Lineaariset ryhmät

Pro gradu -tutkielma
Miia Lillstrang 2187044
Matematiikan yksikkö
Oulun yliopisto 2016

Sisältö

Johdanto

Ryhmä on matematiikan algebraksi kutsutun haaran kenties perustavin käsite. Ryhmä koostuu joukosta alkioita sekä operaatiosta, joka on määritelty joukon minkä tahansa kahden alkion välille. Jotta kyseessä olisi ryhmä, on alkioiden ja operaation toteutettava vain muutamia yksinkertaisia ominaisuuksia.

Erilaisten ryhmien ja niiden ominaisuuksien maailma on suuri ja ihmeellinen. Alaluvussa 1.1 tutustutaan *aliryhmiin*, *normaaleihin aliryhmiin*, *tekijäryhmiin* ja *syklisiin ryhmiin*. Luvussa 2 esitellään kolme tyyppiä *lineaarisia ryhmiä* eli päästään työn nimikkoaiheeseen. Lineaaristen ryhmien idea on se, että niiden yhteydessä käsitellään matriiseja. -Tämän työn tapauksessa hillitysti vain pieniä 2×2 -matriiseja. Kahdessa ensimmäisessä lineaaristen ryhmien tyypissä ryhmän alkiot ovat matriiseja. Kolmas tyyppi on tekijäryhmä toisen tyypin suhteen; hieman mutkikkaampi tapaus siis, mutta erityisen mielenkiintoinen.

Tämä kolmas ja mielenkiintoinen lineaaristen ryhmien tyyppi on lyhyeltä nimeltään $PSL(2, K)$, pitkältä nimeltään *astetta kaksi oleva projektiivinen erityinen lineaarinen ryhmä kunnan K suhteen*. Lajin yksilöistä tarkastellaan lähemmin tapauksia $PSL(2, 5)$ (luku3), $PSL(2, 4)$ (luku 4) sekä $PSL(2, 7)$ (luku 5). Kaikissa tarkasteluissa käytetään alaluvussa 1.2 rakennettua työvälinettä: *konjugaatteja*. Tarkastelun päämääräänä on kussakin tapauksessa selvittää, onko yksilö kenties *yksinkertainen* eli onko sillä ainoastaan *triviaalit normaalit aliryhmät*. Ryhmien maailmassa yksinkertaisuus on jännittävä, jopa toivottava ominaisuus ja olemme ylpeitä, jos onnistumme löytämään yksinkertaisia ryhmiä.

Jännitystä ei valitettavasti ole syytä pitää yllä, koska lopputulema näkyy jo sisällysluettelosta: kaikki kolme tarkkaan tarkasteltua lineaarista ryhmää osoittautuvat yksinkertaisiksi. Työ huipentuu viimeiseen lukuun 6, jossa osoitetaan, ettei kyseessä ole sattuma: kaikki tyyppiä $PSL(2, K)$ olevat lineaariset ryhmät ovat yksinkertaisia (kunhan *kunnan K* (ks. alaluku 1.3) *kertaluku* on vähintään neljä).

Työn sisältö on pyritty optimoimaan kahden tavoitteen mukaan. Ensimmäinen tavoite on se, että esitietoja vaadittaisiin mahdollisimman vähän eikä tuloksia nyhjäistä tyhjästä. Toisena tavoitteena on, että tarvittavia tuloksia varten ei kuljettaisi tarpeettoman pitkää reittiä, vaan jos mahdollista, oikoreittiä. Näiden kahden paineessa tasapainottelu on ollut haastavaa, mutta ainakin kirjoittaja on innoissaan tuloksena syntyneestä retkestä.

Lukuiloa!

1 Esitietoja

Tässä luvussa luodaan tulevan työn perusta ja käydään läpi sellaiset perustavat määritelmät ja lauseet, joita tarvitaan työssä myöhemmin. Kuten matematiikassa yleensä, kertyy läpi käytävää melko paljon, kun halutaan tunnollisesti avata lukijalle edistyneempään tulokseen johtavan matematiikan puu.

Joitakin asioita lukijan oletetaan tietävän ennestään: Kongruenssin ja jäännösluokkien käsitteet sekä niihin liittyvät perustulokset oletetaan tutuiksi. Relaation käsitteen sekä ekvivalenssirelaation ja sen perusominaisuuksien oletetaan myös olevan ennestään tuttuja. Jakoalgoritmi oletetaan tutuksi ja sitä käytetään ilman erillisiä perusteluja. Myöskään operaation tai binäärioperaation määritelmiä ei esitetä, sillä ne oletetaan tunnetuiksi.

Merkintöjä

Tässä työssä käytetään seuraavia merkintöjä:

- Luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, 2, \ldots\}$
- Kokonaislukujen joukko $\mathbb{Z}$
- Positiivisten kokonaislukujen joukko $\mathbb{Z}^+ = \{1, 2, \ldots\}$
- Ryhmän G aliryhmän H vasen sivuluokka alkion $a \in G$ suhteen: yleisesti aH, yhteenlaskun tapauksessa $a + H$.
- Alkion a generoima ryhmän G syklinen aliryhmä: $\langle a \rangle$.

1.1 Ryhmät

On olemassa monenlaisia *ryhmiä*. On *Abelin ryhmiä* ja *tekijäryhmiä*. *Lineaariset ryhmätkin* ovat ryhmiä. Ryhmä ryhmän sisällä on *aliryhmä*, ja *sykliset ryhmät* käyttäytyvät kesysti.

Määritellään ryhmä, jotta päästään alkuun. Tutustumme tässä myös ryhmiin liittyviin perustuloksiin, joista kaikki tulevat olemaan tarpeellisia myöhemmin.

1.1.1 Ryhmä ja aliryhmä

Tässä kappaleessa määritellään ryhmä sekä aliryhmä ja osoitetaan niihin liittyviä perustuloksia.

Määritelmä 1.1. Pari $(G, *)$ eli joukko G yhdessä binäärioperaation $*$ kanssa on *ryhmä*, mikäli

(i) Joukko G on *suljettu* operaation $*$ suhteen, eli jos alkiot $a, b \in G$, niin myös $a * b \in G$.

(ii) Joukossa G on *neutraalialkio* e eli $e * a = a * e = a$ kaikilla $a \in G$.

(iii) Kaikilla joukon G alkioilla $a \in G$ löytyy joukosta G *käänteisalkio* a^{-1}, jolla $a * a^{-1} = a^{-1} * a = e$.

(iv) Kaikilla joukon G alkioilla a, b, c pätee $(a*b)*c = a*(b*c)$, eli operaatio $*$ on *assosiatiivinen*.

Jos ryhmässä G on ääretön määrä alkioita, se on *ääretön ryhmä*. Jos alkioita on äärellinen määrä, ryhmä G on *äärellinen*.

Huomautus (Merkintöjä)**.** Kun on selvää, että käytetään ryhmässä määriteltyä operaatiota $*$, merkitään $a * b = ab$. Alkion a operoimista n kertaa itsensä kanssa merkitään a^n. Merkinnällä a^{-n} tarkoitetaan alkion a^n käänteisalkiota $(a^n)^{-1}$. Määritellään lisäksi $a^0 = e$.

Määritelmä 1.2. Ryhmä G on *Abelin ryhmä*, mikäli kaikilla sen alkioilla a ja b on $ab = ba$. Mikäli $ab = ba$ sanotaan alkioiden a ja b *kommutoivan*.

Esimerkki tutusta ryhmästä on kokonaislukujen joukko $\mathbb{Z}$ varustettuna yhteenlaskuoperaatiolla. Tämän ryhmän $(\mathbb{Z}, +)$ neutraalialkio on 0 ja luvun t käänteisalkio on sen vastaluku $-t$. Kokonaislukujen summat ovat kokonaislukuja ja summaamisen tiedetään olevan assosiatiivinen operaatio kokonaislukujen joukossa. Ryhmä $(\mathbb{Z}, +)$ on ääretön ryhmä. Luonnollisten lukujen joukko $\mathbb{N}$ sen sijaan ei ole ryhmä yhteenlaskuoperaation suhteen, sillä sen sisältä käänteisalkio löytyy ainoastaan alkiolle nolla.

Tarkastellaan jäännösluokkia modulo neljä eli joukkoa $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. Taulukkoon 1 on laskettu joukon alkioiden summat ja tulot. Taulukon 1 avulla voidaan helposti todeta, että yhteenlaskuoperaation suhteen $\mathbb{Z}_4$ on ryhmä: alkio $[0]$ on neutraalialkio, kaikille alkioille löytyy käänteisalkio, joukko on suljettu ja jäännösluokkien summaoperaation tiedetään olevan assosiatiivinen. Kertolaskun suhteen joukko $\mathbb{Z}_4$ ei kuitenkaan ole ryhmä useammastakaan syystä: taulukosta nähdään, että $[1]$ on ainut alkio, joka kerrottaessa säilyttää muut alkiot itsenään. Se on siis ainut mahdollinen neutraalialkio kertolaskuoperaation suhteen. $[0] * [a]$ on kuitenkin $[0]$ kaikilla joukon $\mathbb{Z}_4$ alkioilla $[a]$, eli jos $[1]$ on neutraalialkio, alkiolla $[0]$ ei ole käänteisalkiota. Edes joukko $\mathbb{Z}_4 \setminus [0]$ ei ole ryhmä kertolaskun suhteen. Se ei esimerkiksi ole suljettu, sillä vaikka alkio $[2]$ kuuluu joukkoon $\mathbb{Z}_4 \setminus [0]$, niin alkio $[2] * [2] = [0]$ ei kuulu.

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$*$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Taulukko 1: Joukon $\mathbb{Z}_4$ alkioiden väliset tulot ja summat.

Lause 1.1. Ryhmän G neutraalialkio sekä alkioiden käänteisalkiot ovat yksikäsitteisiä.

Todistus. Oletetaan ensin, että ryhmässä G on kaksi toisistaan eroavaa neutraalialkiota e ja e'. Nyt neutraalialkion määritelmästä seuraa $e = ee' = e'$, eli saatiin välittömästi ristiriita. Ryhmän G neutraalialkion on siis oltava yksikäsitteinen.
Oletetaan sitten, että ryhmän G alkiolla a on kaksi toisistaan eroavaa käänteisalkiota a^{-1} ja $(a')^{-1}$. Nyt käänteisalkion määritelmän nojalla $aa^{-1} = e = a(a')^{-1}$, josta operoimalla vasemmalta puolen käänteisalkiolla a^{-1} saadaan

$$\begin{aligned} a^{-1}\left(aa^{-1}\right) &= a^{-1}\left(a(a')^{-1}\right) \\ \Leftrightarrow \left(a^{-1}a\right)a^{-1} &= \left(a^{-1}a\right)(a')^{-1} \\ \Leftrightarrow ea^{-1} &= e(a')^{-1} \\ \Leftrightarrow a^{-1} &= (a')^{-1}, \end{aligned}$$

mikä on ristiriita. Näin ollen alkion a käänteisalkion on oltava yksikäsitteinen. □

Lause 1.2. Jos alkiot a ja b kuuluvat ryhmään G, niin yhtälöllä $ax = b$ on yksikäsitteinen ratkaisu $x \in G$. Samoin yhtälöllä $ya = b$ on yksikäsitteinen ratkaisu $y \in G$.

Todistus. Osoitetaan tapaus $ax = b$. Tapaus $ya = b$ osoitetaan vastaavalla tavalla.
Alkio a^{-1} kuuluu ryhmään G ja siten myös $a^{-1}b \in G$. Alkio $a^{-1}b$ on yhtälön ratkaisu, sillä $a(a^{-1}b) = (aa^{-1})b = eb = b$. Ratkaisu on yksikäsitteinen, sillä

jos yhtälöllä olisi ryhmässä G kaksi toisistaan eroavaa ratkaisua x_1 ja x_2, niin

$$\begin{aligned} ax_1 &= b = ax_2 && \| \ a^{-1}* \\ \Leftrightarrow a^{-1}(ax_1) &= a^{-1}(ax_2) \\ \Leftrightarrow (a^{-1}a)x_1 &= (a^{-1}a)x_2 \\ \Leftrightarrow ex_1 &= ex_2 \\ \Leftrightarrow x_1 &= x_2. \end{aligned}$$

Saatiin ristiriita oletuksen kanssa, eli ratkaisu $x_1 = x_2 \in G$ on yksikäsitteinen. □

Määritelmä 1.3. Ryhmän G osajoukko H on *aliryhmä*, mikäli H varustettuna ryhmän G operaatiolla $*$ on itse ryhmä. Tällöin merkitään $H \leq G$.

Aliryhmän H neutraalialkio on sama kuin ryhmän G neutraalialkio, sillä koska kaikki ryhmän H alkiot ovat myös ryhmän G alkioita, on ryhmän G neutraalialkiolla vaaditut ominaisuudet myös aliryhmässä H.

Selvästi ryhmä G on aina itsensä aliryhmä samoin kuin yhden alkion ryhmä $\{e\}$. Nämä ovat niin kutsutut *triviaalit aliryhmät*. Mikäli aliryhmä $H \neq G$, sanotaan aliryhmää H *aidoksi aliryhmäksi* ja tällöin voidaan merkitä $H < G$.

Lause 1.3 (Aliryhmäkriteeri)**.** Ryhmän G epätyhjä osajoukko H on aliryhmä, mikäli

(i) Jos alkio $a \in H$, niin myös käänteisalkio $a^{-1} \in H$.

(ii) Jos alkiot $a, b \in H$, niin myös alkio $ab \in H$.

Todistus. Olkoot lauseen kaksi ehtoa voimassa. Ehdoista nähdään suoraan kaikki ryhmältä vaaditut ominaisuudet neutraalialkion olemassaoloa ja operaation assosiatiivisuutta lukuunottamatta.

Koska joukko H on epätyhjä, on siellä ainakin yksi alkio a. Ensimmäisestä ehdosta seuraa, että alkion a käänteisalkio $a^{-1} \in H$ ja toisesta ehdosta, että $aa^{-1} = e \in H$. Koska kaikki joukon H alkiot kuuluvat ryhmään G, on ryhmän G neutraalialkio e myös joukon H neutraalialkio. Lisäksi operaatio on assosiatiivinen myös joukossa H. Näin ollen joukko H on ryhmä. □

Lause 1.4. Olkoot g ja h ryhmän G alkioita ja olkoot r ja s kokonaislukuja. Tällöin normaalit potenssien laskusäännöt ovat voimassa eli

(i) $g^s g^r = g^{r+s} = g^r g^s$

(ii) $(g^r)^s = g^{rs}$

(iii) $g^{-r} = (g^{-1})^r = (g^r)^{-1}$

(iv) $(gh)^{-1} = h^{-1}g^{-1}$

Todistus. Kolmen ensimmäisen kohdan todistus on pitkähkö, koska on käytävä erikseen läpi tilanteita sen mukaan, ovatko r ja s positiivisia, negatiivisia sekä keskenään yhtä- vai erisuuria. Tässä sivuutettu todistus löytyy muun muassa teoksesta [1, s. 22-24]. Viimeinen kohta seuraa siitä, että

$$(gh)\left(h^{-1}g^{-1}\right) = g\left(hh^{-1}\right)g^{-1} = geg^{-1} = gg^{-1} = e \text{ ja}$$
$$\left(h^{-1}g^{-1}\right)gh = h^{-1}\left(g^{-1}g\right)h = h^{-1}eh = h^{-1}h = e.$$

□

Määritelmä 1.4. Ryhmän G alkion a *kertaluku* $|a|$ on pienin positiivinen kokonaisluku n, jolla $a^n = e$. Mikäli tällaista lukua ei ole olemassa eli $a^n \neq e$ kaikilla $n \in \mathbb{Z}^+$, määritellään $|a| = \infty$.

Huomautus. Jos ryhmä G on äärellinen, on sen jokaisen alkion kertaluku äärellinen. Tämä voidaan todeta tarkastelemalla alkion $a \in G$ potensseja a^n, missä n on luonnollinen luku. Jos kaikilla toisistaan eroavilla luonnollisilla luvuilla r ja s olisi $a^r \neq a^s$ niin alkiolla a olisi ääretön määrä toisistaan eroavia potensseja. Koska G on ryhmä, kuuluvat kaikki nämä alkion a potenssit kuitenkin äärelliseen ryhmään G, mikä on ristiriita. Siten on olemassa sellaiset luonnolliset luvut s ja r, $s > r$ että $a^s = a^r$. Nyt $a^s a^{-r} = a^r a^{-r}$, mistä lauseen 1.4 nojalla saadaan $a^{s-r} = a^{r-r} = a^0 = e$. Siten alkion a kertaluku on korkeintaan $s - r \in \mathbb{Z}^+$.

Lause 1.5. Olkoon G äärellinen ryhmä ja alkio $a \in G$. Nyt joukko $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ on ryhmän G aliryhmä.

Todistus. Koska ryhmä G on äärellinen, on alkion a kertaluku äärellinen. Selvästi joukko $\langle a \rangle$ sisältää tarkalleen $|a|$ alkiota, jotka ovat a, a^2, $\ldots$, $a^{|a|-1}$ ja $a^{|a|} = e$. Siis $\langle a \rangle$ sisältää neutraalialkion e. Lisäksi jokaista kokonaislukua m kohti löytyy luonnollinen luku $1 \leq m' \leq |a|$ siten, että $a^m = a^{m'}$. Nyt $a^{|a|-m'}$ on alkion a^m käänteisalkio, sillä

$$a^m a^{|a|-m'} = a^{m'} a^{|a|-m'} = a^{m'+|a|-m'} = a^{|a|} = e$$

ja samoin saadaan $a^{|a|-m'}a^m = e$. Joukko $\langle a \rangle$ on suljettu, sillä kaikilla sen alkioilla a^r ja a^s kuuluu alkio $a^r a^s = a^{r+s}$ joukkoon $\langle a \rangle$. Näin ollen lauseen 1.3 nojalla $\langle a \rangle$ on ryhmän G aliryhmä. □

Määritelmä 1.5. Lauseen 1.5 aliryhmää $\langle a \rangle$ kutsutaan ryhmän G *alkion* a *generoimaksi sykliseksi aliryhmäksi.* Alkiota a kutsutaan aliryhmän $\langle a \rangle$ *generaattoriksi.*

Lause 1.6. Olkoon g ryhmän G alkio, jonka kertaluku on n. Nyt $g^r = g^s$ jos ja vain jos n jakaa luvun $r - s$. Erityisesti $g^k = e$ jos ja vain jos $n \mid k$.

Todistus. (ks. [1], s.25) Olkoon n sellainen, että n jakaa luvun $r - s$, eli $r - s = mn$ jollakin kokonaisluvulla m. Tällöin

$$g^r = g^{mn+s} = g^{mn} g^s = (g^n)^m g^s = e^m g^s = g^s.$$

Olkoon sitten $g^r = g^s$. Nyt

$$g^{r-s} = g^r g^{-s} = g^r (g^s)^{-1} = g^r (g^r)^{-1} = e.$$

Jakoalgoritmin nojalla $r - s = qn + t$ joillakin kokonaisluvuilla q ja t, missä $0 \leq t < n$. Siten nähdään, että

$$\begin{aligned} g^{r-s} &= g^{qn+t} \\ &= g^{qn} g^t \\ &= (g^n)^q g^t \\ &= e^q g^t \\ &= g^t. \end{aligned}$$

Nyt siis $g^t = g^{r-s} = e$. Koska $0 \leq t < n$, on oltava $t = 0$, sillä muuten jouduttaisiin ristiriitaan alkion g kertaluvun n suhteen. Näin on osoitettu, että $r - s = qn$ eli n jakaa luvun $r - s$. □

1.1.2 Normaalit aliryhmät ja tekijäryhmät

Seuraavaksi määritellään normaali aliryhmä ja tutkitaan, kuinka sen avulla voidaan luoda uusia ryhmiä, niin sanottuja tekijäryhmiä. Normaalin aliryhmän määritelmää varten on tarpeen tutustua sivuluokkiin, joilla huomataan olevan mielenkiintoisia ominaisuuksia. Sivuluokkien avulla osoitetaan, että aliryhmän kertaluku jakaa aina ryhmän kertaluvun. Tämän tärkeä tulos tunnetaan nimellä Lagrangen lause.

Määritelmä 1.6. Olkoon G ryhmä, H sen aliryhmä ja a ryhmän G mielivaltainen alkio. Joukko $aH = \{ah : h \in H\}$ on alkion a määräämä aliryhmän H *vasen sivuluokka* ryhmässä G.

Alkio kuuluu aina itse määräämäänsä vasempaan sivuluokkaan. Jos nimittäin a on ryhmän G alkio, niin koska $e \in H$, niin $a = ae \in aH$. Tästä seuraa, että ryhmä G on aliryhmän H vasempien sivuluokkien yhdiste.

Kuinka monta alkiota on vasemmassa sivuluokassa aH? Selvästi $|aH| = |\{ah : h \in H\}| \leq |H|$. Sivuluokassa voi olla vähemmän alkioita kuin ryhmässä H vain siinä tapauksessa, että kahdella toisistaan eroavalla aliryhmän H alkiolla h_1 ja h_2 on $ah_1 = ah_2$. Tästä saadaan kuitenkin välitön ristiriita kertomalla alkion a käänteisalkiolla yhtälön molemmat puolet. Jokaisessa vasemmassa sivuluokassa aH on siis tarkalleen yhtä monta alkiota kuin aliryhmässä H.

Apulause 1.7. Olkoon H ryhmän G aliryhmä. Määritellään relaatio R siten, että kaikilla ryhmän G alkioilla a ja b

$$aRb \Leftrightarrow b^{-1}a \in H.$$

Nyt relaatio R on ekvivalenssirelaatio.

Todistus. Olkoot a, b ja c ryhmän G mielivaltaisia alkioita ja H ryhmän G aliryhmä. Koska H on ryhmä, $a^{-1}a = e \in H$ ja siten aRa. Olkoon sitten aRb eli $b^{-1}a \in H$. Jälleen koska H on ryhmä, kuuluu alkio

$$(b^{-1}a)^{-1} = a^{-1}(b^{-1})^{-1} = a^{-1}b$$

ryhmään H eli bRa. Olkoon lopuksi aRb ja bRc, eli $b^{-1}a \in H$ ja $c^{-1}b \in H$. Koska ryhmä H on suljettu, kuuluu myös tulo

$$(c^{-1}b)(b^{-1}a) = c^{-1}(bb^{-1})a = c^{-1}a$$

ryhmään H, joten aRc. On näytetty, että relaatio R toteuttaa kaikki ekvivalenssirelaation ominaisuudet, eli se on ekvivalenssirelaatio. □

Lause 1.8. Olkoon G ryhmä, a ja b ryhmän G mielivaltaisia alkioita ja $H \leq G$. Nyt vasemmat sivuluokat aH ja bH ovat täsmälleen samat, mikäli $a \in bH$, ja täysin erilliset, mikäli $a \notin bH$. Lisäksi $aH = bH$ täsmälleen silloin, kun $b^{-1}a \in H$.

Todistus. Apulauseen 1.7 relaation R osoitettiin olevan ekvivalenssirelaatio. Osoitetaan, että aRb jos ja vain jos $aH = bH$, mistä seuraa, että vasemmat sivuluokat ovat itseasiassa relaation R ekvivalenssiluokkia. Tällöin ekvivalenssiluokkien ominaisuuksista seuraa suoraan koko lauseen sisältö.

Olkoon ensin aRb eli $b^{-1}a \in H$. Nyt $b(b^{-1}a) = (bb^{-1})a = a \in bH$, eli $a = bh_1$ jollakin $h_1 \in H$. Olkoon alkio $x \in aH$ mielivaltainen. Tällöin $x = ah_2$ jollakin $h_2 \in H$. Näillä merkinnöillä nähdään, että

$$x = ah_2 = (bh_1)h_2 = b(h_1h_2),$$

missä alkio $h_1h_2 \in H$ ja siten $x \in bH$. On osoitettu, että $aH \subseteq bH$. Koska R on ekvivalenssirelaatio, bRa, ja vastaavalla tavalla voidaan osoittaa, että $bH \subseteq aH$. Siten $aH = bH$.

Olkoon sitten $aH = bH$. Nyt $b \in bH = aH$, joten $b = ah_3$ jollakin $h_3 \in H$. Siten nähdään, että

$$b^{-1}a = (ah_3)^{-1}a = ({h_3}^{-1}a^{-1})a = {h_3}^{-1}(a^{-1}a) = {h_3}^{-1}e = h_3^{-1}$$

on ryhmän H alkion h_3 käänteisalkio ja kuuluu ryhmään H. Siis aRb.

On osoitettu, että aRb on yhtäpitävää sen kanssa, että $aH = bH$. Tarkistetaan vielä, että joukkoon aH kuuluvat tarkalleen ne alkiot, jotka ovat alkion a määräämässä ekvivalenssiluokassa relaation R suhteen: Jos aRb, niin $aH = bH$ ja koska $b \in bH$, niin $b \in aH$. Jos taas $b \in aH$, niin $b = ah_4$ jollakin $h_4 \in H$ ja tällöin on todettu, että aRb. Vasempaan sivuluokkaan aH kuuluvat siis tarkalleen ne alkiot, jotka ovat relaatiossa alkion a kanssa.

Vasemmat sivuluokat ovat siis ekvivalenssirelaation R ekvivalenssiluokkia. Lauseen sisältö saadaan ekvivalenssiluokkien ominaisuuksista. □

Seuraus 1.9 (Lagrangen lause)**.** Olkoon G äärellinen ryhmä ja H sen aliryhmä. Aliryhmän H kertaluku jakaa ryhmän G kertaluvun, eli $|G| = n|H|$ jollakin luonnollisella luvulla n.

Todistus. Ryhmä G on vasempien sivuluokkien yhdiste ja jokaisessa sivuluokassa on $|H|$ alkiota. Lauseen 1.8 perusteella vasemmat sivuluokat ovat lisäksi erillisiä, eli jokainen ryhmän G alkio kuuluu ainoastaan yhteen vasempaan sivuluokkaan. Koska ryhmä G on äärellinen, on vasempia sivuluokkia äärellinen määrä, olkoon se $n \in \mathbb{N}$. Nyt $G = \bigcup_{i=1}^{n} a_iH$ ja $|G| = n|H|$. □

Seuraus 1.10. Millä tahansa ryhmän G alkiolla a on $a^{|G|} = e$.

Todistus. Selvästi $|\langle a\rangle| = |a|$. Koska $\langle a\rangle \leq G$, jakaa sen kertaluku eli alkion a kertaluku ryhmän G kertaluvun, eli $|G| = n|a|$ jollakin $n \in N$. Nyt

$$a^{|G|} = a^{n|a|} = (a^{|a|})^n = e^n = e.$$

□

Määritelmä 1.7. Ryhmän G aliryhmän H sivuluokkien määrä on aliryhmän H *indeksi* ryhmässä G. Aliryhmän H indeksiä n merkitään $n = [G : H]$.

Huomautus. Lagrangen lauseen 1.9 perusteella äärellisen ryhmän G aliryhmän H indeksi $[G : H] = \frac{|G|}{|H|}$.

Kaikki, mikä edellä on osoitettu vasemmille sivuluokille, pätee myös oikeille sivuluokille, jotka määritellään vastaavasti: Jos H on ryhmän G aliryhmä ja a ryhmän G mielivaltainen alkio, on joukko $Ha = \{ha : h \in H\}$ alkion a määräämä aliryhmän H *oikea sivuluokka* ryhmässä G. Normaalin aliryhmän määritelmässä tarvitaan sekä oikean että vasemman sivuluokan käsitteitä.

Määritelmä 1.8. Ryhmän G aliryhmä N on *normaali aliryhmä*, jos $aN = Na$ kaikilla ryhmän G alkioilla a. Normaalia aliryhmää merkitään $N \trianglelefteq G$.

Lause 1.11. Olkoon G ryhmä ja N sen aliryhmä. Seuraavat väittämät ovat yhtäpitäviä:

(a) $N \trianglelefteq G$

(b) $a^{-1}Na = N$ kaikilla $a \in G$

(c) $a^{-1}na \in N$ kaikilla $n \in N$ ja $a \in G$

Todistus. $(a) \Rightarrow (b)$: Olkoon $N \trianglelefteq G$ eli $aN = Na$. Nyt joukko

$$\begin{aligned} a^{-1}Na &= \{a^{-1}na : n \in N\} = \{a^{-1}(na) : n \in N\} \\ &= a^{-1}(Na) = a^{-1}(aN) = \{a^{-1}(an) : n \in N\} \\ &= \{(a^{-1}a)n : n \in N\} = \{n : n \in N\} = N. \end{aligned}$$

$(b) \Rightarrow (a)$: Olkoon $a^{-1}Na = N$. Jos $x \in aN$, niin $x = an_1$ jollakin $n_1 \in N$. Lisäksi $n_1 \in N = a^{-1}Na$, eli $n_1 = a^{-1}n_1'a$ jollakin $n_1' \in N$. Siis

$$x = an_1 = a(a^{-1}n_1'a) = (aa^{-1})n_1'a = n_1'a \in Na,$$

eli $aN \subseteq Na$. Koska alkio a on mielivaltainen, on myös $(a^{-1})^{-1}Na^{-1} = aNa^{-1} = N$, mistä vastaavasti saadaan $Na \subseteq aN$. Näin ollen $aN = Na$.

$(b) \Rightarrow (c)$: Olkoon $a^{-1}Na = N$ ja $n \in N$. Nyt $a^{-1}na \in a^{-1}Na = N$.

$(c) \Rightarrow (b)$: Olkoon $a^{-1}na \in N$ kaikilla $n \in N$. Nyt

$$a^{-1}Na = \{a^{-1}na : n \in N\} \subseteq N,$$

eli $|a^{-1}Na| \leq |N|$. Joukossa $a^{-1}Na$ voi olla joukkoa N vähemmän alkioita vain, jos joillakin toisistaan eroavilla ryhmän N alkioilla n_1 ja n_2 on $a^{-1}n_1a = a^{-1}n_2a$. Tällöin kuitenkin saadaan

$$\begin{aligned} a(a^{-1}n_1a)a^{-1} &= a(a^{-1}n_2a)a^{-1} \\ \Leftrightarrow (aa^{-1})n_1(aa^{-1}) &= (aa^{-1})n_2(aa^{-1}) \\ \Leftrightarrow en_1e &= en_2e \\ \Leftrightarrow n_1 &= n_2, \end{aligned}$$

mikä on ristiriita. Siis $|a^{-1}Na| = |N|$ ja $a^{-1}Na \subseteq N$, eli $a^{-1}Na = N$. □

Lause 1.12. Abelin ryhmän G jokainen aliryhmä on normaali.

Todistus. Olkoon H ryhmän G aliryhmä. Nyt kaikilla $a \in G$ ja $h \in H$ on

$$a^{-1}ha = a^{-1}ah = eh = h \in H,$$

joten lauseen 1.11 perusteella $H \trianglelefteq G$. □

Lause 1.13. Olkoon N ryhmän G normaali aliryhmä. Nyt vasemmat sivuluokat aN, missä $a \in G$, muodostavat ryhmän, kun ryhmän operaatioksi määritellään $aN \circ bN = (ab)N$ kaikilla aliryhmän N vasemmilla sivuluokilla aN ja bN.

Todistus. Olkoot sivuluokat aN ja bN mielivaltaisia joukon $\{gN : g \in G\}$ alkioita. Osoitetaan, että operaatio $aN \circ bN = abN$ on hyvin määritelty, eli että operaation tulos ei riipu vasemman sivuluokan edustajien a ja b valinnasta. Olkoon $a' \in aN$ ja $b' \in bN$. Tällöin lauseen 1.8 perusteella $aN = a'N$ ja $bN = b'N$, ja on osoitettava, että nyt $(ab)N = (a'b')N$. Lauseen 1.8 perusteella aRa' ja bRb', eli $(a')^{-1}a \in N$ ja $(b')^{-1}b \in N$. Nyt

$$\begin{aligned} (a'b')^{-1}(ab) &= (b')^{-1}(a')^{-1}ab = (b')^{-1}e(a')^{-1}ab \\ &= (b')^{-1}\left(bb^{-1}\right)(a')^{-1}ab = \left((b')^{-1}b\right)b^{-1}\left((a')^{-1}a\right)b, \end{aligned}$$

missä tiedetään tulojen $(b')^{-1}b$ ja $(a')^{-1}a$ kuuluvan aliryhmään N. Merkitsemällä $(b')^{-1}b = n_1$ ja $(a')^{-1}a = n_2$, saadaan lauseke muotoon

$$n_1b^{-1}n_2b.$$

Koska N on normaali aliryhmä, kuuluu tulo $b^{-1}(n_2)b$ lauseen 1.11 perusteella ryhmään N. On siis esitetty tulo $(a'b')^{-1}(ab)$ ryhmän N alkioiden tulona, joten se kuuluu ryhmään N. Näin ollen $(ab)R(a'b')$, eli sivuluokat $(ab)N$ ja $(a'b')N$ ovat samat. Sivuluokkien välinen operaatio $\circ$ on siis hyvin

määritelty.

Nyt on helppo osoittaa, että joukko $\{gN : g \in G\}$ toteuttaa ryhmän ominaisuudet. Aliryhmä $N = eN$ on ryhmän neutraalialkio, sillä mielivaltaiselle alkiolle $aN \in \{gN : g \in G\}$ on

$$aN \circ eN = eN \circ aN = (ae)N = aN.$$

Sivuluokan aN käänteisalkio on $a^{-1}N$, sillä

$$aN \circ a^{-1}N = a^{-1}N \circ aN = (aa^{-1})N = eN = N.$$

Koska G on ryhmä, on operaatio $\circ$ assosiatiivinen ja joukko $\{gN : g \in G\}$ suljettu operaation $\circ$ suhteen. □

Määritelmä 1.9. Lauseessa 1.13 esitettyä sivuluokkien muodostamaa ryhmää $(\{aN : a \in G\}, \circ)$ kutsutaan ryhmän G *tekijäryhmäksi* normaalin aliryhmän N suhteen ja merkitään G/N. Ryhmän neutraalialkio on sivuluokka $eN = N$.

Huomautus. Tekijäryhmän G/N kertaluku on aliryhmän N vasempien sivuluokkien määrä eli indeksi. Kun ryhmä G on äärellinen, indeksi on $|G|/|N|$.

Jos ryhmä G on Abelin ryhmä, on myös tekijäryhmä G/N Abelin ryhmä, sillä millä tahansa vasemmilla sivuluokilla aN ja bN on $aNbN = (ab)N = (ba)N = bNaN$.

1.1.3 Sykliset ryhmät

Edellisessä kappaleessa käsiteltiin ryhmän G alkion a generoimaa syklistä aliryhmää $\langle a \rangle$. Seuraavaksi tutustutaan tarkemmin syklisiin ryhmiin eli tapaukseen, jossa $G = \langle a \rangle$.

Määritelmä 1.10. Ryhmä G on *syklinen*, jos on olemassa sellainen alkio $g \in G$, että $\langle g \rangle = G$.

Ryhmä $(\mathbb{Z}, +)$ on esimerkki äärettömästä syklisestä ryhmästä. Sen generoi alkio 1. Ryhmä $(\mathbb{Z}_5 \setminus [0], *)$ taas on eräs äärellinen syklinen ryhmä. Sen generoivat itseasiassa sen kaikki alkiot neutraalialkiota [1] lukuunottamatta eli alkiot [2],[3] ja [4]. Useiden generaattoreiden olemassaololle ei ole mitään estettä. Esimerkiksi alkiolle [2] voidaan laskemalla todeta, että $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [3]$ ja $[2]^4 = [1]$, eli $\langle [2] \rangle = \mathbb{Z}_5 \setminus [0]$.

Lause 1.14. Jos ryhmän G kertaluku on alkuluku, niin ryhmä G on syklinen.

Todistus. Olkoon $|G|$ alkuluku eli $|G| \geq 2$ ja alkio $e \neq a \in G$. Lauseen 1.5 perusteella $\langle a \rangle$ on ryhmän G aliryhmä ja seurauksen 1.9 perusteella aliryhmän $\langle a \rangle$ kertaluku jakaa ryhmän G kertaluvun. Nyt $|G|$ on alkuluku, eli sen ainoat tekijät ovat 1 ja $|G|$. Koska aliryhmään $\langle a \rangle$ kuuluvat ainakin alkiot a ja e, on $|\langle a \rangle| \geq 2$, eli $|\langle a \rangle| = |G|$. Siis $G = \langle a \rangle$ eli ryhmä G on alkion a generoima syklinen ryhmä. □

Lause 1.15. Syklisen ryhmän aliryhmät ovat syklisiä.

Todistus. Olkoon $G = \langle a \rangle$ kertalukua n oleva syklinen ryhmä ja H ryhmän G aliryhmä. Olkoon r pienin positiivinen kokonaisluku, jolla $a^r \in H$. Osoitetaan, että $H = \langle a^r \rangle$.
Koska H on ryhmä, $\langle a^r \rangle \subseteq H$. Olkoon a^n mielivaltainen ryhmän H alkio. Nyt jakoalgoritmin nojalla $n = dr + s$, missä $d, s \in \mathbb{Z}$ ja $0 \leq s < r$. Nyt on siis $a^n = a^{dr+s} = a^{dr}a^s$. Alkion a^{dr} käänteisalkio $(a^{dr})^{-1} = a^{-dr} = (a^r)^{-d} \in H$, joten tulo

$$\begin{aligned} a^{-dr}a^n &= a^{-dr}(a^{dr}a^s) = (a^{-dr}a^{dr})a^s \\ &= a^{dr-dr}a^s = a^0a^s = ea^s = a^s \end{aligned}$$

kuuluu aliryhmään H. Alkion a^r valinnasta ja ehdosta $0 \leq s < r$ seuraa, että $s = 0$ eli $a^n = a^{dr} = (a^r)^d \in \langle a^r \rangle$. Siis $H \subseteq \langle a^r \rangle$ ja on osoitettu, että $H = \langle a^r \rangle$. □

Lause 1.16. Olkoon G äärellinen syklinen ryhmä, jonka kertaluku on n. Nyt jokaista luvun n tekijää d kohti on olemassa yksikäsitteinen ryhmän G aliryhmä G_d, jonka kertaluku on d. Lisäksi ryhmässä G on d sellaista alkiota x, jotka toteuttavat yhtälön $x^d = 1$. Nämä alkiot ovat tarkalleen ne d alkiota, jotka kuuluvat aliryhmään G_d.

Todistus. (ks. [1], s.35) Olkoon g alkio, joka generoi ryhmän G, eli $G = \langle g \rangle$ ja $|g| = n$. Nyt

$$\langle g^{n/d} \rangle = \{g^{n/d}, g^{2n/d}, \ldots, g^{(d-1)n/d}, g^{dn/d} = g^n = e\},$$

eli $|\langle g^{n/d} \rangle| = d$. Olkoon H toinen aliryhmä, jonka kertaluku on d. Lauseen 1.15 perusteella $H = \langle g^r \rangle$ jollakin $g^r \in G$. Koska $|g^r| = d$, on $g^{rd} = (g^r)^d = e = g^n$, joten lauseen 1.6 perusteella n jakaa luvun dr. Siis $dr = mn$ jollakin m eli $r = mn/d$. Nyt siis $g^r = g^{mn/d} = (g^{n/d})^m$, eli $g^r \in \langle g^{n/d} \rangle$ ja siten $H = \langle g^r \rangle \leq \langle g^{n/d} \rangle$. Koska $|H| = |\langle g^{n/d} \rangle|$, on $H = \langle g^{n/d} \rangle$. On osoitettu, että kertalukua d oleva aliryhmä on yksikäsitteinen.

Jos $x^d = e$, niin edellisen perusteella alkio x on alkion $g^{n/d}$ potenssi. Jos toisaalta $y \in \langle g^{n/d} \rangle$, niin seurauksen 1.10 nojalla $y^d = y^{|\langle g^{n/d} \rangle|} = e$. Siis yhtälöllä $x^d = e$ on tasan d ratkaisua ryhmässä G. □

1.2 Konjugaatit

Kun pitää katseen tulevaisuudessa eli aikomuksessa tutkia ryhmien normaaleja aliryhmiä, on selkeää, miksi seuraavaksi tutustutaan konjugaatteihin. Toistensa kanssa konjugoivat alkiot nimittäin muodostavat ryhmään ekvivalenssiluokat erään relaation suhteen. Normaalit aliryhmät ovat aina näiden konjugointiluokiksi kutsuttujen ekvivalenssiluokkien yhdisteitä. Jos siis hallitsemme konjugointiluokkien etsimisen, on käytössämme oiva tapa tutkia normaaleja aliryhmiä. Juuri tätä varten osoitetaan kappaleessa 3 hieman edistyneempi lause 3.2, jonka avulla konjugointiluokan kertaluvun selvittäminen helpottuu huomattavasti.

Määritelmä 1.11. Olkoon a ryhmän G alkio. Tulo $g^{-1}ag$, missä $g \in G$, on alkion a *konjugaatti* ryhmässä G, merkitään a^g. Jos on olemassa sellainen ryhmän G alkio g, että $a^g = b$, sanotaan alkioiden a ja b konjugoivan ryhmässä G. Alkion a kaikkien konjugaattien joukkoa $\{a^g : g \in G\}$ merkitään a^G.

Lause 1.17. Olkoon G ryhmä ja a, b ja c sen mielivaltaisia alkioita. Tällöin

(a) $(a^b)^c = a^{bc}$

(b) $\left(a^b\right)^{-1} = (a^{-1})^b$

(c) $a = b^c \Leftrightarrow b = a^{(c^{-1})}$

(d) $(ab)^c = a^c b^c$

(e) $(a^b)^n = (a^n)^b$ kaikilla luonnollisilla luvuilla n.

Todistus. (a) $(a^b)^c = c^{-1}(a^b)c = c^{-1}b^{-1}abc = (bc)^{-1}a(bc) = a^{bc}$

(b) Lauseen 1.4 kohdan (iv) avulla saadaan $(a^b)^{-1} = (b^{-1}ab)^{-1} = (ab)^{-1}(b^{-1})^{-1} = b^{-1}a^{-1}b = (a^{-1})^b$

(c) $a = b^c = c^{-1}bc \Leftrightarrow cac^{-1} = b \Leftrightarrow (c^{-1})^{-1}\, ac^{-1} = b \Leftrightarrow a^{(c^{-1})} = b$

(d) $(ab)^c = c^{-1}(ab)c = c^{-1}a(cc^{-1})bc = (c^{-1}ac)(c^{-1}bc) = a^c b^c$

(e) Osoitetaan väite induktion avulla. Jos $k = 0$, niin $(a^b)^0 = e = e^b = (a^0)^b$. Oletetaan induktio-oletuksena, että $(a^b)^k = (a^k)^b$. Nyt

$$\begin{aligned}
(a^b)^{k+1} &= a^b(a^b)^k && \text{lauseen 1.4 perusteella}\\
&= a^b(a^k)^b && \text{induktio-oletuksen perusteella}\\
&= (b^{-1}ab)(b^{-1}a^kb)\\
&= b^{-1}a(bb^{-1})a^kb\\
&= b^{-1}aa^kb\\
&= b^{-1}a^{k+1}b && \text{lauseen 1.4 perusteella}\\
&= (a^{k+1})^b,
\end{aligned}$$

mikä päättää induktiotodistuksen.

□

Lause 1.18. Toistensa kanssa konjugoivilla alkioilla on sama kertaluku, eli jos G on ryhmä ja a ja g ovat sen alkioita, niin $|a| = |a^g|$.

Todistus. Olkoot a ja g ryhmän G alkioita ja alkion a kertaluku n. Nyt lauseen 1.17 perusteella

$$(a^g)^n = (a^n)^g = e^g = g^{-1}eg = g^{-1}g = e,$$

eli $|a^g| \leq n$. Jos olisi $|a^g| = m < n$ eli $(a^g)^m = e$, niin saataisiin ristiriita alkion a kertaluvun suhteen: $(a^g)^m = (a^m)^g = e$, eli

$$\begin{aligned}
&g^{-1}(a^m)g = e && \| \; g*\\
\Leftrightarrow\ &(a^m)g = g && \| \; *g^{-1}\\
\Leftrightarrow\ &a^m = e.
\end{aligned}$$

Tämä on ristiriita, koska oli $m < n = |a|$. □

Määritellään seuraavaksi myös ryhmän G aliryhmän H konjugaatti.

Määritelmä 1.12. Ryhmän G *aliryhmän* H *konjugaatti* H^g on joukko $\{h^g : h \in H\}$, missä g on ryhmän G alkio.

Lause 1.19. Ryhmän G aliryhmän H konjugaatit ovat myös ryhmän G aliryhmiä.

Todistus. Olkoon $H \leq G$ ja $g \in G$. Nyt joukko $H^g \neq \emptyset$, sillä $e^g = e \in H^g$. Olkoon $a \in H^g$ eli $a = (a')^g$ jollakin $a' \in H$. Nyt $(a')^{-1} \in H$, joten lauseen 1.17 perusteella

$$\left((a')^{-1}\right)^g = ((a')^g)^{-1} = a^{-1} \in H^g.$$

Lisäksi joukko H on suljettu, sillä jos myös $b \in H^g$, niin $b = (b')^g$ jollakin $b' \in H$ ja jälleen lauseen 1.17 avulla saadaan $ab = (a')^g(b')^g = (a'b')^g \in H^g$, koska $a'b' \in H$. Nyt lauseen 1.3 perusteella $H^g \leq G$. □

Huomautus. Selvästi aliryhmän H konjugaatissa H^g on korkeintaan $|H|$ alkiota. Jos a ja b ovat aliryhmän H kaksi erisuurta alkiota ja $g \in G$, nähdään helposti, että myös $a^g \neq b^g$. Näin ollen konjugaatin H^g kertaluku on sama kuin aliryhmän H.

Apulause 1.20. Määritellään ryhmän G alkioilla relaatio $\sim$ seuraavasti: $a \sim b$ jos ja vain jos on olemassa sellainen ryhmän G alkio g, että $b = a^g$. Tällöin relaatio $\sim$ on ekvivalenssirelaatio.

Todistus. $a \sim a$, sillä $e^{-1}ae = a$. Jos $a \sim b$, niin $b = a^d$ jollakin ryhmän G alkiolla d. Tällöin lauseen 1.17 perusteella $a = b^{\left(d^{-1}\right)}$ ja siten $b \sim a$.
Olkoot lopuksi ryhmän G alkiot a, b ja c sellaisia, että $a \sim b$ ja $b \sim c$. Nyt siis $b = a^d$ ja $c = b^f$ joillakin ryhmän G alkioilla d ja f. Tällöin saadaan $c = b^f = (a^d)^f$, josta lauseen 1.17 nojalla $c = a^{df}$, eli $a \sim c$. On osoitettu, että relaatio $\sim$ on ekvivalenssirelaatio ryhmässä G. □

Seuraus 1.21. Apulauseen 1.20 relaatio $\sim$ jakaa ryhmän G pistevieraisiin ekvivalenssiluokkiin, joiden yhdiste ryhmä G on. Alkion a määräämä ekvivalenssiluokka on $a^G = \{a^g : g \in G\}$.

Määritelmä 1.13. Relaation $\sim$ ekvivalenssiluokkia ryhmässä G kutsutaan ryhmän G *konjugointiluokiksi.*

Lause 1.22. Normaalit aliryhmät ovat aina konjugointiluokkien yhdisteitä.

Todistus. Olkoon N ryhmän G normaali aliryhmä ja a sen mielivaltainen alkio. Merkitään $\{a^g : g \in G\} = N_a$. Nyt alkio $a = a^e$ kuuluu joukkoon N_a kaikilla $a \in N$, joten

$$N \subseteq \bigcup_{a \in N} N_a.$$

Lauseen 1.11 perusteella $b^{-1}ab = a^b \in N$ kaikilla $b \in G$, eli $N_a \subseteq N$. Näin ollen on myös

$$\bigcup_{a \in N} N_a \subseteq N$$

eli joukot ovat samat. Normaali aliryhmä N on siis konjugointiluokkien yhdiste. □

1.3 Kunnat

Seuraavaksi tarkastellaan kuntia. Olennainen ero ryhmän ja kunnan välillä on se, että ryhmässä joukon alkioiden välillä on määritelty yksi operaatio, kunnassa taas kaksi. Kappaleen loppupuolella käytetään suurimman yhteisen tekijän käsitettä, joka oletetaan lukijalle ennestään tutuksi.

Määritelmä 1.14. *Kunta* on kolmikko $(K, +, \cdot)$, missä pari $(K, +)$ on Abelin ryhmä eli yhteenlaskuoperaatio $+$ on kommutatiivinen ryhmässä K. Lisäksi alkioiden välillä on määritelty kertominen siten, että $(K \setminus \{e_{(+)}\}, \cdot)$ on Abelin ryhmä ja $a \cdot e_{(+)} = e_{(+)} \cdot a = e_{(+)}$ kaikilla $a \in K$. Lisäksi kaikilla joukon K alkioilla a, b ja c pätevät näiden operaatioiden suhteen osittelulait

1. $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ ja
2. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,

Ryhmä $(K, +)$ on kunnan *additiivinen ryhmä* ja ryhmä $(K \setminus \{e_{(+)}\}, \cdot)$ on kunnan *multiplikatiivinen ryhmä*.

Kun väärinkäsityksen vaaraa ei ole, merkitään kolmikkoa $(K, +, \cdot)$ lyhyemmin K.

Kunnassa K on aina neutraalialkio sekä yhteenlaskun että kertomisen suhteen. Neutraalialkiota yhteenlaskun suhteen merkitään $e_{(+)} = \mathbf{0}$ ja kutsutaan *nolla-alkioksi*. Neutraalialkiota kertomisen suhteen merkitään $e_{(\cdot)} = \mathbf{1}$ ja kutsutaan *ykkösalkioksi*.

Kaikilla kunnan nolla-alkiosta poikkeavilla alkioilla on olemassa käänteisalkio sekä yhteenlaskun että kertomisen suhteen. Alkion a käänteisalkiota yhteenlaskun suhteen kutsutaan *vasta-alkioksi* ja merkitään $-a$. Käänteisalkiota kertomisen suhteen merkitään a^{-1}.

Kunnan kaikilla alkioilla on kertaluku sekä yhteenlaskun että kertomisen suhteen. Kun siis jatkossa puhutaan kunnan alkion kertaluvusta, on kerrottava kummasta kertaluvusta on kyse.

Kunnan kaksi neutraalialkiota on syytä pitää tarkasti erillään. Tulee huomata esimerkiksi se, että $\mathbf{0} + \mathbf{1} = \mathbf{1}$ kun taas $\mathbf{0} \cdot \mathbf{1} = \mathbf{0}$.

Huomautus. Jos alkiot a ja b kuuluvat kuntaan K, niin koska $(K \setminus \{\mathbf{0}\})$ on ryhmä, on $ab = \mathbf{0}$ jos ja vain jos $a = \mathbf{0}$ tai $b = \mathbf{0}$.

Esimerkiksi $(\mathbb{R}, +, \cdot)$ eli reaalilukujen joukko yhdessä normaalien yhteen- ja kertolaskujen kanssa on kunta. Tämä on helposti todettavissa tarkastamalla, että $(\mathbb{R}, +)$ ja $(\mathbb{R} \setminus \{\mathbf{0}\}, \cdot)$ ovat ryhmiä, ja että määritelmän 1.14 osittelulait ovat voimassa.

Esimerkki äärellisestä kunnasta on jäännösluokkien joukko $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$. Yhteenlaskun ja kertomisen tiedetään olevan suljettuja, assosiatiivisia ja kommutatiivisia jäännösluokkien joukossa. Lisäksi vaaditut osittelulait pätevät. Neutraali- ja käänteisalkioiden löytymisen voi tarkistaa taulukosta 2, johon on laskettu alkioiden väliset summat ja tulot.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Taulukko 2: Joukon $\mathbb{Z}_5$ alkioiden väliset tulot ja summat.

Määritelmä 1.15. Kunnan K ykkösalkion $\mathbf{1}$ additiivista kertalukua kutsutaan kunnan K *karakteristikaksi* ja merkitään $\mathrm{char}K$. Jos siis $\mathrm{char}K = n$, niin $\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{n kappaletta}} = \mathbf{0}$.

Lause 1.23. Olkoon K kunta, n sen karakteristika ja $\mathbf{0} \neq a \in K$. Nyt

(a) $na = \mathbf{0}$

(b) alkion a additiivinen kertaluku on n.

(c) karakteristika n on alkuluku.

Todistus. (ks. [5])

(a) Käyttämällä $n - 1$ kertaa osittelulakia $(ac) + (bc) = (a + b)c$ saadaan

$$\underbrace{(\mathbf{1}a) + \cdots + (\mathbf{1}a)}_{\text{n kappaletta}} = \left(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{n kappaletta}} \right) a.$$

Siten

$$na = \underbrace{a + \cdots + a}_{\text{n kappaletta}} = \underbrace{(\mathbf{1}a) + \cdots + (\mathbf{1}a)}_{\text{n kappaletta}} = \left(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{n kappaletta}} \right) a = \mathbf{0}a = \mathbf{0}.$$

(b) Kohdan (a) nojalla $na = \mathbf{0}$. Jos olisi $ma = \mathbf{0}$ jollakin luvulla $m < n$, niin

$$ma = \underbrace{a + \cdots + a}_{\text{m kappaletta}} = \underbrace{(\mathbf{1}a) + \cdots + (\mathbf{1}a)}_{\text{m kappaletta}} = \left(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{m kappaletta}} \right) a = (m\mathbf{1})a = \mathbf{0},$$

ja koska $a \neq \mathbf{0}$, on $m\mathbf{1} = \mathbf{0}$, mikä on ristiriita karakteristikan määritelmän suhteen.

(c) Oletetaan, että kunnan K karakteristika n on yhdistetty luku, eli $n = st$ joillakin luonnollisilla luvuilla $1 < t, s < n$. Nyt karakteristikan määritelmän nojalla $s\mathbf{1} \neq \mathbf{0}$ ja $t\mathbf{1} \neq \mathbf{0}$, joten koska $(K \setminus \{\mathbf{0}\}, \cdot)$ on ryhmä, $(s\mathbf{1})(t\mathbf{1}) \neq \mathbf{0}$. Tämä on ristiriita, sillä

$$\begin{aligned}(s\mathbf{1})(t\mathbf{1}) &= \left(\underbrace{1 + \cdots + 1}_{\text{s kappaletta}} \right) \left(\underbrace{1 + \cdots + 1}_{\text{t kappaletta}} \right) = \left(\underbrace{1 + \cdots + 1}_{\text{st kappaletta}} \right) \\ &= (st)\mathbf{1} = n\mathbf{1} = \mathbf{0}.\end{aligned}$$

□

Tavoitteena on seuraavaksi osoittaa, että äärellisen kunnan kertaluku on aina muotoa p^n, missä alkuluku p on kunnan karakteristika. Ensin osoitetaan, että jos alkuluku p jakaa Abelin ryhmän kertaluvun, ryhmässä on kertalukua p oleva alkio. Tämä vaatii hieman vaivaa ja pari apulausetta, mutta työ palkitaan: kunnan kertalukua koskevan lauseen todistaminen onnistuu hyvän pohjatyön jälkeen muutamassa rivissä.

Apulause 1.24. Jos a on ryhmän G alkio kertalukua $n = mk$, missä m,$k \geq 1$, niin $|a^k| = m$.

Todistus. Koska $(a^k)^m = a^{km} = a^n = e$, on $|a^k| \leq m$. Kaikilla $1 \leq s < m$ on $(a^k)^s = a^{ks}$, missä $ks < km = n$, joten $(a^k)^s \neq e$. Siis alkion a^k kertaluku on m. □

Apulause 1.25. Olkoon x Abelin ryhmän G alkio ja alkuluku p kertaluvun $|G|$ tekijä. Jos on olemassa sellainen tekijäryhmän $G/\langle x \rangle$ alkio y', että $|y'| = p$, niin ryhmässä G on alkio, jonka kertaluku on luvun p monikerta.

Todistus. Koska G on Abelin ryhmä, on lauseen 1.12 nojalla $\langle x \rangle \trianglelefteq G$ eli tekijäryhmä $G/\langle x \rangle$ on olemassa. Nyt alkio $y' = y\langle x \rangle$ jollakin ryhmän G alkiolla y. Alkio kuuluu aina itse määräämäänsä vasempaan sivuluokkaan,

joten jos $y^m = e$, niin $y^m \in y^m\langle x\rangle = e\langle x\rangle = \langle x\rangle$. Alkion y kertaluvulle n pätee siis $y^n\langle x\rangle = \langle x\rangle$ eli $(y\langle x\rangle)^n = \langle x\rangle$. Huomataan, että tässä yhtälössä $y\langle x\rangle = y'$ on tekijäryhmän $G/\langle x\rangle$ alkio ja $\langle x\rangle$ tekijäryhmän neutraalialkio. Siis koska $|y'| = p$, niin lauseen 1.6 nojalla $(y\langle x\rangle)^n = \langle x\rangle$ jos ja vain jos kertaluku $|y'| = p$ jakaa potenssin n. On siis osoitettu, että alkion y kertaluku n on luvun p monikerta. □

Lause 1.26. Olkoon G äärellinen Abelin ryhmä ja p alkuluku, joka jakaa ryhmän kertaluvun $|G|$. Tällöin ryhmässä G on alkio, jonka kertaluku on p.

Todistus. (ks. [3], s.73) Olkoon ryhmän G kertaluku $|G| = pm$, missä $m \geq 1$. Todistetaan lause induktiolla luvun m suhteen.

1. Olkoon ensin $m = 1$. Nyt $|G| = p$, eli lauseen 1.14 nojalla ryhmä G on syklinen ja tällöin sen generaattorin kertaluku on p.
2. Tehdään induktio-oletus: Aina jos $|G| = pm$, missä $m < m'$, niin ryhmässä G on kertalukua p oleva alkio.
3. Olkoon nyt $|G| = pm'$ ja x ryhmän G alkio, jolla $|x| > 1$. Tarkastellaan erikseen tapaukset $p \mid |x|$ ja $p \nmid |x|$:
   (a) Jos $p \mid |x|$, niin $|x| = np$ jollakin $n \in \mathbb{Z}^+$ ja apulauseen 1.24 nojalla $|x^n| = p$. Tällöin lause on todistettu.
   (b) Olkoon $p \nmid |x|$. Koska G on Abelin ryhmä, niin lauseen 1.12 nojalla $\langle x\rangle \trianglelefteq G$ ja siten tekijäryhmä $G/\langle x\rangle$ on olemassa. Lisäksi $G/\langle x\rangle$ on Abelin ryhmä, jonka kertaluku $|G|/|x| = pn$ jollakin luonnollisella luvulla $n < m'$. Induktio-oletuksen perusteella tekijäryhmässä $G/\langle x\rangle$ on nyt alkio y', jonka kertaluku on p. Täten apulauseen 1.25 nojalla ryhmässä G on alkio y, jonka kertaluku $|y| = qp$ jollakin $q \in \mathbb{Z}^+$. Näin ollen todistus palaa tapaukseen (a), joten lause on todistettu.

□

Lause 1.27. Äärellisen kunnan K kertaluku $|K| = p^n$, missä alkuluku p on kunnan karakteristika ja $n \in \mathbb{Z}^+$.

Todistus. (ks. [5], s.16) Olkoon $\mathrm{char}K = p$. Lauseen 1.23 nojalla p on alkuluku ja kaikkien kunnan alkioiden $a \neq \mathbf{0}$ additiivinen kertaluku on p. Tehdään vastaoletus, eli olkoon olemassa sellainen alkuluku $q \neq p$, että $q \mid |K|$. Nyt lauseen 1.26 nojalla kunnan additiivisessa ryhmässä $(K, +)$ on alkio b, jonka additiivinen kertaluku on $q \neq p$, mikä on ristiriita. Siis ainoa alkuluku, joka jakaa kertaluvun $|K|$, on p, eli $|K| = p^n$ jollakin $n \in \mathbb{Z}^+$. □

1.4 Homomorfismit

Tässä kappaleessa esitellään suppeasti homomorfiset ja isomorfiset kuvaukset. Tämä tehdään, jotta voitaisiin määritellä, milloin kaksi kuntaa ovat rakenteeltaan yhtäläiset eli isomorfiset. Lopuksi osoitetaan, että samaa kertalukua olevat kunnat, joiden kertaluku on alkuluku, ovat keskenään isomorfisia eli rakenteeltaan yhtäläisiä. Homomorfismien yksinkertaisistakaan ominaisuuksista ei esitellä muita kuin ne, joita tullaan jatkossa tarvitsemaan.

Määritelmä 1.16. Olkoon joukossa A määritelty binäärioperaatio $(\cdot)$ ja joukossa A' binäärioperaatio $(\odot)$. Kuvausta $f : A \to A'$ sanotaan *homomorfismiksi*, mikäli kaikilla $a, b \in A$ on $f(a \cdot b) = f(a) \odot f(b)$. Homomorfismia, joka on bijektio, sanotaan *isomorfismiksi*.

Määritelmä 1.17. Homomorfismi f ryhmältä $(A, \cdot)$ ryhmälle $(A', \odot)$ on *ryhmähomomorfismi*. Mikäli f on isomorfismi, se on *ryhmäisomorfismi*.

Jos on olemassa isomorfismi ryhmältä A ryhmälle A', sanotaan ryhmien olevan keskenään *isomorfiset* eli *rakenneyhtäläiset*, merkitään $A \cong A'$.

Lause 1.28. Jos kuvaus f ryhmältä $(A, \cdot)$ ryhmälle $(A', \odot)$ on ryhmähomomorfismi, niin

(a) f säilyttää neutraalialkion.

(b) kaikilla $a \in A$ on $f(a^{-1}) = f(a)^{-1}$.

Todistus. (a) Merkitään ryhmän A neutraalialkiota e ja ryhmän A' neutraalialkiota e'. Homomorfismin ja neutraalialkion määritelmien perusteella kaikilla $a \in A$ on $f(a) \odot f(e) = f(a \cdot e) = f(a)$. Operoimalla vasemmalta puolelta alkiolla $f(a)^{-1}$ saadaan $f(e) = e'$ eli kuvaus f säilyttää neutraalialkion.

(b) Kohdan (a) perusteella millä tahansa $a \in A$ on $e' = f(e) = f(a \cdot a^{-1})$ $= f(a) \odot f(a^{-1})$ ja samoin $e' = f(a^{-1}) \odot f(a)$. Näin ollen $f(a^{-1})$ on alkion $f(a) \in A'$ käänteisalkio eli $f(a^{-1}) = f(a)^{-1}$.

□

Huomautus. Isomorfiset ryhmät ovat nimensä mukaisesti rakenteeltaan yhtäläisiä, toisin sanoen ne ovat alkioiden nimeämistä vaille samat. Tämän vuoksi rakenneyhtäläiset ryhmät voidaan samaistaa.

Määritelmä 1.18. Olkoot $(K, +, \cdot)$ ja $(K', \oplus, \odot)$ kuntia. Kuvausta $f : K \to K'$ sanotaan *kuntahomomorfismiksi*, mikäli kaikilla $a, b \in K$ on

- $f(a \cdot b) = f(a) \odot f(b)$

- $f(a+b) = f(a) \oplus f(b)$

Bijektiivistä kuntahomomorfismia f sanotaan *kuntaisomorfismiksi*. Mikäli on olemassa kuntaisomorfismi kunnalta K kunnalle K', kunnat ovat keskenään isomorfiset eli rakenneyhtäläiset ja merkitään $K \cong K'$.

Kuntahomomorfismi on ryhmähomomorfismi sekä kuntien additiivisten ryhmien että multiplikatiivisten ryhmien välillä. Kuntahomomorfismi siis säilyttää sekä kunnan nolla- että ykkösalkiot. Lisäksi kaikilla $a \in A$ on $f(-a) = -f(a)$ ja $f(a^{-1}) = f(a)^{-1}$. Samoin kuin rakenneyhtäläiset ryhmät, voidaan rakenneyhtäläiset kunnat samaistaa.

Huomautus. Usein on tapana määritellä kuntahomomorfismin sijaan *rengashomomorfismi*. Rengas on kuntaa muistuttava rakenne, jossa kertomisen ei kuitenkaan tarvitse olla kommutatiivinen operaatio eikä alkioilla tarvitse olla käänteisalkioita kertomisen suhteen. Tässä työssä ei tarvita sellaisia renkaita, jotka eivät olisi myös kuntia, joten homo- ja isomorfismit on käytännöllisempää määritellä suoraan kunnille.

Lause 1.29. Jos $(K, +, \cdot)$ ja $(K', \oplus, \odot)$ ovat kuntia, joiden kertaluku on alkuluku p, niin $K \cong K'$.

Todistus. Lauseen 1.23 nojalla molempien kuntien karakteristika on p. Näin ollen kuntien ykkösalkiot $\mathbf{1}$ ja $\mathbf{1}'$ generoivat kuntien additiiviset ryhmät $(K, +)$ ja $(K', \oplus)$. Kunnan K kaikki alkiot ovat siis muotoa $n\mathbf{1}$ ja kunnan K' alkiot muotoa $n\mathbf{1}'$ jollakin $n \in \mathbb{N}$. Olkoon kuvaus $f : K \to K'$ sellainen, että $f(n\mathbf{1}) = n\mathbf{1}'$ kaikilla $n \in \mathbb{N}$. Osoitetaan, että tällöin kuvaus f on kuntaisomorfismi.

Olkoot $a, b \in K$. Nyt $a = n\mathbf{1}$ ja $b = m\mathbf{1}$ joillakin $n, m \in \mathbb{N}$, joten

$$\begin{aligned} f(a+b) &= f(n\mathbf{1} + m\mathbf{1}) = f((n+m)\mathbf{1}) = (n+m)\mathbf{1}' \\ &= n\mathbf{1}' + m\mathbf{1}' = f(n\mathbf{1}) + f(m\mathbf{1}) = f(a) + f(b). \end{aligned}$$

Käyttämällä kunnan osittelulakeja $a(b+c) = ab+ac$ ja $(a+b)c = ac+bc$ toistuvasti saadaan

$$\begin{aligned} n\mathbf{1} \cdot m\mathbf{1} &= (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{n kpl}}) \cdot (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{m kpl}}) \\ &= \underbrace{(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{m kpl}}) + \cdots + (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{m kpl}})}_{\text{n kpl}} \\ &= \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{\text{nm kpl}} \\ &= (nm)\mathbf{1}. \end{aligned}$$

Sama pätee myös kunnan K' ykkösalkiolle $\mathbf{1}'$. Näin ollen on

$$\begin{aligned} f(a \cdot b) &= f(n\mathbf{1} \cdot m\mathbf{1}) = f\left((nm)\mathbf{1}\right) = (nm)\mathbf{1}' = n\mathbf{1}' \odot m\mathbf{1}' \\ &= f(n\mathbf{1}) \odot f(m\mathbf{1}) = f(a) \odot f(b). \end{aligned}$$

Näin on osoitettu, että kuvaus f on kuntahomomorfismi. On osoitettava vielä, että se on bijektio.

Olkoon $f(a) = f(b) \in K'$ eli $f(n\mathbf{1}) = f(m\mathbf{1})$. Nyt siis $n\mathbf{1}' = m\mathbf{1}'$ eli lauseen 1.6 nojalla $p \mid (n-m)$. Saman lauseen nojalla on siis myös $n\mathbf{1} = m\mathbf{1}$ eli $a = b$. Näin ollen kuvaus f on injektio.

Olkoon sitten $c \in K'$ mielivaltainen. Nyt $c = q\mathbf{1}'$ jollakin $q \in \mathbb{N}$. Alkio $q\mathbf{1} \in K$ ja $f(q\mathbf{1}) = q\mathbf{1}' = c$ eli on osoitettu, että kuvaus f on surjektio.

Nyt on osoitettu, että kuvaus f on bijektiivinen homomorfismi eli isomorfismi. Näin ollen kunnat K ja K' ovat keskenään isomorfiset. □

Jatkossa kunnan K kertaluvun ollessa alkuluku p merkitään kunnan alkioita $K = \{\mathbf{0}, \mathbf{1}, 2, \cdots, p-1\}$. Kullakin luvulla n on tässä merkitty kunnan alkiota $n\mathbf{1}$. Näillä kunnan alkioilla lasketaan kuten jäännösluokilla.

1.5 Polynomeista

Esitiedoista viimeisimpänä tutustutaan hieman polynomeihin. Käyttöön tahdotaan saada tulos, jonka mukaan astetta $n \in \mathbb{N}$ olevalla polynomilla on korkeintaan n toisistaan eroavaa nollakohtaa. Kyseistä tulosta tarvitaan lauseen 6.4 todistuksessa. Lukija, jolle tämä polynomien ominaisuus on tuttu, voi huoletta siirtyä lukuun 2.

Määritelmä 1.19. Kun K on kunta, sanotaan *polynomeiksi* joukon

$$K[x] = \{a_n x^n + \cdots + a_1 x + a_0 : n \geq \mathbf{0}, a_i \in K, a_n \neq \mathbf{0}\}$$

alkioita.

Suurin polynomissa $f(x) \in K[x]$ esiintyvä tuntemattoman x potenssi on polynomin *aste*, jota merkitään $\deg f(x)$. Vakiopolynomin $c \neq \mathbf{0}$ aste on siis nolla. Määritellään lisäksi, että nollapolynomin aste on $\deg \mathbf{0} = -\infty$.

Huomautus. Se, kuinka polynomien summat ja tulot muodostetaan, seuraa suoraan tavasta, jolla lasketaan kunnan K alkioilla. Joukko $K[x]$ on suljettu polynomien yhteenlaskun ja kertomisen suhteen, sillä polynomien tulot ja summat ovat edelleen polynomeja.

Jos $f(x)$, $g(x) \in K[x] \setminus \{\mathbf{0}\}$, on helppo huomata, että $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ ja $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$. Nollapolynomin aste on määritelty olemaan $-\infty$, jotta tämä pätisi myös nollapolynomille. Mielivaltaisen polynomin $f(x) \in K[x]$ aste on joko $n \in \mathbb{N}$ tai $-\infty$ ja kaikilla $n \in \mathbb{N}$ on $n - \infty = -\infty - \infty = -\infty$. Näin ollen tulon $f(x) \cdot \mathbf{0}$ asteeksi saadaan

$$deg(f(x) \cdot \mathbf{0}) = \deg \mathbf{0} = -\infty = \deg f(x) - \infty = \deg f(x) + \deg \mathbf{0}.$$

Koska $f(x) + \mathbf{0} = f(x)$, seuraa määrittelystä $\deg \mathbf{0} = -\infty$ selvästi myös $\deg(f(x) + \mathbf{0}) = \deg f(x) = \max\{\deg f(x), \deg \mathbf{0}\}$.

Lause 1.30. Olkoon K kunta, $f(x)$, $g(x) \in K[x]$ ja $g(x) \neq \mathbf{0}$. Tällöin on olemassa sellaiset joukon $K[x]$ polynomit $q(x)$ ja $r(x)$, että $\deg r(x) < \deg g(x)$ ja $f(x) = q(x)g(x) + r(x)$.

Todistus. (ks. [5]) Olkoot $f(x)$, $g(x) \in K[x]$ ja $g(x) \neq \mathbf{0}$. Tarkastellaan joukkoa

$$S = \{f(x) - s(x)g(x) : s(x) \in K[x]\}.$$

Selvästi $S \subseteq K[x]$ ja $S \neq \emptyset$. Olkoon $r(x) \in S$ polynomi, jonka aste on mahdollisimman pieni. Nyt $r(x) = f(x) - q(x)g(x)$ jollakin $q(x) \in K[x]$ eli $f(x) = q(x)g(x) + r(x)$.

On osoitettava enää, että $\deg r(x) < \deg g(x)$. Tehdään tämä vastaoletuksen avulla eli oletetaan, että $\deg r(x) \geq \deg g(x)$. Merkitään

$$\begin{aligned} r(x) &= r_n x^n + \cdots + r_0 & r_n &\neq \mathbf{0} \\ g(x) &= g_m x^m + \cdots + g_0 & g_m &\neq \mathbf{0}, \end{aligned}$$

missä vastaoletuksen perusteella on $n \geq m$. Nyt $k(x) = g_m^{-1} r_n x^{n-m} \in K[x]$. Avaamalla hieman joukon $K[x]$ polynomia $t(x) = r(x) - k(x)g(x)$ nähdään, että

$$\begin{aligned} t(x) &= (r_n x^n + \cdots + r_0) - (g_m^{-1} r_n x^{n-m})(g_m x^m + \cdots + g_0) \\ &= (r_n x^n + \cdots + r_0) - (r_n x^n + \cdots + g_m^{-1} r_n g_0 x^{n-m}), \end{aligned}$$

joten termi $r_n x^n$ supistuu ja siten $\deg t(x) < n = \deg r(x)$.

Toisaalta

$$\begin{aligned} t(x) &= r(x) - k(x)g(x) \\ &= (f(x) - q(x)g(x)) - k(x)g(x) \\ &= f(x) - ((q(x) + k(x))g(x)), \end{aligned}$$

joten $t(x) \in S$. Tämä on ristiriita, koska polynomi $r(x)$ valittiin joukosta S siten, että sen aste on mahdollisimman pieni. Koska saatiin ristiriita, on vastaoletus $\deg r(x) \geq \deg g(x)$ epätosi, eli $\deg r(x) < \deg g(x)$. □

Määritelmä 1.20. Mikäli $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ ja α on kunnan K sellainen alkio, että

$$f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = \mathbf{0},$$

niin α on polynomin $f(x)$ *nollakohta* kunnassa K.

Jos $f(x) = q(x)g(x)$ joillakin $q(x)$, $g(x) \in K[x]$, $g(x) \neq \mathbf{0}$, niin polynomin $g(x)$ sanotaan jakavan polynomin $f(x)$, merkitään $g(x) \mid f(x)$.

Lause 1.31. Alkio $\alpha \in K$ on polynomin $f(x) \in K[x]$ nollakohta jos ja vain jos $(x - \alpha) \mid f(x)$.

Todistus. (ks. [5]) Oletetaan ensin, että $(x - \alpha) \mid f(x)$. Nyt siis $f(x) = q(x)(x - \alpha)$ jollakin $q(x) \in K[x]$. Siis

$$f(\alpha) = q(\alpha)(\alpha - \alpha) = q(\alpha)\mathbf{0} = \mathbf{0}.$$

Olkoon sitten $f(\alpha) = \mathbf{0}$. Lauseen 1.30 perusteella on olemassa sellaiset $q(x)$ ja $r(x) \in K[x]$, että $f(x) = q(x)(x - \alpha) + r(x)$ ja $\deg r(x) < \deg (x - \alpha) = 1$. Siten $r(x)$ on vakiopolynomi $c \in K$. Nyt $f(\alpha) = q(\alpha)(\alpha - \alpha) + c = c$ ja toisaalta oletuksen perusteella $f(\alpha) = \mathbf{0}$. Siis $c = \mathbf{0}$ joten $f(x) = q(x)(x - \alpha)$ eli $(x - \alpha) \mid f(x)$. □

Seuraus 1.32. Astetta n olevalla polynomilla on korkeintaan n erisuurta nollakohtaa kunnassa K.

Todistus. Olkoon $f(x)$ astetta n oleva joukon $K[x]$ polynomi, jonka toisistaan poikkeavat nollakohdat ovat $x_1, x_2, \ldots, x_m$. Nyt $f(x) = (x - x_1)g(x)$ jollakin $g(x) \in K[x]$. Koska $f(x_2) = (x_2 - x_1)g(x_2) = \mathbf{0}$ ja $x_2 - x_1 \neq \mathbf{0}$, on $g(x_2) = \mathbf{0}$ eli $g(x) = (x - x_2)h(x)$ jollakin $h(x) \in K[x]$. Näin on saatu $f(x) = (x - x_1)(x - x_2)h(x)$ ja samoin jatkamalla nähdään, että

$$t(x) = (x - x_1)(x - x_2) \ldots (x - x_m)$$

jakaa polynomin $f(x)$. Siten $m = \deg t(x) \leq \deg f(x) = n$ eli erisuuria nollakohtia on korkeintaan n kappaletta. □

2 Lineaariset ryhmät

Tässä luvussa määritellään kolme erilaista lineaaristen ryhmien tyyppiä: yleinen, erityinen ja erityinen projektiivinen lineaarinen ryhmä. Kaksi ensimmäistä lineaarista ryhmää ovat neliömatriisien muodostamia ryhmiä, joiden operaationa on matriisien välinen kertolasku ja joissa matriisien sisältämät alkiot kuuluvat johonkin äärelliseen kuntaan K. Kolmas määriteltävä ryhmä on näistä jälkimmäisen eräs tekijäryhmä. Vaikka lineaariset ryhmät voidaan määritellä $m \times m$ -matriiseille millä tahansa $2 \leq m \in \mathbb{N}$, käsitellään tässä vain 2×2 -matriisien muodostamia lineaarisia ryhmiä.

Matriisien välisen kertolaskun oletetaan olevan lukijalle tuttu. Samoin tutuksi oletetaan determinantin käsite, sen laskeminen, identiteettimatriisin käsite sekä seuraavat $m \times m$ -matriisien ja niiden determinanttien ominaisuudet:

- Matriisien A ja B tulon AB determinantti $\det(AB)$ on $\det A \det B$.
- Identiteettimatriisille $I_{m\times m}$ pätee $AI = IA = A$ kaikilla $m \times m$ -matriiseilla A.
- $m \times m$-matriisilla A on olemassa käänteismatriisi A^{-1}, jolla $AA^{-1} = A^{-1}A = I$ jos ja vain jos $\det A \neq \mathbf{0}$
- Kaikilla $m \times m$ -matriiseilla A,B ja C on $(AB)C = A(BC)$.
- Jos matriisin A alkiot kuuluvat kuntaan K, matriisi $-A = -\mathbf{1}A$ saadaan korvaamalla kukin matriisin A alkio $a \in K$ vasta-alkiollaan $-a \in K$.

Edellisistä nähdään helposti, että jos A^{-1} on matriisin A käänteismatriisi, niin $\det(A^{-1}) = (\det A)^{-1}$.

2.1 Ryhmä $GL(2, K)$

Olkoon $GL(2, K)$ joukko, johon kuuluvat kaikki 2×2 -matriisit, joiden alkiot ovat äärellisestä kunnasta K ja joiden determinantti ei ole $\mathbf{0}$. Tällöin $GL(2, K)$ varustettuna matriisien kertolaskuoperaatiolla on ryhmä:

$$\det I = \det \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = \mathbf{11} - \mathbf{00} = \mathbf{1} \neq \mathbf{0},$$

joten $I \in GL(2,K)$. Matriisi I on ryhmän neutraalialkio, sillä $AI = IA = A$ kaikilla $A \in GL(2,K)$. Koska joukon määritelmän mukaan mielivaltaisen alkion $A \in GL(2,K)$ determinantti ei ole nolla, on olemassa käänteismatriisi A^{-1}. Lisäksi A^{-1} kuuluu joukkoon $GL(2,K)$, sillä $\det A^{-1} = (\det A)^{-1} \neq \mathbf{0}$. Matriisien kertolaskun tiedetään olevan assosiatiivinen operaatio. Lisäksi joukko $GL(2,K)$ on suljettu matriisien kertolaskun suhteen, sillä $\det(AB) = \mathbf{0}$ jos ja vain jos $\det A = \mathbf{0}$ tai $\det B = \mathbf{0}$.

Määritelmä 2.1. Ryhmä $GL(2,K)$ on *yleinen lineaarinen ryhmä* astetta kaksi. Sen operaatio on matriisien kertolasku ja siihen kuuluvat kaikki 2×2 -matriisit, joiden alkiot kuuluvat kuntaan K ja joiden determinantti ei ole $\mathbf{0}$. Jos kunnan K kertaluku on p, voidaan merkitä $GL(2,K) = GL(2,p)$.

Lause 2.1. Jos kunnan K kertaluku on p, niin ryhmässä $GL(2,K)$ on $(p-1)^2p(p+1)$ alkiota.

Todistus. Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,K)$. On selvitettävä, kuinka monella tapaa alkiot a, b, c ja d voidaan valita kunnasta K siten, että $\det A = ad - bc \neq \mathbf{0}$. Tarkastellaan erikseen tapaukset $ad = \mathbf{0}$ ja $ad \neq \mathbf{0}$:

1. Jos $ad = \mathbf{0}$, niin joko $a = \mathbf{0}$ ja $d \in K$ tai $a \in K$ ja $d = \mathbf{0}$. Alkiot a ja d voidaan siis valita $2p$ eri tavalla. Jotta tämän jälkeen $ad - bc \neq \mathbf{0}$ toteutuisi, on oltava $bc \neq \mathbf{0}$ eli b,$c \in K \setminus \{\mathbf{0}\}$. Alkiot b ja c voidaan siis valita $(p-1)^2$ tavalla. Yhteensä alkioiden a,b,c ja d mahdollisia valintoja on siis $2p(p-1)^2$ kappaletta.

2. Jos $ad \neq \mathbf{0}$, niin a,$d \in K \setminus \{\mathbf{0}\}$, eli alkiot a ja d voidaan valita $(p-1)^2$ eri tavalla. Jotta yhtälö $ad - bc \neq \mathbf{0}$ toteutuisi, on nyt oltava $ad \neq bc$ eli $c \neq b^{-1}ad$. Alkio b voidaan siis valita vapaasti joukosta K, minkä jälkeen alkio c on valittava joukosta $K \setminus \{b^{-1}ad\}$. Mahdollisia alkioiden b ja c valintoja on siis yhteensä $p(p-1)$ kappaletta. Siten alkiot a,b, c ja d voidaan valita yhteensä $(p-1)^2p(p-1) = (p-1)^3p$ tavalla.

Näistä tapauksista saadaan yhteensä

$$(2p)(p-1)^2 + (p-1)^3p = (p-1)^2p(2 + (p-1)) = (p-1)^2p(p+1)$$

mahdollista valintaa matriisin A alkioille. □

Tarkastellaan pienintä mahdollista yleistä lineaarista ryhmää, joka on $GL(2,2)$. Nyt matriisien alkiot kuuluvat kahden alkion kuntaan $K = \{\mathbf{0}, \mathbf{1}\}$. Juuri osoitetun lauseen mukaan ryhmässä on $(2-1)^2 \cdot 2 \cdot 3 = 6$ alkiota. Jos jokainen matriisin neljästä alkiosta saisi olla kunnan kumpi tahansa alkio, olisi

mahdollisia matriiseja tällöinkin yhteensä vain $2^4 = 16$ kappaletta. Tarkastelemalla ehtoa $\det A \neq \mathbf{0}$ tai kirjaamalla mahdolliset 16 matriisia ja laskemalla niiden determinantit voidaan todeta, että ryhmän $GL(2,2)$ kertaluku tosiaan on kuusi ja että

$$GL(2,2) = \left\{ \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{pmatrix}, \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}, \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} \end{pmatrix}, \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \right\}.$$

Merkitään samassa järjestyksessä ryhmän alkioita seuraavasti:

$$GL(2,2) = \{I, R, S, T, U, U^2\}$$

Tutkitaan, millaisia ei-triviaaleja aliryhmiä ryhmällä $GL(2,2)$ on: Todetaan ensin, että todellakin

$$UU = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} = U^2,$$

eli merkintä on järkevä. Koska $U^3 = I$, on $|U| = 3$ ja $\langle U \rangle = \{U, U^2, I\} = \langle U^2 \rangle$. Matriiseilla R, S ja T on $R^2 = S^2 = T^2 = I$, eli näiden matriisien kertaluku on kaksi. Siten $\langle R \rangle = \{I, R\}$, $\langle S \rangle = \{I, S\}$ ja $\langle T \rangle = \{I, T\}$.

Yksittäisten matriisien generoimia aliryhmiä on siis löydetty yhteensä neljä kappaletta, joista kolme on kertalukua kaksi ja yksi on kertalukua kolme. Näiden lisäksi ryhmällä $GL(2,2)$ ei ole muita ei-triviaaleja aliryhmiä; jos nimittäin H on ryhmän $GL(2,2)$ ei-triviaali aliryhmä, niin Lagrangen lauseen 1.9 perusteella $|H| \mid 6$ eli $|H| \in \{2, 3\}$. Näin ollen lauseen 1.14 perusteella ryhmä H on syklinen eli jokin aiemmin löydetyistä.

Selvitetään vielä ovatko löydetyt ryhmän $GL(2,2)$ aliryhmät normaaleja: Laskemalla on helppo todeta, että $RS = U$ ja $RT = U^2$. Kuitenkin $SR = U^2$ ja $TR = U$ ja siten

$$\begin{aligned} R\langle S \rangle &= \{R, U\} \neq \{R, U^2\} = \langle S \rangle R, \\ S\langle R \rangle &= \{S, U^2\} \neq \{S, U\} = \langle R \rangle S \text{ ja} \\ T\langle R \rangle &= \{T, U\} \neq \{T, U^2\} = \langle R \rangle T, \end{aligned}$$

joten aliryhmät $\langle R \rangle$, $\langle S \rangle$ ja $\langle T \rangle$ eivät ole normaaleja. Aliryhmä $\langle U \rangle$ sen sijaan on normaali aliryhmä. Lauseen 1.19 perusteella nimittäin $\langle U \rangle^A$ on ryhmän $GL(2,2)$ kertalukua kolme oleva aliryhmä kaikilla $A \in GL(2,2)$. Koska $\langle U \rangle$ on ryhmän $GL(2,2)$ ainut kertalukua kolme oleva aliryhmä, on siis $A^{-1}\langle U \rangle A = \langle U \rangle$ eli $\langle U \rangle A = A\langle U \rangle$ kaikilla $A \in GL(2,2)$. Näin ollen $\langle U \rangle$ on normaali aliryhmä.

2.2 Ryhmä $SL(2, K)$

Tiedetään, että matriisien A ja B determinanteille pätee $\det A \det B = \det(AB)$. Siten kaikkien sellaisten 2×2 -matriisien joukko, joiden alkiot ovat äärellisestä kunnasta K ja joiden determinantti on $\mathbf{1}$, on suljettu matriisien kertolaskun suhteen. Merkitään tätä joukkoa $SL(2, K)$. Koska 2×2 -identiteettimatriisin determinantti on $\mathbf{1}$, kuuluu se tähän joukkoon. Myös joukon jokaisen matriisin käänteismatriisi kuuluu joukkoon, sillä jos $A \in SL(2, K)$, niin

$$\det(A^{-1}) = (\det A)^{-1} = \mathbf{1}^{-1} = \mathbf{1}.$$

Lisäksi matriisien kertolaskun tiedetään olevan assosiatiivinen, joten joukko $SL(2, K)$ varustettuna matriisien kertolaskulla on ryhmä.

Määritelmä 2.2. Ryhmä $SL(2, K)$ on *erityinen lineaarinen ryhmä* astetta kaksi. Sen operaationa on matriisien kertolasku ja siihen kuuluvat kaikki matriisit, joiden alkiot ovat äärellisestä kunnasta K ja joiden determinantti on $\mathbf{1}$. Jos kunnan K kertaluku on p, voidaan merkitä $SL(2, K) = SL(2, p)$.

Aiemmin tarkasteltiin pienintä mahdollista yleistä lineaarista ryhmää $GL(2, 2)$. Koska $\det A \in K \setminus \{\mathbf{0}\}$ kaikilla $A \in GL(2, K)$, on ryhmän $GL(2, 2)$ alkioiden determinantti $\mathbf{1}$. Näin ollen yleinen lineaarinen ryhmä $GL(2, 2)$ on itseasiassa sama kuin erityinen lineaarinen ryhmä $SL(2, 2)$. Kahden alkion kunta K on ainut tapaus, jossa tämä on totta. Jos nimittäin $|K| > 2$, on kunnassa K alkio a, joka ei ole nolla- eikä ykkösalkio. Matriisi $\begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ kuuluu ryhmään $GL(2, 2)$ ja sen determinantti on $a \neq \mathbf{1}$ eli se ei kuulu ryhmään $SL(2, 2)$. Jos kunnan K kertaluku on suurempi kuin kaksi, on $SL(2, K)$ ryhmän $GL(2, K)$ aito aliryhmä.

Lause 2.2. Jos kunnan K kertaluku on p, niin ryhmän $SL(2, K)$ kertaluku on $(p-1)p(p+1)$.

Todistus. $SL(2, K)$ on ryhmän $GL(2, K)$ aliryhmä. Tarkastellaan sen vasempien sivuluokkien määrää. Olkoon $A \in GL(2, K)$ ja $\det A = a \in K$. Nyt kaikki sivuluokan $A(SL(2, K))$ alkiot ovat muotoa AX, missä $X \in SL(2, K)$ ja

$$\det(AX) = \det A \det X = a\mathbf{1} = a.$$

Jos toisaalta $\det B = \det A = a$, niin

$$\det(B^{-1}A) = \det(B^{-1}) \det A = (\det B)^{-1} \det A = a^{-1}a = \mathbf{1}$$

eli alkio $B^{-1}A \in SL(2,K)$. Siten lauseen 1.8 perusteella on $B(SL(2,K)) = A(SL(2,K))$.

On osoitettu, että jokaista ryhmän $GL(2,K)$ matriisien mahdollista determinanttia vastaa tasan yksi aliryhmän $SL(2,K)$ vasen sivuluokka. Determinantit kuuluvat joukkoon $K \setminus \{\mathbf{0}\}$ eli mahdollisia determinantteja on $p-1$ kappaletta, joten tämä on myös aliryhmän $SL(2,K)$ vasempien sivuluokkien lukumäärä. Siten Lagrangen lauseen 1.9 nojalla

$$|SL(2,K)| = \frac{|GL(2,K)|}{p-1} = \frac{(p-1)^2 p(p+1)}{p-1} = (p-1)p(p+1).$$

□

Määritellään ennen uutta esimerkkiä tärkeä mielenkiintomme kohde:

Määritelmä 2.3. Jos ryhmän G ainoat normaalit aliryhmät ovat $\{\mathbf{1}\}$ ja G, niin G on yksinkertainen ryhmä.

Seuraavien kappaleiden ajan tulemme olemaan kiinnostuneita siitä, ovatko tarkastelemamme ryhmät yksinkertaisia. Aiemmin ryhmästä $GL(2,2)$ löydettiin aito normaali aliryhmä $\langle U \rangle$. Tämän löydön vuoksi voidaan todeta, että ryhmä $GL(2,2)$ ei ole yksinkertainen.

Tarkastellaan lyhyesti ryhmää $SL(2,K) = SL(2,3)$, jossa matriisien alkiot ovat kunnasta $K = \{\mathbf{0}, \mathbf{1}, 2\}$. Tässä ryhmässä on lauseen 2.2 perusteella $2 \cdot 3 \cdot 4 = 24$ alkiota.

Meitä erityisesti kiinnostava kysymys ryhmän $SL(2,3)$ mahdollisesta yksinkertaisuudesta on ratkaistavissa ilman pitkiä tarinoita. Nimittäin matriisin $A = \begin{pmatrix} 2 & \mathbf{0} \\ \mathbf{0} & 2 \end{pmatrix} \in SL(2,3)$ kertaluku on kaksi eli $\langle A \rangle = \{A, I\}$ ja A kommutoi kaikkien 2×2 -matriisien kanssa. Jos siis $X \in SL(2,3)$, niin

$$X\langle A \rangle = \{XA, X\} = \{AX, X\} = \langle A \rangle X.$$

Siten aliryhmä $\langle A \rangle$ on ei-triviaali normaali aliryhmä ja $SL(2,3)$ ei ole yksinkertainen.

2.3 Ryhmä $PSL(2,K)$

Seuraavaksi tutustutaan kolmanteen ja meitä eniten kiinnostavaan lineaaristen ryhmien tyyppiin. Ennen kuin päästään asiaan, on kuitenkin tunnettava ryhmän keskuksen käsite.

Määritelmä 2.4. Ryhmän G *keskus* $Z(G)$ on niiden ryhmän G alkioiden joukko, jotka kommutoivat kaikkien ryhmän alkioiden kanssa. Siis $Z(G) = \{a \in G : ag = ga \text{ kaikilla } g \in G\}$.

Huomautus. Selvästi ryhmän G keskus $Z(G)$ on ryhmän G normaali aliryhmä.

Lause 2.3. Erityisen lineaarisen ryhmän $SL(2, K)$ keskus on $\{I, -I\}$.

Todistus. (ks. [9]) Selvästi matriisit I ja $-I$ kommutoivat kaikkien ryhmän $SL(2, K)$ matriisien kanssa eli $\{I, -I\} \subseteq Z(G)$.

Jos matriisi $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(SL(2, K))$, niin A kommutoi matriisien $\begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ ja $\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{pmatrix}$ kanssa. Siis

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ ja}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Kun nämä tulot kerrotaan auki, saadaan

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \text{ ja } \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix} = \begin{pmatrix} a & b \\ a+c & b+d \end{pmatrix}.$$

Näistä yhtälöistä nähdään, että $c = b = \mathbf{0}$ ja $a = d$. Siten A on muotoa $\begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & a \end{pmatrix}$ ja koska $A \in SL(2, K)$, on $\det A = \mathbf{1}$, joten

$$\begin{aligned} \det A = a^2 &= \mathbf{1} \\ \Leftrightarrow a^2 - \mathbf{1} &= \mathbf{0} \\ \Leftrightarrow (a + \mathbf{1})(a - \mathbf{1}) &= \mathbf{0} \\ \Leftrightarrow a = \mathbf{1} &\text{ tai } a = -\mathbf{1}, \end{aligned}$$

Siten ainoat ryhmän $SL(2, K)$ keskukseen $Z(SL(2, K))$ kuuluvat matriisit ovat I ja $-I$. □

Huomautus. Mikäli kunnan K karakteristika on kaksi, on $\mathbf{1} = -\mathbf{1}$ ja $I = -I$, joten $Z(SL(2, K)) = \{I\}$. Tällöin ja vain tällöin keskuksen $Z(SL(2, K))$ kertaluku on yksi. Jos karakteristika ei ole kaksi, on $I \neq -I$ ja siten keskuksen kertaluku on kaksi.

Koska ryhmän keskus on ryhmän normaali aliryhmä, voidaan sen suhteen muodostaa tekijäryhmä. Tekijäryhmä $SL(2,K)/Z(SL(2,K))$ on kolmas lineaaristen ryhmien tyyppi, jonka määrittelemme.

Määritelmä 2.5. Tekijäryhmä $PSL(2,K) = SL(2,K)/Z(SL(2,K))$ on *projektiivinen erityinen lineaarinen ryhmä* astetta kaksi.

Koska ryhmien $SL(2,K)$ ja $Z(SL(2,K))$ kertaluku on tiedossa, tekijäryhmän $PSL(2,K)$ kertaluku on näiden osamääränä laskettavissa. Jos siis kunnan karakteristika ei ole kaksi, on

$$|PSL(2,K)| = |SL(2,K)|/|Z(SL(2,K))| = (p-1)p(p+1)/2.$$

Jos kunnan karakteristika on kaksi, todettiin keskuksen $Z(SL(2,K))$ olevan kertalukua yksi ja siten $|PSL(2,K)| = (p-1)p(p+1)$.

Tässä vaiheessa voidaan todeta päässeemme asiaan. Seuraavissa kappaleissa aiotaan nimittäin tarkastella ryhmien $PSL(2,K)$ yksinkertaisuutta kunnan K eri kertaluvuilla. Ensin osoitetaan, että mikäli kunnan K kertaluku on neljä, viisi tai seitsemän on ryhmä $PSL(2,K)$ yksinkertainen. Nämä tapaukset eivät ole erityistapauksia; Kappaleessa 6 nimittäin osoitetaan juhlallisesti, että $PSL(2,K)$ on yksinkertainen ryhmä aina kun kunnan K kertaluku on vähintään neljä.

3 Ryhmän $PSL(2,5)$ yksinkertaisuus

Tässä luvussa osoitetaan, että ryhmä $PSL(2,5)$ on yksinkertainen. Tärkeänä työvälineenä toimivat konjugointiluokat, joiden yhdisteitä normaalien aliryhmien tiedetään olevan (lause 1.22). Ennen kuin ryhdymme osoittamaan ryhmän yksinkertaisuutta, todistamme erityisen kätevän tuloksen, joka auttaa selvittämään alkion konjugaattien määrän eli sen määräämän konjugointiluokan kertaluvun. Kyseinen lause tulee olemaan käytössä seuraavissakin luvuissa.

3.1 Apulauseita

Seuraavaksi esitellään kaksi työvälinettä, joiden avulla voidaan tehokkaasti etsiä ryhmien $PSL(2,K)$ normaaleja aliryhmiä. Ensimmäinen apulause ei ehkä ensikatsauksella vaikuta erityisen mielenkiintoiselta. Siitä on kuitenkin suuri hyöty, koska sen ansiosta jatkossa ei tarvitse juurikaan työskennellä tekijäryhmän $PSL(2,K)$ alkioiden kanssa. Apulauseessa osoitetaan ryhmän ja tekijäryhmän normaaleille aliryhmille yhteys, jonka ansiosta saadaan siirrettyä normaalien aliryhmien etsiminen tekijäryhmästä $PSL(2,K)$ ryhmään $SL(2,K)$.

Lause 3.2 helpottaa konjugointiluokkien kertaluvun selvittämistä ja on jatkossa erityisen ahkerassa käytössä. Sen todistaminen onnistuu osoittamalla erään kuvauksen olevan bijektio, minkä seurauksena äärellisissä lähtö- ja maalijoukoissa on yhtä monta alkiota. Bijektion määritelmä ja sen edellä mainittu ominaisuus oletetaan lukijalle tutuiksi.

Apulause 3.1. Olkoon G äärellinen ryhmä. Nyt

$$N/Z(G) \trianglelefteq G/Z(G) \Leftrightarrow N \trianglelefteq G \text{ ja } Z(G) \subseteq N.$$

Todistus. Olkoon ensin $N/Z(G) \trianglelefteq G/Z(G)$. Koska tekijäryhmä $N/Z(G)$ on olemassa, on $Z(G) \trianglelefteq N$ eli $Z(G) \subseteq N$. Olkoot alkiot $g \in G$ ja $n \in N$ mielivaltaisia. Tällöin

$$\begin{aligned} gZ(G) &= G_1 \in G/Z(G), \\ nZ(G) &= N_1 \in N/Z(G) \end{aligned}$$

ja lauseen 1.11 perusteella $G_1^{-1}N_1G_1 \in N/Z(G)$. Auki kirjoitettuna siis

$$\begin{aligned} &\left(gZ(G)\right)^{-1}\left(nZ(G)\right)\left(gZ(G)\right) \\ =&\left(g^{-1}Z(G)\right)\left(nZ(G)\right)\left(gZ(G)\right) \\ =&(g^{-1}ng)Z(G) \in N/Z(G) \end{aligned}$$

eli alkio $g^{-1}ng \in N$ ja siten lauseen 1.11 nojalla $N \trianglelefteq G$.

Olkoon sitten $N \trianglelefteq G$ ja $Z(G) \subseteq N$. Selvästi $Z(G) \trianglelefteq N$, joten tekijäryhmä $N/Z(G)$ on olemassa. Olkoot $N_1 = nZ(G) \in N/Z(G)$ ja $G_1 = gZ(G) \in G/Z(G)$ tekijäryhmien mielivaltaiset alkiot. Jälleen

$$G_1^{-1}N_1G_1 = (g^{-1}ng)Z(G),$$

missä oletuksen $N \trianglelefteq G$ ja lauseen 1.11 perusteella $g^{-1}ng \in N$. Siis $G_1^{-1}N_1G_1 \in N/Z(G)$ eli edelleen lausetta 1.11 käyttäen saadaan $N/Z(G) \trianglelefteq G/Z(G)$. □

Kuvitelkaamme tässä vaiheessa itsemme aarrejahtiin saarelle, jonka kilometrien pituiselle hiekkarannalle on kätketty kalleuksia. Kätketyt aarteet ovat konjugointiluokkia ja seuraava apulause on metallinpaljastin. Metallinpaljastimemme ansiosta meidän ei tarvitse kaivella rantahiekkaa summanmutikassa sieltä sun täältä. Toisin sanoen: meidän ei tarvitse luetella ryhmän alkioita ja laskeskella suuria määriä niiden konjugaatteja selvittääksemme, mitkä alkioista konjugoivat keskenään. Metallinpaljastin vain päälle (eli ryhmän alkio tarkasteluun) ja etsimään kätköpaikkaa, toisin sanoen konjugointiluokan kertalukua. Tätä päivän pelastavaa välinettä varten tarvitaan yksi uusi määritelmä:

Määritelmä 3.1. Ryhmän G alkion a *sentralisoija* $C_G(a)$ on joukko $\{g \in G : ag = ga\}$.

On helppo todeta, että $C_G(a)$ on ryhmän G aliryhmä. Nyt olemme valmiita kaivamaan esiin kullanarvoisen apuvälineemme:

Lause 3.2. Alkion a konjugaattien lukumäärä äärellisessä ryhmässä G on $|G|/|C_G(a)|$.

Todistus. (ks. [3], s.44) Merkitään lukemisen helpottamiseksi $C_G(a) = C$. Merkitään lisäksi aliryhmän C vasempien sivuluokkien joukkoa $\{gC : g \in G\} = G/C$. Joukko G/C ei nyt ole tekijäryhmä, koska aliryhmän C normaalisuudesta ei ole tietoa.

Määritellään kuvaus $f : a^G \to G/C$ siten, että $f(a^g) = gC$. Osoitetaan ensin, että kuvaus on hyvin määritelty, eli jos $a^g = a^h$ niin $gC = hC$: olkoon $a^g = a^h$. Nyt siis

$$\begin{aligned} & g^{-1}ag = h^{-1}ah \\ \Leftrightarrow\ & g^{-1}agh^{-1} = h^{-1}a \\ \Leftrightarrow\ & a(gh^{-1}) = (gh^{-1})a \\ \Leftrightarrow\ & gh^{-1} \in C, \end{aligned}$$

eli lauseen 1.8 perusteella $hC = gC$. Siis kuvaus f on hyvin määritelty. Koska äskeiset yhtälöt ovat keskenään yhtäpitäviä, nähdään samalla kertaa kuvauksen olevan injektio. Mielivaltaisille lähtöjoukon alkioille a^g ja a^h nimittäin on $gC = hC$ eli $f(a^g) = f(a^h)$ jos ja vain jos $a^g = a^h$.

On selvää, että kuvaus on surjektio, sillä mielivaltainen maalijoukon alkio gC on alkion a^g kuva: $f(a^g) = gC$.

Koska kuvaus on injektio ja surjektio, se on bijektio, joten äärelliset lähtö- ja maalijoukot ovat samaa kertalukua. Siis $|a^G| = [G : C] = |G|/|C|$. □

Tätä lausetta käytettäessä tulee tehtäväksi sentralisoijan kertaluvun selvittäminen. Tämä on huomattavasti helpompi tehtävä kuin konjugointiluokan kertaluvun löytäminen ilman tätä lausetta. Samaan tapaan kuin metallinpaljastimen kanssa käveleminen on helpompaa kuin sattumanvarainen hiekan kaiveleminen.

3.2 Ryhmän $PSL(2,5)$ yksinkertaisuuden osoittaminen

Tässä luvussa osoitetaan, että ryhmä $PSL(2,5)$ on yksinkertainen. Juoni kulkee seuraavasti: on osoitettava, että ryhmällä $PSL(2,5)$ on ainoastaan triviaalit normaalit aliryhmät, jotka ovat $Z(SL(2,5))$ ja se itse eli $PSL(2,5)$. Apulauseessa 3.1 osoitettiin, että tekijäryhmän $PSL(2,5) = SL(2,5)/Z(SL(2,5))$ normaaleista aliryhmistä saadaan tietoa tutkimalla ryhmän $SL(2,5)$ normaaleja aliryhmiä.

Normaalien aliryhmien tiedetään olevan konjugointiluokkien yhdisteitä, minkä vuoksi aiomme lauseen 3.2 avulla selvittää kaikki ryhmän $SL(2,5)$ konjugointiluokat: jokaisen konjugointiluokan kertaluku tulee olemaan tiedossa samoin kuin se, mitä kertalukua ovat konjugointiluokan alkiot. Konjugointiluokkia etsittäessä suurin osa työstä on itseasiassa sentralisoijan kertaluvun selvittämistä. Sentralisoijaan päästään käsiksi avaamalla sen määritelmä kussakin tapauksessa. Valitaan siis matriisi, jonka määräämää konjugointiluokkaa halutaan tutkia, ja selvitetään, millaiset matriisit kuuluvat sen sentralisoijaan eli kommutoivat sen kanssa.

Kaikkien konjugointiluokkien tiedetään löytyneen, kun niiden alkioiden yhteenlaskettu lukumäärä on ryhmän $SL(2,5)$ kertaluku. Tässä vaiheessa tunnetaan konjugointiluokkien kertaluvut sekä konjugointiluokkiin kuuluvien alkioiden kertaluvut. Näiden avulla osoitetaan, ettei konjugointiluokkien yhdisteenä saada ryhmälle $SL(2,5)$ ei-triviaaleja normaaleja aliryhmiä. Tämä päättää lauseen todistuksen.

Suunnitelma on selvä, olemme valmiina töihin!

Lause 3.3. Ryhmä $PSL(2,5)$ on yksinkertainen.

Todistus. Tässä tehty todistus seurailee J. F. Humphreysin kirjan A Course in Group Theory todistusta (ks. [1] s.205-207). Kirjassa pois jätetyt välivaiheet on tässä avattu perusteellisesti.

Koska kunnan K kertaluku on alkuluku, tiedetään lauseen 1.29 perusteella, kuinka kunnan K alkioilla $\{\mathbf{0}, \mathbf{1}, 2, 3, 4\}$ lasketaan. Lukemisen helpottamiseksi merkitään $SL(2,5) = G$, jolloin $PSL(2,5) = G/Z(G)$. Mielessä kannattaa pitää, että viiden alkion kunnassan $4 = -\mathbf{1}$ ja millä tahansa kunnan alkiolla k on $4k = -k$.

Ryhmä $G/Z(G)$ on yksinkertainen, jos sillä on vain triviaalit normaalit aliryhmät $Z(G)$ ja $G/Z(G)$. Lauseen 3.1 mukaan $N/Z(G) \trianglelefteq G/Z(G)$ jos ja vain jos $N \trianglelefteq G$ ja $Z(G) \subseteq N$. Ryhmän $G/Z(G)$ yksinkertaisuus voidaan siis todistaa osoittamalla, että ryhmän G ainoat joukon $Z(G)$ sisältävät normaalit aliryhmät ovat $Z(G)$ ja G, sillä tällöin lauseen 3.1 mukaan ryhmän $G/Z(G)$ ainoat normaalit aliryhmät ovat $Z(G)/Z(G) = \{Z(G)\} = \{e_{\{PSL(2,5)\}}\}$ ja $G/Z(G) = PSL(2,5)$. Tämän tavoitteen saavuttamiseksi selvitetään ryhmän G konjugointiluokat.

Lauseen 2.2 nojalla ryhmän $SL(2,5)$ kertaluku on $6 \cdot 5 \cdot 4 = 120$. Kun on löydetty niin monta toisistaan eroavaa konjugointiluokkaa, että niissä on alkioita yhteensä 120 kappaletta, tiedetään siis kaikkien konjugointiluokkien löytyneen.

Yksinkertaisimmin selviävät konjugointiluokat $\{I\}$ ja $\{-I\}$. Nämä ovat konjugointiluokkia, koska matriisit I ja $-I$ kommutoivat kaikkien ryhmän G matriisien kanssa ja siten

$$\begin{aligned} I^G &= \{I^A : A \in G\} = \{A^{-1}IA : A \in G\} \\ &= \{A^{-1}AI : A \in G\} = \{I : A \in G\} = \{I\} \end{aligned}$$

ja samoin saadaan $(-I)^G = \{-I\}$. Merkitään näitä konjugointiluokkia $K_1 = \{I\}$ ja $K_2 = \{-I\}$.

Konjugointiluokka $K_3 = T^G = \begin{pmatrix} \mathbf{0} & 4 \\ \mathbf{1} & \mathbf{0} \end{pmatrix}^G$

Matriisi $T = \begin{pmatrix} \mathbf{0} & 4 \\ \mathbf{1} & \mathbf{0} \end{pmatrix}$ kuuluu ryhmään G, sillä $\det T = \mathbf{0} \cdot \mathbf{0} - \mathbf{1} \cdot 4 = -4 = \mathbf{1}$. Tarkastellaan matriisin T määräämää konjugointiluokkaa. Kuten suunniteltu, aloitetaan sentralisoijan $C_G(T)$ kertaluvun selvittämisellä. Sentralisoija $C_G(T)$ on joukko $\{A \in G : AT = TA\}$, joten tutkitaan, millaiset matriisit kommutoivat matriisin T kanssa.

Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Tällöin

$$\begin{aligned} AT = TA &\Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{0} & 4 \\ \mathbf{1} & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{0} & 4 \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} b & 4a \\ d & 4c \end{pmatrix} = \begin{pmatrix} 4c & 4d \\ a & b \end{pmatrix} \\ &\Leftrightarrow \begin{cases} a = d \\ b = 4c \end{cases} \end{aligned}$$

Siis $A = \begin{pmatrix} a & 4c \\ c & a \end{pmatrix}$, missä $\det A = a^2 - 4c^2 = \mathbf{1}$ eli $a^2 + c^2 = \mathbf{1}$. Kunnan K alkioiden neliöt ovat $\mathbf{0}^2 = \mathbf{0}$, $\mathbf{1}^2 = \mathbf{1}$, $2^2 = 4$, $3^2 = 4$ ja $4^2 = \mathbf{1}$, joten yhtälön ainoat ratkaisuparit (x, y), missä $x, y \in K$, ovat $(\mathbf{0}, \mathbf{1}), (\mathbf{0}, 4), (\mathbf{1}, \mathbf{0})$ ja $(4, \mathbf{0})$. Jokainen ratkaisupari vastaa tarkalleen yhtä sentralisoijan alkiota, joten $|C_G(T)| = 4$ ja lauseen 3.2 avulla nähdään, että

$$|T^G| = |G|/|C_G(T)| = 120/4 = 30.$$

Lauseen 1.18 perusteella samassa konjugointiluokassa olevien alkioiden kertaluku on sama. Tämän ansioista tiedämme, että jos jonkin ryhmän G matriisin kertaluku on eri kuin matriisin T, sen on kuuluttava eri konjugointiluokkaan. Lasketaan matriisin T kertaluku: $T^2 = \begin{pmatrix} \mathbf{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{-1} \end{pmatrix} = -I$ eli $T^4 = (-I)^2 = I$ ja matriisin T kertaluku on siis neljä.

Konjugointiluokka $K_4 = S^G = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ 4 & 4 \end{pmatrix}^G$

Matriisi $S = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ 4 & 4 \end{pmatrix}$ kuuluu ryhmään G, sillä $\det S = \mathbf{0} \cdot 4 - \mathbf{1} \cdot 4 = -4 = \mathbf{1}$. Tarkastellaan matriisin S määräämää konjugointiluokkaa. $S^2 = \begin{pmatrix} 4 & 4 \\ \mathbf{1} & \mathbf{0} \end{pmatrix}$ ja

$S^3 = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$, joten $|S| = 3 \neq |T|$. Näin ollen S^G ja T^G eivät ole sama konjugointiluokka, joten tarkastelua kannattaa jatkaa.

Kuten edellä siirrytään tarkastelemaan sentralisoijaa $C_G(S)$. Tutkitaan siis, mitä ryhmän G matriisille $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ seuraa ehdosta $AS = SA$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ 4 & 4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$\Leftrightarrow \begin{pmatrix} -b & a-b \\ -d & c-d \end{pmatrix} = \begin{pmatrix} c & d \\ -a-c & -b-d \end{pmatrix},$$

joten matriisin A alkioiden on toteutettava yhtälöt

$$\begin{cases} -b = c \\ a - b = d \\ -d = -a - c \\ c - d = -b - d \end{cases} \Leftrightarrow \begin{cases} -b = c \\ a - b = d. \end{cases}$$

Siis matriisi A on muotoa $\begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}$, missä

$$\det A = a(a-b) - b(-b) = a^2 + b^2 - ab = \mathbf{1}.$$

Taulukkoon 3 on laskettu determinantin lausekkeen $f(a,b) = a^2 + b^2 - ab$ arvoja alkioiden a ja b eri arvoilla. Yhtälön $f(a,b) = \mathbf{1}$ ratkaisemiseksi riittävät taulukkoon lasketut arvot, koska $f(a,b) = f(b,a)$ kaikilla $a,\, b \in K$.

	$a = \mathbf{0}$	$\mathbf{1}$	2	3	4
$b = \mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	4	4	$\mathbf{1}$
$\mathbf{1}$		$\mathbf{1}$	3	2	3
2			4	2	2
3				4	3
4					$\mathbf{1}$

Taulukko 3: lausekkeen $f(a,b) = a^2 + b^2 - ab$ arvoja viiden alkion kunnassa K.

Taulukosta 3 nähdään, että yhtälön ratkaisuparit $(x,y), x, y \in K$ ovat $(\mathbf{0}, 4)$, $(\mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}), (4, \mathbf{0}), (\mathbf{1}, \mathbf{1})$ ja $(4, 4)$. Jokainen ratkaisupari vastaa yhtä

sentralisoijan alkiota, joten sentralisoijan kertaluku on kuusi ja lauseen 3.2 ansiosta tiedämme, että konjugointiluokan S^G kertaluku on

$$|S^G| = \frac{|SL(2,5)|}{|C_G(S)|} = \frac{120}{6} = 20.$$

Konjugointiluokka $K_5 = (-S)^G$

Koska $S \in G$, on $-S = -\begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix} \in G$. Tarkastellaan matriisin $-S$ määräämää konjugointiluokkaa. Matriisin S aiemman tarkastelun perusteella tiedetään, että S^n ei ole koskaan $-I$ ja $S^n = I$ tarkalleen silloin, kun luku n on matriisin S kertaluvun kolme monikerta. Lisäksi matriisin $-S$ potensseille on

$$(-S)^n = \begin{cases} S^n, \text{ n parillinen} \\ -(S^n), \text{ n pariton .} \end{cases}$$

Pienin parillinen luvun kolme monikerta on kuusi, joten $|-S| = 6$. Kertalukunsa perusteella $-S$ määrää aiemmista poikkeavan konjugointiluokan.

Matriisi A kuuluu alkion $-S$ sentralisoijaan jos ja vain jos $A(-S) = (-S)A$ eli $AS = SA$. Ehto on sama kuin alkion S sentralisoijan alkioille, joten $C_G(-S) = C_G(S)$. Siten $|C_G(-S)| = 6$ ja lauseesta 3.2 seuraa, että myös $|(-S)^G| = |S^G| = 20$.

Konjugointiluokka $K_6 = R^G = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}^G$

Matriisi $R = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ kuuluu ryhmään G, sillä $\det R = \mathbf{1} \cdot \mathbf{1} - \mathbf{1} \cdot \mathbf{0} = \mathbf{1}$. Tarkastellaan matriisin R määräämää konjugointiluokkaa. Matriisin R kertalukua voidaan etsiä laskemalla vain parillisia potensseja. Jos nimittäin kertaluku n on pariton, tulee se löydetyksi kun havaitaan, että $R^{n+1} = R$. Nyt $R^2 = \begin{pmatrix} \mathbf{1} & 2 \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$. $R^4 = \begin{pmatrix} \mathbf{1} & 4 \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ ja $R^6 = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = R$, joten $R^5 = I$ ja siten $|R| = 5$. Alkio R määrää siis aiemmista poikkeavan konjugointiluokan.

Olkoon sitten $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_G(R)$ eli $AR = RA$. Nyt

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix},$$

mistä nähdään, että

$$\begin{cases} a = d \\ c = \mathbf{0} \\ b \in K. \end{cases}$$

Matriisi A on siis muotoa $\begin{pmatrix} a & b \\ \mathbf{0} & a \end{pmatrix}$, missä $\det A = a^2 = \mathbf{1}$ eli $a = \mathbf{1}$ tai $a = -\mathbf{1} = 4$. Alkio a voi siis saada kaksi ja alkio b viisi erilaista arvoa, joten sentralisoijan matriisin A alkiot voidaan valita yhteensä $2 \cdot 5 = 10$ toisistaan eroavalla tavalla. Näin ollen $|C_G(R)| = 10$ ja lauseen 3.2 nojalla saadaan konjugointiluokan kertaluvuksi

$$|R^G| = \frac{120}{10} = 12.$$

Konjugointiluokka $K_7 = (R^2)^G$

Tarkastellaan seuraavaksi matriisin $R^2 = \begin{pmatrix} \mathbf{1} & 2 \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ määräämää konjugointiluokkaa. Matriisi R^2 kuuluu ryhmään G, koska $R \in G$. Suurin työ on osoittaa, että R^2 määrää eri konjugointiluokan kuin R. Konjugointiluokan kertaluvun selvittäminen on tämän jälkeen melko vaivatonta.

Selvästi $\langle R^2 \rangle \leq \langle R \rangle$, joten Lagrangen lauseen 1.9 perusteella $|\langle R^2 \rangle| \mid |\langle R \rangle| = 5$. Siten $|\langle R^2 \rangle| \in \{1, 5\}$ ja koska $\langle R^2 \rangle \neq \{\mathbf{1}\}$, on $|\langle R^2 \rangle| = 5$.

Matriisi R^2 voisi kertalukunsa puolesta kuulua samaan konjugointiluokkaan kuin R. Näin ei kuitenkaa ole, sillä jos R^2 olisi matriisin R konjugaatti, olisi olemassa matriisi $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, K)$, jolla $A^{-1}RA = R^2$ eli

$RA = AR^2$. Tämä tarkoittaa, että

$$\begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{1} & 2 \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & 2a+b \\ c & 2c+d \end{pmatrix},$$

mistä nähdään, että

$$\begin{cases} b \in K \\ c = \mathbf{0} \\ d = 2a. \end{cases}$$

Matriisi A on siis muotoa $\begin{pmatrix} a & b \\ \mathbf{0} & 2a \end{pmatrix}$, missä $\det A = 2a^2 = \mathbf{1}$. Aiemmin on todettu, että $a^2 \in \{\mathbf{0}, \mathbf{1}, 4\}$, eli $2a^2 \in \{\mathbf{0}, 2, 3\}$. Yhtälöllä $2a^2 = \mathbf{1}$ ei siis ole ratkaisuja kunnassa K, eli ei ole olemassa matriisia $A \in SL(2, K)$, jolla olisi $R^A = R^2$. Näin ollen R^2 kuuluu eri konjugointiluokkaan kuin R.

Olkoon nyt matriisi $B = \begin{pmatrix} q & r \\ s & t \end{pmatrix} \in C_G(R^2)$ eli $BR^2 = R^2B$. Tällöin

$$\begin{pmatrix} q & r \\ s & t \end{pmatrix} \begin{pmatrix} \mathbf{1} & 2 \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & 2 \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} q & r \\ s & t \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{pmatrix} q & 2q+r \\ s & 2s+t \end{pmatrix} = \begin{pmatrix} q+2s & r+2t \\ s & t \end{pmatrix},$$

mistä nähdään, että

$$\begin{cases} q = t \\ s = \mathbf{0} \\ r \in K. \end{cases}$$

Tämä ehto on yhtenevä matriisin R tapauksessa saadun ehdon kanssa, joten $C_G(R^2) = C_G(R)$ ja siten $|C_G(R^2)| = |C_G(R)| = 10$. Lauseen 3.2 nojalla nyt on myös

$$|(R^2)^G| = |R^G| = 12.$$

Konjugointiluokka $K_8 = (-R)^G$

Samoin kuin aiemmin matriisin $-S$ tapauksessa voidaan päätellä, että matriisin $-R$ kertaluku on $2|R| = 10$. Siten $-R$ määrää aikaisemmista poikkeavan konjugointiluokan. Edelleen samoin kuin alkion $-S$ tapauksessa ovat

alkion ja vasta-alkion sentralisoijat samat eli $C_G(-R) = C_G(R)$. Siten $|C_G(-R)| = |C_G(R)| = 10$ ja jälleen lauseen 3.2 perusteella $|(-R)^G| = |R^G| = 12$.

Konjugointiluokka $K_9 = ((-R)^2)^G$

Samoin perustein kuin edellisissä tapauksissa on matriisin $(-R)^2$ kertaluku $|(-R)^2| = 2|R^2| = 10$. Aiemmin on todettu myös, että alkion ja vasta-alkion sentralisoijat ovat samat. Näin ollen myös sentralisoijien kertaluvut ovat samat, eli lauseesta 3.2 seuraa, että

$$|\left((-R)^2\right)^G| = |(R^2)^G| = 12.$$

Nyt $|(-R)^2| = |-R|$ ja $|\left((-R)^2\right)^G| = |\left(-R\right)^G|$, joten on tarkistettava, ettei kyseessä ole sama konjugointiluokka eli $K_9 = K_8$. Jos näin olisi, löytyisi sellainen matriisi $A \in SL(2, K)$, että $A^{-1}(-R)A = -R^2$ eli $A^{-1}RA = R^2$. Tätä ehtoa tutkittiin edellä, tarkistettaessa etteivät konjugointiluokat K_6 ja K_7 ole samat, ja ehdosta havaittiin seuraavan ristiriita. Näin ollen tällaista matriisia A ei ole olemassa eli matriisit $-R$ ja $(-R)^2$ eivät kuulu samaan konjugointiluokkaan eivätkä konjugointiluokat K_9 ja K_8 siis ole samat.

Yhteenveto konjugointiluokista ja todistuksen päätös

Alla olevaan taulukkoon 4 on koottu löydetyt konjugointiluokat, niiden kertaluvut ja niissä olevien alkioiden kertaluvut. Koska konjugointiluokissa on yhteensä 120 alkiota, tiedetään kaikkien konjugointiluokkien löytyneen.

Nyt $Z(G) = \{I, -I\} = K_1 \cup K_2$. Olkoon N sellainen ryhmän G normaali aliryhmä, että $Z(G) < N$. Osoitetaan, että tällöin $N = G$. Tarkastellaan erikseen kaksi tapausta sen mukaan sisältääkö N kertalukua viisi olevan alkion:

Oletetaan ensin, että aliryhmä N ei sisällä kertalukua viisi olevaa alkiota. Tällöin se ei sisällä myöskään kertalukua 10 olevaa alkiota, sillä jos $B \in N$ ja $|B| = 10$, niin myös $B^2 \in N$ ja $|B^2| = 5$. Ryhmään N ei nyt sisälly yhtäkään konjugointiluokista K_6, K_7, K_8 ja K_9. Keskus $Z(G) = K_1 \cup K_2$ sisältyy aidosti aliryhmään N, minkä lisäksi jäljelle jäävät konjugointiluokat K_3, K_4 ja K_5. Näiden kertalukuja tarkastelemalla nähdään helposti, ettei niiden yhdisteenä saada joukkoa, jonka kertaluku jakaisi ryhmän G kertaluvun. Näin ollen N ei voi olla ryhmän G aliryhmä, mikä on ristiriita.

Oletetaan siis, että aliryhmä N sisältää kertalukua viisi olevan alkion M. Nyt $M \in R^G$ tai $M \in (R^2)^G$.

K_i	$\lvert K_i \rvert$	alkioiden kertaluku
$K_1 = I^G$	1	1
$K_2 = (-I)^G$	1	2
$K_3 = T^G$	30	4
$K_4 = S^G$	20	3
$K_5 = (-S)^G$	20	6
$K_6 = R^G$	12	5
$K_7 = (R^2)^G$	12	5
$K_8 = (-R)^G$	12	10
$K_9 = ((-R)^2)^G$	12	10
Yhteensä	120	

Taulukko 4: Yhteenveto ryhmän $SL(2,5)$ konjugointiluokista.

Lauseen 1.11 perusteella kaikki normaaliin aliryhmään kuuluvan matriisin konjugaatit kuuluvat kyseiseen normaaliin aliryhmään. Jos $M \in R^G$, niin matriisi R on matriisin M konjugaatti ja näin ollen $R \in N$. Koska $-I \in Z(G) \subset N$, seuraa ryhmän ominaisuuksista, että myös matriisit R^2, $-R$ ja $-(R^2)$ sekä niiden määräämät konjugointiluokat K_6, K_7, K_8 ja K_9 kuuluvat aliryhmään N.

Jos taas $M \in (R^2)^G$, niin R^2 on matriisin M konjugaatti ja kuuluu siten aliryhmään N. Tästä seuraa, että $(R^2)^3 = R^6 = R \in N$ eli jälleen konjugointiluokat K_6, K_7, K_8 ja K_9 kuuluvat aliryhmään N.

Nyt tiedetään, että ryhmän G keskuksen $K_1 \cup K_2$ lisäksi ainakin konjugointiluokat K_6, K_7, K_8 ja K_9 sisältyvät aliryhmään N. Siten $|N| \geq 50$. Koska loppujen ryhmän G konjugointiluokkien kertaluku on suurempi kuin kymmenen, on $|N| \neq 60$. Siten $|N|$ voi jakaa kertaluvun $|G| = 120$ vain jos $|N| = |G|$ eli $N = G$.

Näin on osoitettu, että ryhmän $G = SL(2,5)$ ainoat normaalit aliryhmät, joihin $Z(G)$ sisältyy, ovat $\{I, -I\} = Z(G)$ ja G itse. Näin ollen apulauseen 3.1 perusteella ryhmän $PSL(2,5)$ ainoat normaalit aliryhmät ovat $\{Z(G)\}$ ja $PSL(2,5)$. Siten ryhmä $PSL(2,5)$ on yksinkertainen. □

4 Ryhmän $PSL(2,4)$ yksinkertaisuus

Tässä luvussa osoitetaan konjugointiluokkien avulla ryhmän $PSL(2,4)$ yksinkertaisuus. Ennen varsinaista osoitusta tarkastellaan hieman neljän alkion kuntia ja osoitetaan, että ne ovat keskenään isomorfisia.

4.1 Kertalukua neljä oleva kunta

Neljän alkion kunnasta tekee mielenkiintoisen se, että kunnan kertaluku ei ole alkuluku. Siksi neljän alkion kunnassa laskeminen eroaa viiden alkion kunnasta olennaisesti, nyt nimittäin karakteristika ei ole sama kuin kunnan kertaluku.

Sudokuja täyttänyt lukija huomaa nopeasti, että ryhmän alkioiden välisistä operaatioista laaditut taulukot voidaan täyttää hieman sudokun tavoin. Se, että tämä näppärä tapa toimii, on seurausta lauseesta 1.2. Mielenkiinnosta asiaa kohtaan tarkastelemme tässä kuitenkin myös muita tapoja summien ja tulojen selvittämiseen.

Lauseesta 1.27 seuraa, että kertalukua neljä olevan kunnan karakteristika on kaksi. Jos merkitsemme kuntamme alkioita aluksi $K = \{\mathbf{0}, \mathbf{1}, a, b\}$, näemme karakteristikan avulla, että $\mathbf{1} + \mathbf{1} = a + a = b + b = \mathbf{0}$. Tämän vuoksi alkion lisääminen ja vähentäminen (eli vasta-alkion lisääminen) ovat neljän alkion kunnassa sama asia. Tämän tiedon ja neutraalialkioiden avulla voidaan kunnan alkioiden välisten operaatioiden taulukoita täyttää melko pitkälle (ks. taulukko 5).

$+$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$		
a	a		$\mathbf{0}$	
b	b			$\mathbf{0}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	a	b
a	$\mathbf{0}$	a		
b	$\mathbf{0}$	b		

Taulukko 5: Kertalukua neljä olevan kunnan alkioiden välisiä summia ja tuloja.

Entä summat $a+\mathbf{1}$ ja $b+\mathbf{1}$? Jos $a+\mathbf{1} = \mathbf{0}$, niin lisäämällä yhtälön molemmille puolille alkio a saadaan $a+a+\mathbf{1} = a$ ja kun muistetaan, että $a+a = \mathbf{0}$, päädytään yhtälöön $\mathbf{1} = a$, mikä on ristiriita. Jos taas $a + \mathbf{1} = \mathbf{1}$, saadaan ristiriita $a = \mathbf{0}$ lisäämällä ykkösalkio yhtälön molemmille puolille. Kun niin

ikään yhtälöstä $a + \mathbf{1} = a$ seuraa ristiriita $\mathbf{1} = \mathbf{0}$, on poissulkumenetelmällä osoitettu, että $a + \mathbf{1} = b$. Samalla tavalla voidaan osoittaa, että $b + \mathbf{1} = a$.

Summista ainoastaan $a + b$ on selvittämättä. Summa $a + b = \mathbf{1}$, mikä voidaan todeta monella eri tavalla. Samaan tapaan kuin edellä voidaan osoittaa kaikkien muiden vaihtoehtojen johtavan ristiriitaan. Voidaan myös tarkastella sivuluokkaa $a + K$ ja päätellä alkion $a + b$ arvo siitä, että $a + K = K$. Tai voidaan täyttää alkioiden summien taulukko saman kaltaisesti kuin sudoku eli siten, että kunnan kaikki alkiot esiintyvät joka rivillä ja joka sarakkeessa tarkalleen kerran.

Viimeisimpänä kuvaillulla "sudokutekniikalla"voidaan selvittää alkioiden a^2, b^2 ja $ab = ba$ arvot. Tarkasteltaessa alkion ab mahdollisia arvoja nähdään nimittäin taulukosta, että $ab \notin \{\mathbf{0}, a, b\}$ eli $ab = ba = \mathbf{1}$. Tämän tiedon avulla ryhmätaulut saadaan täytettyä loppuun kuten taulukossa 6.

$+$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$	b	a
a	a	b	$\mathbf{0}$	$\mathbf{1}$
b	b	a	$\mathbf{1}$	$\mathbf{0}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	a	b
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	a	b
a	$\mathbf{0}$	a	b	$\mathbf{1}$
b	$\mathbf{0}$	b	$\mathbf{1}$	a

Taulukko 6: Loputkin kertalukua neljä olevan kunnan alkioiden väliset summat ja tulot.

Nyt on huomattu, että $a + \mathbf{1} = a^2 = b$. Tämän tiedon valossa sovitaan jatkossa merkittävän kunnan alkioita $K = \{\mathbf{0}, \mathbf{1}, \omega, \omega^2\}$. Näillä merkinnöillä alkioiden välisistä operaatioista saadaan taulukko 7.

$+$	$\mathbf{0}$	$\mathbf{1}$	ω	ω^2
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	ω	ω^2
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$	ω^2	ω
ω	ω	ω^2	$\mathbf{0}$	$\mathbf{1}$
ω^2	ω^2	ω	$\mathbf{1}$	$\mathbf{0}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	ω	ω^2
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	ω	ω^2
ω	$\mathbf{0}$	ω	ω^2	$\mathbf{1}$
ω^2	$\mathbf{0}$	ω^2	$\mathbf{1}$	ω

Taulukko 7: Kunnan $K = \{\mathbf{0}, \mathbf{1}, \omega, \omega^2\}$ alkioiden väliset operaatiot.

Huomionarvoista on se, että alkioiden väliset laskutoimitukset on selvitetty ainoastaan kunnan kertaluvun avulla. Tästä seuraa, että kertalukua neljä

olevat kunnat ovat keskenään rakenneyhtäläisiä eli alkioiden nimeämistä vaille samoja. Jatkossa tullaan kertalukua neljä olevat kunnat samaistamaan ja puhutaan ainoastaan yhdestä kunnasta, jonka alkiot ovat $\mathbf{0}, \mathbf{1}, \omega$ ja ω^2.

Kunnan kertaluvun ollessa alkuluku tiedetään, että sen alkioilla laskeminen toimii samoin kuin jäännösluokilla. Neljän alkion kunnassa tilanne on aivan toinen. Kappaleessa 1.1.1 tarkasteltiin jäännösluokkien joukon $\mathbb{Z}_4$ alkioiden välisiä summia ja tuloja ja tehtiin näistä taulukot 1. Vertaamalla taulukoita nyt laadittuihin nähdään, että ne poikkeavat toisistaan runsaasti. Summaoperaation suhteen sekä kunta K että joukko $\mathbb{Z}_4$ ovat ryhmiä, vaikka taulukot ovatkin erilaiset. Kertolaskun suhteen $(K \setminus \{\mathbf{0}\}, \cdot)$ on jo kunnan määritelmän perusteella ryhmä, kun taas kappaleessa 1.1.1 nähtiin, että $(\mathbb{Z}_4 \setminus \{\mathbf{0}\}, *)$ ei ole.

4.2 Ryhmän $PSL(2,4)$ yksinkertaisuuden osoittaminen

Seuraavaksi osoitetaan ryhmän $PSL(2,4)$ yksinkertaisuus. Nyt on huomattava, että koska neljän alkion kunnan karakteristika on kaksi, on jokainen alkio oma vasta-alkionsa. Tämä tarkoittaa että myös $\mathbf{1} = -\mathbf{1}$ ja siten $Z(SL(2,4)) = \{I\}$. Näin ollen $PSL(2,4) = SL(2,4)/\{I\} \cong SL(2,4)$. Ryhmä $SL(2,4)$ koostuu omista alkioistaan ja ryhmä $PSL(2,4)$ näiden alkioiden muodostamista yhden alkion joukoista. Selvästi $f : PSL(2,4) \to SL(2,4)$ on isomorfismi, kun $f(\{A\}) = A$ kaikilla $\{A\} = A\{I\} \in PSL(2,4)$. Koska ryhmät ovat rakenteeltaan yhtäläiset, ne samaistetaan jatkossa.

Lause 4.1. Ryhmä $PSL(2,4)$ on yksinkertainen.

Todistus. Merkintöjen helpottamiseksi merkitsemme $SL(2,4) = G$. On osoitettava, että ryhmän G ainoat normaalit aliryhmät ovat $\{I\}$ ja G. Kuten edellisessä luvussa, tarkastellaan jälleen ryhmän G konjugointiluokkia. Jokainen normaali aliryhmä on niiden yhdiste.

Identiteettimatriisi I määrää oman konjugointiluokkansa $\{I\} = K_1$. Tarkastellaan matriisien

$$A = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}, \; B = \begin{pmatrix} \omega & \mathbf{0} \\ \mathbf{0} & \omega^2 \end{pmatrix}, \; C = \begin{pmatrix} \mathbf{1} & \omega \\ \omega & \omega \end{pmatrix} \text{ ja } C^2 = \begin{pmatrix} \omega & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix},$$

määräämiä konjugointiluokkia.

Konjugointiluokka $K_2 = A^G = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}^G$

Tutkitaan alkion $A = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}$ määräämää konjugointiluokkaa. Nyt $A^2 = I$, joten $|A| = 2$. Jotta saataisiin tietää matriisin A konjugaattien määrä ryhmässä G, tarkastellaan matriisin A sentralisoijaa $C_G(A)$. Olkoon $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_G(A)$. Tällöin $AX = XA$ eli

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{pmatrix} c & d \\ a & b \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{cases} c = b \\ a = d \end{cases}$$

Siis $X = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, missä $\det X = a^2 + b^2 = \mathbf{1}$. Merkitään $f(a,b) = a^2 + b^2$ ja havaitaan, että $f(a,b) = f(b,a)$. Taulukosta 8 nähdään, että yhtälön $a^2 + b^2 = \mathbf{1}$ ratkaisuparit $(a,b), a,b \in K$ ovat $(\mathbf{0},\mathbf{1}), (\mathbf{1},\mathbf{0}), (\omega^2,\omega)$ ja (ω,ω^2). Jokainen ratkaisupari vastaa yhtä sentralisoijan $C_G(A)$ matriisia, joten $|C_G(A)| = 4$ ja siten lauseen 3.2 perusteella $|A^G| = \frac{60}{4} = 15$.

	$a = \mathbf{0}$	$\mathbf{1}$	ω	ω^2
$b = \mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	ω^2	ω
$\mathbf{1}$		$\mathbf{0}$	ω	ω^2
ω			$\mathbf{0}$	$\mathbf{1}$
ω^2				$\mathbf{0}$

Taulukko 8: lausekkeen $f(a,b) = a^2 + b^2$ arvoja neljän alkion kunnassa K.

Konjugointiluokka $K_3 = B^G = \begin{pmatrix} \omega & \mathbf{0} \\ \mathbf{0} & \omega^2 \end{pmatrix}^G$

Selvitetään seuraavaksi, millaiseen konjugointiluokkaan kuuluu matriisi $B = \begin{pmatrix} \omega & \mathbf{0} \\ \mathbf{0} & \omega^2 \end{pmatrix}$. Koska $B^2 = \begin{pmatrix} \omega^2 & \mathbf{0} \\ \mathbf{0} & \omega \end{pmatrix}$ ja $B^3 = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$, on $|B| = 3$ ja siten B

kuuluu eri konjugointiluokkaan kuin A.

Tarkastellaan, millaiset matriisit kuuluvat sentralisoijaan $C_G(B)$. Olkoon $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_G(B)$ eli $BX = XB$. Nyt siis

$$\begin{pmatrix} \omega & \mathbf{0} \\ \mathbf{0} & \omega^2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega & \mathbf{0} \\ \mathbf{0} & \omega^2 \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{pmatrix} a\omega & b\omega \\ c\omega^2 & d\omega^2 \end{pmatrix} = \begin{pmatrix} a\omega & b\omega^2 \\ c\omega & d\omega^2 \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{cases} b\omega = b\omega^2 \\ c\omega^2 = c\omega \end{cases} \Leftrightarrow b = c = \mathbf{0}.$$

Näin ollen matriisi X on muotoa $\begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & d \end{pmatrix}$, missä $\det X = ad = \mathbf{1}$. Tämän yhtälön ratkaisuparit (a, d) nähdään suoraan taulukosta 7 ja ne ovat $(\mathbf{1}, \mathbf{1})$, (ω, ω^2) ja (ω^2, ω). Koska jokainen ratkaisupari vastaa yhtä sentralisoijan $C_G(B)$ matriisia, on $|C_G(B)| = 3$. Siten matriisilla B on lauseen 3.2 perusteella $|B^G| = |G|/|C_G(B)| = 60/3 = 20$ konjugaattia ryhmässä G.

Konjugointiluokka $K_4 = C^G = \begin{pmatrix} \mathbf{1} & \omega \\ \omega & \omega \end{pmatrix}^G$

Tarkastellaan seuraavaksi matriisin $C = \begin{pmatrix} \mathbf{1} & \omega \\ \omega & \omega \end{pmatrix}$ määräämää konjugointiluokkaa. Nyt

$$C^2 = \begin{pmatrix} \omega & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}, \; C^4 = \begin{pmatrix} \omega & \omega \\ \omega & \mathbf{1} \end{pmatrix} \text{ ja } C^6 = \begin{pmatrix} \mathbf{1} & \omega \\ \omega & \omega \end{pmatrix} = C,$$

joten $|C| = 5$. Tiedetään siis, että C määrää aiemmista poikkeavan konjugointiluokan.

Jos matriisi $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ kuuluu sentralisoijaan $C_G(C)$ eli $CX = XC$,

niin

$$\begin{pmatrix} \mathbf{1} & \omega \\ \omega & \omega \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathbf{1} & \omega \\ \omega & \omega \end{pmatrix}$$
$$\Leftrightarrow$$
$$\begin{pmatrix} a+\omega c & b+\omega d \\ a\omega+c\omega & b\omega+d\omega \end{pmatrix} = \begin{pmatrix} a+b\omega & a\omega+b\omega \\ c+d\omega & c\omega+d\omega \end{pmatrix}.$$

Matriisit ovat samat jos ja vain jos $b = c$ ja $b+d\omega = a\omega+b\omega$. Ratkaistaan yhtälöstä $b + d\omega = a\omega + b\omega$ alkio b:

$$\begin{aligned} b + d\omega &= a\omega + b\omega && \| +d\omega + b\omega \\ \Leftrightarrow b + b\omega &= a\omega + d\omega \\ \Leftrightarrow b(1+\omega) &= (a+d)\omega \\ \Leftrightarrow b\omega^2 &= (a+d)\omega && \| \cdot\omega \\ \Leftrightarrow b &= (a+d)\omega^2 \end{aligned}$$

Nyt on selvitetty, että matriisi X on muotoa $\begin{pmatrix} a & (a+d)\omega^2 \\ (a+d)\omega^2 & d \end{pmatrix}$, missä

$$\begin{aligned} \det X &= ad + ((a+d)\omega^2)^2 \\ &= ad + ((a+d)^2\omega) \\ &= ad + (a^2 + 2ad + d^2)\omega && \| \ 2ad = \mathbf{0} \\ &= ad + (a^2 + d^2)\omega = \mathbf{1} \end{aligned}$$

Lausekkeen $f(a,d) = ad+(a^2+d^2)\omega$ arvoja on kirjattu taulukkoon 9. Koska $f(a,d) = f(d,a)$, yhtälön $f(a,d) = \mathbf{1}$ ratkaisemiseksi riittävät taulukkoon lasketut arvot.

	$a = \mathbf{0}$	$\mathbf{1}$	ω	ω^2
$d = \mathbf{0}$	$\mathbf{0}$	ω	$\mathbf{1}$	ω^2
$\mathbf{1}$		$\mathbf{1}$	$\mathbf{1}$	ω
ω			ω^2	ω^2
ω^2				ω

Taulukko 9: lausekkeen $f(a,d) = ad+(a^2+d^2)\omega$ arvoja neljän alkion kunnassa K.

Taulukosta 9 nähdään, että yhtälöllä $\det X = f(a,d) = \mathbf{1}$ on viisi toisistaan eroavaa ratkaisuparia (a,d). Siten $|C_G(C)| = 5$ ja lauseen 3.2 perusteella $|C^G| = 60/5 = 12$.

Konjugointiluokka $K_5 = (C^2)^G$

Viimeisenä tutkitaan, millaisen konjugointiluokan määrää alkio $C^2 = \begin{pmatrix} \omega & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}$. Tämän konjugointiluokan tarkastelu vaatii enemmän työtä kuin aiempien. Koska $|\langle C \rangle| = 5$ ja selvästi $\langle C^2 \rangle \leq \langle C \rangle$, täytyy Lagrangen lauseen 1.9 nojalla aliryhmän $\langle C^2 \rangle$ kertaluvun jakaa luku viisi. Koska $|\langle C^2 \rangle| > 1$, on kertaluku siis viisi ja siten $\langle C^2 \rangle = \langle C \rangle$ eli $|C^2| = |C| = 5$. Alkiot C ja C^2 voisivat siis kertalukunsa puolesta kuulua samaan konjugointiluokkaan.

Osoitetaan, että $(C^2)^G \neq C^G$

Tehdään vastaoletus eli oletetaan, että $C^2 \in C^G$. Nyt on siis olemassa sellainen matriisi $S = \begin{pmatrix} q & r \\ s & t \end{pmatrix} \in G$, että $S^{-1}CS = C^2$ eli $CS = SC^2$. Kun tulot CS ja SC^2 kirjoitetaan auki, saadaan

$$\begin{pmatrix} q + \omega s & r + \omega t \\ \omega q + \omega s & \omega r + \omega t \end{pmatrix} = \begin{pmatrix} \omega q + r & q \\ \omega s + t & s \end{pmatrix}.$$

Jotta matriisit olisivat samat, on alkioiden q, r, s ja t toteutettava yhtälöt

$$\begin{cases} q + \omega s = \omega q + r \\ r + \omega t = q \\ \omega q + \omega s = \omega s + t \\ \omega r + \omega t = s \end{cases}$$

Poistamalla yhtälöiden molemmilla puolin esiintyvät termit ja sijoittamalla ensimmäiseen ja kolmanteen yhtälöön $q = r + \omega t$ ja $s = \omega r + \omega t$ saadaan yhtälöpari

$$\begin{cases} (r + \omega t) + \omega(\omega r + \omega t) = \omega(r + \omega t) + r \\ \omega(r + \omega t) = t. \end{cases}$$

Alemmasta yhtälöstä saadaan

$$\begin{aligned}
&\omega(r+\omega t) = t \\
\Leftrightarrow\ &\omega r + \omega^2 t = t && \| +\omega^2 t \\
\Leftrightarrow\ &\omega r = t + \omega^2 t \\
\Leftrightarrow\ &\omega r = (\mathbf{1} + \omega^2) t \\
\Leftrightarrow\ &\omega r = \omega t \\
\Leftrightarrow\ &r = t,
\end{aligned}$$

mikä vie tilannetta huomattavasti eteenpäin. Nyt nimittäin ylemmästä yhtälöstä saadaan runsaalla mutta helpolla sieventämisellä

$$\begin{aligned}
(r+\omega r) + \omega(\omega r + \omega r) &= \omega(r+\omega r) + r && \| \ \omega r + \omega r = \mathbf{0} \\
r + \omega r &= \omega r + \omega^2 r + r && \| \ -r - \omega r \\
\mathbf{0} &= \omega^2 r
\end{aligned}$$

Tämä yhtälö toteutuu jos ja vain jos $r = \mathbf{0}$. Tästä seuraa, että myös $t = r = \mathbf{0}$ ja aiemmin saatujen alkioiden q ja s yhtälöiden perusteella myös $q = s = \mathbf{0}$. Matriisin S kaikki alkiot ovat siis nolla ja $\det S = \mathbf{0}$, mikä on ristiriita, sillä $S \in G$. Ristiriita seurasi siitä oletuksesta, että C ja C^2 kuuluvat samaan konjugointiluokkaan, joten on osoitettu, ettei näin ole.

Määrätään konjugointiluokan $K_5 = (C^2)^G$ kertaluku

Kun nyt ollaan varmistuttu siitä, että C^2 määrää aiemmista poikkeavan konjugointiluokan, siirrytään selvittämään tämän konjugointiluokan kertalukua. Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_G(C^2)$ eli $AC^2 = C^2A$. Nyt siis

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \omega & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\Leftrightarrow$$

$$\begin{pmatrix} a\omega + b & a \\ c\omega + d & c \end{pmatrix} = \begin{pmatrix} a\omega + c & b\omega + d \\ a & b \end{pmatrix}.$$

Nämä matriisit ovat samat jos ja vain jos $b = c$ ja $a = b\omega + d$. Siten matriisi A on muotoa $\begin{pmatrix} b\omega + d & b \\ b & d \end{pmatrix}$, missä

$$\det A = (b\omega + d)d - b^2 = b^2 + d^2 + bd\omega = \mathbf{1}.$$

Lausekkeen $g(b,d) = b^2 + d^2 + bd\omega$ arvoja on laskettu taulukkoon 13. Koska $g(b,d) = g(d,b)$, riittävät taulukkoon lasketut arvot yhtälön $g(b,d) = \mathbf{1}$ ratkaisujen löytämiseen.

	$b = \mathbf{0}$	$\mathbf{1}$	ω	ω^2
$d = \mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	ω^2	ω
$\mathbf{1}$		ω	$\mathbf{1}$	ω
ω			$\mathbf{1}$	ω^2
ω^2				ω^2

Taulukko 10: lausekkeen $g(b,d) = b^2 + d^2 + bd\omega$ arvoja neljän alkion kunnassa K.

Taulukosta 13 nähdään, että yhtälön $\det A = g(b,d) = \mathbf{1}$ viisi toisistaan eroavaa ratkaisuparia kunnassa K ovat $(\mathbf{1},\mathbf{0}), (\mathbf{0},\mathbf{1}), (\omega,\mathbf{1}), (\mathbf{1},\omega)$ ja (ω,ω). Sijoittamalla nämä ratkaisuparit (b,d) matriisiin A nähdään sentralisoijan $C_G(C^2)$ sisältävän tasan viisi matriisia. Siten lauseen 3.2 perusteella $|(C^2)^G| = 60/5 = 12$.

Yhteenveto konjugointiluokista ja todistuksen päättäminen

Taulukkoon 11 on koottu löydetyt konjugointiluokat ja niiden kertaluvut. Olkoon nyt N ryhmän $SL(2,4)$ normaali aliryhmä ja $Z(SL(2,4)) = \{I\} = K_1 < N$. Normaalin aliryhmän N tiedetään olevan konjugointiluokkien yhdiste ja sen kertaluvun tiedetään jakavan ryhmän $SL(2,4)$ kertaluvun. Konjugointiluokkien kertalukuja tarkastelemalla nähdään, että aliryhmä N täyttää nämä ehdot vain jos $N = SL(2,4)$.

Näin on osoitettu, että ryhmän $SL(2,4)$ ainoat normaalit aliryhmät ovat $\{I\}$ ja $SL(2,4)$. Aluksi todettiin, että koska $Z(SL(2,4)) = \{I\}$, voidaan ryhmät $SL(2,4)$ ja $PSL(2,4)$ samaistaa. Siten on osoitettu, että ryhmä $PSL(2,4)$ on yksinkertainen.

□

K_i	$\lvert K_i \rvert$
$K_1 = I^G$	1
$K_2 = A^G$	15
$K_3 = B^G$	20
$K_4 = C^G$	12
$K_5 = (C^2)^G$	12
Yhteensä	60

Taulukko 11: Yhteenveto ryhmän $SL(2,4)$ konjugointiluokista.

5 Ryhmän $PSL(2,7)$ yksinkertaisuus

Tässä luvussa osoitetaan edellisten lukujen tapaan konjugointiluokkien avulla ryhmän $PSL(2,7)$ yksinkertaisuus. Todistuksen juoni on sama kuin tapauksissa $PSL(2,5)$ ja $PSL(2,4)$. Koska menetelmät ovat jo tuttuja ja konjugointiluokkia on aiempia tapauksia enemmän, ei välivaiheita tulla aukaisemaan yhtä tarkasti kuin edellisissä tapauksissa.

Ryhmän $SL(2,7)$ matriisien alkiot ovat nyt kunnasta, jonka kertaluku on alkuluku. Siten lauseen 1.29 perusteella kunnan alkioita voidaan merkitä $\{\mathbf{0}, \mathbf{1}, 2, 3, 4, 5, 6\}$ ja niillä laskeminen toimii tuttuun tapaan kuten jäännösluokilla $\mathbb{Z}_7$.

5.1 Huomioita ryhmän $SL(2,7)$ konjugointiluokkien määrittämisestä

Välivaiheiden tarkan kirjaamisen sijaan avataan ennen konjugointiluokkien määrittämistä hieman, kuinka työn eri vaiheissa on edetty:

Tarkasteltavien matriisien kuuluminen ryhmään $SL(2,7)$ todetaan jatkossa ilman perusteluja. Lukija voi halutessaan tarkistaa asian laskemalla matriisin determinantin ja varmistumalla siitä, että se on $\mathbf{1}$.

Matriisien kertaluvut annetaan jatkossa ilman perusteluja. Kertaluku on selvitettävissä suoraviivaisesti laskemalla matriisin potensseja kunnes saadaan ykkösmatriisi. Joidenkin vastaan tulevien matriisien kertaluku on jopa neljätoista. Jokaista potenssia ei kertaluvun selvittämiseksi ole tarpeen laskea, sillä jos on laskettu esimerkiksi kolme ensimmäistä potenssia, riittää jatkossa joka neljännen potenssin laskeminen. Mikäli nimittäin jokin väliin jääneistä potensseista on ykkösmatriisi, havaitaan tämä siitä, että laskettu potenssi on sama kuin jokin kolmesta ensimmäisestä.

Kunkin matriisin tarkastelussa on tavoitteena selvittää, montako konjugaattia sillä on ryhmässä $SL(2,7)$ eli mikä on sen konjugointiluokan kertaluku, johon kyseinen matriisi kuuluu. Lisäksi osoitetaan, että konjugointiluokka on todella uusi eikä mikään aiemmin tarkastelluista. Kertaluvun selvittämisessä siirrytään suoraan selvittämään matriisin sentralisoijan kertalukua. Jos matriisi X kuuluu matriisin A sentralisoijaan, on sentralisoijan määritelmän perusteella $XA = AX$. Tämä ehto aukaistaan kussakin tapauksessa ja koska matriisien XA ja AX alkioiden täytyy olla samat, saadaan ehdon kanssa yhtäpitävä yhtälöryhmä. Yhtälöryhmän perusteella saadaan tietoa sentralisoijan matriisin X muodosta.

Seuraavaksi otetaan kussakin tapauksessa avuksi se tieto, että $\det X = \mathbf{1}$. Muodostuu yhtälö, jonka jokainen ratkaisu vastaa yhtä sentralisoijan $C_G(A)$ matriisia. Näin selviää sentralisoijan kertaluku, josta lauseen 3.2 perusteella saadaan matriisin A konjugointiluokan kertaluku.

Mikäli aiemmin on löydetty konjugointiluokka, joka on samaa kertalukua ja jonka alkiot ovat samaa kertalukua kuin viimeisimpänä löydetyn, on mahdollista, että konjugointiluokat ovat samat. Tällaisessa tapauksessa on varmistettava, ettei näin ole. Tällöin tehdään vastaoletus, eli mikäli tarkastelussa ovat matriisien A ja B määräämät konjugointiluokat, oletetaan löytyvän sellainen matriisi $Y \in SL(2,7)$, että $Y^{-1}AY = B$. Tämä on yhtäpitävää sen kanssa, että $AY = YB$. Jälleen tarkastellaan tästä saatua yhtälöryhmää yhdessä ehdon $\det Y = \mathbf{1}$ kanssa ja toivotaan, että päädytään ristiriitaan.

Useiden konjugointiluokkien tapauksessa päädytään kahden muuttujan yhtälön $f(x,y) = \mathbf{1}$ ratkaisemiseen, missä $x, y \in K$. Muutamassa tapauksessa yhtälön ratkaisut löytyvät näppärimmin taulukoimalla lausekkeen $f(x,y)$ arvoja. Taulukot löytyvät liitteestä A. Jos $f(a,b) = f(b,a)$, on lausekkeen arvoista taulukoitu vain yhtälön ratkaisuun riittävä osa.

5.2 Ryhmän $PSL(2,7)$ yksinkertaisuuden osoittaminen

Tarinan pituuden vuoksi emme tällä kertaa muotoile ryhmän $PSL(2,7)$ yksinkertaisuuden osoittamista lauseeksi ja todistukseksi. Tämä ei olisi mielekästä senkään vuoksi, että seuraavassa luvussa todistetaan ryhmän $PSL(2,K)$ yksinkertaisuus yleisessä tapauksessa, jolloin tämän luvun tarkastelu on lopputuloksensa puolesta turhaa. Seuraavaan tarkastelun arvo ei olekaan sen lopputuloksessa vaan tavassa, jolla lopputulokseen päästään. Lukijan kannattaa suhtautua edessä olevaan tutkimusretkeen edistyneenä esimerkkinä konjugointiluokkien potentiaalista.

Jatkossa merkitään seitsemän alkion kuntaa $\{\mathbf{0}, \mathbf{1}, 2, \ldots, 6\}$ yksinkertaisesti K, lisäksi merkitsemme $SL(2,7) = G$, jolloin $PSL(2,7) = G/Z(G)$. Ellei toisin mainita, ryhmän G mielivaltaisen matriisin X alkioita merkitään

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, missä $a, b, c, d \in K$. Osoituksen aikana on hyvä pitää mielessä, että kunnassa K on $-6 = \mathbf{1}$.

Lauseen 2.2 nojalla ryhmässä G on $6 \cdot 7 \cdot 8 = 336$ alkiota. Yksinkertaisimmat konjugointiluokat ovat jälleen $K_1 = \{I\}$ ja $K_2 = \{-I\}$. Molemmat konjugointiluokat ovat kertalukua yksi, ja matriisien kertaluvut ovat $|I| = 1$ ja $|-I| = 2$.

Konjugointiluokka $K_3 = A^G = \begin{pmatrix} \mathbf{0} & 6 \\ \mathbf{1} & \mathbf{1} \end{pmatrix}^G$

Matriisi $A = \begin{pmatrix} \mathbf{0} & 6 \\ \mathbf{1} & \mathbf{1} \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on kuusi. Sentralisoijan $C_G(A)$ alkiolle X saadaan nyt ehto $AX = XA$, josta aukaisemalla

$$\begin{pmatrix} -c & -d \\ a+c & b+d \end{pmatrix} = \begin{pmatrix} b & b-a \\ d & d-c \end{pmatrix} \Leftrightarrow \begin{cases} c = -b \\ d = a - b. \end{cases}$$

Siis $X = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}$ ja $\det X = a^2 + b^2 - ab$. Taulukoimalla lausekkeen $a^2 + b^2 - ab$ arvoja (ks. liite A taulukko 13) nähdään, että ratkaisupari (a, b) kuuluu joukkoon

$$\{(0,1), (0,6), (1,1), (6,6), (1,0), (6,0)\}.$$

Siten sentralisoijaan $C_G(A)$ kuuluu kuusi toisistaan eroavaa matriisia eli $|C_G(A)| = 6$ ja $|A^G| = 336/6 = 56$.

Konjugointiluokka $K_4 = (A^2)^G$

Matriisi $A^2 = \begin{pmatrix} \mathbf{-1} & \mathbf{-1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on kolme. Sentralisoijan $C_G(A^2)$ alkiolle X seuraa ehdosta $A^2X = XA^2$, että

$$\begin{pmatrix} -a-c & -b-d \\ a & b \end{pmatrix} = \begin{pmatrix} b-a & -a \\ d-c & -c \end{pmatrix} \Leftrightarrow \begin{cases} c = -b \\ d = a - b. \end{cases}$$

Nämä ehdot ovat samat kuin sentralisoijalla $C_G(A)$, eli $C_G(A^2) = C_G(A)$. Siis $|C_G(A^2)| = 6$ ja $|(A^2)^G| = 56$.

Konjugointiluokka $K_5 = B^G = \begin{pmatrix} 2 & 6 \\ 4 & 2 \end{pmatrix}^G$

Matriisi $B = \begin{pmatrix} 2 & 6 \\ 4 & 2 \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on kahdeksan. Sentralisoijan $C_G(B)$ alkiolle X saadaan nyt ehto $BX = XB$, josta aukaisemalla

$$\begin{pmatrix} 2a-c & 2b-d \\ 4a+2c & 4b+2d \end{pmatrix} = \begin{pmatrix} 2a+4b & 6a+2b \\ 2c+4d & 6c+2d \end{pmatrix} \Leftrightarrow \begin{cases} a = d \\ c = 3b. \end{cases}$$

Siis $X = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$ ja $\det X = a^2 - 3b^2 = \mathbf{1}$. Neliöt a^2 ja b^2 kuuluvat joukkoon $\{\mathbf{0}, \mathbf{1}, 2, 4\}$, koska kunnan K neliöinä saadaan vain nämä alkiot. Siten $3b^2 \in \{\mathbf{0}, 3, 5, 6\}$, ja jotta yhtälö $a^2 - 3b^2 = \mathbf{1}$ toteutuisi, on oltava

$$(a^2, 3b^2) \in \{(\mathbf{1}, \mathbf{0}), (\mathbf{0}, 6), (4, 3)\}.$$

Tästä nähdään, että

$$(a, b) \in \{(1,0), (6,0), (0,3), (0,4), (2,1), (2,6), (5,1), (5,6)\}.$$

Sentralisoijaan $C_G(B)$ kuuluu siis kahdeksan toisistaan eroavaa matriisia ja siten $|B^G| = 336/8 = 42$.

Konjugointiuokka $K_6 = (B^2)^G$

Matriisi $B^2 = \begin{pmatrix} \mathbf{0} & 3 \\ 2 & \mathbf{0} \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on neljä. Sentralisoijan $C_G(B^2)$ matriisille X seuraa ehdosta $B^2X = XB^2$, että

$$\begin{pmatrix} 3c & 3d \\ 2a & 2b \end{pmatrix} = \begin{pmatrix} 2b & 3a \\ 2d & 3c \end{pmatrix} \Leftrightarrow \begin{cases} a = d \\ c = 3b. \end{cases}$$

Ehdot ovat samat kuin sentralisoijan $C_G(B)$ tapauksessa, eli $C_G(B^2) = C_G(B)$ ja siten $|(B^2)^G| = |B^G| = 42$.

Konjugointiluokka $K_7 = C^G = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 2 \end{pmatrix}^G$

Matriisi $C = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 2 \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on kahdeksan. Jos matriisi X kuuluu sentralisoijaan $C_G(C)$, on $CX = XC$ eli

$$\begin{pmatrix} a+c & b+d \\ a+2c & b+2d \end{pmatrix} = \begin{pmatrix} a+b & a+2b \\ c+d & c+2d \end{pmatrix} \Leftrightarrow \begin{cases} b = c \\ d = a+b. \end{cases}$$

Siis $X = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}$ ja $\det X = a^2 - b^2 + ab$. Taulukoimalla lausekkeen $a^2 - b^2 + ab$ arvot (ks. liite A taulukko 14) nähdään, että ratkaisupari (a, b) kuuluu joukkoon

$$\{(1,0),(6,0),(1,1),(6,6),(2,3),(5,1),(5,4),(2,6)\}.$$

Siten sentralisoijaan $C_G(C)$ kuuluu kahdeksan matriisia eli $|C_G(C)| = 8$ ja $|C^G| = 336/8 = 42$.

Koska $|C| = |B|$ ja $|C^G| = |B^G|$, on vielä varmistettava, ettei C^G ole sama konjugointiluokka kuin B^G. Jos näin olisi, löytyisi sellainen matriisi $Y = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in G$, että $CY = YB$ eli

$$\begin{pmatrix} e+g & f+h \\ e+2g & f+2h \end{pmatrix} = \begin{pmatrix} 2e+4f & 2f-e \\ 2g+4h & 2h-g \end{pmatrix} \Leftrightarrow \begin{cases} e+g = 2e+4f \\ f+h = 2f-e \\ e+2g = 2g+4h \\ f+2h = 2h-g. \end{cases}$$

Vähentämällä yhtälöiden molemmilla puolilla esiintyvät alkiot saadaan yhtäpitävä yhtälöryhmä

$$\begin{cases} g = e+4f \\ h = f-e \\ e = 4h \\ f = -g. \end{cases}$$

Sijoittamalla kahden viimeisen yhtälön $e = 4h$ ja $f = -g$ ensimmäisiin kahteen yhtälöön saadaan

$$\begin{cases} g = 4h - 4g \\ h = -g + 4h. \end{cases}$$

Ylemmän yhtälön perusteella $4h = 5g$ eli $h = 3g$, minkä seurauksena alimmasta yhtälöstä saadaan ristiriita $3g = 4g$. Näin ollen vastaoletus on epätosi eli konjugointiluokat C^G ja B^G eivät ole samat.

Konjugointiluokka $K_8 = D^G = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}^G$

Matriisi $D = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on seitsemän. Sentralisoijan $C_G(D)$ alkiolle X on $DX = XD$ eli

$$\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \Leftrightarrow \begin{cases} b \in K \\ c = \mathbf{0} \\ a = d. \end{cases}$$

Siis $X = \begin{pmatrix} a & b \\ \mathbf{0} & a \end{pmatrix}$ ja $\det X = a^2 = \mathbf{1}$ eli $a = \pm\mathbf{1}$. Matriisin X alkiot voidaan valita siis yhteensä 14 eri tavalla eli $|C_G(D)| = 14$ ja $|D^G| = 336/14 = 24$.

Konjugointiluokka $K_9 = (-D)^G$

Matriisi $-D = \begin{pmatrix} 6 & 6 \\ \mathbf{0} & 6 \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on neljätoista. Sentralisoijan $C_G(-D)$ alkiolle X on $(-D)X = X(-D)$ eli $DX = XD$. Ehto on täsmälleen sama kuin sentralisoijan $C_G(D)$ tapauksessa. Siten $C_G(D) = C_G(-D)$ ja $|C_G(-D)| = 14$ eli $|(-D)^G| = 24$.

Konjugointiluokka $K_{10} = E^G = \begin{pmatrix} 3 & 4 \\ 3 & 2 \end{pmatrix}^G$

Matriisi $E = \begin{pmatrix} 3 & 4 \\ 3 & 2 \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on 14. Sentralisoijan $C_G(E)$ matriisille X on $EX = XE$ eli

$$\begin{pmatrix} 3a+4c & 3b+4d \\ 3a+2c & 3b+2d \end{pmatrix} = \begin{pmatrix} 3a+3b & 4a+2b \\ 3c+3d & 4c+2d \end{pmatrix} \Leftrightarrow \begin{cases} c = -b \\ d = a+5b. \end{cases}$$

Siis $X = \begin{pmatrix} a & b \\ -b & a+5b \end{pmatrix}$ ja $\det X = a^2 + b^2 + 5ab$. Taulukoimalla lausekkeen $a^2 + b^2 + 5ab$ arvoja (ks. liite A taulukko 15) nähdään, että yhtälöllä $\det X = \mathbf{1}$ on yhteensä neljätoista ratkaisuparia (a, b), missä $a, b \in K$. Siis $|C_G(E)| = 14$ ja $|E^G| = 24$.

Nyt $|-D| = |E| = 14$ ja $|(-D)^G| = |E^G| = 24$, joten on tarkistettava, etteivät konjugointiluokat K_9 ja K_10 ole samat. Jos näin olisi, löytyisi sellainen

matriisi $Y = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in G$, että $EY = Y(-D)$ eli

$$\begin{pmatrix} -e & -e-f \\ -g & -g-h \end{pmatrix} = \begin{pmatrix} 3e+4g & 3f+4h \\ 3e+2g & 3f+2h \end{pmatrix} \Leftrightarrow \begin{cases} e = -g \\ f = 2g - h. \end{cases}$$

Matriisi Y on siis muotoa $\begin{pmatrix} -g & 2g-h//g & h \end{pmatrix}$ ja $\det Y = -gh - g(ag-h) = 5g^2$. Tämä on ristiriita, koska $g^2 \in \{\mathbf{0}, \mathbf{1}, 2, 4\}$ ja siten $5g^2 \in \{\mathbf{0}, 3, 5, 6\}$, mutta toisaalta Y kuuluu ryhmään G ja siten $\det Y = \mathbf{1}$. Näin on osoitettu, että konjugointiluokat $(-D)^G$ ja E^G eivät ole samat.

Konjugointiluokka $K_{11} = (E^2)^G$

Matriisi $E^2 = \begin{pmatrix} \mathbf{0} & 6 \\ \mathbf{1} & 2 \end{pmatrix}$ kuuluu ryhmään G ja sen kertaluku on seitsemän. Sentralisoijan $C_G(E^2)$ alkiolle X on $E^2X = XE^2$ eli

$$\begin{pmatrix} -c & -d \\ a+2c & b+2d \end{pmatrix} = \begin{pmatrix} b & 2b-a \\ d & 2d-c \end{pmatrix} \Leftrightarrow \begin{cases} c = -b \\ d = a + 5b. \end{cases}$$

Ehto on sama kuin sentralisoijan $C_G(E)$ alkioille, joten $C_G(E^2) = C_G(E)$. Näin ollen $|C_G(E^2)| = 14$ ja $|(E^2)^G| = 24$.

Koska $|E^2| = |D|$ ja $|(E^2)^G| = |D^G|$, on vielä tarkistettava, etteivät konjugointiluokat $(E^2)^G$ ja D^G ole samat. Jos näin olisi, löytyisi sellainen matriisi $Y = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in G$, että $E^2Y = YD$ eli

$$\begin{pmatrix} -g & -h \\ e+2g & f+2h \end{pmatrix} = \begin{pmatrix} e & e+f \\ g & g+h \end{pmatrix} \Leftrightarrow \begin{cases} g = -e \\ h = -e - f. \end{cases}$$

Matriisi Y on siis muotoa $\begin{pmatrix} e & f \\ -e & -e-f \end{pmatrix}$ ja $\det Y = e(-e-f) - f(-e) = -e^2$. Tämä on ristiriita, koska $-e^2 \in \{\mathbf{0}, 3, 5, 6\}$, mutta toisaalta Y kuuluu ryhmään G ja siten $\det Y = \mathbf{1}$. Näin on osoitettu, että konjugointiluokat D^G ja $(E^2)^G$ eivät ole samat.

Yhteenveto konjugointiluokista ja osoituksen päättäminen

Taulukkoon 12 on kerätty löydetyt konjugointiluokat, niiden kertaluvut sekä niiden alkioiden kertaluvut.

K_i	$\lvert K_i \rvert$	alkioiden kertaluku
$K_1 = I^G$	1	1
$K_2 = (-I)^G$	1	2
$K_3 = A^G$	56	6
$K_4 = (A^2)^G$	56	3
$K_5 = B^G$	42	8
$K_6 = (B^2)^G$	42	4
$K_7 = C^G$	42	8
$K_8 = D^G$	24	7
$K_9 = (-D)^G$	24	14
$K_{10} = E^G$	24	14
$K_{11} = (E^2)^G$	24	7
Yhteensä	336	

Taulukko 12: Yhteenveto ryhmän $SL(2,7)$ konjugointiluokista.

Olkoon nyt N ryhmän G normaali aliryhmä, johon joukko $\{I, -I\} = K_1 \cup K_2$ sisältyy. Lauseen 1.22 nojalla N on konjugointiluokkien yhdiste. Lisäksi aliryhmän N kertaluku jakaa ryhmän G kertaluvun. Tarkastelemalla löydettyjen konjugointiluokkien kertalukuja nähdään, että ryhmä N täyttää edellämainitut ehdot vain, jos $N = \{I, -I\}$ tai $N = G$. Tarkastelu on tilaavievä mutta suoraviivainen, joten sitä ei tässä aukaista. Mikäli lukija haluaa tarkistaa asian, helpottaa tarkastelua hieman tieto siitä, että mikäli konjugointiluokka K_3 kuuluu aliryhmään N, kuuluu siihen myös konjugointiluokka K_4 ja päinvastoin. Samoin aliryhmään N yhdessä kuuluvat tai ovat kuulumatta konjugointiluokkien parit K_8 ja K_9 sekä K_{10} ja K_{11}.

On osoitettu, että ryhmän $G = SL(2,7)$ ainoat joukon $Z(G)$ sisältävät normaalit aliryhmät ovat $Z(G)$ ja G. Näin ollen lauseen 3.1 perusteella ryhmän $PSL(2,7) = G/Z(G)$ ainoat normaalit aliryhmät ovat $\{Z(G)\}$ sekä $G/Z(G)$ eli $PSL(2,7)$ itse. Siten ryhmä $PSL(2,7)$ on yksinkertainen.

6 Yleinen tapaus: Ryhmän $PSL(2, K)$ yksinkertaisuus

Tässä luvussa osoitetaan, että ryhmä $PSL(2, K)$ on yksinkertainen aina kun kunnan K kertaluku on vähintään neljä. Tämän osoittamisen tärkeänä apuvälineenä toimivat transvektioiksi kutsutut matriisit.

6.1 Transvektiot

Tutustumme tässä kappaleessa transvektioiksi kutsuttuihin matriiseihin.

Määritelmä 6.1. Ryhmän $GL(2, K)$ matriisi on transvektio, mikäli se on muotoa $\begin{pmatrix} \mathbf{1} & \lambda \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ tai $\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \lambda & \mathbf{1} \end{pmatrix}$, missä $\lambda \neq \mathbf{0}$.

Huomautus. Jokaisen transvektion determinantti on $\mathbf{1}$, joten kaikki ryhmän $GL(2, K)$ transvektiot kuuluvat ryhmään $SL(2, K)$. Lisäksi jokaisen transvektion käänteismatriisi on transvektio: jos $\lambda \in K$, niin

$$\begin{pmatrix} \mathbf{1} & \lambda \\ \mathbf{0} & \mathbf{1} \end{pmatrix}^{-1} = \begin{pmatrix} \mathbf{1} & -\lambda \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$$

ja

$$\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \lambda & \mathbf{1} \end{pmatrix}^{-1} = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ -\lambda & \mathbf{1} \end{pmatrix}.$$

Kahdella seuraavalla lauseella tasoittelemme tien valmiiksi ryhmän $PSL(2, K)$ yksinkertaisuuden osoittamista varten. Ensin osoitetaan, että jokainen ryhmän $SL(2, K)$ alkio voidaan esittää transvektioiden tulona. Tämä tarkoittaa, että mikäli kaikkien transvektioiden voidaan osoittaa kuuluvan ryhmän $SL(2, K)$ aliryhmään N, on N tällöin koko ryhmä $SL(2, K)$.

Lause 6.1. Jokainen ryhmän $SL(2, K)$ matriisi voidaan esittää transvektioiden tulona.

Todistus. (ks. [8], s.22-23) Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, K)$ eli $\det A = ad - bc = \mathbf{1}$. Tarkastellaan erikseen tilanteet $c \neq \mathbf{0}$ ja $c = \mathbf{0}$.

1. Olkoon $c \neq \mathbf{0}$. Tällöin alkiolla c on käänteisalkio c^{-1} kunnassa K. Nyt matriisit

$$T_1 = \begin{pmatrix} \mathbf{1} & (\mathbf{1} - a)c^{-1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, T_2 = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ -c & \mathbf{1} \end{pmatrix} \text{ ja } T_3 = \begin{pmatrix} \mathbf{1} & (d - \mathbf{1})c^{-1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$$

kuuluvat ryhmään $SL(2,K)$. Näillä merkinnöillä on

$$\begin{aligned} T_1A &= \begin{pmatrix} \mathbf{1} & (\mathbf{1}-a)c^{-1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} a+(\mathbf{1}-a)c^{-1}c & b+(\mathbf{1}-a)c^{-1}d \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{1} & b+(\mathbf{1}-a)c^{-1}d \\ c & d \end{pmatrix}, \end{aligned}$$

missä determinantin $\det A = ad - bc = \mathbf{1}$ avulla voidaan sieventää

$$\begin{aligned} & b+(\mathbf{1}-a)c^{-1}d \\ =& bcc^{-1} + (d-ad)c^{-1} \\ =& (bc+d-ad)c^{-1} && \| -ad+bc = -\mathbf{1} \\ =& (d-\mathbf{1})c^{-1}. \end{aligned}$$

Merkitään tuloa $T_1A = \begin{pmatrix} \mathbf{1} & (d-\mathbf{1})c^{-1} \\ c & d \end{pmatrix} = C$.

Lisäksi

$$T_2C = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ -c & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{1} & (d-\mathbf{1})c^{-1} \\ c & d \end{pmatrix} = \begin{pmatrix} \mathbf{1} & (d-\mathbf{1})c^{-1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = T_3.$$

Koska $\det T_2 = \mathbf{1} \neq \mathbf{0}$, kuuluu T_2^{-1} ryhmään $SL(2,K)$ ja siten $C = T_2^{-1}T_3$. Näin saadaan $T_1A = C = T_2^{-1}T_3$ ja koska myös $\det T_1 = \mathbf{1} \neq \mathbf{0}$, kuuluu T_1^{-1} ryhmään $SL(2,K)$ ja siten $A = T_1^{-1}T_2^{-1}T_3$.

Koska $c \neq \mathbf{0}$, on T_2 transvektio. Matriisi T_1 on transvektio, ellei ole $a = \mathbf{1}$. Tilanne $a = \mathbf{1}$ ei kuitenkaan aiheuta ongelmia, sillä tällöin $T_1 = T_1^{-1} = I$ ja se voidaan jättää merkitsemättä tuloon. Samoin on matriisin T_3 kanssa, mikäli $d = \mathbf{1}$. Koska transvektion käänteismatriisi on transvektio, on $A = T_1^{-1}T_2^{-1}T_3$ onnistuttu esittämään transvektioiden tulona.

2. Olkoon sitten $c = \mathbf{0}$ eli $A = \begin{pmatrix} a & b \\ \mathbf{0} & d \end{pmatrix}$. Nyt transvektio $T_4 = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{pmatrix}$ kuuluu ryhmään $SL(2,K)$ ja

$$T_4A = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{pmatrix} \begin{pmatrix} a & b \\ \mathbf{0} & d \end{pmatrix} = \begin{pmatrix} a & b \\ a & b+d \end{pmatrix},$$

missä $a \neq \mathbf{0}$ sillä $\det A = ad = \mathbf{1} \neq \mathbf{0}$. Nyt kohdan 1. nojalla $T_4 A = B$ on transvektioiden tulo, joten myös $A = T_4^{-1} B$ on transvektioiden tulo.

□

Seuraavaksi edetään osoittamaan, että mikäli ryhmän $SL(2, K)$ normaali aliryhmä N sisältää yhdenkin transvektion $U = \begin{pmatrix} \mathbf{1} & u \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$, se sisältää kaikki transvektiot. Tämä yhdessä edellisen lauseen 6.1 kanssa antaa mahdollisuuden käydä tehokkaasti käsiksi ryhmän normaaliuden osoittamiseen. Riittää nimittäin osoittaa, että normaali aliryhmä N sisältää yhden transvektion, jolloin lauseista 6.1 ja 6.3 seuraa, että $N = SL(2, K)$. Ennen varsinaisen lauseen osoittamista tarvitaan yksi aputulos.

Apulause 6.2. Olkoon K äärellinen kunta ja $a \in K$. Nyt yhtälöllä $x^2 - y^2 = a$ on ainakin yksi ratkaisupari (x, y), missä $x, y \in K$.

Todistus. (ks. [9]) Tarkastellaan erikseen tapaukset $charK = 2$ ja $charK \neq 2$.

1. Olkoon ensin $charK = 2$. Tällöin lauseen 1.27 nojalla $|K| = 2^n$ jollakin $n \in \mathbb{Z}^+$ eli $|K \setminus \{\mathbf{0}\}| = 2^n - 1$. Jos $a \in K \setminus \{\mathbf{0}\}$, niin seurauksen 1.10 perusteella $a^{|K \setminus \{\mathbf{0}\}|} = a^{2^n - 1} = \mathbf{1}$ eli $a^{2^n} = (a^{2^{n-1}})^2 = a$. Näin ollen $(a^{2^{n-1}}, \mathbf{0})$ on yhtälön $x^2 - y^2 = a$ ratkaisupari.

2. Olkoon sitten $charK \neq 2$. Nyt $x^2 - y^2 = (x+y)(x-y) = a = a\mathbf{1}$. Osoitetaan, että kunnassa K on sellaiset alkiot x ja y, että $\begin{cases} x + y = a \\ x - y = \mathbf{1}. \end{cases}$ Tällöin (x, y) on yhtälön ratkaisupari. Lisäämällä alempi yhtälö ylempään saadaan yhtäpitävä yhtälöpari $\begin{cases} 2x = a + \mathbf{1} \\ x - y = \mathbf{1}. \end{cases}$ Tästä yhtälöparista voidaan ratkaista muuttujat x ja y. Ylempää yhtälöä on ensin kuitenkin muokattava, koska luonnollisella luvulla kaksi jakaminen ei sisälly käytössämme oleviin työvälineisiin. Tilanne selviää avaamalla

$$2x = x + x = \mathbf{1}x + \mathbf{1}x = (\mathbf{1} + \mathbf{1})x,$$

jonka avulla merkitsemällä kunnan K alkiota $\mathbf{1}+\mathbf{1} = \mathbf{2}$ saadaan yhtälöt muotoon $\begin{cases} \mathbf{2}x = a + \mathbf{1} \\ x - y = \mathbf{1}. \end{cases}$ Koska nyt $\mathbf{2}^{-1} \in K$, tästä voidaan ratkaista

$$\begin{cases} x = \mathbf{2}^{-1}(a + \mathbf{1}) \\ y = x - \mathbf{1} \end{cases}$$

eli

$$\begin{cases} x = \mathbf{2}^{-1}(a + \mathbf{1}) \\ y = \mathbf{2}^{-1}(a + \mathbf{1}) - \mathbf{1}. \end{cases}$$

Tämä on yhtälön $x^2 - y^2 = a$ ratkaisupari. Ratkaisupari voidaan vielä sieventää muotoon

$$\begin{cases} x = \mathbf{2}^{-1}(a + \mathbf{1}) \\ y = \mathbf{2}^{-1}(a - \mathbf{1}). \end{cases}$$

□

Lause 6.3. Olkoon $N \trianglelefteq SL(2, K)$. Jos N sisältää ainakin yhden transvektion $U = \begin{pmatrix} \mathbf{1} & u \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$, niin $N = SL(2, K)$.

Todistus. (ks. [9]) Olkoon $N \trianglelefteq SL(2, K)$ ja transvektio $U = \begin{pmatrix} \mathbf{1} & u \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \in N$. Millä tahansa kunnan K alkiolla $y \neq \mathbf{0}$ kuuluu matriisi

$$B = \begin{pmatrix} y^{-1} & \mathbf{0} \\ \mathbf{0} & y \end{pmatrix}$$

ryhmään $SL(2, K)$. Koska aliryhmä N on normaali, niin lauseen 1.11 perusteella tulo $B^{-1}UB$ kuuluu aliryhmään N. Nyt

$$\begin{aligned} B^{-1}UB &= \begin{pmatrix} y & \mathbf{0} \\ \mathbf{0} & y^{-1} \end{pmatrix} \begin{pmatrix} \mathbf{1} & u \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} y^{-1} & \mathbf{0} \\ \mathbf{0} & y \end{pmatrix} \\ &= \begin{pmatrix} y & yu \\ \mathbf{0} & y^{-1} \end{pmatrix} \begin{pmatrix} y^{-1} & \mathbf{0} \\ \mathbf{0} & y \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{1} & y^2u \\ \mathbf{0} & \mathbf{1} \end{pmatrix}. \end{aligned}$$

Jos z on toinen mielivaltainen nollasta poikkeava alkio kunnasta K, niin äskeisen perusteella $\begin{pmatrix} \mathbf{1} & z^2u \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \in N$. Nyt aliryhmään N kuuluu siis myös tulo

$$\begin{aligned} \begin{pmatrix} \mathbf{1} & y^2u \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{1} & z^2u \\ \mathbf{0} & \mathbf{1} \end{pmatrix}^{-1} &= \begin{pmatrix} \mathbf{1} & y^2u \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{1} & -z^2u \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \\ = \begin{pmatrix} \mathbf{1} & -z^2u + y^2u \\ \mathbf{0} & \mathbf{1} \end{pmatrix} &= \begin{pmatrix} \mathbf{1} & (y^2 - z^2)u \\ \mathbf{0} & \mathbf{1} \end{pmatrix}. \end{aligned}$$

Osoitetaan, että alkioiden y ja z sopivilla valinnoilla saadaan lausekkeen $u(y^2 - z^2)$ arvoiksi kaikki kunnan K alkiot: olkoon alkio $c \in K$ mielivaltainen. Nyt $u^{-1}c \in K$ ja apulauseen 6.2 perusteella yhtälöllä $y^2 - z^2 = u^{-1}c$ on ainakin yksi ratkaisupari (y, z) kunnassa K. Näillä alkioiden y ja z arvoilla on $c = u(y^2 - z^2)$, eli transvektio $\begin{pmatrix} \mathbf{1} & c \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & (y^2 - z^2)u \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ kuuluu normaaliin aliryhmään N. Alkio $c \in K$ oli mielivaltainen, joten on osoitettu kaikkien muotoa $\begin{pmatrix} \mathbf{1} & u \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, u \in K \setminus \{\mathbf{0}\}$ olevien transvektioiden kuuluvan aliryhmään N.

Koska aliryhmä N on normaali, kuuluu lauseen 1.11 perusteella myös matriisi

$$\begin{aligned} &\begin{pmatrix} \mathbf{0} & \mathbf{-1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}^{-1} \begin{pmatrix} \mathbf{1} & c \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{-1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \\ =& \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{-1} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{1} & c \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{-1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \\ =& \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{-1} & -c \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{-1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \\ =& \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ -c & \mathbf{1} \end{pmatrix} \end{aligned}$$

aliryhmään N. Siten on osoitettu, että N sisältää kaikki transvektiot. Näin ollen lauseen 6.1 nojalla $N = SL(2, K)$. □

6.2 Ryhmän $PSL(2, K)$ yksinkertaisuuden osoittaminen

Nyt aiomme osoittaa, että kun kunnan K kertaluku on suurempi tai yhtäsuuri kuin neljä, ryhmä $PSL(2, K)$ on yksinkertainen.

Lause 6.4. Kun kunnan K kertaluku $|K| \geq 4$, ryhmä $PSL(2, K)$ on yksinkertainen.

Todistus. (ks. [2], s.75-76)

$PSL(2, K)$ on tekijäryhmä $SL(2, K)/Z(SL(2, K))$. Lauseen 3.1 perusteella ryhmän $PSL(2, K)$ yksinkertaisuus voidaan osoittaa näyttämällä, että ryhmän $SL(2, K) = G$ ainoat keskuksen $Z(G)$ sisältävät normaalit aliryhmät ovat G ja $Z(G)$.

Tiedetään, että $Z(G)$ on ryhmän G normaali aliryhmä. Olkoon nyt $Z(G) < N \trianglelefteq G$. Osoitetaan, että tällöin N sisältää ainakin yhden transvektion.

Koska $Z(G) = \{I, -I\} < N$, sisältää aliryhmä N matriisin $A \neq \pm I$. Merkitään

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

ja tarkastellaan erikseen tapaukset $c = \mathbf{0}$ ja $c \neq \mathbf{0}$:

1. Olkoon ensin $c = \mathbf{0}$ eli $A = \begin{pmatrix} x & y \\ \mathbf{0} & x^{-1} \end{pmatrix}$, missä $\mathbf{0} \neq x \in K$. Jos $x = \pm\mathbf{1}$, niin $y \neq \mathbf{0}$, sillä $A \neq \pm I$. Tällöin siis joko A tai $-A$ on ryhmään N kuuluva transvektio, mikä juuri piti osoittaa. Oletetaan sitten, että $x \neq \pm\mathbf{1}$. Tällöin $x^2 \neq \mathbf{1}$, sillä

$$\begin{aligned} & x^2 = \mathbf{1} \\ \Leftrightarrow\ & x^2 - \mathbf{1} = \mathbf{0} \\ \Leftrightarrow\ & (x + \mathbf{1})(x - \mathbf{1}) = \mathbf{0} \\ \Leftrightarrow\ & x = \pm\mathbf{1}. \end{aligned}$$

   Nyt matriisi $\begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \in SL(2, K)$, joten lauseen 1.11 perusteella tulo

$$\underbrace{A \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}^{-1} A^{-1} \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}}_{\in N}$$

   kuuluu ryhmään N. Avataan tulo:

$$\begin{aligned} & A \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}^{-1} A^{-1} \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \\ &= \begin{pmatrix} x & y \\ \mathbf{0} & x^{-1} \end{pmatrix} \begin{pmatrix} \mathbf{1} & -\mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} x^{-1} & -y \\ \mathbf{0} & x \end{pmatrix} \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \\ &= \begin{pmatrix} x & y - x \\ \mathbf{0} & x^{-1} \end{pmatrix} \begin{pmatrix} x^{-1} & x^{-1} - y \\ \mathbf{0} & x \end{pmatrix} = \begin{pmatrix} \mathbf{1} & x(x^{-1} - y) + x(y - x) \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{1} & (\mathbf{1} - xy) + (xy - x^2) \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{1} - x^2 \\ \mathbf{0} & \mathbf{1} \end{pmatrix}. \end{aligned}$$

   Koska $x \neq \mathbf{1}$, nähdään nyt, että tämä tulo on transvektio. On siis osoitettu, että kun $c = \mathbf{0}$, aliryhmä N sisältää transvektion.

2. Olkoon sitten $c \neq \mathbf{0}$. Tarkastellaan seuraavaksi matriisia B, jota käytään apuna aliryhmän N transvektion löytämisessä: Jos $f \in K^*$, niin sopivalla alkion $g \in K$ valinnalla

$$B = \begin{pmatrix} af & g \\ cf & -af \end{pmatrix}$$

kuuluu ryhmään $SL(2, K)$. Tässä alkio g määräytyy ehdosta $\det B = \mathbf{1}$, eli

$$\begin{aligned} -a^2f^2 - cfg &= \mathbf{1} \\ \Leftrightarrow -cfg &= \mathbf{1} + a^2f^2 \qquad \| \; cf \neq \mathbf{0} \Rightarrow (cf)^{-1} \in K \\ \Leftrightarrow g &= -(cf)^{-1}(\mathbf{1} + a^2f^2) \in K. \end{aligned}$$

Huomataan ensin, että

$$\begin{aligned} B(-B) &= \begin{pmatrix} af & g \\ cf & -af \end{pmatrix} \begin{pmatrix} -af & -g \\ -cf & af \end{pmatrix} \\ &= \begin{pmatrix} -a^2f^2 - cfg & \mathbf{0} \\ \mathbf{0} & -cfg - a^2f^2 \end{pmatrix}, \end{aligned}$$

missä $-a^2f^2 - cfg = \det B = \mathbf{1}$ eli $B(-B) = I$ ja siten $B^{-1} = -B$.

Nyt matriisit $-I$, $B^{-1}AB$ ja A kuuluvat normaaliin aliryhmään N, joten myös niiden tulo

$$-IB^{-1}ABA = -I(-B)ABA = BABA = (BA)^2$$

kuuluu aliryhmään N. Avataan tämä tulo:

$$\begin{aligned} (BA)^2 &= \left[\begin{pmatrix} af & g \\ cf & -af \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right]^2 \\ &= \begin{pmatrix} a^2f + cg & baf + dg \\ acf - caf & bcf - daf \end{pmatrix}^2 \\ &= \begin{pmatrix} (-\det B)f^{-1} & baf + dg \\ \mathbf{0} & -(\det A)f \end{pmatrix}^2 \\ &= \begin{pmatrix} -f^{-1} & baf + dg \\ \mathbf{0} & -f \end{pmatrix}^2 \\ &= \begin{pmatrix} f^{-2} & z \\ \mathbf{0} & f^2 \end{pmatrix}. \end{aligned}$$

Oikeaan yläkulmaan syntyvää alkiota on merkitty z. Tätä alkiota ei ole tarpeen kirjoittaa auki, sillä seuraavassa tarkastelussa sen huomataan sieventyvän pois. Merkitään äsken avattua tuloa $(BA)^2 = E$ ja lasketaan vielä auki tulo $E^{-1}\underbrace{\begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix}^{-1} E \begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix}}_{\in N}$. Myös tämä tulo kuuluu normaaliin aliryhmään N.

$$
\begin{aligned}
& E^{-1}\begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix}^{-1} E \begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix} \\
&= \begin{pmatrix}f^{-2} & z\\ \mathbf{0} & f^2\end{pmatrix}^{-1}\begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix}^{-1}\begin{pmatrix}f^{-2} & z\\ \mathbf{0} & f^2\end{pmatrix}\begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix} \\
&= \begin{pmatrix}f^{2} & -z\\ \mathbf{0} & f^{-2}\end{pmatrix}\begin{pmatrix}\mathbf{1} & -\mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix}\begin{pmatrix}f^{-2} & z\\ \mathbf{0} & f^2\end{pmatrix}\begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix} \\
&= \begin{pmatrix}f^{2} & -f^2-z\\ \mathbf{0} & f^{-2}\end{pmatrix}\begin{pmatrix}f^{-2} & f^{-2}+z\\ \mathbf{0} & f^2\end{pmatrix} \\
&= \begin{pmatrix}\mathbf{1} & f^2(f^{-2}+z)-f^2(f^2+z)\\ \mathbf{0} & \mathbf{1}\end{pmatrix} \\
&= \begin{pmatrix}\mathbf{1} & (\mathbf{1}+f^2z)-(f^4+f^2z)\\ \mathbf{0} & \mathbf{1}\end{pmatrix} \\
&= \begin{pmatrix}\mathbf{1} & \mathbf{1}-f^4\\ \mathbf{0} & \mathbf{1}\end{pmatrix}
\end{aligned}
$$

näin on löydetty normaalin aliryhmän N alkio, joka vaikuttaa transvektiolta. Saatu matriisi on transvektio jos ja vain jos joukosta K^* löytyy alkio f, jolla $\mathbf{1} - f^4 \neq \mathbf{0}$. Koska astetta n olevalla polynomilla on lauseen 1.32 nojalla korkeintaan n erisuurta nollakohtaa kunnassa K, on yhtälöllä $\mathbf{1} - f^4 = \mathbf{0}$ korkeintaan neljä ratkaisua kunnassa K. Jos siis $|K| > 5$, on joukossa K^* enemmän kuin neljä alkiota eli sieltä löytyy sopiva alkio f.

On osoitettu, että ryhmän $SL(2, K)$ normaali aliryhmä $N > \{I, -I\}$ sisältää transvektion aina kun $|K| > 5$. Tällöin lauseen 6.1 nojalla kaikki transvektiot kuuluvat aliryhmään N ja edelleen lauseen 6.3 perusteella $N = SL(2, K)$. Näin ollen ryhmän $SL(2, K)$ ainoat normaalit aliryhmät ovat $\{I, -I\} = Z(SL(2, K))$ ja $SL(2, K)$ itse. Tästä seuraa lauseen 3.1 perusteella, että tekijäryhmän $PSL(2, K)$ ainoat aliryhmät ovat $\{Z(SL(2, K)\}$ ja se itse, eli $PSL(2, K)$ on yksinkertainen, kun

$|K| > 5$. Kun $|K| = 4$ tai $|K| = 5$, on ryhmän $PSL(2, K)$ yksinkertaisuus osoitettu lauseissa 3.3 ja 4.1.

□

LIITTEET

A Lausekkeiden arvoja taulukoituna

	$a = \mathbf{0}$	**1**	2	3	4	5	6
$b = \mathbf{0}$	**0**		**1**	4	2	2	4	**1**
1		**1**	3	**0**	6	**0**	3
2			4	**0**	5	5	**0**
3				2	6	5	6
4					2	**0**	**0**
5						4	3
6							**1**

Taulukko 13: lausekkeen $f(a, b) = a^2 + b^2 - ab$ arvoja seitsemän alkion kunnassa K.

	$a = \mathbf{0}$	**1**	2	3	4	5	6
$b = \mathbf{0}$	**0**		**1**	4	2	2	4	**1**
1	6		**1**	5	4	5	**1**	6
2	3		6	4	4	6	3	2
3	5		2	**1**	2	5	3	3
4	5		3	3	5	2	**1**	2
5	3		2	3	6	4	4	6
6	6		6	**1**	5	4	5	**1**

Taulukko 14: lausekkeen $f(a, b) = a^2 - b^2 + ab$ arvoja seitsemän alkion kunnassa K.

	$a = \mathbf{0}$	$\mathbf{1}$	2	3	4	5	6
$b = \mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	4	2	2	4	$\mathbf{1}$
$\mathbf{1}$		$\mathbf{0}$	$\mathbf{1}$	4	2	2	4
2			$\mathbf{0}$	$\mathbf{1}$	4	2	2
3				$\mathbf{0}$	$\mathbf{1}$	4	2
4					$\mathbf{0}$	$\mathbf{1}$	4
5						$\mathbf{0}$	$\mathbf{1}$
6							$\mathbf{0}$

Taulukko 15: lausekkeen $f(a, b) = a^2 + b^2 + 5ab$ arvoja seitsemän alkion kunnassa K.

Viitteet

[1] J.F. Humphreys, *A Course in Group Theory*, Oxford Science Publications, 1996.

[2] M.I. Kargapolov ja Ju.I. Merzljakov, *Fundamentals of the Theory of Groups*, Springer-Verlag New York, Inc., 1979.

[3] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag New York, Inc., 1995.

[4] J. J. Rotman, *The Theory of Groups, an Introduction*, Allyn and Bacon, Inc., 1979.

[5] Renkaat, kunnat ja polynomit luentomuistiinpanot, Kari Myllylän luentojen pohjalta, 2011.

[6] Kauppi, Jukka (Markku Niemenmaan luentojen pohjalta), Algebra II luentomoniste, matemaattisten tieteiden laitos, Oulun yliopisto, 2008.

[7] Permutaatiot, kunnat ja Galois'n teoria luentomuistiinpanot, Markku Niemenmaan luentojen pohjalta, 2013.

[8] Kauppi, Jukka (Markku Niemenmaan luentojen pohjalta), Ryhmäteoria luentomoniste, matemaattisten tieteiden laitos, Oulun yliopisto, 2009.

[9] Ryhmäteoria luentomuistiinpanot ja harjoitukset, Markku Niemenmaan luentojen pohjalta, 2013.