttajalauseen perusteella ryhmän kooksi 24. Kärjen vakauttavat täsmälleen ne kierrot, joitten symmetria-akseli menee kärjen läpi, ja diagonaalisesti toiseen kärkeen. Tämän akselin ympäri voimme kiertää kuutiota joko $2\pi/3$ tai $4\pi/3$:n verran säilyttäen kuution symmetrian.

2. Toiseksi todistamme, että on olemassa homomorfismi $\phi : G \longrightarrow S_4$. Merkitään S:llä kuution päädiagonaalien joukkoa

$$S := \{(AA'), (BB'), (CC'), (DD')\}.$$

   Mikä tahansa kuution symmetriaryhmään kuuluva $g \in G$ permutoi näitä neljää diagonaalia. Joten G indusoi toiminnan joukossa S joka tuottaa homomorfismin $\phi : G \longrightarrow S_4$. Ensimmäisen isomorfialauseen perusteella $Im\phi \cong G/Ker\phi$.

3. Viimeksi todistamme, että $Ker\phi = 1$, sillä silloin homomorfismi on injektio, ja koska $|G| = |S_4|$, tästä seuraa, että se on isomorfismi.

   Olkoon $g \in Ker\phi$. Tämä tarkoittaa sitä, että g toimii triviaalisti joukossa S, esimerkiksi se kuvaa $\{A, A'\} \longrightarrow \{A, A'\}$. Oletamme, että $g \neq 1$ ja menettämättä mitään, voimme tarkemmin olettaa, että g kuvaa A:n A':ksi. Nyt tarkastelemme B:tä. B on kärki, joka on yhden särmän päässä A:sta, joten g:n pitää kuvata B johonkin sellaiseen kärkeen, joka yhdistyy särmällä A':n. Muistamme, että $g : \{B, B'\} \longrightarrow \{B, B'\}$, joten g kuvaa B:n B':ksi. Samalla tavalla g kuvaa C:n C':ksi ja D:n D':ksi.

   Nyt muistamme, että $g \in SO(3)$, jonka alkioita voidaan ajatella myös 3×3-matriiseina. Sellainen 1-dimensioinen $\mathbb{R}^3$:n aliavaruus, joka sisältää pisteet A ja A' on jonkun g:n ominaisvektorin virittämä. Lisäksi tämän ominaisvektorin ominaisarvo on -1. Sama on totta tietysti B, B', C, C' ja D, D':lle. Kaikenkaikkiaan siis g:llä on kolme lineaarisesti riippumatonta ominaisvektoria, joiden kaikkien ominaisarvo on -1. Tämä tarkoittaa sitä, että g:n determinantti on -1, mikä on tietysti ristiriita, sillä $SO(3)$:n alkioiden determinanttien pitää olla 1. Kuvaus on siis injektio, kuten haluttua.

□

Korollaari 5.24. *Oktaedrin kiertosymmetriaryhmä on S_4.*

Todistus seuraa siitä, että oktaedri on kuution duaalikappale. Eli voimme käyttää ylläolevaa todistusta suoraan, mutta nyt tarkastelemme kunkin sivutahkon vakauttajaa, kun symmetria-akseli menee sivutahkokolmion keskipisteen lävitse.

Lause 5.25. *Tetraedrin kiertosymmetriaryhmä on A_4.*

Todistus. Tetraedrillä on neljä kärkeä, ja tetraedrin symmetriaryhmän tulee toimia transitiivisesta näissä kärjissä. Kunkin kärjen vakauttaja on kierto, jonka akseli menee yhdestä kärjestä vastakkaisen sivutahkon keskelle. Tähän ryhmään kuuluu kolme alkiota, joten rata-vakauttajalauseen nojalla ryhmän koko on 12. Tämä on ryhmän A_4 koko. Nyt tehtäväksi jää todistaa, että tetraedrin symmetriaryhmä on isomorfinen ryhmän A_4 kanssa. □

Ryhmän A_5 rakenteen selvitämme seuraavassa luvussa tarkemmin. Tässä vain toteamme seuraavat lauseet.

Lause 5.26. *Dodekaedrin kiertosymmetriaryhmä on A_5.*

Korollaari 5.27. *Ikosaedrin kiertosymmetriaryhmä on A_5.*

Todistus. Lasketaan symmetriaryhmän koko rata-vakauttajalauseen perusteella. Dodekaedrissä on 12 tahkoa ja kunkin tahkon vakauttaja on viitossykli, jonka akseli menee tahkon viisikulmion kärjen läpi. Näin ollen symmetriaryhmän koko on $5 \times 12 = 60$. □

Palaamme nyt toimintojen teoreettisempaan puoleen, jotta voimme esittää mainion ja hyödyllisen lauseen, jota myös ei-Burnsiden lauseeksi kutsutaan. Lauseen nimi kaivannee hieman selittämistä. Noin 1960-luvulta lähtien monet matemaatikot ovat kutsuneet lausetta Burnsiden lauseeksi, ja se kyllä esiintyy William Burnsiden ryhmäteorian opuksessa vuodelta 1897, joten Burnside kyllä tunsi lauseen, kuten myös muut hänen aikalaisensa. Lause itse on vanhempi ja esiintyy ainakin Cauchyn paperissa 1845 ja nykymuodossa Frobeniuksen paperissa 1887 (luultavasti karakteeriateorian yhteydessä). Tavallaan on reilua kutsua lausetta ei-Burnsiden lauseeksi, sillä lähes kaikki muut tuon ajan ryhmäteorian lauseista olivat Burnsiden käsialaa.

Määritelmä 5.28. Ryhmä G toimii joukossa Ω. Alkion g kiinnittämien alkioitten joukko on

$$\chi(g) = \{\omega \in \Omega : \omega * g = \omega\}.^3$$

[3]Merkitsemme tätä joukkoa kreikkalaisella kirjaimella χ, koska tällä joukolla on yhteys karakteeriteoriaan, josta ehkä jollain myöhemmällä kurssilla.

Huomautus 5.29. Tämä ei ole sama joukko kuin alkion vakauttaja

$$Stab_G(\omega) = G_\omega = \{g \in G : \omega * g = \omega\}.$$

Erityisesti, $\chi(g)$ on Ω:n osajoukko, eikä G:n aliryhmä.

Lause 5.30 (ei-Burnsiden lause)**.** *Toimikoon G joukossa Ω. Silloin G:n ratojen lukumäärä Ω:ssa on*

$$\frac{1}{|G|} \sum_{g \in G} |\chi(g)|.$$

Todistus. Olkoon S järjestettyjen parien joukko $\{(\omega, g) : g \in G, \omega \in \Omega, \omega * g = \omega\}$. Lasketaan joukon S mahtavuus kahdella eri tavalla. Ensiksi lasketaan tämä G:n alkioiden mukaan. Näin saamme täsmälleen $\sum_{g \in G} |\chi(g)|$. Lasketaan joukko nyt Ω:n alkioiden mukaan. Ω hajoaa G-radoiksi Ω_1, Ω_2,...Ω_k. Voimme edelleen laskea jokaisen Ω_i alkiot erikseen.

Olkoon $\omega \in \Omega_i$, jotta pari $(\omega, g) \in S$ vaaditaan, että $\omega * g = \omega$, toisin sanoen sopivien alkioiden g lukumäärä on täsmälleen $|Stab_G(\omega)|$. Ratavakauttajalauseen perusteella $|G| = |\Omega_i||Stab_G(\omega)|$. Tästä seuraa $|S| = |G| \times$ ratojen luku. □

5.3 Platonin kappaleiden väritysongelmat

Ei-Burnsiden lause on hyödyllinen erilaisissa kombinatorisissa laskutehtävissä. Esimerkiksi, voimme kysyä, kuinka monta erilaista tapaa on värittää tetraedri kolmella eri värillä. Määrittelemme kaksi tetraedrin väritystä samaksi, jos on olemassa kiertosymmetria, jonka avulla väritykset näyttävät samalta.

Koska värejä on kolme, vaikkapa sininen, valkoinen ja punainen, voidaan jokainen tahko värittää 3 tavalla ja koska tahkoja on neljä, on värityksiä yhteensä $3^4 = 81$. Nyt tutkimme, mitkä väritykset näistä ovat samoja, eli näyttävät samalta kiertosymmetrian suhteen. Olkoon Ω näiden 81 eri tavalla väritetyn tetraedrin joukko, jonka alkiot ovat siis $T_1, T_2, \ldots, T_{81}$. G on tetraedrin kiertosymmetrioiden ryhmä, joka on siis A_4. G toimii Ω:ssa luonnollisella tavalla, eli kuvaa jokaisen $T_1, \ldots, T_{81}$ joksikin toiseksi tetraedriksi $T_1, \ldots, T_{81}$. Kaksi tetraedria S ja T ovat värityksen suhteen sama tetraedri, jos on olemassa $g \in G$, joka $S * g = T$. Tästä seuraa, että tetraedrin väritykset voidaan laskea laskemalla kuinka monta G-rataa on joukossa Ω. Nimittäin jokaiseen rataan on kerätty täsmälleen sellaiset tetraedrit, jotka ovat väritykseltään samat.

Voimme käyttää ratojen lukumäärän laskemiseen ei-Burnsiden lausetta. Jotta voimme soveltaa sitä, on tarkasteltava kunkin G:n alkion kiinnittämää joukkoa.

1. Ykkösalkio kiinnittää kaiken, eli $\chi(1) = 81$.

2. Kolmossyklin θ akseli on tetraedrin yksi kärki ja siitä suora vastakkaisen tahkon keskipisteeseen. θ kiinnittää värityksen, jos sivutahkot ovat kaikki samanvärisiä. Tällaisia värityksiä on yhteensä 9, koska on kolme väriä, joilla voimme värittää sivutahkot samanvärisiksi. Pohja voi olla tämän lisäksi minkä värinen tahansa.

3. Alkio ϕ, jonka kertaluku on kaksi, toimii kuten (12)(34) tahkojen suhteen. Joten, jos halutaan sen kiinnittävän värityksen, vaadimme, että tahkot 1 ja 2 ovat samaa väriä, kuten myös tahkot 3 ja 4. Erilaisia värityksiä saamme jälleen 9.

Ryhmässä A_4 on yhteensä kahdeksan kolmossykliä, ja kaikille näille $\chi(\theta) = 9$. Kertalukua kaksi olevia alkioita on yhteensä kolme, ja kaikille näille $\chi(\phi) = 9$. Nyt ei-Burnsiden lause sanoo, että värityksiä on

$$\frac{1}{|A_4|} \sum_{g \in A_4} |\chi(g)| = \frac{1}{12}(81 + 8 \cdot 9 + 3 \cdot 9) = 15.$$

Tehtävä 35. 1. Kuinka monta eri tapaa on värittää kuutio keltaisella ja sinisellä?

2. Kuinka monta eri tapaa on luoda helminauha, jonka pituus on 14 helmeä, käyttämällä hopeisia, kultaisia sekä norsunluisia helmiä?

3. Osoita, että on 9099 tapaa värittää dodekaedri kolmella värillä.

6 A_5, alternoiva ryhmä ja muita yksinkertaisia ryhmiä

Tutustukaamme ensin ryhmään S_5. Jos käytämme syklinotaatiota, toteamme, että se sisältää syklejä, jotka ovat muotoa (12), (123), (1234), (12345), (12)(34), (123)(45). Kukin syklityyppi määrittää konjugaattiluokan. Jos rajoitamme vain parillisiin sykleihin, niin saamme alternoivan ryhmän A_5

Kuten totesimme edellisessä kappaleessa, ei syklityyppi määritä enää täysin konjugaatioluokkia ryhmässä A_5. Viitossyklien luokka hajoaa kahteen yhtäsuureen osaan.

Taulukko 8: Ryhmän A_5 alkiot

Konjugaatioluokka	1	2	3	4a	4b
edustaja	1	(12)(34)	(123)	(12345)	(13524)
alkion kertaluku	1	2	3	5	5
konjugaattien määrä	1	15	20	12	12
keskittäjän koko	60	4	3	5	5

Tehtävä 36.

1. Kuinka monta nelossykliä on ryhmässä S_5, entä ryhmässä S_n?
2. Kuinka monta alkiota, jonka syklityyppi on (123)(45) on ryhmässä S_5, entä ryhmässä S_n?
3. Osoita, että jos $H \leq S_n$, joko kaikki H:n alkiot ovat parillisia permutaatioita, tai täsmälleen puolet ovat parillisia ja puolet parittomia.

Määritelmä 6.1. Äärellistä ryhmää G kutsutaan yksinkertaiseksi, jos sen ainoat normaalit aliryhmät ovat ryhmä itse ja ykkösalkio.

Esimerkki 6.2.

1. Jokainen syklinen ryhmä C_p, jonka kertaluku on joku alkuluku p, on yksinkertainen.
2. Ryhmä A_4 ei ole yksinkertainen, sillä $V_4 \lhd A_4$.

Pienin epätriviaali esimerkki yksinkertaisesta ryhmästä on A_5. Tämä on erityisen tärkeä myös todistuksessa, että viidennen asteen polynomille ei ole olemassa ratkaisukaavaa. Todistamme hieman laajemmin.

Propositio 6.3. *Alternoiva ryhmä A_n on yksinkertainen, kun $n \geq 5$.*

Huomautus 6.4. Todistamme myöhemmin, että jos G on yksinkertainen ryhmä ja sen kertaluku on 60, on $G \cong A_5$.

Todistus. Jaamme todistuksen kolmeen osaan.

1. Jos $H \neq 1$ ja $H \lhd A_n$, silloin H sisältää kolmossyklin.

2. H sisältää kaikki kolmossyklit.

3. kolmossyklit virittävät A_n:n.

Tällöin $H = A_n$, joten A_n on yksinkertainen.

1. Olkoon $H \lhd A_n$ ja olkoon h sellainen alkio, jonka kertaluku on joku alkuluku p. Kirjoitamme h:n nyt alkiovieraina sykleinä, joista luonnollisesti jokaisen pituuden pitää olla p. Vaihtoehdot ovat
(a) $o(h) = p \geq 5$ ja jos $h = (a_1, \ldots, a_p) \ldots (r_1, \ldots, r_p)$ voimme kirjoittaa

$$(a_1a_2a_3)h(a_3a_2a_1)h^{-1} = (a_2a_3a_p),$$

joten H sisältää 3-syklin.
(b) Jos $o(h) = 3$ ja $h = (abc)(def)\ldots$ saamme

$$(abcde)h(edcba)h^{-1} = (bcdef) \in H.$$

Jos nyt käytämme kohtaa (a), saamme todistettua, että h sisältää kolmossyklin.
(c) Jos $o(h) = 2$, silloin $h = (ab)(cd)$ tai $h = (ab)(cd)\cdot(ef)(gh)\ldots$ jälkimmäisessä tietysti parillinen määrä transpositioita. Ensimmäisessä tapauksessa

$$(bde)h(edb)h = (aebdc) \in H$$

ja nyt voimme taas löytää (a)-kohdan perusteella kolmossyklin. Toisessa tapauksessa

$$(bde)(h(edb)h = (afc)(bde)$$

ja voimme käyttää (b)-kohtaa kolmossyklin löytämiseen.

Joten jokaisessa tapauksessa H sisältää kolmossyklin.

2. Haluamme todistaa, että jos H:ssa on yksi kolmossykli, ovat kaikki kolmossyklit H:ssa.

Tiedämme, että kaikki kolmossyklit ovat toistensa konjugaatteja ryhmässä S_n ja niitä on ja yhteensä näitä on $\binom{n}{3} \cdot 2$ kappaletta.

Jos $\alpha = (xyz) \in H$ on kolmossykli ryhmässä S_n, saamme α:n keskittäjän koon laskettua rata-vakauttajalauseella. Sillä $|Orb_{S_n}| = |S_n : C_{S_n}(\alpha)| =$

$\frac{n(n-1)(n-2)}{3}$, mistä seuraa, että $|C_{S_n}(\alpha)| = 3(n-3)!$. Olemme kuitenkin kiinnostuneita konjugoinnista ryhmässä A_n, ja laskemalla $C_{A_n}(\alpha)$:n koon, saamme selville α:n konjugaattien määrän.

Nyt $C_{S_n}(\alpha)$ on symmetrisen ryhmän aliryhmä ja yllä olevan tehtävän perusteella, joko kaikki sen alkiot ovat parillisia, tai täsmälleen puolet ovat parillisia ja puolet parittomia. Olemme selvästikin jälkimmäisessä tapauksessa, sillä $(xyz)(lm)$ on pariton permutaatio, joka keskittää α:n. Muista, että $n \geq 5$. Jos tarkastelemme siis parillisia permutaatioita tässä ryhmässä, on niitä $\frac{1}{2}3(n-3)! = |C_{A_n}(\alpha)|$. Rata-vakauttajalauseen perusteella

$$|A_n : C_{A_n}(\alpha)| = \frac{n(n-1)(n-2)}{3},$$

joten kaikki S_n:n kolmossyklit ovat konjugaatteja keskenään. Koska $H \lhd A_n$, tästä seuraa, että kaikki kolmossyklit kuuluvat H:n.

3. Haluamme osoittaa, että kolmossyklit generoivat A_n:n. Jokainen A_n:n alkio voidaan kirjoittaa parillisena määränä transpositioita. Koska $(ab)(bc) = (abc)$ ja $(ab)(cd) = (ab)(bc)(bc)(ad) = (abc)(bcd)$, jokainen A_n:n alkio voidaan kirjoittaa kolmossyklien tulona.

□

Huomautus 6.5. Yksi esseen aihe on etsiä ja esittää joku toinen todistus sille, että A_n on yksinkertainen, kun $n \geq 5$. Tämä voi liittää myös dodekaedrin ja ikosaedrin symmetriaryhmien käsittelyyn. Minulta saa materiaalia ainakin sellaiseen todistukseen, jossa pyöritellään viitossyklejä. Vielä yksi tuntemani todistus käyttää Sylowin teoriaa.

Yksinkertaiset ryhmät ovat kaikkien äärellisten ryhmien rakennuspalikoita samaan tapaan kuin alkuluvut ovat kaikkien luonnollisten lukujen rakennuspalikoita. Rakennuspalikoiden määritelmä kaipaa tarkempaa tutkimista.

Määritelmä 6.6. Äärellisen ryhmän G hajoamisjono (kompositiojono) on ketju

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G,$$

jossa jokainen $G_{i+1} \lhd G_i$ ja G_i/G_{i+1} on yksinkertainen ryhmä. Kutsumme ryhmiä G_i/G_{i+1} hajoamistekijöiksi.

Esimerkki 6.7.

1. Jos G on yksinkertainen.
2. S_3
3. V_4. Tällä on kolme hajoamisjonoa.

Propositio 6.8. *Jokaisella äärellisellä epätriviaalilla ryhmällä on hajoamisjono.*

Todistus. Olkoon $G \neq 1$ äärellinen ryhmä. Jos G on yksinkertainen, on hajoamisjono $1 \leq G$. Tämä on induktion perustapaus.

Oletetaan, että kaikille ryhmillä H, jotka ovat $1 < |H| < |G|$ on olemassa hajoamisjono. Haluamme tietysti nyt konstruoida hajoamisjonon G:lle. Valitaan kaikista G:n aidoista normaaleista aliryhmistä maksimaalinen, ja kutsutaan tätä N:ksi. Tämä siis tarkoittaa, sitä, että jos $N \leq M \leq G$ ja $M \lhd G$, silloin $M = N$ tai $M = G$. Nyt kolmannen isomorfialauseen perusteella G/N on yksinkertainen.

Induktion perusteella, N:llä on hajoamisjono, ja nyt saamme hajoamisjonon G:lle luonnollisella tavalla. □

Tehtävä 37. Olkoon $H_1 \lhd G$ ja $G_1 \lhd G$. Todista, että $H_1G_1 \lhd G$ sekä $H_1 \cap G_1 \lhd G$.

Lause 6.9 (Jordan-Hölderin lause)**.** *Olkoon G äärellinen epätriviaali ryhmä ja olkoot*

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G \tag{2}$$

ja

$$1 = H_m \lhd H_{m-1} \lhd \ldots \lhd H_1 \lhd H_0 = G \tag{3}$$

kaksi G hajoamissarjaa. Silloin $m = n$ ja kummankin sarjan tekijäryhmät ovat samat (emme vaadi samaa järjestystä). Tässä tapauksessa kompositiojonoja kutsutaan isomorfisiksi.

Todistus. Oletetaan, että meille on annettu kaksi jonoa, kuten yllä. Jos $G_1 = H_1$, silloin saamme kaksi kompositiojonoa G_{n-1}:lle

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1$$

ja

$$1 = H_m \lhd H_{m-1} \lhd \ldots \lhd H_1 = G_1.$$

Nyt induktion perusteella, nämä kaksi kompositiojonoa ovat isomorfiset ja siksi G:n kompositiojonot ovat isomorfiset.

Toinen tapaus on, kun $G_1 \neq H_1$. Kompositiojonon määritelmän perusteella tiedämme, että $H_1 \lhd G$ ja $G_1 \lhd G$. Siispä $H_1G_1 \lhd G$ sekä $H_1 \cap G_1 \lhd G$. Todistamme, että $H_1G_1 = G$. Tämä seuraa siitä, että $G_1 \lneq H_1G_1 \leq G$ ja koska G_1 on G:n maksimaalinen normaali aliryhmä. Nyt voimme käyttää toista isomorfialausetta

$$G/H_1 \cong G_1/H_1 \cap G_1$$

ja

$$G/G_1 \cong H_1/H_1 \cap G_1.$$

Olkoon nyt

$$1 = K_l \lhd K_{l-1} \lhd \ldots \lhd K_1 = H_1 \cap G_1$$

kompositiojono ryhmälle $H_1 \cap G_1$. Tämän perusteella saamme kaksi uutta kompositiojonoa ryhmälle G.

$$1 = K_l \lhd K_{l-1} \lhd \ldots K_1 \lhd H_1 \lhd G \tag{4}$$

$$1 = K_l \lhd K_{l-1} \lhd \ldots K_1 \lhd G_1 \lhd G \tag{5}$$

Nyt ensimmäisen osan perusteella (2) $\cong$ (4) ja (3) $\cong$ (5) ja (4) $\cong$ (5), koska niillä on samat kompositiotekijät, vain ensimmäiset kaksi on vaihdettu keskenään. Siksi (2) $\cong$ (3). □

Tehtävä 38. Laske ryhmän S_4 hajoamissarja. Laske ryhmän D_{24} hajoamissarja. Onko näillä samat hajoamistekijät? Entä ryhmällä C_{24}. Mikä on ryhmän S_n hajoamissarja?

Olemme todistaneet, että ryhmä A_5 on yksinkertainen. Seuraava tavoitteemme on todistaa, että pienin kertaluku, jolloin ryhmä on yksinkertainen, on 60 ja että jos ryhmän kertaluku on 60 ja se on yksinkertainen, on ryhmä isomorfinen ryhmän A_5 kanssa. Tärkeä työkalu tässä todistuksessa ovat Sylowin lauseet.

6.1 Sylowin lauseet

Muistamme, että Lagrangen lause ja Cauchyn lause kertoivat ryhmän rakenteesta jotain pelkästään ryhmän kertaluvun perustella. Vielä hieman Cauchyn lausetta tarkempi tämäntyyppinen lause ovat Sylowin lauseet. Sylowin lauseita voidaan käyttää myös yksinkertaisuuden tutkimiseen.

Sylowin lauseet edustavat myös matemaattisessa ajattelussa yleistä lokaali-globaali-periaatetta. Lukuteoriassa alkuluvut palvelevat samaa tarkoitusta. Mitä voimme sanoa ryhmästä, jos keskitymme kuhunkin alkulukuun kerrallaan. Samaan tapaan kuin lukuteoria ratkaisee yhtälöitä $\pmod p$.

Lause 6.10 (Sylow)**.** *Olkoon G äärellinen ryhmä, kertalukua $p^n r$, jossa p ei jaa r:ää. Tällöin*

(i) G sisältää Sylowin p-aliryhmän P, jonka kertaluku on p^n.

(ii) Mitkä tahansa kaksi Sylowin p-aliryhmää ovat keskenään konjugaatteja.

(iii) Sylowin p-aliryhmien lukumäärä n_p, on $n_p \equiv 1 \pmod{p}$ ja jakaa luvun m.

Todistus. Todistamme lauseen ryhmän toimintojen avulla.
(i) Olkoon $\Omega = \{M \subseteq G : |M| = p^n\}$. Määrittelemme G:n toimimaan tässä joukossa oikeanpuolisella kertolaskulla

$$M * g = \{mg : m \in M\}.$$

Tarkista, että tämä on toiminta. Tarkastelemme G-ratoja. Olkoon Σ tällainen. Silloin $\Sigma = \{M, Mg_2, Mg_3 \ldots, Mg_k\}$. Huomaamme, että Σ:n alkiot kattavat koko G:n. Nimittäin, olkoon $m \in M$, jos g on mikä tahansa G:n alkio, voimme kirjoittaa $g = m * m^{-1}g \in Mm^{-1}g \in \Sigma$. Tästä seuraa, että $k \geq r$. Jaamme tarkastelun kahteen tapaukseen.

Tapaus 1. $k = r$. Tässä tapauksessa G on Σ:n alkioiden pistevieras yhdiste. Alkion M vakauttaja ryhmässä G on kertalukua p^n (rata-vakauttajalauseen nojalla), ja koska vakauttaja on aliryhmä, on se väistämättä kertaluvun perusteella myös Sylowin p-aliryhmä.

Päättelemme, että jokainen vastaava G-rata koostuu yksikäsitteisestä Sylowin p-aliryhmästä ja tämän oikeista sivuluokista.

Tapaus 2. $k \neq r$, siispä $k > r$. Koska rata-vakauttajalauseen nojalla $k \mid |G| = p^n r$, tästä seuraa, että $p \mid k$.

Nyt jokainen rata, jonka koko on r sisältää yksikäsitteisen Sylowin aliryhmän, ja kaikkien muiden ratojen koko on jaollinen p:llä. Tästä seuraa

$$|\Omega| = \binom{p^n r}{p^n} = n_p r + \sum_{p \mid |\Sigma|} |\Sigma| \equiv n_p r \mod p.$$

Toisaalta $\binom{p^n r}{p^n} \equiv r \mod p$ (Yllä oleva tulos on voimassa kaikille ryhmille, joiten kertaluku on $p^n r$, joten se ei voi riippua n_p:stä. Syklisessä ryhmässä $C_{p^n r}$ on vain yksi aliryhmä, jonka koko on p^n ja siksi $n_p = 1$. Tämä todistaa kongruenssin) ja koska $p \nmid r$, tästä seuraa $n_p \equiv 1 \mod p$. Erityisesti huomaamme, että Sylowin aliryhmien lukumäärä ei ole nolla.

(ii) Konjugaatio seuraa seuraavasta aputuloksesta, joka osoittaa, että jokainen G:n p-aliryhmä kuuluu johonkin Sylowin p-aliryhmään.

Lemma 6.11. *Jos Q on G:n p-ryhmä ja P on Sylowin p-aliryhmä. Silloin jollekin $g \in G$ pätee $Q \subseteq g^{-1}Pg$.*

Todistus. Toimikoon Q oikeanpuoleisen kertolaskun avulla P:n sivuluokkien joukossa $(G : P)$. Sivuluokkia on m kappaletta, ja sivuluokat hajoavat radoiksi $O_1, \ldots, O_k$, joitten yhteenlaskettu mahtavuus on $|O_1| + \cdots + |O_k| = r$. Rata-vakauttajalauseen perustella, kunkin radan koko jakaa Q:n koon, eli

on joko 1 tai p. Koska $p \nmid r$, kaikki radat eivät voi olla kokoa p, joten tässä Q-toiminnassa on välttämättä rata, jonka mahtavuus on 1, sanokaamme, että tämä on $\{Pg\}$. Mikä tarkoittaa sitä, etta $Pg * Q \subseteq Pg$, mistä seuraa $gQg^{-1} \subseteq P$ ja näin ollen $Q \subseteq g^{-1}Pg$. □

Jos nyt valitsemme Q:n Sylowin p-aliryhmäksi, tulos seuraa.

(iii) Olemme jo todistaneet, että $n_p \equiv 1 \mod p$. Jäljellä on todistaa, että n_p jakaa r:n. Yllä todistimme, että Sylowin aliryhmien joukko muodostaa yhden radan alkion g konjugaatiotoiminnan kautta. Rata-vakauttajalauseen perusteella $n_p \mid |G|$. Koska p ei jaa n_p:tä, tästä seuraa, että n_p jakaa r:n. □

Tarkastelemme seuraavassa pieniä yksinkertaisia ryhmiä Sylowin lauseen avulla. Ensin kuitenkin todistamme hyödyllisen lemman.

Lemma 6.12 (Poincaré)**.** *Olkoon $H \leq G$, ja $|G : H| = n$. Olkoon $K = \cap_{g \in G} g^{-1}Hg$. Silloin $K \lhd G$, ja $K \leq H$ ja kaiken lisäksi*

$$n \mid |G : K| \mid n!$$

Todistus. Olkoon $\Omega = (G : H)$. Kun G toimii näissä sivuluokissa oikealla kertolaskulla, on toiminnan ydin täsmälleen K, sillä jokaisen sivuluokan Hg vakauttaja on $g^{-1}Hg$. Tämän lisäksi K on normaali aliryhmä (koska se on homomorfismin ydin, tai koska se on sulkettu konjugaatiotoiminnan suhteen). Lisäksi $K \leq H$, sillä voimme valita myös alkion 1 konjugoimaan H:ta ja loppu on leikkausta tämän suhteen. Muista, että toiminta indusoi homomorfismin $G \longrightarrow Sym(\Omega)$, joten ensimmäisen isomorfialauseen perusteella G/K on isomorfinen $Sym(\Omega)$:n (transitiivisen) aliryhmän kanssa. Tästä seuraa, että $|G : K \mid \mid n!$. Koska $K \leq H$, saamme myös $n = |G : H| \mid |G : K|$. □

Tehtävä 39. Osoita, että ryhmä, jonka kertaluku on kahden alkuluvun tulo pq, ei ole yksinkertainen. Voit käyttäää tähän Sylowin lauseita. Edelleen päättele, että jos G on yksinkertainen ryhmä, joka ei ole Abelin ryhmä, niin $|G| \geq 60$.

Lause 6.13. *Jos G on yksinkertainen, ja sen kertaluku on 60, on $G \cong A_5$.*

Todistus. Tarkastellaan ryhmää G Sylowin lauseiden avulla. Ensiksikin $60 = 2^2 \cdot 3 \cdot 5$, joten ryhmässä on Sylowin 5-aliryhmä, jonka on generoinut alkio, jonka kertaluku on 5. Cauchyn lauseen perusteella tällainen alkio on olemassa. Sylowin lauseen kolmannen kohdan perusteella Sylowin 5-aliryhmien lukumäärä on $n_5 \equiv 1 \mod 5$. Koska ryhmä on yksinkertainen, on Sylowin 5-aliryhmiä enemmän kuin yksi (Sylowin lauseen toisen kohdan perusteella kaikki Sylowin 5-aliryhmät ovat toistensa konjugaatteja, joten jos niitä on

vain yksi, on se väistämättä normaali, mikä on ristiriidassa yksinkertaisuuden kanssa). Tämän lisäksi $n_5 \mid 12$, joten ainoastaan $n_5 = 6$ on mahdollinen. Olkoon P siis Sylowin 5-aliryhmä ja $\Omega = \{g^{-1}Pg : g \in G\}$. Ymmärrettävästi $|\Omega| = 6$. Ryhmä G toimii joukossa Ω konjutaatiotoiminnalla, joka indusoi kuvauksen $\rho : G \longrightarrow S_6$. Tämä homomorfismi on injektio, sillä G on yksinkertainen. Olkoon $H \leq S_6$ tämän homomorfismin kuva. $H \cong G$ ja siis yksinkertainen. Nyt $H \cap A_6 \lhd H$ (koska leikkaus on aliryhmä, jonka indeksi on kaksi) ja koska H on yksinkertainen ($H \cong G$) on $H \leq A_6$.

Olkoon $\Gamma := cos(A_6 : H)$. Nyt $|\Gamma| = \frac{1}{2}6!/60 = 6$, joten kun A_6 toimii joukossa Γ, saamme homomorfismin $\sigma : A_6 \longrightarrow S_6$. Itseasiassa σ on ryhmän A_6 automorfismi. Ensinnäkin se on injektio, sillä A_6 on yksinkertainen ja sen kuvan pitää olla A_6:n aliryhmä. Homomorfismi σ kuvaa H:n vakauttajan, vakauttajaksi ryhmässä A_6, joka on A_5, joten olemme osoittaneet, että $G \cong H \cong A_5$. □

Tehtävä 40. Jos pidämme tunnettuna lauseen "Jos G on yksinkertainen ja G:n kertaluku on $2^a \cdot 3 \cdot 5$, on $a = 2$ ja $G \cong A_5$", osoita, että jos ryhmä G on yksinkertainen ja sen kertaluku on korkeintaan 300, on ryhmän kertaluku joko 60 tai 168.

Tehtävä 41. Kirjoita essee yksinkertaisesta ryhmästä, jonka kertaluku on 168. Tämä on ryhmä $\mathrm{PSL}_2(7)$.

6.2 Ratkeavat ryhmät

Tärkeä luokka ryhmiä, jotka eivät varmasti ole yksinkertaisia, ovat ratkeavat ryhmät. Niitä käymme tutkimaan seuraavaksi.

Määritelmä 6.14. Kahden alkion $g, h \in G$ vaihdannaistaja on alkio $[g, h] = g^{-1}h^{-1}gh$. Vaihdannaistajien virittämää aliryhmää $G' = [G, G] = \{g^{-1}h^{-1}gh : g, h \in G\}$ kutsutaan vaihdannaistaja-aliryhmäksi. Jos $G' = G$, kutsumme ryhmää G täydelliseksi.

Huomaa, että Abelin ryhmässä pätee aina $[g, h] = 1$, joten jos A on Abelin ryhmä, on $A' = 1$.

Tehtävä 42. Osoita, että kaikille (äärellisille) ryhmille G, vaihdannaistaja-aliryhmä $[G, G]$ on normaali, ja että $G/[G, G]$ on Abelin ryhmä. Edelleen osoita, että G/H on Abelin ryhmä jos ja vain jos $[G, G] \leq H$.

Määritelmä 6.15. Ryhmää $G/[G, G]$ kutsutaan ryhmän G Abelistukseksi.

Määritelmä 6.16. Ryhmää kutsutaan ratkeavaksi, jos se hajoaa ketjuksi aliryhmiä

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G,$$

jossa kaikki G_i/G_{i+1} ovat syklisiä yksinkertaisia ryhmiä (eli niiden kertaluku on alkuluku). Ketju voi olla joko normaali tai alinormaali.

Esimerkki 6.17.

$$1 \lhd C_2 \lhd C_4 \lhd D_8,$$

joten D_8 on ratkeava ryhmä, sillä kaikki tekijäryhmät ovat isomorfisia C_2:n kanssa.

Määritelmä 6.18. Ryhmä G on ratkeava, jos ketju, jossa $G^{(1)} = [G, G]$ ja $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ päättyy triviaaliin aliryhmään. Kutsumme tätä ketjua vaihdannaistajajonoksi. Pienin n, jolle tämä $G^{(n)} = 1$ on nimeltään ryhmän G vaihdannaistajapituus.

Myöhemmin todistamme, että tämä on yhtäpitävä ensimmäisen määritelmän kanssa.

Lemma 6.19. *Kaikille ryhmille G, on $G^{(k)} \lhd G$ jokaiselle k.*

Todistus. Induktio k:n suhteen. Jos $k = 0$, silloin $G \lhd G$, mikä on selvästi totta. Oletetaan, että $G^{(k)} \lhd G$ ja tarkastellaan $G^{(k+1)}$:n virittäjiä. Virittäjät ovat määritelmän mukaan muotoa $[g, h]$, jossa $g, h \in G^{(k)}$. Nyt jos $x \in G$, silloin $[g, h]^x = [g^x, h^x] \in G^{(k+1)}$, sillä $g^x, h^x \in G^{(k)}$, koska $G^{(k)} \lhd G$. Tästä seuraa, että $G^{(k+1)} \lhd G$ □

Tehtävä 43. Osoita, että seuraavat ryhmät ovat ratkeavia.

1. S_3 laskemalla vaihdannaistajat ja vaihdannaistajajono.

2. S_4 konstruoimalla alinormaali sarja, jonka tekijäryhmät ovat on Abelin ryhmiä tekijäryhmät.

Osoita, että ryhmä S_n ei ole ratkeava, kun $n \geq 5$.

Tehtävä 44. Osoita, että jos G on ratkeava, on jokainen $H \leq G$ ratkeava. Ja edelleen, jos $N \lhd G$, silloin G/N on ratkeava. (Vinkki: tekijäryhmän kohdalla todista, että $(G/N)^{(k)} = G^k N/N$, tarkastelemalla minkä muotoisia alkoita kummallakin puolella on.)

Ratkeavat ryhmät on ensimmäinen ryhmäluokka, joka on suljettu, niin laajennusten kuin aliryhmienkin suhteen.

Lause 6.20. *Olkoon G ryhmä ja $N \lhd G$. Silloin G on ratkeava jos ja vain jos sekä N että G/N ovat ratkeavia.*

Todistus. Jos G on ratkeava, ylläolevasta tehtävästä seuraa, että $N \lhd G$ ja G/N ovat ratkeavia. Olkoon N:n vaihdannaistajapituus k ja G/N:n vaihdannaistajapituus l. Silloin edellisen tehtävän perusteella $(G/N)^{(l)} = G^{(l)}N/N = N/N$, jälkimmäinen yhtäsuuruus ratkeavuuden perusteella, sillä N/N on ryhmän G/N triviaali aliryhmä. Tästä seuraa ensin $G^{(l)}N = N$ ja edelleen, että $G^{(l)} \leq N$. Nyt aliryhmän perusteella $G^{(l+1} \leq N'$ ja induktiivisesti edeten $G^{(l+k)} \leq N^{(k)} = 1$, koska N oli ratkeava ja sen vaihdannaistajapituus oli k. Olemme siis todistaneet, että G on ratkeava ja sen vaihdannaistajapituus on $l + k$. □

Huomaa, että jos sekä N että G/N ovat Abelin ryhmiä, ryhmä G on ratkeava (toisinaan sitä kutsutaan myös meta-abelin ryhmäksi), mutta ei välttämättä Abelinen. Abelin ryhmät eivät siis ole suljettu ryhmäluokka.

Tehtävä 45. Osoita, että $G \times H$ on ratkeava silloin, kun G ja H ovat ratkeavia.

Nimitys ratkeava ryhmä tulee siitä, että alunperin ryhmäteoria syntyi yhtälön ratkaisukaavojen etsinnästä. Viidennen asteen yhtälölle ei ole ratkaisukaavaa, ja se johtuu siitä, että ryhmä A_5 on yksinkertainen, eikä siis ratkeava – kuten ei myöskään tällä perusteella S_5. Nimittäin, polynomiyhtälö ratkeaa radikaalien avulla täsmälleen silloin kun sen yhtälöön liitetty Galois'n ryhmä on ratkeava.

Tehtävä 46. Kirjoita essee ryhmän ratkeavuuden yhteydestä yhtälöitten ratkeavuuteen ratkaisukaavojen avulla. Esseen tarkoituksena on pintapuolisesti käydä läpi Galois'n teorian pääpiirteet. Joitain todistuksia ja teknisyyksiä voi ohittaa. Voit kysyä näistä tarkemmin minulta.

6.3 Äärellisten yksinkertaisten ryhmien luokittelu

Olemme tarkastelleet ryhmiä A_n, ja osoitimme niiden yksinkertaisuuden, kun $n \geq 6$. Alternoivien ryhmien perhe on yksi esimerkki yksinkertaisista äärellisistä ryhmistä. Yksi ryhmäteorian suurimpia saavutuksia 1900-luvulla oli äärellisten yksinkertaisten ryhmien luokittelu. Nämä ovat Jordan-Hölderin lauseen perusteella kaikkien äärellisten ryhmien rakennuspalikoita.

Yksi lopullisen luokitteluhankkeen liikkeellesaattajista oli Feitin ja Thompsonin kuuluisa parittoman kertaluvun lause (the odd order theorem), joka on huima yleistys klassiselle Burnsiden lauseelle.

Lause 6.21 (Burnside)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^a q^b$. Silloin G on ratkeava.*

Lause 6.22 (Feit-Thompson)**.** *Paritonta kertalukua oleva äärellinen ryhmä on ratkeava.*

Tässä tapauksessa siis ryhmän kertaluku jo määrittelee, milloin ryhmä on ratkeava, eikä siis taatusti yksinkertainen. Tästä seuraa helposti.

Korollaari 6.23. *Äärellisen yksinkertaisen ryhmän kertaluku on jaollinen kahdella, lukuunottamatta yksinkertaisia Abelin ryhmiä.*

Olemme jo moneen kertaan itsekin havainneet, että jos ryhmän kertaluku on parillinen, sisältää ryhmä alkion, jonka kertaluku on kaksi, eli involuution. Tämä havainto on tärkeä yksinkertaisten ryhmien luokittelussakin.

Luokittelussa on lisäksi neljä muuta ääretöntä perhettä, jotka kaikki kuuluvat yksinkertaisiin Lien tyypin ryhmiin. Näitä ovat matriisiryhmät projektiivinen spesiaalinen lineaariryhmä, unitaariset, symplektiset ja ortogonaaliset transformaatiot äärellisen kunnan ylitse. Näiden lisäksi on myös poikkeukselliset Lien ryhmät ovat G_2, F_4, E_6, E_7, ja E_8, jotka eivät siis ole äärettömien perheitten jäseniä.

Näiden lisäksi on 26 sporadista yksinkertaista ryhmää. Ensimmäiset niistä olivat viisi Mathieun ryhmää, jotka löysi Emile Mathieu 1860-luvulla. Loput 21 ryhmää löydettiin 1965-1975. Uusien äärellisten yksinkertaisten ryhmien löytämisestä käytiin kovaa kilpailua. Yksi tärkeimmistä matemaatikoista alalla on John Conway. Hänen mukaansa on nimetty Conwayn ryhmät. Suurimman kertaluvun yksinkertainen ryhmä on hirviöryhmä. Se sisältää 20 muuta sporadista ryhmää.

Tehtävä 47. Kirjoita essee joko symplektisistä, ortogonaalisista tai unitaarisista ryhmistä.

Vaikka äärellisistä yksinkertaiset ryhmät luokiteltiinkin jo viimeistään 1980-luvulla, ei yksinkertaisten ryhmien tutkimus tähän loppunut. Ne tuottavat edelleen uutta tutkimusta. Tässä esimerkiksi helposti ymmärrettävä, mutta vaikea lause tältä vuodelta.

Muista, että ryhmän G vaihdannaistaja-aliryhmä on $[G, G]$. Kutsumme ryhmää täydelliseksi, jos pätee $G = [G, G]$. Ennen kaikkea huomaamme, että täydelliset ryhmät eivät ole ratkeavia, koska niiden vaihdannaistajasarja jumiutuu heti ensimmäiseen askeleeseen, eikä siis koskaan saavuta triviaalia ryhmää. Seuraava uusi tulos kertoo jotain äärellisistä yksinkertaisista ryhmistä.

Oren konjektuuri (1960-luvulta).

Lause 6.24 (Liebeck, O'Brien, Shalev, Tiep, 2008)**.** *Jokaisen epäkommutatiivisen äärellisen yksinkertaisen ryhmän jokainen alkio on vaihdannaistaja.*

Yksinkertaisten äärellisten ryhmien luokittelu (Classification of finite simple groups CFSG) on nykyään tärkeä työkalu matemaatikoille. Jos haluaa todistaa jonkun väitteen ryhmäteoriasta, usein jossain vaiheessa todistusta pitää käydä läpi, onko lause totta yksinkertaisille äärellisille ryhmille.

6.4 Ryhmät, joiden kertaluku on pienempi kuin 60

Tässä kappaleessa osoitamme, että ryhmät, joiden kertaluku on aidosti pienempi kuin 60, eivät voi olla yksinkertaisia, elleivät ne ole Abelin ryhmiä. Tästä lähtien sovimme, että yksinkertaisuus tarkoittaa sitä, että ryhmä on ei-Abelin ryhmä ja yksinkertainen.

Tarvitsemme muutaman lemman.

Lemma 6.25. *Jos $|G| = p^n$, silloin G ei ole yksinkertainen.*

Todistus. Todistimme rata-vakauttajalauseen avulla, että $Z(G) \neq 1$ kaikille p-ryhmille, ja lisäksi olemme todistaneet, että $Z(G) \lhd G$, kaikille ryhmillä G. Näin ollen G sisältää epätriviaalin normaalin aliryhmän. □

Lemma 6.26. *Jos ryhmän kertaluku on pq, missä p ja q ovat erisuuria alkulukuja, silloin ryhmä ei ole yksinkertainen.*

Todistus. Voimme olettaa yleisyyttä menettämättä, että $p > q$, silloin $n_p \equiv 1 \mod p$ ja $n_p \mid q$. Tämä pakottaa $n_p = 1$ ja siksi Sylowin p-aliryhmä on normaali. □

Lemma 6.27. *Olkoon $|G| = pr$, missä p on alkuluku ja $p > r \neq 1$. Silloin G ei ole yksinkertainen.*

Todistus. Sylowin lauseen perusteella $n_p \equiv 1 \mod p$ ja $n_p \mid r$, joten $n_p = 1$, ja Sylowin p-aliryhmä on normaali. □

Kirjoittakaamme myös Poincaren lause meille hyödyllisemmässä muodossa.

Lemma 6.28. *Jos G on yksinkertainen ryhmä, ja $H \leq G$, silloin*

$$|G| \mid |G : H|!.$$

Näillä konstein pääsemme eroon jo ryhmistä, joiden kertaluku on joku alkuluvun potenssi, kahden alkuluvun tulo tai muotoa pr.

Mikä tarkoittaa sitä, että luvuista

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28, 29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53, 54,55,56,57,58,59

Jäljelle jäävät

12,18,24,30,36,40,45,48,50,54,56.

Näistä $18 = 2 \cdot 3^2$, $50 = 2 \cdot 5^2$ ja $54 = 2 \cdot 3^2$, joten kaikissa tapauksissa on Sylowin p-aliryhmä, jonka indeksi on kaksi, joten sen on pakko olla normaali. Jäljelle jäävät:

12,24,30,36,40,45,48,56.

Sylowin lauseen perusteella pääsemme eroon ryhmistä, joiden kertaluvut ovat 40 ja 45. Näissä kummassakin Sylowin 5-aliryhmien määrä on viisi, sillä $n_5 \equiv 1 \mod 5$ ja $n_5 \mid 8, 9$, mikä pakottaa $n_5 = 1$ kummassakin tapauksessa.

Jäljellä ovat

12,24,30,36,48,56.

Nyt käytämme Poincaren argumenttia ryhmiin, joiden kertaluku on 12,24,48 tai 36. Oletetaan, että nämä ovat yksinkertaisia. Ensimmäiset kolme sisältävät Sylowin 2-aliryhmän, jonka indeksi on kolme. Yksinkertaisuuden perusteella $|G| \mid 3!$, mutta tämä ei tietysti ole totta millekään luvuista 12,24,48.

Jos $|G| = 36$, sisältää ryhmä Sylowin 3-aliryhmän, jonka indeksi on 4, mutta $36 \nmid 4! = 16$.

Viimeiset kaksi kertalukua, 30 ja 56 vaativat erillisen argumentin.

Jos 30 alkion ryhmä on yksinkertainen, sisältää se 6 Sylowin 5-aliryhmää ja näin ollen siinä olisi 24 alkiota, joiden kertaluku on 5. Yksinkertaisuus pakottaa sen sisältämään myös 10 Sylowin 3-aliryhmää, joten kertalukua 3 olevien alkioitten määrä on 20. Mutta nyt meillä on jo 44 alkiota ja ryhmän kertaluku on 30. Tämä on selvästi mahdoton yhtälö.

Jos kertaluku on 56 ja ryhmä on yksinkertainen, sisältää se 8 Sylowin 7-aliryhmää. Näissä on yhteensä 48 alkiota, joiden kertaluku on 7. Loppujen 56-48=8 alkion tulee siis muodostaa ryhmän ainoa Sylowin 2-aliryhmä (tällainen on olemassa Sylowin lauseen perusteella), mikä ainoana olisi väistämättä normaali. Ristiriita.

Tehtävä 48. Esseen aiheena voi jatkaa tästä ja miettiä, miksi ei ole yhtään yksinkertaista ryhmää, jonka kertaluku on $60 < |G| < 168$.

7 Ryhmälaajennukset: puolisuorat tulot ja köynnöstulot

Yksinkertaisista ryhmistä puhuessa todistettiin Jordan-Hölderin lauseen, jota asetti yksinkertaiset ryhmät tärkeään asemaan äärellisten ryhmien rakennuspalikoina. Toisaalta ensimmäisessä luvussa tarkasteltiin ryhmiä, joiden kertaluku on 2^n ja todettiin, että näitten lukumäärä kasvaa todella nopeasti n:n kasvaessa. On selvää, että jokaisen ryhmän, jonka koko on 2^n kompositiojono sisältää tekijäryhminä pelkästään ryhmiä C_2 ja on näin ollen myös ratkeava. Kahden alkion syklinen ryhmä on tietysti yksinkertaisesta ryhmistä yksinkertaisin, ja silti siitä voidaan koota suuri määrä monimutkaisia ryhmiä. On olemassa siis monta eri tapaa koota kahdesta ryhmästä kolmas. Tässä luvussa tutustumme kahteen uuteen tapaan rakentaa uusia ryhmiä vanhoista.

Abelin ryhmien kappaleessa tutuistuimme (ulkoisen) suoran tulon käsitteeseen. Olkoot $G_1, \ldots, G_n$ ryhmiä. Muodostamme karteesisen tulon $G := G_1 \times G_2 \times \cdots \times G_n$ ja tälle joukolle määrittelemme kaksipaikkaisen operaation yksinkertaisesti $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$, eli jokaisessa komponentissa i tulo noudattaa ryhmän G_i tuloa.

Esimerkki 7.1. Otetaan C_3 ja C_2 kaksi syklistä ryhmää. Niiden suora tulo on ryhmä $C_3 \times C_2 \cong C_6$.

Tämä esimerkin taustalla on se, että kahden joukon C_3 ja C_2 karteesiselle tulolle, voidaan antaa ryhmärakenne. Toisaalta samaisten kahden joukon karteesiselle tulolle voidaan antaa toinenkin ryhmä rakenne, eli tietysti S_3. Tarkastellaan tätä alkioitten tasolla. Merkitään C_2:n alkioita $1, a$ ja C_3:n alkioita $1, b, b^2$. Silloin karteesisen tulon alkiot ovat $(1,1), (b,1), (b^2,1), (1,a), (b,b), (b^2,a)$. Jos määrittelemme kertolaskun komponenttien mukaan, saamme vain suoran tulon, mutta voimme määritellä kertolaskuun myös pienen kierron. Unohdetaan siis merkinnästä sulut ja pilkut. Tavoitteena on kertoa esim. $b^2a * ba = b^2a * aa^{-1}ba = b^2a^{-1}ba$. Jos tämä ei olisi ulkoinen konstruktio, tietäisimme, miten konjugoida alkiota b alkiolla a. Nyt emme tiedä, mikä itseasiassa antaa meille vapauden päättää itse, minne konjugaatio lähettää tämän alkion. Voimme siis määritellä a:n tuottamaan tietyn C_3:n automorfismin. Jos määrittelemme automorfismiksi identiteetin, saamme suoran tulon. Jos taas määritämme automorfismiksi $1 \mapsto 1, b \mapsto b^2, b^2 \mapsto b$, saamme uuden ryhmärakenteen, joka tuottaa seuraavan kertolaskutaulukon 9.

Kuten jo kurssin alussa totesimme, kuuden alkion joukolla on täsmälleen kaksi ryhmärakennetta. Tässä esimerkissä laajennettiin ryhmää C_3 ryhmällä C_2, saatiin kaksi eri ryhmärakennetta, nimittäin $C_2 \times C_3$ ja S_3. Jälkimmäinen voidaan ylläolevan konstruktion perusteella esittää rakenteella, jota

Taulukko 9: Kuuden alkion epäkommutatiivinen ryhmä

$*$	1	a	b	ab	b^2	ab^2
1	1	a	b	ab	b^2	ab^2
a	a	1	ab	b	ab^2	b^2
b						
ab						
b^2	b^2		1			
ab^2						

kutsutaan puolisuoraksi tuloksi. Tämä ei ole ihan vieras käsite. Huomaamme jatkossa, että kaikki diedriryhmät D_{2n} ovat puolisuoria tuloja.

7.1 Puolisuorat tulot

Määritelmä 7.2. Ryhmää G kutsutaan ryhmän K laajennukseksi ryhmällä H, jos

$$K \lhd G \text{ ja } G/K \cong H.$$

Ryhmän laajennus ei ole yksikäsitteinen, kuten jo yllä olevasta esimerkistä huomasimme. Huomaa, että ryhmän laajennuksissa H:n ei välttämättä tarvitse olla G:n aliryhmä.

Voimme merkitä tällaista laajennusta kätevästi lyhyellä eksaktilla jonolla

$$1 \to K \to G \to H \to 1.$$

Seuraava konsruktio yleistää suoraa tuloa ja sitä kutsutaan ryhmien K ja H puolisuoraksi tuloksi, sillä se joukkojen K ja H karteesinen tulo.

Olkoot K ja H ryhmiä, ja olkoon $\phi : H \longrightarrow Aut(K)$ homomorfismi. Muotostamme joukon $K \rtimes_\phi H = \{(k, h) : k \in K, h \in H\}$ ja määrittelemme kahden alkion kertolaskun tässä ryhmässä $(k_1, h_1)(k_2, h_2) := (k_1 k_2^{\phi(h_1)}, h_1 h_2)$. Erona suoraan tuloon on se, että ennen kertolaskua K:ssa, alkio k_2 kuvataan joksikin toiseksi alkioksi automorfismilla $\phi(h_1)$.

Huomautus 7.3. Puolisuoraa tuloa määritellessä pitää aina sopia homomorfismi $\phi : G \longrightarrow Aut(K)$, ja on hyväksi merkitä tämä myös puolisuoran tulon merkkiin.

Viimeksi osoitimme, että $G = K \rtimes_\phi H$ on ryhmä. Liitännäisyys on hankalin, mutta kyllä sekin kärsivällisyydellä menee. Jos et ollut luennolla, tee tämä harjoitustehtävänä.

Tehtävä 49. Osoita , että aliryhmä $K_1 = \{(k, 1) : k \in K\}$ on G:n normaali aliryhmä, joka on isomorfinen K:n kanssa. Osoita myös, että $H_1 = \{(1, h) : h \in H\}$ on isomorfinen H:n kanssa. Ja lopulta myös, että $K \rtimes_\phi H = K \times H$ jos ja vain jos $h\phi = 1$ kaikille $h \in H$.

Yllä oleva konstruktio on ulkoiselle puolisuoralle tulolle. Sisäinen versio tästä saadaan seuraavasti. Jos on niin, että $K \lhd G$ ja $H \leq G$ sekä $G = HK$ ja $H \bigcap K = 1$, kutsumme H:ta K:n komplementiksi G:ssä. Tässä tapauksessa voimme käyttää merkintää

$$G = K \rtimes H,$$

ja sanoa, että laajennus halkeaa. Huomaa, että pikkukolmion kärki osoittaa normaaliin aliryhmään päin. Halkeavassa laajennuksessa, voimme kirjoittaa jokaisen G:n alkion yksikäsitteisesti hk, jossa $h \in H$ ja $k \in K$. Tämä, sillä $h_1k_1 = h_2k_2$ johtaa siihen, että $h_2^{-1}h_1 = k_2k_1^{-1} = H \bigcap K = 1$.

Esimerkki 7.4. Diedriryhmä $D_{2n} = C_n \rtimes_\phi C_2$, missä $C_2 =< t >$ ja t indusoi kuvauksen, joka kuvaa jokaisen a :n sen käänteisalkioon ryhmässä $C : n$ Voimme yleistää tämän konstruktion tapaukseen, jossa $C : n$ on ääretön syklinen ryhmä. Diedriryhmä $D_\infty = \mathbb{Z} \rtimes_\phi C_2$, missä $C_2 =< t >$ ja edelleen t indusoi kuvauksen, joka kuvaa jokaisen a:n sen käänteisalkioon ryhmässä $\mathbb{Z}$.

Esimerkki 7.5. Tarkastellaan puolisuoraa tuloa $A_5 \rtimes C_2$. Määritellään ensiksi ryhmän A_5 automorfismit. Kaikki sen automorfismit ovat sisäisiä automorfismeja, joten ryhmä C_2 indusoi sisäautomorfismin, ja toimii siis normaalisti konjugoimalla. Voimme valita alkioksi $t \in C_2$, minkä tahansa involuution, eli kakkosyklin, esimerkiksi (12). Koska puolisuorassa tulossa $A_5C_2 = G$ ja tiedämme, että viitossykli ja kakkossykli generoivat ryhmän S_5 on puolisuoran tulon pakko olla isomorfinen ryhmän S_5 kanssa.

7.2 Tapettikuviot

Kun mikä tahansa kaksiulotteinen taso on jaettu osiin tai koristeltu, voidaan sille antaa symmetriaryhmä. Usein symmetriaryhmä on vain triviaaliryhmä, mutta esimerkiksi tiiliseinän ryhmä ei ole triviaali, jos tiiliseinä on muurattu jonkun säännöllisen järjestelmän mukaan. Tiiliseinän symmetriaryhmä riippuu siitä, minkä muotoisia tiilet ovat, kuten myös siitä, miten ne on aseteltu limittäin.

Voimme ryhmäteorian avulla luokitella kaikki mahdolliset kaksiulotteiset tapettikuviot. Jotta käsite olisi järkevä ryhmäteoreettisesti oletamme aina, että peitämme tapettikuviolla äärettömän tason.

Määritellään ensin ryhmäteoreettisia perusteita.

Määritelmä 7.6. Tason $\mathbb{R}^2$ isometria on surjektiivinen kuvaus $\tau : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, joka säilyttää etäisyydet.

Esimerkkejä isometrioista ovat kierrot, siirrot, peilaukset sekä liukupeilaukset.

Siirto ja kierto säilyttävät orientaation, peilaukset ja liukupeilaukset kääntävät sen.

Propositio 7.7. *Jokainen $\mathbb{R}^2$:n aito (suunnat säilyttävä) isometria on joko kierto tai siirto. Jokainen epäaito isometria (eli suunnat kääntävä) on joko peilaus tai liukupeilaus.*

Tason $\mathbb{R}^2$ kaikki isometriat muodostavat ryhmän. Voidaan ajatella näitä tiettynä 2×2-matriisien ryhmänä. Kuvan perusteella kahden aidon tai epäaidon isometrian tulo on aina aito isometria, kun taas aito ja epäaito ovat tulona epäaito.

Tapettikuvion perusajatus on, että siinä on joku kuvion perusyksikkö, joka toistuu jaksottain ja äärettömästi kahdessa dimensiossa, kahden ei-paralleelin akselin suuntaisesti. Oletamme, että tämä peruskuvion toisto täyttää koko tason. Tämä jaksoittainen, mutta epäjatkuva toistuminen tarkoittaa sitä, että käsittelemme $\mathbb{R}^2$:n diskreettejä isometrioita.

Määritelmä 7.8. $\mathbb{R}^2$:n isometriaryhmä G on diskreetti jos ja vain jos, jokaista pistettä $p \in \mathbb{R}^2$ kohden on olemassa ympyrä Y_p, jonka keskipiste on p ja jokainen $g \in G$ joko kiinnittää pisteen p tai siirtää sen pisteeseen gp, joka on tämän ympyrän Y_p ulkopuolella.

Tapettikuvioryhmä on eräs diskreettin ryhmän muoto. Tässä tapauksessa tasosymmetria ryhmä.

Määritelmä 7.9. Tasosymmetriaryhmä on $\mathbb{R}^2$:n isometria ryhmän diskreetti aliryhmä, joka sisältää siirrot s, t kahteen ei-paralleeliin suuntaan.

Olkoon G on tällainen ryhmä, ja olkoon $p \in \mathbb{R}^2$. Silloin kun käytämme isometrioita $s^i t^j$ missä $i, j \in \mathbb{Z}$ pisteeseen p, saamme tulokseksi äärettömän hilan.

Jos valitsemme s, t:n pienimmiksi mahdollisiksi siirroiksi, tiedämme, että jokainen siirto on muotoa $s^i t^j$. Ja näiden 'vektorien' väliin jäävää aluetta kutsutaan hilan perusalueeksi (fundamental domain). Joka tapauksessa, siirtojen ryhmä vaatii vain kaksi virittäjää ja se on isomorfinen ryhmän $\mathbb{Z}^2$ kanssa, koska siirrot ovat luonnollisesti vaihdannaisia.

Tehtävä 50. Ylläolevan määritelmän nojalla yksinkertaisin tasosymmetriaryhmä on $\mathbb{Z}^2$. Kuviossa ei siis ole ollenkaan kiertosymmetriaa. Etsi tällainen jostain ympäristöstäsi ja piirrä tai ota siitä kuva digi/kännykkäkameralla, jos omistat sellaisen.

On kuitenkin olemassa myös tapettikuvioita, joissa on jonkunlaista kierto- tai peilisymmetriaa.

Tarkastellaan siis seuraavaksi mahdollisia kiertoja. Oletetaan, että t on pienin siirto ja r kierto, jonka kulma on pienin mahdollinen $\theta = \frac{2\pi}{n}$

Valitaan kolme pistettä c_0, c_1, c_1' niin, että t siirtää c_0:n c_1:een, ja r siirtää pisteen c_1 pisteeseen c_1'. Nyt alkio $t' = rtr^{-1}$, joka kuuluu ryhmään G, on siirto, joka siirtää pisteen c_0 pisteeseen c_1'. Ja sitten alkio $t't^{-1}$ on siirto, joka siirtää c_1:n pisteeseen c_1'. Koska t oli valittu pienimmäksi mahdolliseksi, näemme, että etäisyys c_1c_1' ei voi olla lyhyempi kuin c_0c_1. Tämä tarkoittaa sitä, että kulma $c_1c_0c_1'$ on ainakin $\pi/3$. Tästä seuraa, että $\frac{2\pi}{n} \geq \frac{\pi}{3}$, joten $n \leq 6$.

Tehtävä 51. Osoita, että $n = 5$ ei myöskään toimi.

Lause 7.10. *Olkoon G tasosymmetriaryhmä. Silloin siihen kuuluvat kierrot ovat kertalukua 1,2,3,4 tai 6.*

Seuraavaksi tarkastelemme, minkälaisia hiloja tasosymmetriaryhmä voi tuottaa. Tavoitteena on todistaa, että niittä on viittä eri perustyyppiä.

Unohdetaan siirrot hetkeksi, ja tarkastellaan kiertojen tuottamaa hilaa. Jokaisella hilalla on luonnollinen kiertosymmetria kulman π ympäri (jompikumpi hilan luonnollinen akseli).

Tarkastellaan nyt kiertoa, jonka kertaluku on 3. On olemassa kaksi eri tapausta riippuen siitä, onko kierron keskipiste hilan piste vai ei. Itseasiassa kumpikin näistä tapauksesti antaa identtisen hilan, joka koostuu tasasivuisista kolmioista. Tällaisessa hilassa on myös kertalukua 6 oleva kierto jokaisen hilan pisteen ympäri. Tällaista hilaa kutsutaan heksagonaaliseksi hilaksi.

Jos taas kierron kertaluku on 4, edelleen kierron keskipiste on joko hilan piste tai ei. Joka tapauksessa, kumpikin antaa lopulta neliöhilan.

Toiseksi tarkastelemme hiloja, joilla on peilisymmetria, jonkun suoran suhteen. Huomaa, että tämä suora ei välttämättä sisällä yhtään hilan pistettä. Koska peilauksen pitää toimia yhdessä kiertojen kanssa (ääretön kuvia, joka toistuu), peilisymmetriaa sisältävä hila ei voi olla heksagonaalinen. Tällainen hila on väistämättä koottu joko nelikulmioista tai timanteista (tasasivuinen suunnikas). Jos hilassa on liukupeilauksia, on se väistämättä koottu timanteista, eli on keskitetyn nelikulmiohilan muotoinen.

On siis vain viittä eri hilatyyppiä, joiden kuvat voit piirtää alle.

Jatketaan hilan lokaalia tarkastelua, jonkun pisteen ympäristössä, sillä siirrot jo hallitsemme.

Määritelmä 7.11. Kaksiulotteinen kristallograafinen **pisteryhmä** K on $\mathbb{R}^2$:n sellaisten isometrioitten ryhmä, joka kiinnittää pisteen p ja kuvaa 2-dimensioisen hilan, joka sisältää p:n itseensä.

Tällaisessa ryhmässä ei voi olla siirtoja tai liukupeilauksia, sillä kumpikaan niistä ei kiinnitä mitään pistettä p. Siispä kaikki K:n alkiot ovat joko kiertoja tai puolet niistä ovat kiertoja ja puolet ovat peilauksia, joten koska kiertojen kertaluvut ovat 1,2,3,4,6 on ryhmä K isomorfinen joko C_n tai D_{2n}:n kanssa kun $n = 1, 2, 3, 4, 6$.

Lopulta osoitamme, että tapettiryhmä koostuu sekä siirtoryhmästä, että pisteryhmästä ja itseasiassa on näiden kahden puolisuora tulo, eli $G \cong H \rtimes K$.

Tarkemmin, osoitamme, että on olemassa homomorfismi $\phi : G \longrightarrow K$ ja $Ker\phi = H$ ja $G/H \cong K$.

Valitaan piste O tasolta $\mathbb{R}^2$. Jos ρ on mikä tahansa isometria, joka siirtää pisteen O pisteeseen a, ja t on siirto, joka siirtää pisteen a pisteeseen O, silloin $s = t^{-1}\rho$ kiinnittää pisteen O, mikä tarkoittaa sitä, että s on joko kierto pisteen O ympäri tai peilaus sellaisen viivan suhteen, joka menee O:n läpi. Nyt voimme kirjoittaa isometrian $\rho = ts$.

Tiedämme, että siirtoaliryhmä T on normaali aliryhmä ryhmässä kaikkien isometrioitten ryhmässä E. Määritellään $H = T \cap G$, joka on siirtoaliryhmä diskreetissä ryhmässä G. Silloin $H \lhd G$.

Oletetaan, että $g_1 = t_1 s_1$ ja $g_2 = t_2 s_2$ ovat kaksi ryhmän g alkiota, jossa t_i on siirto ja s_i kierto tai peilaus, kuten yllä. A priori, emme oleta, että $s_i, t_i \in G$. Nyt

$$g_1 g_2 = t_1 s_1 \cdot t_2 s_2 = t_1 \cdot s_1 t_2 s_1^{-1} \cdot s_1 s_2,$$

jossa $s_1 t_2 s_1^{-1}$ on siirto ja $s_1 s_2$ kiinnittää pisteen O (koska kumpainenkin, s_1 ja s_2 kiinnittää sen).

Samalla tavalla voimme kirjoittaa alkion

$$g_1^{-1} = (t_1 s_1)^{-1}$$

muotoon

$$s_1^{-1} t_1^{-1} s_1 s_1^{-1},$$

missä s_1^{-1} on kierto O:n ympäri, ja $s_1^{-1} t_1^{-1} s_1$ on siirto.

Muistamme, että s_i oli alunperin alkio $t^{-1}\rho$, mutta nämä operaatiot osoittavat, että itseasiassa tällaiset alkiot s_i hajotelmissa $g_i = t_i s_i$ muodostavat ryhmän K, joka kiinnittää pisteen O.

Näin ollen kuvaus $\theta : G \longrightarrow K$, joka kuvaa $\theta(g_1) = \theta(t_1 s_1) = s_1$ on surjektio G:stä ryhmään K. Sen ydin on $Ker\theta = H$. Jos nyt vielä annamme H:n alkioiden toimia pisteeseen O, huomaamme, että näin saamme muodostettua hilan L.

Oletetaan nimittäin, että $a \in L$, joten $a = tO$, jollekin sopivalle $t \in H$. Olkoon $s \in K$. Silloin on olemassa $g \in G$ siten, että $g = t_1 s$, jollekin sopivalle $t_1 \in T$. Koska

$$sa = stO = t_1^{-1} gtO = t_1^{-1} gtg^{-1} gO = t_1^{-1} gtg^{-1} t_1 sO.$$

Mutta s kiinnittää O:n ja gtg^{-1} siirtää hilan itseensä, joten $sa = gtg^{-1}O$ on piste hilassa L, joten $K \cong G/H$ on pisteryhmä, joka kuvaa hilan, jonka määrittävät ryhmä H ja piste O itseensä.

Jotta siis saisimme luokiteltua ryhmät G jotka ovat tapettikuvioryhmiä, pitää meidän määritellä hila L, piste O ja pisteryhmä K. Tässä emme käy luokittelua läpi, mutta toteamme, että ylläolevan proseduurin mukaisesti tämä on täysin mahdollista.

Tarkastellaan paria esimerkkiä kuvallisesti.

Yksinkertaisin tapettikuvioryhmä on $\mathbb{Z}^2$. Sen hila koostuu suunnikkaista, joiden sivujen pituudet ovat erisuuret. Heksagonaalisessa hilalla voi olla monta symmetriaryhmää, ja ne riippuvat koristeluista.

Yksi tapettikuvioryhmä on $\mathbb{Z}^2 \rtimes C_2$, jossa C_2 toimii $\mathbb{Z}$:ssa kääntämällä kunkin alkion. Tämän ryhmän tapettikuvio on klassinen symmetrinen köynnös yhteen suuntaan.

Liukupeilaus saadaan vain keskitetyn neliöhilan suhteen.

Tehtävä 52. Gradun aihe: Mikä on ryhmän $\mathbb{Z}^2 \rtimes C_2$ aliryhmäin kasvu? Miten karakteroisit aliryhmiä? Vertaa tätä aliryhmän kasvu funktiota ryhmän $\mathbb{Z}^2$ vastaavaan. Mitä huomaat?

7.3 Lampunvartijan ryhmä ja köynnöstulot

Tapettikuvioryhmien luvussa käsittelimme puolisuoran tulon käsitettä. On myös hankalampi ryhmä, jonka voimme luoda kahden ryhmän tulona. Tämä on niin kutsuttu köynnöstulo.

Köynnöstulo määritellään helpoiten ryhmän toimintojen avulla. Olkoot siis H ja K ryhmiä, joista H toimii joukossa $|\Gamma| = g$ ja K joukossa $|\Delta| = d$. Haluamme määritellä ryhmän, joka toimii transitiivisesti joukossa $\Omega = \Gamma \times \Delta$.

Määrittelemme köynnöstulon kantaryhmäksi ryhmän, joka muodostuu kuvauksista $f : \Delta \to H$. Ryhmäoperaatio on pisteittäinen kertolasku, eli $f_1 f_2(\delta) := f_1(\delta) f_2(\delta)$. Tämän operaation suhteen $\mathcal{F}(\Delta, H) \cong H^d$. Tämä siis tarkoittaa sitä, että meillä on H:n kopioita yhteensä d kappaletta, ja ne on numeroitu Δ:n alkioilla.

Kantaryhmä toimii joukossa Ω seuraavasti

$$(\gamma, \delta)f = (\gamma f(\delta), \delta).$$

Kun taas ryhmä K toimii permutoimalla H:n kopiot

$$(\gamma, \delta)k = (\gamma, \delta k).$$

Määrittelemme ryhmän $HwrK = B \rtimes K = \{fk : f \in B, k \in K\}$. Puolisuorassa tulossa K:n toiminta B:ssä on juuri sellainen kuin odotamme,

eli $f_1k_1f_2k_2 = f_1f_2^{k_1^{-1}}k_1k_2$, missä

$$f^k(\delta) := f(\delta k^{-1})$$

Tutkikaamme pienintä mahdollista esimerkkiä C_2wrC_2, jotta saamme jotain järkeä tähän rakenteeseen. Ensiksikin ryhmän koko on 2^3, sillä kantaryhmä on $C_2 \times C_2$, jossa C_2 toimii vaihtamalla C_2:n kopiot. Ryhmä on siis $(C_2 \times C_2) \rtimes C_2$. Laadimme Cayleyn taulukon tästä ryhmästä. Merkitään alkioita $(aa)a$, jossa $a^2 = 1$.

Taulukko 10: kertolaskutaulu ryhmälle C_2wrC_2

*	(11)1	(1a)1	(a1)1	(aa)1	(11)a	(1a)a	(a1)a	(aa)a
(11)1	(11)1	(1a)1	(a1)1	(aa)1	(11)a	(1a)a	(a1)a	(aa)a
(1a)1	(1a)1	(11)1	(aa)1	(a1)1	(1a)a	(11)a	(aa)a	(a1)a
(a1)1								
(aa)1								
(11)a								
(1a)a								
(a1)a								
(aa)a								

Tehtävä 53. Täydennä ylläoleva taulukko ja päättele, mikä ryhmä on kyseessä. Luokittelimme viisi kertalukua kahdeksan olevaa ryhmää ensimmäisessä luvussa.

Tehtävä 54. Kuinka monta alkiota on ryhmässä S_5wrC_3? Osoita, että ryhmän S_n Sylowin p-aliryhmä on köynnöstulo.

7.4 Lampunvartijan ryhmä

Kutsumme köynnöstuloa $(\mathbb{Z}/2\mathbb{Z})wr\mathbb{Z}$ lampunvartijan ryhmäksi, ja merkitsemme sitä kirjaimella L. Köynnöstulon kantaryhmä B on

$$\bigoplus_{n\in\mathbb{Z}} \mathbb{Z}/2\mathbb{Z},$$

ja tämän perusteella L/B on isomorfinen ryhmän $\mathbb{Z}$ kanssa.

Jos haluamme kuvailla ryhmää virittäjien ja suhteitten avulla, vakioesitys lampunvartijan ryhmälle annetaan köynnöstulon rakenteen kautta

$\langle a, t : [t^m a t^{-m}, t^n a t^{-n}], m, n \in \mathbb{Z} \rangle$. Esitystä voidaan yksinkertaistaa $\langle a, t : (at^n a t^{-n})^2, n \in \mathbb{Z} \rangle$. Näiden lisäksi $a^2 = 1$.

Ryhmän nimi tulee ryhmän hyödyllisestä visualisoinnista. Voimme ajatella tämän ryhmän toimivan kumpaankiin suuntaan äärettömässä jonossa katulamppuja ..., $l_{-2}, l_{-1}, l_0, l_1, l_2$, ..., (huomaa, että nämä on indeksoitu ylemmän ryhmän alkioilla). Jokainen näistä lampuista voi joko palaa tai olla sammutettu. Lisäksi jonkun lampun, sanokaamme, l_k:n alla seisoo lampunvartija. Ryhmän virittäjä t kehottaa lampunvartijaa kulkemaan seuraavalle lampulle (vastaavasti t^{-1} kehottaa lampunvartijaa kulkemaan edelliselle lampulle), kun taas virittäjä a ilmoittaa, että lampun l_k status muuttuu, eli jos lamppu palaa, sammutetaan se, ja jos lamppu on sammuksissa, sytytetään se.

Lyhyesti, ryhmän alkio siis toimii äärellisenä jonona siirtoja. Lampun vartija lähtee lampusta l_k liikkeelle, kulkee tietyille lampuille, sammuttaa tai sytyttää ne, ja pysähtyy lampulle l_m. Tämän perusteella on helpompi ymmärtää virittäjiä ja suhteita.

Voimme olettaa, että vain äärellinen määrä lamppuja on sytytettynä minä tahansa hetkenä, koska minkä tahansa L:n alkion toiminta muuttaa korkeintaan äärellisen määrän lamppuja. Tämä ei kuitenkaan estä sitä, että rajoittamaton määrä lamppuja olisi sytytettynä.

Ryhmän toiminta on tämän vuoksi samankaltainen/samanlainen Turingin koneen toiminnan kanssa.

Tehtävä 55. Millainen on ryhmä $\mathbb{Z}wrC_2$? Miten se eroaa äärettömästä diedriryhmästä $\mathbb{Z} \rtimes_\phi C_2$, jossa ϕ toimii käänteisoperaationa.

Lopuksi tutkimme ryhmää $\mathbb{Z}wr\mathbb{Z}$.

Tämän ryhmän alkiot ovat muotoa (f, n), jossa $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, $n \in \mathbb{Z}$, joten $B \cong (\Pi_{n\in\mathbb{Z}}\mathbb{Z})$ kanssa. Tämän alkiot ovat muotoa $(f, 0)$. Luonnollisesti $\mathbb{Z}wr\mathbb{Z} = B \rtimes \mathbb{Z}$, jossa $\mathbb{Z}$ toimii joukossa B luonnollisesti permutoimalla. Kertolasku ryhmässä on määritelty $(f, n)(h, m) = (k, n + m)$, missä $k(i) = f(i)+h(i+n)$. Konjugointi alkiolla $(0, 1)$ toimii seuraavasti: $(f, n)^{(0,1)} = (g, n)$, jossa $g(i) = f(i+1)$, joten konjugointi siirtää kuvaa yhden pykälän eteenpäin.

Tehtävä 56. Olkoon

$$f(n) = \begin{cases} 1 & \text{, jos n on parillinen} \\ -1 & \text{, jos n on pariton.} \end{cases}$$

Laske $(f, 0)^{(0,1)}$.

8 Vapaa ryhmä

Kolmosluvussa määrittelimme vapaan Abelin ryhmän. Se oli vapaa Abelin ryhmien kategoriassa. Edellisessä luvussa tutustuimme ratkeavien ryhmien kategoriaan. Nyt määrittelemme vapaan ryhmän kaikkien ryhmien kategoriassa.

Intuitiivisesti, vapaa ryhmä on se ryhmä, josta on mahdollista tuottaa kaikki ryhmät. Samaan tapaan kuin kaikki äärelliset ryhmät ovat symmetrisen ryhmän aliryhmiä, ovat kaikki ryhmät vapaan ryhmän tekijäryhmia. Tarkastelemalla ryhmiä vapaan ryhmän tekijäryhminä, saamme myös uuden tavan esittää ryhmiä, johon olemme pari kertaa jo tällä kurssilla törmänneet.. Jo ryhmäteorian alkeissa huomataan, ettei ryhmän kertolaskutaulukko (Cayleyn taulukko) ole kaikkein kätevin tapa hahmottaa ryhmää, sillä se kasvaa tavattoman suureksi tavattoman nopeasti, jo kahdeksan alkion ryhmässä oli työlästä laatia Cayleyn taulukko. Tämän kappaleen tärkeintä materiaalia on ryhmän esittäminen virittäjien ja suhteiden avulla. Tähän olemme jo hieman viitanneet aikaisemminkin.

Vapaan ryhmän määritelmä on kategoriateoreettinen.

Määritelmä 8.1. Olkoon $X = \{X_i\}_{i \in I}$ joukko. Vapaa ryhmä joukolle X koostuu ryhmästä $F = F_X$ ja kuvauksesta $i \colon X \longrightarrow F$, jolle pätee kaikille ryhmille G ja kuvauksille $j \colon X \longrightarrow G$ on olemassa yksikäsitteinen homomorfismi $\rho \colon F \longrightarrow G$, joka kommutoi $\rho \circ i = j$.

Kategoriateoreettisen hölynpölyn avulla on selvää, että tämä ryhmä on olemassa, mutta sen konstruointi ei ollut täysin yksinkertaista.

Käsittelemme nyt algebrallista konstruktiota. Olkoon X symmetrinen aakkosto. Symmetrinen tarkoittaa sitä, että jos $x \in X$ on myös $x^{-1} \in X$. Aakkoston voi yleisemmin ymmärtää virittäjäjoukoksi.

Esimerkiksi, olkoon $X = \{a, b\}$, ja olkoon e tyhjä sana. Aakkostosta voidaan muodostaa sanoja a, b, ab, ba, $aaabbbaaababababaa$. Jos ymmärretään aakkoset ryhmän virittäjinä, on kukin sana tietysti ryhmän alkio. Muistamme kuitenkin, että virittäjät oli saatettu valita niin, että $a^2 = 1$, jolloin sana $aaabbbaaababababaa = abbbababababab$, joten kaksi eri sanaa esittävät ryhmän alkiota. Määrittelemme seuraavaksi vapaan tulon ja supistetut sanat, jotta saamme vapaan ryhmän konstruoitua.

Olkoot v ja w kaksi sanaa aakkostossa X. Silloin vw on sana, jossa v ja w on kirjoitettu yhdeksi sanaksi. Jos sana v päättyy kirjaimeen x ja sana w alkaa kirjaimella x^{-1}, supistetaan nämä kirjaimet. Kun kaikki mahdolliset supistukset on tehty, saadaan supistettu sana.

Propositio 8.2. *Olkoon X aakkosto. Supistetut sanat muodostavat vapaan*

ryhmän aakkostossa (virittäjistössä) X. Ryhmän kertolaskuna on sanojen kirjoittaminen vierekkäin.

Todistus. On selvää, että tämä operaatio muodostaa ryhmän. Tarkistamme, että ryhmä on vapaa. □

8.1 Ryhmän esitys virittäjien ja suhteitten avulla

Lause 8.3. *Jokainen ryhmä on vapaan ryhmän tekijäryhmä.*

Todistus. Todistamme äärellisesti viritetyn tapauksen. Vapaan ryhmän määritelmän mukaan jokainen virittäjäkuvaus $\phi : X \longrightarrow A$ laajenee ryhmähomomorfismiksi $\phi : F \longrightarrow G$. Tämä ryhmähomomorfismi on surjektiivinen vapaan ryhmän universaaliominaisuuden perusteella. Niinpä ensimmäisen isomorfialauseen perusteella $G \cong F/Ker\phi$. □

Huomaa, että $Ker\phi$ koostuu niistä sanoista ryhmässä F, jotka ovat triviaaleja sanoja ryhmässä G. Näitä triviaalia sanoja kutsutaan suhteiksi.

Esimerkki 8.4. Tässä joitain tuttujen ryhmien esityksiä. Mitkä näiden ryhmien nimet ovat?

1. $\langle a : a^n = 1 \rangle$
2. $\langle a, b : a^2 = b^2 = 1, ab = ba \rangle$
3. $\langle a, t : a^4 = t^2 = 1, tat = a^{-1} \rangle$.
4. $\langle s_1, s_2, s_3 : s_i^2 = 1, (s_1 s_2)^3 = (s_2 s_3)^5 = (s_1 s_3)^2 = 1 \rangle$
5. $\langle a, b, c : a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}ac = a^2 \rangle$

Tehtävä 57.

Mikä ryhmä saadaan, kun virittäjinä ovat kaikki suomen kielen luonnolliset aakkoset, $a, b, c, \ldots, ,,$ ja relaatioina kaikki suomenkieliset sanat. Eli $auto = 1, talo = 1$ jne? Muuttuuko tulos, jos sallimme taivutusmuodot? Entä, jos otamme pois vierasperäiset kirjaimet?

Olkoon ryhmän virittäjät nyt aakkoset $a, b, c, \ldots, x, y, z$, eli englannin akkosto. Mikä ryhmä saadaan, kun suhteina ovat kaikki homonyymit, eli sanat, jotka kirjoitetaan eri tavalla, mutta lausutaan samalla tavalla. Esim. $pear = pair$ ja $hear = here$.

Tehtävä 58. Ovatko seuraavat ryhmät isomorfiset?

$$\langle a, b : a^2 = b^3 = 1, (ab)^2 = 1, (ab^2)^2 = 1 \rangle$$

ja

$$\langle a, b, c : a^2 = b^2 = c^2 = 1, ab = bc, acbc = 1 \rangle.$$

Tehtävä 59. Olkoon $\langle k, l, m : k^3 = l^4 = m^8 = 1, mkl = lk, m^3k^2 = l^3, \rangle$ supista sanaa $mklk^2l^5mkmk$ niin paljon kuin mahdolista. Onko tämä sana ykkösalkio?

Yksi ryhmän esitysten ongelma on, että niiden perusteella on hyvin hankala sanoa, onko joku tietty sana yksikköalkio. Itseasiassa, tämä ongelma on päättämätön (undecidable). Kuten myös se, milloin kaksi ryhmää ovat isomorfisia tai kaksi alkiota ovat toistensa konjugaatteja. Nämä ongelmat tunnetaan nimillä sanaongelma, isomorfismiongelma ja konjugaatio-ongelma. Yleistä ratkaisua näille ongelmille ei ole, mutta niitä voidaan tutkia tietyissa ryhmätyypeissa, ja joissain ne voidaan päättää. Sanaongelma on ratkeava esimerkiksi hyperbolisissa ryhmissä ja peilausryhmissä. (Rips, Sela, Tits. Tits on viime vuoden Abelin palkinnon voittaja)

Sanaongelmia voidaan hahmottaa Cayleyn verkon ja sen geometristen ominaisuuksien avulla. (Itseasiassa hyperbolisen ryhmän määritelmässä käytetään Cayleyn verkkoa.)

Oletetaan, että ryhmällä G on äärellinen virittäjäjoukko $X \bigcup X^{-1}$. Cayleyn verkon solmut ovat ryhmän G alkiot. Solmut a ja b yhdistetään, jos on olemassa sellainen $x \in X$, että $ax = b$. Joten jokainen ryhmän kaari vastaa siis virittäjäjoukon alkiota.

Esimerkki 8.5. Tarkastelemme ryhmän kahden alkion virittämän vapaan ryhmän Cayleyn verkkoa. Olkoot x ja y ryhmän F_2 virittäjät. Koska haluamme tarkastella symmetristä virittäjäjoukkoa, virittäjät ovat x, x^{-1}, y, y^{-1}. Aloitamme konstruoinnin ykkösalkiosta. Ykkösalkiosta lähtee yhteensä neljä kaarta, alkioihin x, x^{-1}, y, y^{-1}. Alkiosta x lähtee kaari takaisin ykkösalkioon, ja tämän lisäksi alkioihin x^2, xy, xy^{-1}. Kukin verkon solmu on siis redusoitu sana aakkostossa x, y, kuten pitääkin. Lisäksi huomaamme, että verkossa ei ole syklejä, sillä sykli vastaa suhdetta, ja vapaassa ryhmässä ei ole suhteita. Cayleyn verkko on siis yksinkertaisesti ääretön 4-valentti puu.

Tehtävä 60. Mikä on $\mathbb{Z}$:n Cayleyn verkko? Minkälainen on $\mathbb{Z} \times \mathbb{Z}$:n Cayleyn verkko? Piirrä Cayleyn verkko ryhmälle S_3, kun sen virittäjät ovat $(12), (13), (23)$. Piirrä vastaava verkko virittäjille $(12), (123)$. Miten virittäjien valinta vaikuttaa verkkoon?

Verkon ominaisuuksien perusteella voimme määritellä ryhmien ominaisuuksia. Esimerkiksi hyperboliset ryhmät viittaavat ryhmiin, joiden verkko muistuttaa hyperbolista avaruutta. Tämä verkko ei riipu virittäjäjoukon valinnasta.

Cayleyn verkolle voidaan helposti antaa luonnollinen metriikka toteamalla, etta jokaisen sivun pituus on yksi, tätä metriikaa kutsutaan sanametriikaksi. Avoin pallo, jonka säde on ℓ on origosta lähtien kaikkien niiden sanojen joukko, joiden pituus on korkeintaan ℓ. Jos määrittelemme kunkin verkon kaaren pituudeksi 1, saamme geometrisen merkityksen tälle määritelmälle.

Sanojen kasvulla puolestaan tarkoitetaan sitä, kuinka monta ryhmän alkiota voidaan esittää korkeintaan n:n pituisena sanana. Geometrisesti ajatellen tämä tarkoittaa sitä, miten monta alkiota sisältyy n-pallon sisälle tässä metriikassa. Joskus tämä pallo kasvaa lineaarisesti, joskus polynomisesti, joskus eksponenttisesti. On myös joitain ryhmiä, joille kasvu on alieksponenttinen. Nämä ryhmät ovat oksaryhmiä, jotka voidaan määritellä tiettyjen puiden automorfismiryhminä.